Erweiterung des Ermittlungsinstrumentariums zur Bekämpfung schwerer, organisierter und terroristischer Kriminalitätsformen („Online-Durchsuchung“)

Schlussbericht

Wien, im März 2008

Gelöscht: Fehler! Textmarke nicht definiert.

I. Auftrag und Vorgehensweise der Arbeitsgruppe

Die Grundlage für die Einsetzung der interministeriellen Arbeitsgruppe ist in einem gemeinsamen Vortrag der Bundesministerin für Justiz und des Bundesministers für Inneres an den Ministerrat vom Oktober 2007 mit Betreff „Erweiterung des Ermittlungsinstrumentariums zur Bekämpfung schwerer, organisierter und terroristischer Kriminalitätsformen (‚Online-Durchsuchung')“ enthalten.[1]

Für den Auftrag der Arbeitsgruppe sind folgende, aus dem Vortrag an den Ministerrat auszugsweise zu zitierende Passagen unmittelbar maßgebend:

„ … für die Durchführung einer „Online-Durchsuchung“ [werden] Programme benötigt … , die unbemerkt auf einem Computer installiert werden und es dem Angreifer ermöglichen, den Inhalt der Festplatte auszulesen, den E-Mail-Verkehr zu überwachen oder das Aufsuchen bestimmter Internetsites auszuforschen, ohne dass es der Inhaber merkt. Hier ist Bedacht darauf zu nehmen, dass derartige Programme („Trojaner“) zielgerichtet und punktgenau eingesetzt werden. Wichtig ist, dass eine effektive präventive, begleitende und nachprüfende Kontrolle durch den Rechtsschutzbeauftragten gewährleistet ist. Der Frage einer Weiterentwicklung des Systems der Rechtsschutzbeauftragten kommt somit im gegebenen Kontext besondere Bedeutung zu.

Voraussetzung ist für uns, dass der Einsatz der umschriebenen Ermittlungsmaßnahmen auf den Bereich der optischen und akustischen Überwachung von Personen unter Verwendung technischer Mittel gemäß § 149d Abs. 1 Z 3 (bzw. ab. 1.1. 2008 § 136 Abs. 1 Z 3) StPO begrenzt wird, d.h.:

- Notwendigkeit zur Aufklärung eines mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens oder des Verbrechens der kriminellen Organisation oder der terroristischen Vereinigung (§§ 278a und 278b StGB) oder zur Aufklärung oder Verhinderung von im Rahmen einer solchen Organisation oder Vereinigung begangener oder geplanter strafbarer Handlungen;
- dringender Tatverdacht (bzw. Vorbereitungshandlungen im Zusammenhang mit Kriminellen Organisationen und Terroristischen Vereinigungen (278a, 278b StGB) gegen die Person, gegen die sich die Überwachung richtet;

[1] Gesamter Text des Vortrages an den Ministerrat im Anlagenverzeichnis 1.

- Anordnung der Staatsanwaltschaft, die vor ihrer Durchführung durch das Gericht zu genehmigen ist und der Kontrolle des Rechtsschutzbeauftragten unterliegt;
- besondere Anordnung der Staatsanwaltschaft, für den Fall, dass ein Eindringen in eine Wohnung erforderlich ist, die ebenfalls einer Genehmigung durch das Gericht bedarf;
- strenge Beachtung des Verhältnismäßigkeitsgrundsatzes;
- Kontrolle der Durchführung durch Rechtsschutzbeauftragten;
- Verständigung sämtlicher Personen, deren Daten ermittelt wurden und umfängliche Beschwerdemöglichkeiten;
- strenge Vernichtungsregelungen von unzulässig ermittelten oder für die Untersuchung nicht bedeutsamen Daten sowie Beschränkung der Verwertbarkeit von Zufallsfunden;
- Beschwerderecht der DSK;
- eine verschuldensunabhängige Haftung des Bundes für Schäden, die durch eine Online-Durchsuchung verursacht wurden (siehe § 148 StPO idF BGBl. I Nr. 19/2004);
- Aufnahme in den jährlichen Bericht über besondere Ermittlungsmaßnahmen, der Nationalrat, Datenschutzrat und Datenschutzkommission vorzulegen ist.

Wir legen aber – nicht zuletzt im Hinblick auf Artikel 8 Abs. 2 EMRK und § 1 DSG 2000 – auch Wert darauf, dass die Erweiterung der Ermittlungsbefugnisse nach Maßgabe konkreter praktischer Erfahrungen und Notwendigkeiten erfolgt.

Als für die Strafverfolgung zuständige Bundesminister bekennen wir uns dazu, dass den Ermittlungsbehörden moderne und effiziente Befugnisse zur Hand gegeben werden, die es ihnen unter der erforderlichen Kontrolle durch Gerichte und Rechtsschutzbeauftragten ermöglichen, neuen Erscheinungsformen der organisierten Kriminalität und des Terrorismus erfolgreich entgegen zu treten.

Wir beabsichtigen daher die unverzügliche Einsetzung einer interministeriellen Arbeitsgruppe, die unter Einbeziehung von Experten bis Februar 2008 folgenden Auftrag erfüllen soll:

- Klärung der rechtlichen Fragen unter besonderer Berücksichtigung datenschutzrechtlicher, rechtsvergleichender und europarechtlicher Aspekte;
- Klärung der technischen Voraussetzungen und der Möglichkeiten der Steuerung des Einsatzes der „Online-Durchsuchung“ unter Berücksichtigung der Erfahrungen mit solchen Ermittlungsmaßnahmen in anderen Staaten;
- Prüfung der Weiterentwicklung des rechtlichen Kontrollinstrumentariums, etwa durch den Ausbau der Rechtsschutzbeauftragten

Darauf aufbauend wird die Bundesministerin für Justiz der Bundesregierung umgehend legislative Maßnahmen vorschlagen.“

Als Mitglieder der Arbeitsgruppe waren nominiert[2]:

o. Univ.-Prof. Dr. Bernd-Christian Funk	Universität Wien, Institut für Staats- und Verwaltungsrecht; Vorsitzender der AG
o. Univ.-Prof. Dr. Reinhard Posch	CIO des Bundes
GF Dipl.-Ing. Roland Jabkowski, MBA*)	Bundesrechenzentrum GesmbH
GF Mag. Christine Sumper-Billinger*)	Bundesrechenzentrum GesmbH
Ing. Johannes Mariel	Bundesrechenzentrum GesmbH
ao. Univ.-Prof. Mag. Dr. Marianne Hilf*)	Karl-Franzens-Universität Graz, Institut für Strafrecht, Strafprozessrecht und Kriminologie
o. Univ.-Prof. Dr. Helmut Fuchs	Universität Wien, Institut für Strafrecht und Kriminologie
Generalsekretär Dr. Kurt Einzinger	ISPA Internet Service Providers Austria
Hofrat Dr. Hans Valentin Schroll	Oberster Gerichtshof
HR Dr. Michael Danek	Oberster Gerichtshof, Richtervereinigung
Dr. Franz Schmidbauer	LG Salzburg, Internet4jurists.at
Dr. Christian Hubmer	Staatsanwaltschaft Wels, Vereinigung österr. Staatsanwältinnen und StAe
SC DDr. Wolfgang Bogensberger	Bundesministerium für Justiz, Sektion II
LStA Mag. Christian Pilnacek	Bundesministerium für Justiz, Abt. II 3

[2] Die mit *) bezeichneten Mitglieder der AG haben an keiner ihrer Sitzungen teilgenommen

Dr. Johannes Windisch	Bundesministerium für Justiz, Abt. II 3
Dr. Andreas Pscheidl	Bundesministerium für Justiz, Abt. II 3
Dr. Martin Schneider	Bundesministerium für Justiz, Abt. Pr. 5
Franz Kopetzky	Bundesministerium für Justiz, Abt. Pr. 5
Dr. Ewald Schwarzinger	Bundesministerium für Landesverteidigung/Abwehramt
Dr. Karl Satzinger	Bundesministerium für Landesverteidigung
Mjr. Vinzenz Schrank	Bundesministerium für Landesverteidigung
SC Mag. Dr. Mathias Vogl	Bundesministerium für Inneres, Sektion III
MR Mag. Walter Grosinger	Bundesministerium für Inneres, Sektion III
Mag. Bernhard Lukanc	Bundesministerium für Inneres, Abt. II/BK/1.1.
Mag. Leopold Löschl	Bundesministerium für Inneres, Abt. II/BK/5.2
Helmut Dissauer	Bundesministerium für Inneres, Abt. BVT 2
Dr. Martin David	Bundesministerium für Inneres, Abt. BVT/IB
Dr. Nicole Stemmer	Bundesministerium für Inneres, Abt. I/4
Mag. Barbara Schrotter	Bundesministerium für Inneres, Abt. I/4
Mag. Franz Eigner	Bundesministerium für Inneres, Abt. I-II/1
Mag. Peter Webinger	Bundesministerium für Inneres, Abt. I-II/1
KC Dr. Josef Ostermayer*)	Bundesministerium für Verkehr, Innovation und Technologie
Marcin Kotlowski	Bundesministerium für Verkehr, Innovation und Technologie, Kabinett
Dipl.-Ing. Franz Ziegelwanger	Bundesministerium für Verkehr, Innovation und Technologie, Abt III/PT3
Dipl.-Ing. Walter Marxt	Bundesministerium für Verkehr, Innovation und Technologie, Abt III/PT3
Dr. Christian Singer	Bundesministerium für Verkehr, Innovation und Technologie, Abt III/PT2
Dr. Angela Julcher	Bundeskanzleramt-Verfassungsdienst, Abt. V/5
Dr. Patrick Segalla	Bundeskanzleramt-Verfassungsdienst, Abt. 5
Dr. Eva Souhrada-Kirchmayer	Bundeskanzleramt-Verfassungsdienst
Maga. Angelika Hable	Bundeskanzleramt-Verfassungsdienst
Mag. Alexander Flendrovsky	Bundeskanzleramt-Verfassungsdienst, Abt. 3 (Datenschutz)

Die Arbeitsgruppe hat sich in 5 Sitzungen an Hand umfangreichen Materials[3] mit dem Thema befasst und legt nunmehr den folgenden Bericht vor.

II. „Online-Durchsuchung“. Technik und Terminologie

A. Allgemeines

Das Wort „Online-Durchsuchung“ hat weder informationstechnisch noch juristisch gesehen eine fest stehende Bedeutung. Es wird zur Bezeichnung verschiedener Begriffe verwendet. Gleiches gilt für ähnliche Worte, wie „Online-Nachschau“, „Online-Zugriff“, „Online-Überwachung“ und für Bezeichnungen in deren Umfeld. Vorweg sind daher textliche und semantische Klärungen vorzunehmen, die es ermöglichen, terminologisch bedingte Unsicherheiten zu vermeiden.

Dem Vortrag der BMJ und des BMI an den Ministerrat ist folgendes Begriffsbild von einer „Online-Durchsuchung“ zu entnehmen: Der Einsatz von Programmen („Trojaner“), „die unbemerkt auf einem Computer installiert werden und es dem Angreifer ermöglichen, den Inhalt der Festplatte auszulesen, den E-Mail-Verkehr zu überwachen oder das Aufsuchen bestimmter Internetsites auszuforschen, ohne dass es der Inhaber merkt“.

In der informationstechnisch-juristischen Fachdiskussion ist verschiedentlich von „Online-Zugriff“ als Oberbegriff für Online-Durchsuchung und Online-Überwachung die Rede.[4] Erstere besteht in einem ein- oder mehrmaligem heimlichen Zugriff auf fremde Computersysteme zum Zweck der Kopie gespeicherter Daten, letztere erfasst – über die Online-Durchsuchung hinaus – eine länger dauernde heimliche Überwachung von laufenden Aktivitäten eines Computersystems, einschließlich

[3] Register und Dateien in den Anlageverzeichnissen 02 und 03.

[4] Sieber, Stellungnahme, 2.

des Zugriffes auf Informationen, die im Computersystem nur flüchtig gespeichert werden, wie Cryptoschlüssel und Passwörter.

In einer Anfragebeantwortung im dt Bundestag wurde Online-Durchsuchung als „die Suche nach verfahrensrelevanten Inhalten auf Datenträgern … , die sich nicht im direkten Zugriff der Strafverfolgungsbehörden befinden, sondern nur über Kommunikationsnetze erreichbar sind“ definiert.[5]

In der Literatur[6] zeichnen sich folgende informationstechnisch-juristisch orientierte Unterscheidungen und Sprachgewohnheiten ab:

– Online-Durchsuchung als digitaler Zugriff auf den Rechner einer Zielperson zum Zwecke des Auslesens der auf dem Rechner gespeicherten Daten;
– Online-Überwachung als fortlaufende Überwachung der konkreten Nutzung eines Rechners;
– Überwachung des Datenaustausches über das Internet (Internet-Telefonie, E-Mail-Verkehr, Internet-Chats, Online-Spiele, Abfrage von Datenbanken, Surfen im Internet) als besondere Form der Telekommunikation.

Wenn in weiterer Folge ohne näheren Bezug von „Online-Durchsuchung“ gesprochen wird, dann sind damit alle Formen der heimlichen Durchsuchung oder Überwachung informationstechnischer Systeme gemeint.

B. Technische Aspekte für die „Online-Durchsuchung“[7]

- **Einbringungsmethoden**[8]

Die Installation von „Remote Forensic Software“ (RFS) kann grundsätzlich durch zwei, sich im Installationsablauf unterscheidende Verfahren durchgeführt

---

[5] Beleg bei Rux, JZ 2007, 286.

[6] Zuletzt Rux, JZ 2007, 287.

[7] Siehe Anlage, Seite 80 <tec-sum-RFS-Methoden_V1.0>, die gemeinsam von o. Univ-Prof. Dr Posch und BM.I erarbeitet wurde.

[8] Einbringung im Sinne der „Online Durchsuchung“ beschreibt die verdeckte Installation von Überwachungskomponenten auf definierten Kommunikationssystemen zum Zwecke sicherheitspolizeilicher Ermittlungen im Auftrag der Strafjustiz unter den normierten Rahmenbedingungen.

werden. Vor dem tatsächlichen Installationsprozess ist in beiden Anwendungsfällen die zweifelsfreie Identifikation[9] in Frage kommender Zielsysteme notwendig. Der eindeutigen Zuordnung von Zielperson zum Zielsystem kommt vor und während der Maßnahme besondere Bedeutung zu.

– Im Falle der unmittelbaren, verdeckten Installation durch Bedienstete der Sicherheitsbehörden ist der physische Zugriff auf das Kommunikationsgerät erforderlich. Bei dieser Einbringungsart leistet der Beschuldigte keinen aktiven Beitrag zum Installationsvorgang.
– Im Falle einer remote – Installation, das ist die Einbringung durch Bereitstellen der zur Umsetzung der Maßnahme erforderlichen RFS-Komponenten, leistet der Beschuldigte wenngleich auch unbewusst[10] einen aktiven Beitrag zum Installationsvorgang.

Sowohl die Installation durch physischen Zugang, wie auch die remote – Installation setzen eine detaillierte Analyse des Kommunikationsverhaltens und der verwendeten Systemumgebung voraus. In beiden Fällen werden auf dem Kommunikationssystem des Beschuldigten ohne dessen Wissen und ohne seine Zustimmung RFS-Komponenten[11] installiert. Ziel dieser Maßnahme ist es, verfahrensrelevante Kommunikationsvorgänge zu überwachen und lokale Daten bereits in einem sehr frühen Ermittlungsstadium zu durchsuchen. Jede Installation von Softwarekomponenten bewirkt Änderungen am Gesamtsystem. Das wesentliche Element bei der Anwendung einer „Online-Durchsuchung“ ist neben dem Ermittlungsansatz die detaillierte und authentische Dokumentation aller System- und Sicherheits- verändernden Maßnahmen.

---

[9] Die Zielidentifikation, d.h. die Zuordnung des Zielsystems zur Zielperson gewinnt z.B. im Falle der Weitergabe von Kommunikationssystemen besondere Bedeutung. Daraus lässt sich eine allfällige Notwendigkeit von begleitenden Maßnahmen herleiten.

[10] Dies kann auch durch automatisierte Vorgänge im Kommunikationssystem z.B. RSS etc. geschehen.

[11] RFS-Komponenten steht als Synonym für die Bezeichnung „Remote Forensic Software Komponenten“. Diese Komponenten stellen das zur Umsetzung angeordneter Maßnahmen notwendige technische Hilfsmittel zur Verfügung.

- **Systemverändernde Methoden**

Abhängig vom Leistungsspektrum der eingesetzten RFS-Komponenten ergeben sich quantitativ unterschiedliche Auswirkungen auf das betroffene Kommunikationssystem. Um das Risiko einer behaupteten Beweismittelveränderung so gering wie möglich zu halten, sind die mit der Installation verbundenen Veränderungen authentisch und reproduzierbar zu protokollieren[12]. Nach Beendigung der Maßnahme sind alle eingebrachten RFS-Komponenten wieder von dem Kommunikationssystem zu entfernen[13]. Während des Betriebes ist besonderes Augenmerk darauf zu legen, dass die RFS Komponenten nicht auf andere Systeme übertragen werden[14].

- **Reversibilität nach dem Eingriff**

Für die Entfernung der installierten RFS-Komponenten gelten die Anforderungen hinsichtlich Authentizität und Reproduzierbarkeit ebenso, wie für deren Einbringung. Besonderes Augenmerk ist dabei auf die Wiederherstellung des Systemzustandes und auf mögliche Auswirkungen im Zusammenhang mit der lokalen Datensicherung bzw. der Wiederherstellung gesicherter Daten zu legen.

- **Abgrenzung**[15]

Nebenwirkungen auf die sonstige Informationsverarbeitung mit dem betroffenen Kommunikationssystem sollen durch den Einsatz intelligenter Verfahren weitgehend verhindert werden. Die Einbringung von RFS-Komponenten auf Kommunikationssysteme von Beschuldigten darf daher weder die Systemintegrität beeinträchtigen, noch darf die Systembelastung durch die gesetzte Maßnahme nachhaltig negativ

---

[12] Die Auswirkungen der Installation und des Betriebes von RFS Komponenten müssen zweifelsfrei einschätzbar und bekannt sein.

[13] Dies lässt sich ohne Mitwirkung der betroffenen Person nur am aktiven System und nicht am Backup durchführen.

[14] Eine derartige Übertragung könnte z.B. über das Backup bzw. bei Verwendung von virtuellen Systemen geschehen.

[15] Abgrenzung im Kontext zur „Online Durchsuchung“ beschreibt jene Vorkehrungen, die während der Gesamtdauer laufender Maßnahmen einen Ressourcen schonenden Einsatz sicherstellt und somit nachhaltig zur Minimierung des Entdeckungsrisikos beiträgt.

beeinflusst werden. Übermäßigen Leistungseinbußen, die auf die RFS-Komponenten zurückzuführen wären, ist durch geeignete softwaretechnische Maßnahmen bestmöglich zu begegnen. Eine Erkennung sollte auch über Ressourcenmonitoring weitgehend ausgeschaltet sein. Zusätzlich birgt die Umsetzung jeder einzelnen „online Durchsuchungsmaßnahme“ die Gefahr einer behaupteten Kompromittierung[16] von privaten Schlüsseln[17] in sich. Diesem Umstand ist softwaretechnisch in geeigneter Form vorzubeugen.

- **Missbrauchsgefahren**[18]

Zur Erreichung des Primärziels, d.h. der gesicherten Übertragung ermittelter Daten vom betroffenen Kommunikationssystem an das Behördensystem müssen alle nachfolgend angeführten Aspekte einer eingehenden Betrachtung unterzogen werden:

1. Integrität[19] der Daten
2. Authentizität[20] der Kommunikationspartner
3.Verfügbarkeit[21] der Kommunikationswege

Aus diesem Anspruch heraus ergibt sich die Notwendigkeit zur Einrichtung einer geeigneten technischen und personellen Infrastruktur sowie einer geeigneten Prüfung.

---

[16] Eine Kompromittierung von Signaturerstellungsdaten des Signators ist schon dann als gegeben anzusehen, wenn nicht mehr mit hoher Sicherheit ausgeschlossen werden kann, dass diese in einer Weise verwendet werden könnten, die nicht dem Sicherheitskonzept des Zertifizierungsanbieters entspricht. (Quelle: Zentrum für sichere Informationstechnologie – Austria)

[17] Im schlimmsten Fall könnten dies auch Signaturschlüssel sein.

[18] Die missbräuchliche Verwendung behördlich eingesetzter Software für „Online Durchsuchungen“ durch unbefugte Dritte kann neben einem Reputationsschaden auch massive finanzielle Schadenersatzforderungen an die Republik Österreich nach sich ziehen.

[19] Als wesentliches Schutzziel im Zusammenhang mit der „Online Durchsuchung“ ist die Integrität der übermittelten Daten zu betrachten.

[20] Eine weitere unverzichtbare Komponente für die erfolgreiche Umsetzung technischer Maßnahmen zur „Online Durchsuchung“ stellt die Zuverlässigkeit und die eindeutige Zuordnung des Absenders übermittelter Daten **zu einer bestimmten Maßnahme** dar.

[21] Neben Integrität und Authentizität stellt die Verfügbarkeit der benötigten Kommunikationslinien und Systeme eine unerlässliche Säule der „Online Durchsuchung“ dar.

- **Verhinderung der Fremdnutzung**

Die Vermutung oder Behauptung, dass durch die RFS Komponente gesammelte Information auch an andere als die Ermittlungsbehörden abgegeben werden kann, muss wirksam entkräftet werden. Das bedeutet, dass die RFS Komponente ihr Gegenüber eindeutig identifizieren muss und alle Schlüssel der Datensicherheit nur bei einer einzigen Maßnahme verwendet werden. Nur dadurch kann behauptete oder tatsächliche Wirtschaftsspionage verhindert werden.

- **Verhinderung der Nachahmung[22]**

Durch den faktischen operativen Einsatz von Methoden zur effektiven „Online-Durchsuchung“ ergeben sich zwangsläufig Situationen, aus denen eventuell konkrete Rückschlüsse auf die angewendeten Verfahren und Prozesse möglich sind. Diese Erkenntnisse können bei Nachahmung durch unberechtigte Dritte massive wirtschaftliche Folgen implizieren. Es ist daher von besonderer Bedeutung, dass geeignete technische Maßnahmen getroffen werden, um weder die Verfahren, noch die durch sie gewonnenen Daten missbräuchlich verwenden zu können. Diese Gefahr ist vor allem bei der Remote-Einbringung besonders groß. Unter Nachahmung fällt auch das Entdecken und Ersetzen der RFS Komponenten durch den Beschuldigten, wodurch nur harmlose Daten an die Ermittlungsbehörden gelangen würden. Da dies besonders schwierig auszuschließen ist, muss jede eingebrachte Komponente in einem hohen Maße einzigartig bzw. hinreichend stark personalisiert sein.

- **Generelle Rahmenbedingungen**

Abschließend werden aus technischer Sicht die zur erfolgreichen Umsetzung von „online Untersuchungsmaßnahmen“ erforderlichen generellen Rahmenbedingungen beleuchtet. Neben der technischen Implementierung bedarf es einer Reihe

[22] Die Problematik einer allfälligen Nachahmung sowie die unberechtigte Verwendung von vergleichbarer Software stellt bei der Entwicklung der Komponenten eine besondere Herausforderung für Softwaredesigner und Entwickler dar. Dies soll insbesondere im Lichte sich daraus ergebender Möglichkeiten für Betriebsspionage etc. betrachtet werden.

von begleitenden Maßnahmen, die in einem Regelwerk[23] zusammengefasst die technischen und organisatorischen Prozesse sowie die notwendigen Strukturen[24] für die Umsetzung detailliert beschreiben. Die Einführung der „Online- Durchsuchung“ darf daher als ein hoch integrierter Mechanismus, bei welchem dem Grunde nach Parallelen zum großen Lauschangriff erkennbar sind, gesehen werden. Der wesentliche Unterschied zwischen den beiden technischen Hilfsmitteln liegt nicht bloß in der Art der Einbringung oder den angewendeten Verfahren und Prozessen, sondern vielmehr darin, dass durch die gesetzten Maßnahmen auch Rechte Dritter[25] betroffen sein können.

C. Informationstechnische Varianten zur Online- Durchsuchung) [26]

Variante 1
Untersuchung des physischen Gerätes (verdeckte oder offene Hausdurchsuchung, Beschlagnahme technischer Geräte,..).

Der PC, Notebook, PDA oder Server kann vor Ort oder in einem gut ausgerüsteten Labor forensisch untersucht werden. Wenn der Benutzer seine Daten auf einer externen Datenquelle (externe Harddisk, DVD, CD oder andere Medien) speichert und diese nicht verfügbar ist, wird die Untersuchung unter Umständen keine relevan-

[23] Die Beschreibung der technischen, organisatorischen und rechtlichen Verfahrensabläufe soll sicherstellen, dass alle Prozessschritte definiert sind und jederzeit überprüfbar vorliegen.

[24] Die Umsetzung angeordneter Maßnahmen erfordert neben der Bereitstellung der technischen Hilfsmittel (RFS-Komponenten) insbesondere auch die Verfügbarkeit geeigneter personeller Ressourcen. Diese Infrastrukturen sind für die Ermittlung, Analyse und Bewertung der Kommunikationsinfrastrukturen sowie dem Kommunikationsverhalten von Überwachungszielen unerlässlich. Darüber hinaus sind diese Ressourcen für die individuelle Anpassung der RFS-Komponenten und deren Einbringung am Zielsystem von eminenter Bedeutung.

[25] Die Beeinträchtigung von Rechten Dritter (Urheber- Lizenz- oder Wartungs- bzw. Gewährleistungsrechte etc.) kann sich durch Änderungen von Komponenten der Softwarehersteller (z.B. Anwendungsprogramme oder Betriebssysteme) ergeben.

[26] Siehe Anlage, Seite 45 <BMJ.Kopetzky.Informationstechnische Varianten>

ten Ergebnisse liefern. Eine weitere Erschwernis liegt in der erforderlichen Untersuchungszeit. Die Untersuchung einer vollen Festplatte mit mehreren 100GB wird in der Regel einen großen Zeitaufwand verursachen. Der Vorgang ist mit einer normalen Hausdurchsuchung zu vergleichen, die bereits auf vorhandenen gesetzlichen Grundlagen basiert.

Variante 2
Programme zur Ausspähung von Daten (Trojaner)

Ein Trojaner ist ein Programm, das auf einem Computer heimlich oder als nützliches Programm getarnt Funktionen ausführt. Der Trojaner wird vom Benutzer nicht wissentlich installiert und auch nicht kontrolliert. Der Trojaner selbst muss nicht schädlich sein. Häufig ist er aber mit anderer schädlicher Software kombiniert, oder hilft dieser, auf den Computer zu gelangen. Ein Trojaner ist kein Computer-Virus. Ein Computervirus versucht, sich auf immer mehr Dateien und Computer zu verbreiten und sich selbst zu kopieren. Der Trojaner kopiert sich nicht selbst, er kann aber mit einem Virus kombiniert werden. In Deutschland gibt es eine rege Diskussion über den Einsatz des Bundestrojaners. Der Begriff Bundestrojaner steht für die Online-Durchsuchung. Dabei sollen Computer einmal (Online- Durchsuchung) oder während eines gewissen Zeitraums (Online-Überwachung) überprüft bzw. überwacht werden, ohne dass der Nutzer das bemerkt. Das Innenministerium in Österreich spricht nicht von Bundestrojanern, sondern von „Remote Forensic Software“. Im Prinzip funktioniert die „Remote Forensic Software“ gleich wie „normale“ Trojaner. Trojaner erlauben etwa die Installation von Ausspähungs-Software auf dem Rechner, beispielsweise eines ‚keyloggers‘. Ein ‚keylogger‘ ist ein Programm, das Tastatur-Anschläge registriert und so an unverschlüsselte Daten und Passwörter kommt; oder von Programmen, mit denen die Dateien und Dokumente auf dem Computer nach Stichwörtern, Passwörtern oder anderen Inhalten durchsucht werden können. Diese Inhalte überspielt die „Remote Forensic Software“ dann an die Behörden, die sie auswerten. Die Probleme beim Einsatz einer „Remote Forensic Software“ sind:

– Die „Remote Forensic Software“ wird im Wesentlichen eine „customized software“ sein. Die „Remote Forensic Software“ muss an das jeweilige Zielsystem angepasst werden – Einzelanfertigung.

- Wie kommt die „Remote Forensic Software“ auf das Zielsystem
  - durch physische Installation auf das Zielsystem vor Ort
  - durch Einschmuggeln über den Download einer Datei (z.B. ein Photo, ein Text oder ein Software-Update), den Besuch einer „verseuchten“ Website oder den manipulierten Datei-Anhang an einer Mail. Mails können gefälscht werden.
  - Durch Hilfe und Einbau der „Remote Forensic Software“ von Mitarbeitern der IT – Systembetreuung der Firmen-, Privat- oder Behördennetzwerke. Die Identifikation des Zielsystems und der Einbau einer „Remote Forensic Software“ in Systemen innerhalb von Firmen-oder Behördennetzwerken ist ohne Mitarbeit der jeweiligen Organisation nicht möglich.
- Die Übertragung der ausgespähten Daten an die Behörde
  - Online – Problem der unauffälligen Datenübermittlung an die Behörde. Wenn vom Benutzer keine Internetaktivitäten ausgeführt werden, erhöht sich für den Benutzer auf unerklärliche Weise der Paketzähler des Netzwerkanschlusses bei synchroner Übertragung (z.B. Daten des Key-Loggers) der ausgespähten Daten. Die ausgespähten Daten müssen jedenfalls zwischengespeichert werden, da sonst – offline vom Internet – Aktivitäten nicht erfasst werden. Sobald der Rechner wieder online ist können die ausgespähten Daten an die Behörde übermittelt werden. Eine weitere Hürde kann eine am Rechner installierte Firewall Software sein. Die Firewall Software wird jede Anwendung melden und damit für den Benutzer sichtbar machen, die von sich aus einen Zugriff in das Internet versucht.
  - Das Schreiben der Überwachungsdaten auf einen für den Benutzer nicht sichtbaren Festplattenbereich erfordert eine physische Abholung der aufgezeichneten und ausgespähten Daten. Diese Vorgangsweise hätte den Vorteil, dass auch für Rechner ohne Internet Anschluss der Einsatz von „Remote Forensic Software“ möglich wäre.
- Die restlose Entfernung der „Remote Forensic Software“. Grund: Die Gefahr der Entdeckung. Eine bekannte „Remote Forensic Software“ kann nicht mehr verwendet werden. Die Entfernung kann

  - durch Fernsteuerung erfolgen. Das Problem: Löschung der „Remote Forensic Software“ von Backup – Kopien des Betriebsystems und von Anwendungen sind mit dieser Vorgangsweise nicht möglich.
  - durch physischen Zugriff auf das Zielsystem
- Der Nachweis gegenüber dem Benutzer, dass keine Daten durch die „Remote Forensic Software“ verändert wurden, kann problematisch werden.
- Keine Garantie, dass nach etwaiger Entdeckung der „Remote Forensic Software“ durch den/die Benutzer diese übernommen wird und die übermittelten Daten an die Behörde manipuliert werden.

Ein flächenmäßiger Einsatz der „Remote Forensic Software“ ist aus Gründen des hohen Datenanfalles und dem hohen Arbeitsaufwand zur Auswertung der umfangreichen Datenmenge, sowie der Gefahr, dass bei einer großen Verbreitung die „Remote Forensic Software“ vorzeitig entdeckt wird, nicht möglich. Das Programmieren und das Überwachen der Remote-Forensic Software sowie das Auswerten der Daten ist aufwändig und teuer.

Eine weitere Gefahr ist die Entdeckung durch Antivirus-Programme. Antivirus-Programme spüren in erster Linie Viren und Schadprogramme auf, die sie bereits kennen oder die sehr typische Verhaltensweisen haben. Deswegen benötigen Antivirus-Programme ständig aktuelle Virenlisten. Wenn die „Remote Forensic Software“ eine Einzelanfertigung ist, sind die Chancen gut, dass diese Software von Antivirus-Programmen nicht erkannt wird.

Variante 3
Nutzung elektromagnetischer Emissionen

Elektrische und elektronische Geräte geben elektromagnetische Energie an ihre Umwelt und damit auch an die angeschlossenen Datenkabel und Stromversorgungsleitungen ab. Diese Energie verbreitet sich weiter über alle leitenden Gegenstände, wie beispielsweise Wasserleitungen, Heizungsrohre, Stromleitungen oder Klimaanlagen. Des Weiteren verteilt sich diese Energie auch über „**kompromittierende Abstrahlung**“. Grundsätzlich erzeugen alle Datenströme elektromagnetische Emissionen, die mit mehr oder weniger Aufwand empfang- und auswertbar sind. Diese Art der Informations-/ Datenabstrahlung nennt man in Fachkreisen „kompromittierende

Abstrahlung“. Je nach Gebäudebeschaffenheit und Qualität der IT-Geräte variiert die mögliche Entfernung, um mittels Peilantenne an die Informationen über die abgegebene kompromittierende Abstrahlung zu kommen. Tests haben ergeben, dass die Entfernung bis zu 500 Meter betragen kann um die Daten abzugreifen. Selbst der serielle Datenstrom kann noch über eine Entfernung von 40 bis 50 Metern abgegriffen werden.
Quelle: Siemens AG

Variante 4
Einbau eines Hardware Moduls im Zielrechner
(„Remote Forensic Hardware“)

Die Methode der „Remote Forensic Hardware“ kann mit dem Beispiel eines Hardware „keyloggers“ erklärt werden. Die Variante ist in zwei Ausprägungen möglich:

1. Die Verwendung eines kleinen Gerätes, das in der Regel kleiner als 3cm ist und zwischen der Tastatur und Rechner platziert wird. Ein physischer Zugang zum Rechner ist für die Installation und für die Datenbeschaffung erforderlich. Millionen von Tastenanschlägen können gespeichert werden. Für die verdeckte Ermittlung eignet sich ein äußerlich sichtbares Gerät nicht.
2. Eine weit bessere und für den Benutzer völlig unsichtbare Methode ist die Platzierung des Hardware „keyloggers“ in die Tastatur des Benutzers. In die Tastatureinheit wird eine Hardware, für den Benutzer physisch und logisch völlig unsichtbar, installiert. Auch hier ist als Voraussetzung der Zugang zum physischen Rechner erforderlich. Die Wahrscheinlichkeit der Entdeckung ist bei dieser Vorgangsweise sehr gering.

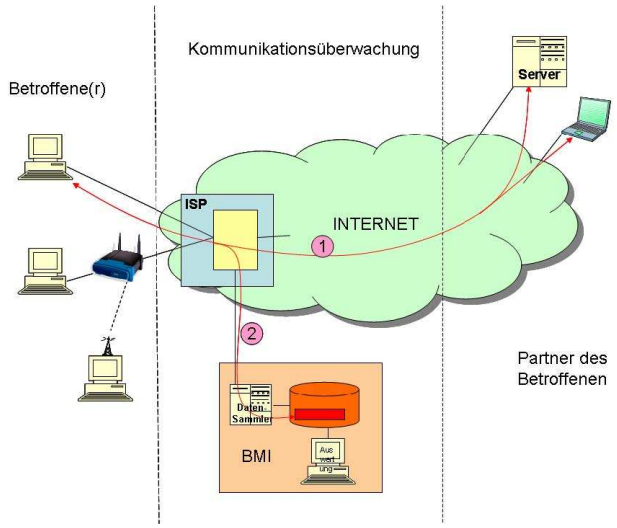
Eine technische Vervollkommnung der „Remote Forensic Hardware“ wäre noch die drahtlose Übertragung der Tastenanschläge an ein Empfangsgerät der Behörde (die würde die Aufspürung des ‚keyloggers‘ für den Benutzer mittels Wanzensuchgeräten erleichtern). Funktionell ähnliche „Remote Forensic Hardware“ ist auch für den Einbau in Systemeinheiten und Monitore denkbar. Die Nutzung dieser Variante würde einer Installation einer Abhöranlage (Audio und Video) gleichen. Eingaben über Mausklick sind auf diese Weise allerdings nicht protokollierbar.

- **Datenverkehrsüberwachung**

Kontrolle über den Zugang zum Internet

Die Überwachung kann nur durch eine gesetzliche Verpflichtung der „Internet Service Provider“ (ISP) und im Falle von Intranets durch Systemadministratoren der jeweiligen Organisation erfolgen. Die ISP bzw. Systemadministratoren müssten Aufzeichnungen über das Surfverhalten ihrer Benutzer anlegen, um entsprechende Informationen über das Internetverhalten einer Zielperson zu erhalten. Die Überwachung kann in mehrere Stufen erfolgen:

– Kontaktadressen (IP-Adressen) – wer sind die Kommunikationspartner der Zielperson?
– Dateninhalte des IP Paketes – welche Informationen werden mit den einzelnen Partnern der Zielperson ausgetauscht?



Bei Verschlüsselung von Daten durch die Zielperson oder den Partner der Zielperson nützt die Datenverkehrsüberwachung der ermittelnden Behörde wenig. Die meisten E-Mail-Benutzer verzichten jedoch auf den Einsatz effektiver Verschlüsselungstechniken, es ist für die Sicherheitsbehörden daher einfach, den E-Mail-Verkehr „abzuhören“ und die Versender oder Empfänger ausfindig zu machen.

Neben den ISP sind auch Firmen- und Behördennetzwerke zu berücksichtigen. Ohne die Mithilfe von Systemadministratoren kann keine Überwachung eines Daten-

verkehrs erfolgen, wenn dieser Rechner im Intranet der jeweiligen Organisation installiert ist. Die IP Adressen eines Rechners in einem Intranet sind im Internet nicht bekannt und daher auch nicht für den ISP sichtbar.

Die Nutzung der Datenverkehrsüberwachung würde einer Installation einer Telefonüberwachung gleichen.

III. Gesetzeslage in Österreich

A. Strafverfahrensrecht

1. Voraussetzungen, Grenzen und Graubereiche einer „geheimen“ Überwachung der Kommunikation und sonstigen Verhaltens einer Person nach den Bestimmungen der StPO [27]

- **Gegenstand und Themenabgrenzung**

Zur Themenabgrenzung scheint eine Klärung vorab notwendig: Der Grundsatz der Gesetz- und Verhältnismäßigkeit bedeutet gemäß § 5 Abs. 1 StPO schon auf einfachgesetzlicher Ebene, dass Strafverfolgungsbehörden nur dann befugt sind, im Rahmen von Ermittlungen in Rechte von Personen einzugreifen, wenn sie hiefür ausdrücklich gesetzlich ermächtigt sind (strafprozessuales Analogieverbot bei Eingriffen in Grund- und Freiheitsrechte – siehe auch Artikel 8 Abs. 2 EMRK). Schon aus diesem Gedanken scheidet eine Anwendung der Bestimmungen über die Durchsuchung von Orten und Gegenständen (§§ 117 Z 2, 119 bis 122 StPO) auf die hier interessierende Fallkonstellation einer „Durchsuchung“ der Daten einer Festplatte eines Computers bzw. der Installierung einer Überwachungssoftware ohne Kenntnis des Betroffenen aus. Gleich wie das Bild der deutschen StPO von einer rechtmäßigen Durchsuchung ist auch jenes der österreichischen StPO dadurch geprägt, dass die Ermittlungsorgane am Ort der Durchsuchung körperlich anwesend sind und die Ermittlun-

[27] Siehe Anlage, Seite 50 <BMJ.Bestehende Überwachungsmöglichkeiten nach der StPO>

gen offen legen. Auch die in §§ 121 und 122 StPO geregelten Pflichten und Rechte (Aufforderung, das Gesuchte herauszugeben; Recht des Beschuldigten und des Inhabers der Wohnung zur Anwesenheit während der Durchsuchung; Pflicht zumindest zwei unbeteiligte, vertrauenswürdige Personen beizuziehen, Zustellung einer Bestätigung über die Durchsuchung und deren Ergebnis an den Betroffenen) zeigen, dass eine heimliche Durchsuchung im Vergleich zu dieser klassischen „Hausdurchsuchung“ wegen ihrer erhöhten Eingriffsintensität eine Zwangsmaßnahme mit einem neuen, eigenständigen Charakter bildet (siehe dazu ausführlich, BGH 18 StB 18/06 vom 31. Jänner 2007 und weiterführend Bär, Urteilsanmerkung, MMR 3/2007, 175 ff.; ders. Online-Durchsuchung, MMR 4/2007, 239 ff.; Kutscha, „Verdeckte Online-Durchsuchung und Unverletzlichkeit der Wohnung“, NJW 2007, 1169 ff.).

Andererseits bedeutet dieser Befund nicht, dass Staatsanwaltschaft und Kriminalpolizei – einen entsprechenden Tatverdacht vorausgesetzt – die „Hände“ gebunden wären. So verpflichtet § 111 Abs. 1 StPO jedermann, der Kriminalpolizei auf Verlangen jene Gegenstände herauszugeben, die sichergestellt werden sollen. Die Bestimmung des § 111 Abs. 2 StPO enthält wiederum besondere Vorschriften für den Datenzugriff im Strafverfahren und verpflichtet Betroffene jene Handlungen vorzunehmen, die den Zugang zu den Informationen gewährleisten, die auf Datenträgern gespeichert sind, sowie zur Duldung der Herstellung einer Sicherungskopie. Für den Fall der Weigerung können entsprechende Zwangsmittel angeordnet und bewilligt werden (Beschlagnahme bzw. die bereits oben erörterte Durchsuchung von Orten und Gegenständen).

Die geltende Rechtslage wäre daher vor allem hinsichtlich der bestehenden „heimlichen“ Überwachungsmöglichkeiten auf die Zulässigkeit von Formen der Online-Durchsuchung bzw. der Online-Überwachung zu prüfen. Das erfordert erneut eine begriffliche Abgrenzung. Soweit im Folgenden von Online-Durchsuchung die Rede ist, soll diese Umschreibung Situationen erfassen, in denen der bestehende Datenbestand eines Datenträgers in dem Sinn „durchsucht“ wird, dass laufende oder in der Zukunft liegende Eingabevorgänge nicht erfasst werden, der Betroffene jedoch dennoch keine Kenntnis von der Zwangsmaßnahme erhält. Online-Überwachung erfasst hingegen alle gegenwärtigen und zukünftigen Eingabevorgänge (vgl. in diesem Sinn auch die Definition der Einsicht in Urkunden und andere Unterlagen eines Kredit-

oder Finanzinstituts über Art und Umfang einer Geschäftsverbindung und damit in Zusammenhang stehende Geschäftsvorgänge und sonstige Geschäftsvorfälle für einen bestimmten vergangenen oder zukünftigen Zeitraum gemäß § 109 Z 3 lit. b StPO).

- **Überwachung von Nachrichten und von Personen (§§ 134 Z 3 und Z 4, 135 Abs. 3 und 136)**

Maßgebliche Begriffe:

Schon das Strafrechtsänderungsgesetz 2002 (BGBl. I Nr. 134/02) stellte klar, dass sich die Bestimmungen der StPO auf die Überwachung sämtlicher moderner Formen der Telekommunikation einschließlich des Datenverkehrs im Internet beziehen. Auch im 5. Abschnitt des 8. Hauptstücks der StPO werden die Bestimmungen über die Überwachung im weiteren Sinn – nämlich die Beschlagnahme von Briefen, die Auskunft über Daten einer Nachrichtenübermittlung, die Überwachung von Nachrichten sowie die optische und akustische Überwachung von Personen – unter einem technologieunabhängigen Ansatz zusammengefasst und neu strukturiert, wodurch **sämtliche Formen moderner Kommunikation und nicht bloß der Telekommunikation erfasst** werden sollen.[28]

§§ 134 Z 3 und 135 StPO stellen anders als § 149a StPO aF **nicht mehr auf das Medium einer Nachricht ab**. Wo § 149a Abs. 1 lit. a StPO aF von *„Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen des Inhalts von Nachrichten, die durch Telekommunikation übermittelt oder empfangen werden“*

sprach, ist nach den Bestimmungen der §§ 134 Z 3 und 135 StPO die **Überwachung von Nachrichten in jeder Form** zulässig[29].

---

[28] *Strasser*, Redebeitrag 5. Rechtsschutztag des BMI, 6.11.2007 (im Druck) unter Bezugnahme auf *Pilnacek/Pleischl*, Das neue Vorverfahren, RZ 584

[29] Das zeigt schon die Definition des § 134 Z 3 StPO, wonach unter dem Begriff der „Überwachung von Nachrichten“ das Ermitteln des Inhalts von Nachrichten (§ 92 Abs. 3 Z 7 TKG), die über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 2 Z 2 des Notifikationsgesetzes) ausgetauscht oder weitergeleitet werden.

§ 136 StPO ermächtigt allgemein **zur optischen und akustischen Überwachung von Personen** und stellt nicht mehr wie § 149d StPO aF auf „nicht öffentliches Verhalten und nicht öffentliche Äußerungen von Personen“ ab. Die maßgebliche Definition des § 134 Z 4 StPO bezieht sich auf solche optische Überwachungen, die in den „Intimbereich“ der überwachten Person eindringen. Als maßgebliches Abgrenzungskriterium dient der Schutz des Privat- und Familienlebens (Artikel 8 EMRK). Damit wird auf jene Form der Überwachung gezielt, die dem Betroffenen nicht bewusst wird, weil er sich von den Umständen her mit Recht unbeobachtet fühlen kann und sich dem entsprechend verhält. Nur ein solcher Eingriff ist regelungsbedürftig. Dies allerdings auch im öffentlichen Raum, wenn die Beobachtung nicht auf übliche Weise erfolgt, sondern nur durch den verdeckten Einsatz technischer Mittel möglich wird.

Zulässigkeitsvoraussetzungen:

- Überwachung von Nachrichten:

Einschlägig ist im gegebenen Umfeld wohl der Eingriffstatbestand des § 135 Abs. 3 Z 3 StPO idF BGBl. I Nr. 93/2007. Die Überwachung muss daher

- Zur Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, erforderlich sein, oder
- Die Aufklärung oder Verhinderung von im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278a bis 278b StGB) begangenen oder geplanten strafbaren Handlung ansonsten wesentlich erschwert wäre, und
  - der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Tat dringend verdächtig ist, oder
  - auf Grund bestimmter Tatsachen anzunehmen ist, dass eine der Tat dringend verdächtige Person die technische Einrichtung benützen oder mit ihr eine Verbindung herstellen werde.

- Optische und akustische Überwachung von Personen:

Gemäß § 136 Abs. 1 Z 3 StPO muss ohne den Einsatz dieser Überwachung

- die Aufklärung eines mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens oder des Verbrechens der kriminellen Organisation oder der terroristischen Vereinigung (§§ 278a und 278b StGB) oder
- die Aufklärung oder Verhinderung von im Rahmen einer solchen Organisation oder Vereinigung begangenen oder geplanten strafbaren Handlung oder die Ermittlung des Aufenthalts des wegen einer solchen Straftat Beschuldigten ansonsten aussichtslos oder wesentlich erschwert sein. Zusätzlich muss
  - die Person, gegen die sich die Überwachung richtet, des mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens nach § 278a oder § 278b StGB dringend verdächtig sein oder
  - auf Grund bestimmter Tatsachen anzunehmen sein, dass ein Kontakt einer solcherart dringend verdächtigen Person mit der Person hergestellt werde, gegen die sich die Überwachung richtet.

<u>Anordnung, Bewilligung und Durchführung der Überwachungsmaßnahmen:</u>

Für sämtliche hier in Betracht zu ziehende Fälle muss eine gerichtlich bewilligte Anordnung der Staatsanwaltschaft vorliegen. Selbst bei Gefahr im Verzug darf die Kriminalpolizei von den beschriebenen Befugnissen keinen Gebrauch machen (§ 137 Abs. 1 StPO). Die Kontrolle der optischen und akustischen Überwachung obliegt gemäß § 147 StPO dem Rechtschutzbeauftragten.

Für die Durchführung gilt der allgemeine Grundsatz, dass damit nach gerichtlicher Bewilligung innerhalb der vom Gericht festgesetzten Frist die Kriminalpolizei zu beauftragen ist (§ 105 Abs. 1 StPO). Zusätzlich ordnet § 138 Abs. 2 und 3 StPO für den Fall einer Überwachung von Nachrichten an, dass Anbieter und sonstige Diensteanbieter verpflichtet sind, nach Maßgabe einer darauf gerichteten Anordnung der Staatsanwaltschaft (§ 138 Abs. 3 StPO) an der Überwachung von Nachrichten mitzuwirken, sie mithin technisch zu ermöglichen.

Eindringen in Wohnungen:

Ein Eindringen in Wohnungen sieht das Gesetz nur vor, soweit es für die Durchführung einer optischen oder akustischen Überwachung unumgänglich ist, wobei dieser Eingriff in das Hausrecht einer gesonderten gerichtlichen Bewilligung bedarf (§ 136 Abs. 2 iVm § 137 Abs. 1 letzter Halbsatz StPO).

Nach dem bereits eingangs erwähnten Grundsatz der Gesetz- und Verhältnismäßigkeit (§ 5 Abs. 1 StPO) verbietet sich eine ausdehnende Interpretation der Art, dass ein Eindringen in Wohnungen oder sonstigen vom Hausrecht geschützten Räumen auch zum Zweck der Durchführung einer Überwachung von Nachrichten zulässig wäre. Der Gesetzgeber hat bereits mit der Einführung besonderer Ermittlungsmaßnahmen durch das BGBl. I Nr. 105/1997 zu erkennen gegeben, dass dies einen zusätzlichen und schwerwiegenden Eingriff in verfassungsgesetzlich geschützte Rechte darstellt, der eines ausdrücklichen gesetzlichen Erlaubnistatbestandes bedarf.[30]

Kombination der Überwachungsmöglichkeiten?

Eine gleichzeitige Anordnung und Bewilligung der Überwachung von Nachrichten und der optischen und akustischen Überwachung von Personen ist wohl zulässig, soweit die Zulässigkeitsvoraussetzungen für beide Überwachungsarten vorliegen. In diesem Fall könnte wohl auch erwogen werden, dass die Bewilligung des Eindringens in eine Wohnung auch die Anbringung von Geräten ermöglicht, die eine Überwachung von Nachrichten ermöglichen, weil doch damit auch Äußerungen von Personen überwacht werden sollen.

[30] Die anlässlich des 5. Rechtschutztages des BMI durch den RSB GP iR Dr. Gottfried Strasser vertretene Ansicht, dass ein Eindringen in den Wohnbereich auch zum Zweck der Durchführung einer Überwachung einer Telekommunikation zulässig sei, weil beide Eingriffsmaßnahmen [nämlich Überwachung einer Telekommunikation und optische und akustische Überwachung] Formen der Äußerungsüberwachung im weiteren Sinn darstelltten und dem Gesetzesvorbehalt des Art. 8 EMRK-legitimer Zweck, Notwendigkeit in einer demokratischen Gesellschaft, Festlegung im Gesetz -in gleicher Weise genüge getan wurde, ist aus Sicht der Abt. II 3 des BMJ daher mit Entschiedenheit abzulehnen.

- **Schlussfolgerungen:**

Nach den vorangestellten Ausführungen kann zusammengefasst werden, dass die de lege lata gegebenen Bestimmungen zwar auf einen Teil der Computeranwendungen (E-Mail, VoIP) passen, nicht jedoch die übrigen, jedenfalls in keinem Fall unter „Kommunikation“ bzw. „Nachrichtenübermittlung“ subsumierbaren Anwendungen (Textverarbeitung, Tabellen, Datenbanken etc.) erfassen. Nicht nachrichten- bzw. kommunikationsbezogene Datenverarbeitung wäre keinesfalls verfassungskonform unter die Ermächtigung des § 135 StPO subsumierbar, weil es sich um keine „Äußerungsüberwachung im weiteren Sinn“ handelt.

Eine akustische Überwachung darf sich wiederum nur auf Äußerungen einer Person beziehen. Schon begrifflich wäre es daher ausgeschlossen, darunter auch die auf einem Speichermedium abgelegten Informationen zu subsumieren. Allerdings wäre es wohl zulässig, eine optische Überwachung so einzurichten, dass damit das Verhalten einer Person in Bezug auf deren Aktivitäten vor einem Bildschirm erfasst und überwacht werden kann (hochauflösbare Kamera, die eine Auswertung der Eingaben auf einer Tastatur ermöglicht).

Einen Graubereich stellt die offenbar in einem Fall praktizierte Anwendung einer Software dar, durch die der Bildschirminhalt („screenshots“) in Abständen von ungefähr einer Minute und die keylog-Daten übertragen und überwacht wurden. Selbst wenn man den Einbau einer solchen Software durch § 135 Abs. 2 Z 3 iVm § 136 Abs. 2 StPO als gedeckt ansieht, so müsste doch deren Eingrenzung auf echte Kommunikationsvorgänge gefordert werden, weil die reine Überwachung der schriftlichen oder bildlichen Darstellung von Gedankenvorgängen von den gegebenen Eingriffstatbeständen der StPO nicht erfasst wird.

2. Materiell-rechtliche Überlegungen zur Online-Durchsuchung[31]

Im Folgenden werden Überlegungen angestellt, welche Tatbestände des materiellen Strafrechts durch eine ohne verfahrensrechtliche Grundlage durchgeführte Online-Durchsuchung erfüllt sein könnten.

---

[31] Siehe Anlage, Seite 57 <BMJ.materiell-rechtliche Überlegungen zur Onlineüberwachung>

- **§ 118a StGB -Widerrechtlicher Zugriff auf ein Computersystem**

Den Tatbestand nach § 118a erfüllt, wer sich Zugang zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen verschafft, indem er spezifische Sicherheitsvorkehrungen im Computersystem verletzt. Der Täter muss in der Absicht handeln, sich oder einem anderen Unbefugten von in einem Computersystem gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen, und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, einem anderen einen Nachteil zuzufügen. Der Täter ist nur mit Ermächtigung des Opfers zu verfolgen.

Von dieser Bestimmung werden nicht nur Computernetzwerke erfasst, sondern **auch einzelne Endgeräte** (vgl. die Definition in § 74 Abs. 1 Z 8 StGB).

Sicherheitsvorkehrungen sind dann als spezifisch anzusehen, wenn sie im Computersystem angebracht worden sind (Passwörter, Zugangscodes etc.). Allgemeine Maßnahmen, die nicht im direkten Zusammenhang mit dem Zugriff stehen, wie etwa ein Versperren des Raumes, in dem sich der Computer befindet oder eine Alarmanlage, sind nicht erfasst (*Fabrizy*, StGB° § 118a Rz 2). Ein **Sicherheitssystem verletzt**, wer es technisch überwindet; die unbefugte Verwendung eines fremden Passwortes ist daher keine Verletzung im Sinne dieser Bestimmung.

Grundsätzlich würde das äußere Tatbild dieser Strafbestimmung Fälle der Online-Durchsuchung erfassen, soweit eine dem Computer innewohnende Sicherheitsvorkehrung überwunden werden muss. Problematisch stellt sich jedoch die **subjektive Tatseite** dar. Während die erste Variante, nämlich die Absicht, sich oder einem anderen durch die Benützung (etc.) der Daten einen Vermögensvorteil zuzuwenden, bei Ermittlungsmaßnahmen im Zug eines Strafverfahrens kaum in Betracht kommt, könnte die zweite Variante, nämlich das absichtliche **Zufügen eines Nachteils** erfüllt sein. Entscheidend ist wohl die subjektive Sphäre des Betroffenen, für den es in jedem Fall von Nachteil ist, in ein Strafverfahren unter Verwendung von „geheimen“ Informationen einbezogen zu werden. Dass der Zweck der Überwachung, nämlich der Nachweis von Straftaten oder deren Verhinderung, von der Rechtsordnung gebilligt wird, kann aus dieser Sicht nur auf der Rechtfertigungsebene eine Rolle spielen. Wie sich jedoch den einschlägigen Verfassungsbestimmungen (vgl. etwa Art. 8 EMRK)

entnehmen lässt, vermag ein zulässiger Zweck nicht jeden Eingriff zu rechtfertigen, sodass – abgesehen von Fällen des übergesetzlichen Notstandes (z.B. Verhinderung eines unmittelbar bevorstehenden Terroranschlags) – grundsätzlich von einer Tatbestandsverwirklichung auszugehen wäre.

- **§ 119 StGB -Verletzung des Telekommunikationsgeheimnisses**

Nach dieser Bestimmung macht sich strafbar, wer eine Vorrichtung an der Telekommunikationsanlage oder am Computersystem benützt, um sich oder einem anderen Unbefugten vom Inhalt einer im Wege einer Telekommunikation oder eines Computersystems übermittelten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen. Der Täter muss mit Absicht handeln und ist nur mit Ermächtigung des Opfers zu verfolgen.

§ 119 StGB wäre daher nur auf jene Fälle einer Online-Durchsuchung anwendbar, in denen die Kriminalpolizei in das Computersystem des Beschuldigten eindringt und dort **Software (oder Geräte) einbringt, um in der Folge eine Kommunikation zu überwachen.** Die Überwachung des Kommunikationsvorgangs selbst ist durch die StPO gerechtfertigt. Da nach geltender Rechtslage jedoch das Anbringen oder sonst Empfangsbereitmachen der Einrichtung nunmehr straffrei ist (*Fabrizy* StGB[9] § 119 Rz 5), sind diese Fälle ebenfalls **nicht strafbar**. Gleiches gilt für § 120 Abs. 2a StGB.

- **§ 119a StGB -Missbräuchliches Abfangen von Daten**

Dieses Delikt begeht, wer eine an einem Computersystem angebrachte Vorrichtung benützt oder die elektromagnetische Abstrahlung eines Computersystems auffängt. Der Täter muss mit der Absicht handeln, sich von im Wege eines Computersystems übermittelten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten benutzt oder einem anderen zugänglich macht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen. Es handelt sich wiederum um ein Ermächtigungsdelikt.

Bezüglich des **Nachteils** kann auf die Ausführungen zu § 118a StGB verwiesen werden. Zur Tathandlung ist auszuführen, dass diese Bestimmung **nicht nur das Abfangen elektronischer Nachrichten** inkriminiert, sondern sich auf alle Arten

von Daten im Sinne des § 74 Abs. 2 StGB bezieht. Viele Fälle der Online-Durchsuchung werden daher unter diesen Tatbestand zu subsumieren sein. Problematisch hingegen scheinen jene Fälle zu sein, bei welchen **überhaupt keine Übermittlung** stattfindet, bei der also bloß auf der Festplatte oder einem anderen Speichermedium **„ruhende“ Daten untersucht** werden. In diesem Fall kann die Bestimmung wohl nicht angewandt werden.

- **§ 123 StGB – Auskundschaften eines Geschäfts- oder Betriebsgeheimnisses**

Diese Bestimmung kommt für Online-Durchsuchungen **nicht in Frage**, da das wirtschaftliche Element, das für den Begriff der Verwertung kennzeichnend ist, im Fall einer Durchsuchung zu Ermittlungszwecken nicht angenommen werden kann.

- **§ 125 StGB -Sachbeschädigung**

Eine Strafbarkeit nach §§ 125 f StGB ist immer dann denkbar, wenn im Zuge der Online-Durchsuchung ein **physischer Schaden am Computersystem** oder auch an sonstigen Einrichtungen des Beschuldigten entsteht. Primär käme das bei der **Installation der Überwachungsprogramme vor Ort** in Betracht, also etwa bei Schäden am Gehäuse, den Platinen oder sonstigen Komponenten des Computers. Ob auch bei einer Einbringung über den Internetzugang des Beschuldigten eine Sachbeschädigung denkbar ist (etwa durch Übertaktung des Prozessors) scheint unwahrscheinlich, wäre aber von Seiten der Technik zu beantworten.

- **§ 126a StGB -Datenbeschädigung**

Das Delikt nach § 126a StGB begeht, wer einen anderen dadurch schädigt, dass er automationsunterstützt verarbeitete, übermittelte oder überlassene Daten über die er nicht oder nicht allein verfügen darf, verändert, löscht oder sonst unbrauchbar macht oder unterdrückt.

Diese Bestimmung ist eine der **zentralen Strafbestimmungen**, die durch eine Online-Durchsuchung verletzt werden können, soweit durch die Überwachung an den **Daten des Beschuldigten oder auch dritter Personen Schäden** entste-

hen (Veränderung, Löschung, Unbrauchbarmachung oder Unterdrückung). Fraglich ist allerdings, inwieweit der für § 126a StGB erforderliche **Vorsatz** angenommen werden kann. Die Überlegungen zum Vorsatz gelten in abgeschwächter Form im Übrigen auch für § 125 StGB.

Ein **direkter Vorsatz** auf Beschädigung von Daten ist dann denkbar, wenn sich die Löschung oder Veränderung auf Programme bezieht, die den Ablauf der Überwachung stören könnten, also etwa Firewalls, Viren-Suchprogramme und andere Sicherheitssoftware. Hier wäre deren gezielte Ausschaltung wohl vom direkten Vorsatz der ermittelnden Beamten erfasst. Daneben ist in einer Reihe von Fällen **Eventualvorsatz** vorstellbar, wenn billigend in Kauf genommen wird, dass durch eine Überwachungsmaßnahme Daten (des Beschuldigten aber auch unbeteiligter Dritter) beschädigt werden.

- **§ 126b StGB -Störung der Funktionsfähigkeit eines Computersystems**

Nach dieser Bestimmung ist strafbar, wer die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt.

Diese Strafbestimmung richtet sich gegen „denial-of-service-attacks“, also die **Überforderung eines Computersystems** durch an sich ungefährliche Übermittlungen von Daten. Eine derartige Lahmlegung eines Computersystems durch eine Online-Durchsuchung scheint schon aus kriminaltaktischen Gründen wenig sinnvoll, zumal dies dem verdeckten Charakter einer Online-Durchsuchung zuwiderlaufen würde. Sollte sich eine unbeabsichtigte und unerwünschte Funktionseinschränkung des Computersystems des Beschuldigten ergeben, so wäre diese schon mangels Vorsatz nicht nach § 126b StGB zu bestrafen.

- **§ 126c StGB -Missbrauch von Computerprogrammen oder Zugangsdaten**

Nach dieser Bestimmung ist strafbar, wer ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung der Delikte nach § 118a, § 119, § 119a, § 126a, 126b oder § 148a geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung oder ein Computerpasswort, einen Zugangscode

oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie zur Begehung einer der genannten strafbaren Handlungen gebraucht werden.

Soweit eine Online-Durchsuchung nach den angeführten Delikten strafbar ist, **kriminalisiert** § 126c StGB über die Beamten, die die Überwachung selbst durchführen und daher nach den entsprechenden Delikten strafbar sind, hinaus **diejenigen Personen, die an der Herstellung (Zurverfügungstellung, Wartung etc.) der entsprechenden Software** bzw. an der Anfertigung entsprechender technischer Einrichtungen **beteiligt** sind. Eine **Rechtfertigung** dieser Personen ist schwer vorstellbar, weil die Online-Durchsuchung selbst de lege lata nicht gerechtfertigt ist. Durch diese Bestimmung würden daher zahlenmäßig die meisten Personen betroffen sein, weil davon praktisch **jeder, der im Um- und Vorfeld von Online-Durchsuchungen tätig ist, betroffen ist.**

- **§ 148a StGB -Betrügerischer Datenverarbeitungsmissbrauch**

Dieser Bestimmung kommt im vorliegenden Zusammenhang auf Grund des vorausgesetzten Bereicherungsvorsatzes keine Bedeutung zu.

- **§ 302 StGB -Amtsmissbrauch**

Die Durchführung einer Online-Durchsuchung kann – zumindest für den **Entscheidungsträger** – auch als Amtsmissbrauch strafbar sein. Weiß der Beamte, dass Online-Durchsuchungen nicht zulässig sind und **handelt er mit dem Vorsatz, den Beschuldigten damit an seinen Rechten zu schädigen**, so kann sein Handeln den Tatbestand nach § 302 StGB erfüllen.

- **§ 303 StGB -Fahrlässige Verletzung der Freiheit der Person oder des Hausrechts**

Insoweit als dadurch das Hausrecht verletzt wird, könnte auch eine Strafbarkeit nach § 303 StGB in Frage kommen, wenn im Zuge einer Online-Durchsuchung auch in das Hausrecht eingegriffen wird. Auf Grund des im materiellen Strafrecht herr-

schenden **Analogieverbots** scheint diese Rechtsansicht jedoch nicht überzeugend zu sein. Da § 303 StGB **ausdrücklich auf Hausdurchsuchungen** (was nach gegenwärtiger Rechtslage der Durchsuchung von Orten und Gegenständen entspricht) abstellt, werden Verletzungen des Hausrechts, welche anlässlich anderer Ermittlungsmaßnahmen erfolgen, nicht unter diesen Tatbestand subsumierbar sein.

- **§ 313 StGB – Strafbare Handlung unter Ausnützung einer Amtsstellung**

Alle Delikte werden in der Regel durch Beamte unter Ausnützung ihrer Amtsstellung begangen werden und unterliegen – mit Ausnahme des Amtsmissbrauchs – der fakultativ anzuwendenden Strafbemessungsvorschrift nach § 313 StGB.

- **§ 51 Datenschutzgesetz**

Nach § 51 DSG ist strafbar, wer in der Absicht (u.a.) einem anderen einen Nachteil zuzufügen, personenbezogene Daten, die (u.a.) er sich widerrechtlich verschafft hat, selbst benützt oder einem anderen zugänglich macht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat.

Während § 126c StGB die Handlungen im Vorfeld einer Online-Durchsuchung kriminalisiert, könnte auf Grund dieser Bestimmung die **Strafverfolgung von „Verwertungshandlungen**“ betrieben werden. So würde diesen Tatbestand jeder erfüllen, der die **widerrechtlich verschafften Daten in der Folge verwertet** (also u.U. ermittelnde Kriminalbeamte, Staatsanwälte und Richter) – außer man verneint bei letzteren auf Grund der Zwischenschaltung der Kriminalpolizei, dass sie sich die Daten widerrechtlich verschafft haben. Die ohne rechtliche Grundlage erfolgte Online-Durchsuchung selbst erfüllt jedenfalls das Tatbestandselement der **widerrechtlichen Beschaffung**. Fraglich wäre, inwieweit an den Daten **ein schutzwürdiges Geheimhaltungsinteresse** besteht, wenn diese für kriminelle Zwecke genutzt werden. Andererseits würde eine enge Sichtweise in dieser Frage zu einer gewissen Entwertung des Datenschutzes führen, sodass wohl anzunehmen ist, dass **grundsätzlich** ein schutzwürdiges Interesse **anzunehmen** ist.

3. Zur Online- Durchsuchung[32]

- **Nach geltendem Recht:**

Eingriffe in fremde Rechte sind auch im Strafverfahren schon aus verfassungsrechtlichen Gründen (insbes. Art 8 Abs 2 EMRK), vor allem aber wegen § 5 Abs 1 StPO nur dann zulässig, wenn sie ausdrücklich gesetzlich vorgesehen sind. Die bestehenden Eingriffsermächtigungen der StPO bieten jedoch keine taugliche Grundlage.

1. Jede Durchsuchung von Orten und Gegenständen (§§ 117, 119 StPO) sowie eine damit verbundene Sicherstellung und Beschlagnahme setzen den körperlichen Eingriff in einen räumlichen Bereich und die physische Anwesenheit der Ermittlungsorgane am Ort der Eingriffshandlung voraus.
2. Die Ermächtigung zur Überwachung von Nachrichten gestattet nur den Zugriff auf Nachrichten, die über ein Kommunikationsnetz usw. „ausgetauscht oder weitergeleitet werden“ (§ 134 Z 3 StPO). Sie betrifft also nur die im Übermittlungsvorgang befindlichen Nachrichten (einschließlich ihrer Speicherung bei den Übermittlungsdiensten). Nachrichten, die übermittelt wurden (und sich schon beim Empfänger befinden) oder möglicherweise übermittelt werden sollen (aber sich noch beim potenziellen Absender befinden), dürfen nach dieser Bestimmung nicht überwacht werden.
3. Die optische und akustische Überwachung von Personen (§ 136 StPO) darf, wie der Name schon sagt, nur mit akustischen (Abhörgerät, Tonübertragung) oder mit optischen (Kameras) Mitteln erfolgen. Die geheime elektronische Überwachung eines Rechners ist durch diese Bestimmung nicht gedeckt.
4. Eine andere Eingriffsgrundlage ist für den Strafprozess nicht ersichtlich. Insbesondere könnte der Eingriff nicht auf „Staatsnotstand“ oder ähnliches gestützt werden, weil es diesbezüglich an einer ausdrücklichen gesetzlichen Ermächtigung fehlt.

[32] Siehe Anlage, Seite 72 <Fuchs, Online Überwachung 2-3 080214>

- **Rechtspolitisch:**

I. Bei jeder Regelung von Online- Durchsuchung ist zu bedenken, dass die geheime Überwachung von privaten Rechnern ein besonders schwer wiegender Eingriff ist.

Denn diese Zwangsmaßnahme betrifft nicht nur jene Gedanken von Menschen, die diese nach außen hin mitteilen und insofern (willentlich) preisgeben, sondern sie erfasst auch die innere Gedankenwelt der überwachten Person, die bloß auf einem privaten Gerät aufgezeichnet ist – nur persönlich zugänglich, passwortgesichert und damit in der Vorstellung besonders geschützter Intimität.

Es sollte daher sorgfältig geprüft werden,

1. ob mit einer solchen Ermittlungsmaßnahme nicht in den absolut geschützten Intimbereich eingegriffen wird, der jedem Menschen aufgrund seiner Menschenwürde und seines unverletzlichen Personalitätsanspruches zukommt.
2. Weiters ist zu fragen, ob eine solche geheime Überwachung privater Rechnern überhaupt notwendig ist, weil andernfalls schon die erste Voraussetzung der Verhältnismäßigkeit, an der alle Maßnahmen verfassungs- und einfachgesetzlich zu messen sind, nicht erfüllt wäre.

   Dies aus folgenden Überlegungen:

   a) Ein so schwer wiegender Eingriff wie die geheime Überwachung kann im Strafverfahren nur bei Bestehen eines dringenden Tatverdachts erlaubt werden. Besteht aber ein solcher Verdacht, so können auch andere Ermittlungsmaßnahmen wie eine Hausdurchsuchung, dann könnte u.U. sogar eine Festnahme erfolgen. Es ist daher zu prüfen, ob diese und ähnliche Möglichkeiten, die das Recht schon jetzt bietet, nicht ausreichen, um das Ziel der Strafverfolgung und der Beweissicherung zu erreichen.
   b) Dagegen könnte eingewendet werden, dass solche offenen Maßnahmen zur Verhinderung von geplanten Taten nicht ausreichen könnten. Dem wäre entgegenzuhalten, dass jemand, der Taten plant und vorbereitet, damit kaum fortfahren wird, wenn ihm die Staatsgewalt (Polizei) klar und deutlich zu erkennen gibt, dass sie um seine Aktivitäten weiß und diese mit Argusaugen be-

obachtet – ganz abgesehen von der Möglichkeit einer Bestrafung wegen einer allenfalls verwirklichten Vorbereitungstat (z.B. Waffendelikt).

3. Allerdings könnte es sein, dass geheime Überwachungsmaßnahmen in der Praxis der Sache nach auch zur Gewinnung eines Anfangsverdachts eingesetzt werden, was insbesondere durch dermaßen unsichere und unbestimmte Eingriffsvoraussetzungen wie den Verdacht einer kriminellen Organisation erleichtert wird. Dies läuft auf eine Überwachung von Personen im Vorfeld des Strafrechts, also auf eine präventive Datenermittlung und -speicherung hinaus.
   Mit der Strafverfolgung bei Bestehen eines dringenden Tatverdachts hat das nicht mehr viel zu tun. Sollte eine solche präventive Überwachung beabsichtigt sein, so sollte dies beim Namen genannt und in der Arbeitsgruppe gesondert und offen diskutiert und bewertet werden.
   Dabei wäre insbesondere zu klären, unter welchen Voraussetzungen diese Überwachung ohne den konkreten Verdacht einer bestimmten begangenen Straftat zulässig sein sollte und wie sich der Personenkreis, der von einer solchen Gefahrenüberwachung betroffen wäre, mit hinreichender Bestimmtheit begrenzen lässt. Die Begrenzung müsste durch eine Umschreibung im Gesetz erfolgen; der Hinweis, dass solche Online-Durchsuchungen wegen des derzeit damit verbundenen hohen technischen Aufwandes faktisch ohnedies nur in seltenen Ausnahmsfällen zu Einsatz kommen könnten, könnte rechtsstaatlichen Grundsätzen nicht genügen.

II. Sollte man die geheime Überwachung und Durchsuchung von privaten Rechnern trotz allem für unentbehrlich halten, so sollte man sich jedenfalls darum bemühen, die materiellen Eingriffsvoraussetzungen im Gesetz möglichst präzise zu formulieren.

Dieses Bemühen stößt jedoch an Grenzen, wenn man die Überwachung – wie etwa die Überwachung von Nachrichten (vgl § 135 Abs 3 Z 3 StPO) – auch bei bloßem Verdacht einer kriminellen Organisation (§ 278 StGB) oder zur Verhinderung von im Rahmen einer solchen Organisation geplanten Straftaten zulassen will.

Denn dann lässt man den Verdacht der Planung eines Delikts oder den Verdacht einer Vorbereitungshandlung genügen, also den bloßen Verdacht eines Geschehens

(wenn überhaupt ein konkretes „Geschehen“ ausgemacht werden kann), das weit ins Vorfeld der eigentlichen Rechtsgutsschädigung vorverlagert ist. Außer (vermutete) Absichten des „Verdächtigen“ und seinen Gedanken hat man kaum ein reales Substrat zur Hand, an das man die Verdachtsprüfung anknüpfen könnte.

Es ist daher unabdingbar, im Sinne des Ministerratsbeschlusses besonders wirksame Sicherungs- und Rechtsschutzmaßnahmen vorzusehen.

Diese sollten zumindest umfassen:

1. Die geheime Überwachung sollte von einem höheren Richtergremium angeordnet werden. Die Genehmigung durch den (bisweilen jungen und unerfahrenen) Ermittlungsrichter der ersten Instanz kann nicht genügen (wobei in diesem Zusammenhang auch auf die Abschaffung der Ratskammer als Genehmigungsinstanz durch das StPRefG hinzuweisen ist). Jedenfalls sollte die Beschwerde gegen den Grundrechtseingriff an den OGH ermöglicht werden.
2. Die Kontrolle durch den Rechtsschutzbeauftragten sollte ausgebaut und verbessert werden. Dieser sollte im aktiven Berufsleben stehen und auch nach Maßgabe seiner bisherigen Berufslaufbahn unabhängig sein, vorzugsweise ein Rechtsanwalt oder ein Universitätslehrer im aktiven Dienst. Er sollte – selbstverständlich bei strikter Pflicht zur Geheimhaltung – den gesetzlichen Auftrag erhalten, vor allem die Rechte der Betroffenen zu wahren, die von den geheimen Maßnahmen nichts wissen und darum ihre Rechte nicht geltend machen können.
   Hegt man Bedenken, dass ein solcher Rechtsschutzbeauftragter zu viel Macht haben könnte, so ist darauf hinzuweisen, dass er keine Entscheidungen treffen soll, sondern – gleichsam als ein Abwesenheitskurator im Auftrag der Öffentlichkeit – die Kontradiktorietät im geheimen Ermittlungsverfahren wahrt (*audiatur et altera pars*).
3. Die Rechtsentscheidungen zu den geheimen Überwachungen (Beschlüsse, Anordnungen, Rechtsmittelentscheidungen) sind nach Beendigung der Maßnahme, jedenfalls aber nach Ablauf eines bestimmten fixen Zeitraumes ab ihrer Erlassung, anonymisiert zu veröffentlichen. Sie wären damit insbesondere der wissenschaftlichen Öffentlichkeit zugänglich, die sie diskutieren und evaluieren könnte.

B. Sicherheitspolizeirecht[33]

- **Begriffsbestimmungen:**

1. „Online-Durchsuchung“ ist der verdeckte (ein- oder mehrmalige) staatliche Zugriff auf entfernte Kommunikationssysteme[34] über Kommunikationsnetze[35]. Durch den Einsatz spezieller Software sollen die auf den betroffenen Systemen gespeicherten Daten durchsucht und ermittlungsrelevante Daten gesichert und anschließend an die Systeme der ermittelnden Sicherheitsbehörden übertragen werden. Die Online-Durchsuchung erstreckt sich regelmäßig – schon aufgrund der technischen Gegebenheiten – über einen längeren Zeitraum.
2. „Remote Forensic Software“[36] ist ein, mit speziellen Funktionen für einen bestimmten Anlassfall ausgestattetes Computerprogramm, welches auf Kommunikationssystemen von Beschuldigten zum Zwecke der Onlinedurchsuchung eingebracht wird. Sie beinhaltet keine Schadfunktion. „Remote“ deshalb, da die Software zB bei der Aktivierung, Deaktivierung ferngesteuert werden kann.
3. „Einbringung“ von „Remote-Forensic Software“ kann auf zwei Arten erfolgen:
   a) Durch Fernzugriff, das ist die Einbringung von ,,Remote-Forensic Software“ aus der Ferne, z.B. durch elektronische Übermittlung an das Zielsystem.
   b) Durch physischen Zugriff, das ist die Einbringung von „Remote-Forensic Software“ durch physischen Zutritt am Standort des Kommunikationssystems.

---

[33] Siehe Anlage, Seite 14 <BMI.Document>

[34] Der Begriff Kommunikationssystem gestattet es, ein breiteres Spektrum an Endgeräten (etwa Personal Digital Assistants, Router, Access Points, u.v.a. zu adressieren.

[35] Der Begriff Kommunikationsnetz ist bedeutend weiter gefasst als der Begriff Internet. So würde die Bezeichnung Internet z.B. bei enger Auslegung nicht auf Extranet- oder Intranet-Umgebungen anwendbar sein, Es könnten somit u.U. private Netzwerkumgebungen von Unternehmen, Vereinen, Universitäten, etc. nicht einbezogen werden

[36] „Remote Forensic Software“ (RFS) beschreibt die Summe aller zur operativen Umsetzung der Onlinedurchsuchung erforderlichen Softwarekomponenten.

Abgrenzung:

Unter Online-Durchsuchung ist nicht die Internetüberwachung nach § 135 StPO gemeint, die sich nicht auf im Kommunikationssystem gespeicherte Daten bezieht. Die Auskunft über Daten einer Nachrichtenübermittlung nach § 135 Abs. 2 StPO und die Überwachung von Nachrichten nach § 135 Abs. 3 StPO sind zwar insoweit technikneutral formuliert, als damit jedes Kommunikationsmedium erfasst ist; sie stellen aber entweder auf eine Auskunft über so genannte äußere Kommunikationsdaten (wer hat wann mit wem kommuniziert) oder auf eine Inhaltsüberwachung ab, solange sich die Daten auf dem Übertragungsweg befinden. Nicht erfasst werden damit Daten, die in einem Kommunikationssystem gespeichert sind.

- **Rechtsgrundlagen im SPG:**

Analyse des Sicherheitspolizeigesetzes nach möglichen Rechtsgrundlagen für eine Onlinedurchsuchung.

o ***Aufgaben der Sicherheitsbehörden auf dem Gebiet der Sicherheitspolizei:***

Nach der Systematik des Sicherheitspolizeigesetzes wird zwischen Aufgaben, die von den Sicherheitsbehörden wahrzunehmen sind, und Befugnissen, die den Sicherheitsbehörden oder den Organen des öffentlichen Sicherheitsdienstes zur Aufgabenerfüllung zur Verfügung stehen, unterschieden. Dieser Systematik folgend werden im 2. Teil des Sicherheitspolizeigesetzes die Aufgaben der Sicherheitsbehörden auf dem Gebiet der Sicherheitspolizei festgelegt, die sich wie folgt darstellen:

1. Hauptstück: § 19 Erste allgemeine Hilfeleistungspflicht

2. Hauptstück: Aufrechterhaltung der öffentlichen Sicherheit
   § 20 Aufgaben im Rahmen der Aufrechterhaltung der öffentlichen Sicherheit
   § 21 Gefahrenabwehr
   § 22 Vorbeugender Schutz von Rechtsgütern
   § 23 Aufschub des Einschreitens
   § 24 Fahndung

§ 25 Kriminalpolizeiliche Beratung
§ 26 Streitschlichtung

3. Hauptstück: § 27 Aufrechterhaltung der öffentlichen Ordnung

4. Hauptstück: § 27a Besonderer Überwachungsdienst

Die **erste allgemeine Hilfeleistungspflicht** ist in vielen Fällen der Ausgangspunkt für sicherheitspolizeiliches Einschreiten. Das Gesetz normiert eine Hilfeleistungsverpflichtung der Sicherheitsbehörden, wenn Leben, Gesundheit, Freiheit oder Eigentum von Menschen gegenwärtig gefährdet sind oder eine solche Gefährdung unmittelbar bevorsteht. Im Rahmen der ersten allgemeinen Hilfeleistungspflicht sind die Sicherheitsbehörden dazu verpflichtet festzustellen, ob eine Gefahrensituation besteht, und, wenn eine sicherheitspolizeiliche oder verwaltungspolizeiliche Gefahrenlage besteht, einzuschreiten. Schon die Aufgabenstellung ist eine subsidiäre, nämlich die Abwehr von Gefährdungen, die der Bundes- oder ein Landesgesetzgeber für einen bestimmten verwaltungspolizeilichen Gefahrenbereich im Rahmen der Zuständigkeit einer Verwaltungsbehörde vorgesehen hat oder die zum Hilfs- und Rettungswesen oder zur Feuerpolizei gehört. Der Systematik des Sicherheitspolizeigesetzes folgend ist aus der Aufgabenstellung noch keine Befugnis abzuleiten; diese wäre im 2. Hauptstück des 3. Teils (Befugnisse für die erste allgemeine Hilfeleistungspflicht) des Gesetzes zu suchen. Die für diese Untersuchung in Frage kommenden Befugnisse werden nachfolgend noch beschrieben, es kann aber schon soviel vorweggenommen werden, dass sich für die in Rede stehende Onlinedurchsuchung aus dem Titel der ersten allgemeinen Hilfeleistung keine Befugnis für einen derartigen Grundrechtseingriff ableiten lässt.

Die **Aufrechterhaltung der öffentlichen Sicherheit** umfasst die Gefahrenabwehr, den vorbeugenden Schutz von Rechtsgütern, die Fahndung, die kriminalpolizeiliche Beratung und die Streitschlichtung. Für die gegenständliche Untersuchung interessiert vor allem die **Gefahrenabwehr.** Den Sicherheitsbehörden obliegt die Abwehr allgemeiner Gefahren. Eine **allgemeine Gefahr** im Sinne des Sicherheitspolizeigesetzes (vgl § 16) besteht bei einem **gefährlichen Angriff** oder sobald sich drei oder mehr Menschen mit dem Vorsatz verbinden, fortgesetzt gericht-

lich strafbare Handlungen zu begehen **(kriminelle Verbindung).** Ein gefährlicher Angriff wird – verkürzt dargestellt – als die Bedrohung eines Rechtsgutes durch die rechtswidrige Verwirklichung des Tatbestandes einer vorsätzlich begangenen gerichtlich strafbaren Handlung definiert. Die **Gefahrenerforschung** ist die Feststellung einer Gefahrenquelle und des für die Abwehr einer Gefahr maßgeblichen Sachverhaltes.

Mit den in § 16 erfolgten Definitionen (allgemeine Gefahr, kriminelle Verbindung, gefährlichen Angriff und Gefahrenerforschung) werden noch keine Aufgaben oder Befugnisse festgelegt; diese finden sich im nachfolgend beschriebenen 3. und 4. Teil des Sicherheitspolizeigesetzes.

- Befugnisse der Sicherheitsbehörden und der Organe des öffentlichen Sicherheitsdienstes im Rahmen der Sicherheitspolizei:

Im 3. und 4. Teil des Sicherheitspolizeigesetzes werden die Befugnisse der Sicherheitsbehörden und der Organe des öffentlichen Sicherheitsdienstes im Rahmen der Sicherheitspolizei festgelegt. Aus diesem Befugnisteil sollen nur jene Befugnisse genannt werden, die als mögliches Instrumentarium für eine Onlinedurchsuchung in Erwägung gezogen werden könnten, wenn auch nur zu dem Zweck, um sie gleich wieder auszuschließen.

<u>Ausgewählte Befugnisse:</u>

– Betreten und Durchsuchen *von* Grundstücken, Räumen und Fahrzeugen

Will ein Organ des öffentlichen Sicherheitsdienstes eine Räumlichkeit betreten, um sich beispielsweise Zugang zu einem Kommunikationssystem zu verschaffen, so könnte dafür § 39 als mögliche Rechtsgrundlage in Frage kommen.

§ 39. (1) Die Organe des öffentlichen Sicherheitsdienstes sind ermächtigt, Grundstücke, Räume sowie Luft-, Land- und Wasserfahrzeuge (Fahrzeuge) zu betreten, sofern dies zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder zur Abwehr eines gefährlichen Angriffs erforderlich ist.
(2) ...
(3) Die Organe des öffentlichen Sicherheitsdienstes sind ermächtigt, Grundstücke,

Räume und Fahrzeuge zu durchsuchen, soweit dies der Suche

1. *nach einem Menschen dient, dessen Leben oder Gesundheit unmittelbar gefährdet erscheint,*
2. *nach einem Menschen dient, von dem ein gefährlicher Angriff ausgeht;*
3. *nach einer Sache dient, die für einen gefährlichen Angriff bestimmt ist.*

(4) …

(5) Die Organe des öffentlichen Sicherheitsdienstes sind ermächtigt, Behältnisse, auch wenn sich diese in Räumen befinden, unter den Voraussetzungen des Abs. 1 zu öffnen und unter den Voraussetzungen des Abs. 3 zu durchsuchen.

(6) …

(7)

(8) Nach einem gefährlichen Angriff gelten für die Durchsuchung von Grundstücken, Räumen, Fahrzeugen und Behältnissen ausschließlich die Bestimmungen der StPO.

Wie sich allein schon aus den verba legalia erkennen lässt, dürfte ein Organ des öffentlichen Sicherheitsdienstes die Räumlichkeit, in der sich der Rechner befindet, nicht einmal betreten. Es liegt keine gegenwärtige oder unmittelbar bevorstehende Gefahr für Leben, Gesundheit, Freiheit oder Eigentum von Menschen vor, bei deren Vorliegen das Organ die Befugnis zum Betreten von Räumlichkeiten zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht hätte. Ebenso wenig dürfte das Sicherheitsorgan den Raum durchsuchen, da dies nur zur Suche nach einer Sache, die für einen gefährlichen Angriff bestimmt ist (von der Gefahr ausgeht) zulässig ist.

– Bewachung von Menschen und Sachen

§ 48. (1) Die Organe des öffentlichen Sicherheitsdienstes sind ermächtigt, Menschen zu bewachen, wenn auf Grund bestimmter Tatsachen anzunehmen ist, es stehe ein gefährlicher Angriff gegen deren Leben, Gesundheit oder Freiheit bevor.

Wie sich unschwer erkennen lässt, stellt diese Bestimmung auf den Schutz potentiell gefährdeter Menschen ab.

Der 4. Teil des Sicherheitspolizeigesetzes widmet sich der Verwendung personenbezogener Daten im Rahmen der Sicherheitspolizei. Auch aus diesem Teil sollen

nur jene Bestimmungen herausgenommen werden, die im obigen Sinn als mögliches Instrumentarium für eine Online-Durchsuchung in Frage kommen könnten.

– Zulässigkeit der *Verarbeitung*

§ 53. *(3a) Die Sicherheitsbehörden sind berechtigt, von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 – TKG 2003, BGBl. 1 Nr. 70) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz – ECG, BGBl. 1 Nr. 152/2001) Auskunft zu verlangen über*

1. *Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses,*
2. *Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung sowie*
3. *Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war,*

wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen und sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen. Die Bezeichnung eines Anschlusses nach Z 1 kann für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer erfolgen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen.

(3b) Ist auf Grund bestimmter Tatsachen anzunehmen, dass eine gegenwärtige Gefahr für das Leben oder die Gesundheit eines Menschen besteht, sind die Sicherheitsbehörden zur Hilfeleistung oder Abwehr dieser Gefahr berechtigt, von Betreibern öffentlicher Telekommunikationsdienste Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der von dem gefährdeten Menschen mitgeführten Endeinrichtung zu verlangen sowie technische Mittel zu ihrer Lokalisierung zum Einsatz zu bringen. Die Sicherheitsbehörde trifft die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens, dessen Dokumentation dem Betreiber unverzüglich, spätestens innerhalb von 24 Stunden nachzureichen ist. Die ersuchte Stelle ist verpflichtet, die Auskünfte unverzüglich und gegen Ersatz der Kosten nach § 7 Z 4 der Überwachungskostenverordnung – ÜKVO, BGBl. 11 Nr.

322/2004, zu erteilen.

(3c) Die Sicherheitsbehörden sind zur Vorbeugung und Abwehr gefährlicher Angriffe gegen die Umwelt berechtigt, von Behörden des Bundes, der Länder und Gemeinden Auskünfte über von diesen genehmigte Anlagen und Einrichtungen zu verlangen, bei denen wegen der Verwendung von *Maschinen oder Geräten, der Lagerung, Verwendung oder Produktion von Stoffen, der Betriebsweise, der Ausstattung oder aus anderen Gründen besonders zu befürchten ist, dass im Falle einer Abweichung der Anlage oder Einrichtung von dem der Rechtsordnung entsprechenden Zustand eine Gefahr für das Leben, die Gesundheit mehrerer Menschen oder in großem Ausmaß eine Gefahr für Eigentum oder Umwelt entsteht. Die ersuchte Behörde ist verpflichtet, die Auskunft zu erteilen.*

(4) Abgesehen von den Fällen der Abs. 2 bis 3b sind die Sicherheitsbehörden für Zwecke des Abs. 1 berechtigt, personenbezogene Daten aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel, insbesondere durch Zugriff auf allgemein zugängliche Daten, zu ermitteln und weiterzuverarbeiten.

Abgesehen davon, dass eine so genannte Rufdatenauswertung nur ein Mosaiksteinchen im Gesamtgefüge einer Online-Durchsuchung sein könnte, wäre mangels Vorliegen von Tatsachen, die die Annahme einer konkreten Gefahrensituation rechtfertigen, schon die Einholung einer Auskunft bei einem Telekommunikationsbetreiber unzulässig.

– § 54 Besondere Bestimmungen für die Ermittlung

(1)

(2) Die Ermittlung personenbezogener Daten durch Beobachten (Observation) ist zulässig

1. zur erweiterten Gefahrenerforschung (§ 21 Abs. 3);

2. um eine von einem bestimmten Menschen geplante strafbare Handlung gegen Leben, Gesundheit, Sittlichkeit, Freiheit, Vermögen oder Umwelt noch während ihrer Vorbereitung (§ 16 Abs. 3) verhindern zu können;

3. wenn sonst die Abwehr gefährlicher Angriffe oder krimineller Verbindungen gefährdet oder erheblich erschwert wäre.

Formatiert: Nummerierung und Aufzählungszeichen

Formatiert: Nummerierung und Aufzählungszeichen

4) Die Ermittlung personenbezogener Daten mit Bild- und Tonaufzeichnungsgeräten ist nur für die Abwehr gefährlicher Angriffe oder krimineller Verbindungen und zur erweiterten Gefahrenerforschung (§ 21 Abs. 3) zulässig; sie darf unter den Voraussetzungen des Abs. 3 auch verdeckt erfolgen. Das Fernmeldegeheimnis bleibt unberührt. Unzulässig ist die Ermittlung personenbezogener Daten jedoch

1. mit Tonaufzeichnungsgeräten, um nichtöffentliche und nicht in Anwesenheit eines Ermittelnden erfolgende Äußerungen aufzuzeichnen;

2. mit Bildaufzeichnungsgeräten, um nichtöffentliches und nicht im Wahrnehmungsbereich eines Ermittelnden erfolgendes Verhalten aufzuzeichnen.

(4a) Die verdeckte Ermittlung (Abs. 3) und der Einsatz von Bild- und Tonaufzeichnungsgeräten (Abs. 4) sind zur Abwehr einer kriminellen Verbindung nur zulässig, wenn die Begehung von mit beträchtlicher Strafe bedrohten Handlungen (§ 17) zu erwarten ist. Bei jeglichem Einsatz von Bild- und Tonaufzeichnungsgeräten ist besonders darauf zu achten, dass Eingriffe in die Privatsphäre der Betroffenen die Verhältnismäßigkeit (§ 29) zum Anlass wahren.

Auch die Regelungen für eine Observation und die Bild- sowie die Tonaufzeichnung stellen keine geeignete Grundlage für eine Online-Durchsuchung dar. Der Einsatz von Bild- und Tonaufzeichnungsgeräten ist auf die Abwehr gefährlicher Angriffe und auf die Abwehr einer kriminellen Verbindung beschränkt, ihr Einsatz ist nur in Anwesenheit eines (verdeckt ermittelnden) Organs des öffentlichen Sicherheitsdienstes zulässig. Allein schon daraus ist ersichtlich, dass die Bild- und Tonaufzeichnung nach dem Sicherheitspolizeigesetz kein taugliches Instrument für eine Online-Durchsuchung sein kann.

- **Zusammenfassung:**

Zusammenfassend lässt sich feststellen, dass sich im Sicherheitspolizeigesetz **keine** Bestimmung findet, die auch nur annähernd eine taugliche Rechtsgrundlage für eine Online-Durchsuchung wäre.

- **Exkurs: Position des Bundesministeriums für Inneres im Zusammenhang mit der Einführung der Online- Durchsuchung :**

Zur Systematik sei vorab festgehalten, dass zwischen zwei Aspekten unterschieden werden soll:

– Normierung der rechtlichen Rahmenbedingungen im Gesetz
– Schaffung eines ausführlichen operativen Regelwerkes in Form von Durchführungsbestimmungen, in denen die Handlungsmaßstäbe und technischen Parameter für den Einsatz der Online-Durchsuchung festgelegt werden.[37]

Angesichts der potenziellen Bedrohungen durch international agierende kriminelle Organisationen und terroristische Vereinigungen stellt die Online-Durchsuchung eine Maßnahme dar, die in unserer demokratischen Gesellschaft für die nationale Sicherheit zum Schutz der Rechte und Freiheiten der Bürgerinnen und Bürger dieses Landes sinnvoll und geradezu geboten erscheint. Die Online-Durchsuchung kann ein zusätzliches technisches Hilfsmittel zur Bekämpfung der Schwer- und Schwerstkriminalität darstellen. Die Tatsache, dass sich Kriminelle mittlerweile aller Formen neuer Kommunikationstechniken, insbesondere der Verschlüsselung von Daten bedienen, macht es erforderlich, die Strafverfolgungsbehörden mit adäquaten Mitteln und Möglichkeiten auszustatten, um mit diesen Entwicklungen zumindest annähernd Schritt halten zu können. Es kann nicht angehen, dass sich kriminelle Elemente in Verfolgung ihrer verbrecherischen Ziele jeder technischen Neuerung bedienen, während den Sicherheitsbehörden unter Hinweis auf grundrechtliche Schranken die Hände gebunden sind. Gewiss stellt die diskutierte Online-Durchsuchung eine eingriffsintensive Maßnahme dar, nicht zuletzt auch deshalb, weil damit auch auf historische Daten (Schriften) zurückgegriffen werden kann. Dennoch wird eine Verhältnismäßigkeitsabwägung zwischen – wenn man so will – Freiheit der Gedanken und dem Recht der Gesellschaft auf ein Leben in Freiheit und

[37] In der darüber in der Arbeitsgruppe geführten Diskussion wurde die Auffassung vertreten, dass ein solches Regelwerk möglichst genaue Guidelines für die Durchführung angeordneter bzw bewilligter Maßnahmen zu enthalten habe. Solche Richtlinien und Regeln seien eine wesentliche Bedingung für die Durchführung einer wirksamen Kontrolle. Sie müssten im Zusammenwirken beider Ressorts erarbeitet und von der Staatsanwaltschaft erlassen werden.

Sicherheit, in der sich eine Gesellschaft auch ungestört weiterentwickeln kann, zulasten derjenigen ausfallen, die diese Gesellschaft in ihrer Existenz bedrohen.

In vielen Bereichen wird man mit den bestehenden Befugnissen das Auslangen finden, dennoch kann es in bestimmten Einzelfällen notwendig sein, auf die Quellinformationen zurückzugreifen. Mit einer laufenden Inhaltsüberwachung kann ein aktueller Wissensstand gewonnen werden, anhand zurückliegender Vorgänge kann aber auch eine Verknüpfung hergestellt und können Zusammenhänge erkannt werden, die sonst unentdeckt blieben. Beispielhaft sei angeführt, dass auf Grund einer Internetüberwachung gewisse Teile einer Kommunikation in Erfahrung gebracht werden, für das Herstellen von kriminalpolizeilichen Zusammenhängen jedoch gewisse wesentliche Kommunikationsteile fehlen oder der Verschlüsselungscode einer Nachricht ohne zusätzliche Information nicht verstanden werden kann. Für sicherheits- und kriminalpolizeiliche Maßnahmen stellt dieses Wissen geradezu eine unabdingbare Notwendigkeit dar. Unter dieser Prämisse erscheint eine entsprechende gesetzliche Ermächtigung als dringend notwendig, wobei im Hinblick auf die Eingriffsintensität und die verfassungsrechtlichen Vorgaben entsprechende Vorkehrungen zu treffen sind.

Wesentliche Eckpunkte:

- Im präventiven Bereich ist Zweck der Maßnahme die Abwehr gefährlicher Angriffe oder die Abwehr krimineller Verbindungen und die erweiterte Gefahrenerforschung. Im repressiven Bereich die Aufklärung und Verfolgung von strafbaren Handlungen. In diesem Zusammenhang soll gemäß dem gemeinsamen Ministerratsvortrag an Verbrechen angeknüpft werden, die mit mehr als zehn Jahren Freiheitsstrafe bedroht sind oder auf das Vorliegen einer terroristischen Vereinigung bzw. kriminellen Organisation abgestellt werden.
  Konkret heißt dies, dem gemeinsamen Ministerratsvortrag der Bundesministerin für Justiz und des Bundesministers für Inneres folgend, dass Online-Durchsuchung jedenfalls nur in folgenden Fällen erfolgen darf:
  - Aufklärung eines mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens oder
  - des Verbrechens der Kriminellen Organisation oder der Terroristischen Vereinigung (§§ 278a und 278b StGB) oder

  - zur Aufklärung oder Verhinderung von im Rahmen einer solchen Organisation oder Vereinigung begangener oder geplanter strafbarer Handlungen
- Eine weitere Voraussetzung ist das Bestehen eines dringenden Tatverdachts (bzw. Vorbereitungshandlungen im Zusammenhang mit Kriminellen Organisationen und Terroristischen Vereinigungen (278a, 278b StGB)) gegen die Person, gegen die sich die Überwachung richtet.
- Besondere Anordnung der Staatsanwaltschaft, für den Fall, dass ein Eindringen in eine Wohnung erforderlich ist, die ebenfalls einer Genehmigung durch das Gericht bedarf.
- Diese Maßnahmen dürfen nur dann ergriffen werden, wenn andere Ermittlungsmaßnahmen nicht zum Ziel führen (ultima ratio, durch eine strenge Beachtung des Verhältnismäßigkeitsgrundsatzes)
- Richtervorbehalt
- Einbindung des Rechtsschutzbeauftragten der Justiz, indem dieser mit der richterlichen Bewilligung verständigt wird, ihm ein Beschwerderecht zukommt und ihm die begleitende und nachprüfende Kontrolle ermöglicht wird.
- Nachträgliche Verständigung aller von der Maßnahme Betroffenen durch die Justiz und umfangreiche Beschwerdemöglichkeiten. Damit eröffnet sich die Möglichkeit der Beschwerde für alle Betroffene.
- Zudem soll ein Beschwerderecht der Datenschutzkommission eröffnet werden, welches sich auf die gesamte Maßnahme erstreckt.
- Auch sind strenge Vernichtungsregelungen von unzulässig ermittelten oder für die Ermittlung bedeutungslosen Daten vorzusehen.
- Zufallsfunde dürfen nur dann verwertet werden, wenn auch für diese die notwendigen Voraussetzungen für eine Online-Durchsuchung vorliegen.
- Darüber hinaus ist eine verschuldensunabhängige Haftung des Bundes für Schäden, die durch eine Online-Durchsuchung verursacht wurden, vorzusehen.
- Aufnahme in den jährlichen Bericht über besondere Ermittlungsmaßnahmen, der dem Nationalrat, dem Datenschutzrat und der Datenschutzkommission vorzulegen ist.

Nochmals betont werden soll, dass es immer eine Einzelfallentscheidung eines Richters sein muss, ob die Durchführung einer Online-Durchsuchung verhältnismäßig ist.

Technische Komponente:

Am Beginn der Durchführung einer Online-Durchsuchung steht aus technischer Hinsicht die Ausbringung. Das heißt, die Installation der notwendigen Systemkomponenten in das Kommunikationssystem des Betroffenen. Dies kann mit oder ohne sofortige Aktivierung der Systemkomponenten erfolgen.

Generell wird der Fernzugriff auf Kommunikationssysteme nicht den Regelfall darstellen, da dadurch nicht ausgeschlossen werden kann, dass durch das Öffnen zB eines Emails mit der mit übermittelten Softwarekomponente eine Installierung der Forensic-Software auf einem falschen System erfolgt. Ein Fernzugriff sollte nur dann eingesetzt werden, wenn ausgeschlossen werden kann, dass die forensische Software nicht in ein Kommunikationssystem eines Dritten installiert wird. Neben der Ausbringung kommt auch für eine Verlängerung der Maßnahme ein Fernzugriff oder ein physischer Zugang in Frage. Dies gilt auch für die Deaktivierung bzw. Deinstallation (zudem Entfernung des technischen Hilfsmittels), wobei hier spezielle Vorsorge getroffen werden kann, dass beides durch Zeitablauf endet.

Ein wesentlicher Punkt – auch in Hinblick auf ein in weiterer Folge allfällig zu führendes Gerichtsverfahren – ist die Nachvollziehbarkeit der Vorgänge und des ursprünglich vorhandenen Datenbestandes am Ziel-Kommunikationssystem. Es muss technisch gewährleistet werden, dass es durch die Durchführung der Online-Durchsuchung zu keiner Veränderung der ursprünglich am Computersystem vorhandenen Daten gekommen ist. Zu diesem Zweck sollen folgende Maßnahmen ergriffen werden:

Installations-. Übermittlungs-, Änderungs- und Deinstallationsprotokoll. Bei der Übertragung der Objekte werden Prüfsummen gebildet, um zu gewährleisten, dass Datenpakete im Quell- und Zielsystem ident sind. Voraussetzung zur Sicherstellung, dass ausschließlich die vom Untersuchungsauftrag betroffenen Kommunikationssysteme miteinander kommunizieren können, ist die Authentifizierung unabdingbar. Die Übermittlung der Datenpakete hat gesichert (d.h. dem jeweiligen Stand

der Technik entsprechend verschlüsselt) an die Strafverfolgungsbehörden zu erfolgen.

Es ist festzuhalten, dass es von Seiten der User von Kommunikationssystemen unterschiedliche Möglichkeiten gibt, sich gegen eine Online-Durchsuchung zu wehren. Die Praxis zeigt jedoch, dass nicht alle Täter ein derart hohes Sicherheitsbewusstsein haben und sich entsprechend schützen. Insbesondere bei großen Netzwerken, wie großen terroristischen Vereinigungen, an denen viele Benutzer beteiligt sind, kann oft ein Ansatzpunkt zur Durchbrechung von Abwehrstrategien von Tätern gefunden werden, weil sich zwar der Großteil der Beteiligten an die auferlegte User-Disziplin hält, aber eben nicht alle Beteiligten. Auch in anderen Bereichen wie der Telefonüberwachung können sehr einfache Abwehrstrategien durch Zielpersonen getroffen werden. Dennoch stellt die Telefonüberwachung nach wie vor eine sehr effiziente Ermittlungsmaßnahme dar.

Von Seiten des Bundesministeriums für Inneres wird die technische Machbarkeit bejaht und angenommen, dass insbesondere bei einem direkten physischen Zugang zum Kommunikationsgerät in einem Großteil der Fälle die Installation von Softwarekomponenten zur Durchführung der Online-Durchsuchung möglich ist.

Der Vorteil einer Online-Durchsuchung liegt darin, dass bereits zu einem sehr frühen Ermittlungszeitpunkt Informationen vorliegen können, deren Kenntnis für die Aufgabenerfüllung der Sicherheitsbehörden wesentlich ist. Beispiel: Im Gegensatz zu einer Hausdurchsuchung, bei der der Betroffene und andere Beteiligte einer terroristischen Organisation unmittelbar Kenntnis vom Vorgang erlangen, ist es durch die verdeckte Durchführung der Online-Durchsuchung möglich, die gesamte Struktur des Terrornetzwerkes zu erhalten.

Zudem ist z.B. im Falle einer Voice over IP (VoIP) Kommunikation, etwa bei einem Telefonat über Skype, für die Sicherheitsbehörden aufgrund der verschlüsselten Kommunikation keine Möglichkeit zur Überwachung des Kommunikationsinhaltes gegeben. Durch die Online-Durchsuchung wäre im Einzelfall das Überwachen des Kommunikationsinhaltes am Entstehungsort wo er noch unverschlüsselt ist, möglich. Die Durchsuchung des Systems selbst soll zudem nach gewissen Kriterien bzw. Datenkategorien ermöglicht werden.

C. Militärbefugnisrecht[38]

Das Ziel dieses Berichtsteils ist die Untersuchung der bestehenden Rechtsgrundlagen im Militärbefugnisgesetz (MBG), BGBl. I Nr. 86/2000 daraufhin, ob das heimliche Eindringen in ein Computersystem[39] unter Ausnutzung einer Online-Verbindung zur Gewinnung von Daten[40] zulässig wäre.

Weiters sollen die Schnittstellen zwischen den im MBG geregelten Aufgaben der nachrichtendienstlichen Aufklärung[41] und Abwehr[42] und den Aufgaben der Strafverfolgungsbehörden nach der Strafprozessordnung (StPO) im hier vorliegenden Zusammenhang kurz dargestellt werden.

Notwendig ist dies deshalb, weil sich bereits in den ersten Diskussionen der Arbeitsgruppe (AG) gezeigt hat, dass es -trotz der Fokussierung des Ministerratsvortrages auf eine Erweiterung des Ermittlungsinstrumentariums für die Strafverfolgungsbehörden zur Beweissicherung -vor allem darum geht, die **Planung und Unterstützung schwerer Straftaten** (§ 278, 278a, 278b StGB) so **rechtzeitig zu erkennen**, dass die Beteiligten noch vor der Verwirklichung der entsprechenden Straftatbestände aus dem Verkehr gezogen bzw. Schutzmaßnahmen getroffen werden können.

---

[38] Siehe Anlage, Seite 63 <BMLV.SCHWARZINGER>

[39] § 74 (1) Z 8. StGB **Computersystem**: sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen.

[40] § 74 (2) StGB Im Sinne dieses Bundesgesetzes sind **Daten** sowohl personenbezogene und nicht personenbezogene Daten als auch Programme.

[41] § 20 (1) MBG Die **nachrichtendienstliche Aufklärung** dient der Beschaffung, Bearbeitung, Auswertung und Darstellung von Informationen über das Ausland oder über internationale Organisationen oder sonstige zwischenstaatliche Einrichtungen betreffend militärische und damit im Zusammenhang stehende sonstige Tatsachen, Vorgänge und Vorhaben.

[42] § 20 (2) Die **nachrichtendienstliche Abwehr** dient dem militärischen Eigenschutz durch die Beschaffung, Bearbeitung, Auswertung und Darstellung von Informationen über Bestrebungen und Tätigkeiten, die vorsätzliche Angriffe gegen militärische Rechtsgüter zur Beeinträchtigung der militärischen Sicherheit erwarten lassen.

- **Schnittstellen SPG – MBG – StPO**

Die Trennlinien zwischen Strafverfolgung und Gefahrenvorbeugung sind durchlässig geworden. Die Grenzen zwischen innerer und äußerer Sicherheit verschwimmen.[43]

Die vorbeugende Gefahrenabwehr (erweiterte Gefahrenforschung) ist zwar eine sicherheitspolizeiliche Aufgabe. Wenn es um den **Schutz militärischer Rechtsgüter**[44] **geht,** liegt aber auch **eine Aufgabe des militärischen Eigenschutzes** – und hinsichtlich der präventiven Informationssammlung – der nachrichtendienstlichen Abwehr vor. Eine Subsidiarität[45] des militärischen Handelns besteht (nur) bei Vorliegen einer allgemeinen Gefahr nach § 16 Abs 1 SPG, also einem gefährlichen Angriff (§ 16 Abs 2 und 3 SPG) oder einer kriminellen Verbindung. Zur Annahme eines „gefährlichen Angriffes“ muss zumindest ein Verhalten gesetzt werden, das in einem **engen zeitlichen Zusammenhang zur angestrebten Tatbestandsverwirklichung** steht, bloße **Planungsaktivitäten im weiteren Vorfeld** fallen daher **nicht** unter diese Bestimmung.

Die zum militärischen Eigenschutz einschreitenden Organe haben gem. § 2 Abs 2 MBG die Sicherheitsbehörden lediglich dann zu verständigen und vom Zeitpunkt des Einschreitens der Sicherheitsorgane an jede Erfüllung militärischer Aufgaben zu unterlassen, wenn ein Verhalten in einer allgemeinen Gefahr gem. § 16 Abs 1 SPG besteht. In **Situationen, in denen noch keine allgemeine Gefahr vorliegt**, aber eine solche wahrscheinlich ist, sind sie **neben den Sicherheitsbehörden zur Informationsermittlung und –weiterverarbeitung berufen**. Sicherheits- bzw. staatspolizeiliches und nachrichtendienstliches Aufgabenfeld decken sich über weite Strecken. Die Sicherheitsbehörden sind erst dann zu verständigen, wenn entweder ein gegenwärtiger gefährlicher Angriff vorliegt oder wenn eine kriminelle Verbindung existiert. Die Subsidiaritätsklausel hat in Bezug auf **gefährliche Angriffe** keine

---

[43] *Bierlein,* Rechtsschutz gestern-heute-morgen, in *Bammer/Holzinger/Vogel/Wenda* (Hrsg), Festgabe zum 80. Geburtstag von Rudolf Machacek und Franz Matscher, nwv (2008), 52 (53). Vgl. §§ 20 – 22 SPG.

[44] § 1 Abs 7 MBG.

[45] Vgl zur Zuständigkeitsproblematik § 2 Abs 2 MBG und ausführlich VfGH 23. 1. 2004, G 363/02.

große praktische Bedeutung, weil die Verständigungspflicht erst greift, wenn sich der Störer bereits im Vorbereitungsstadium befindet. In diesem Stadium wird die Eilbedürftigkeit schon der Verständigung Grenzen setzen, und selbst wenn eine solche erfolgt, werden die Sicherheitsbehörden selten rechtzeitig am Ort des Geschehens eintreffen. Anderes hingegen gilt für **kriminelle Verbindungen**. Wenn sich im Zuge nachrichtendienstlicher Aktivitäten zeigt, dass eine Gruppierung eine kriminelle Verbindung darstellt, ist die weitere Aufgabenerfüllung für die Abwehr nur innerhalb der durch § 2 Abs 2 MBG abgedeckten Grenzen zulässig. Die militärischen Organe müssen die Sicherheitsbehörden über die kriminelle Verbindung informieren und mit ihnen zusammenarbeiten, und sie dürfen nur solange Informationen über die kriminelle Verbindung sammeln, als die Sicherheitsbehörden deren Beobachtung noch nicht in Angriff genommen hat. Im Unterschied zum gefährlichen Angriff, wo ein Tätigwerden vor Ort geboten ist, wird sich eine solche „Übernahme“ der Aufgabenerfüllung aber nicht ohne weiteres mitteilen. Die Sicherheitsbehörden sind daher gut beraten, die nachrichtendienstlichen Organe entsprechend zu informieren.[46]

Liegt der konkrete Verdacht einer gerichtlich strafbaren Handlung vor, so ist gem. § 78 StPO Anzeige zu erstatten und – nach Maßgabe der verfassungsrechtlichen Rahmenbedingungen für jegliches Tätigwerden des Bundesheeres (Art. 79 B-VG) - allenfalls (im Assistenzweg) Amtshilfe für die Kriminalpolizei, Staatsanwaltschaft und Gerichte zu leisten.[47] Eine (eigenständige) **Befugnis zur Sicherung von Beweismitteln** gibt es im MBG nicht.[48]

---

[46] Vgl *Wiederin*, Privatsphäre und Überwachungsstaat, Sicherheitspolizeiliche und nachrichtendienstliche Datenermittlung im Lichte des Art 8 EMRK und der Art 9-10a StGG, MANZ (2003), 167.

[47] § 76 StPO.

[48] *Satzinger*, MBG, Verlag Österreich (2000), 105.

- **Befugnisse der militärischen Nachrichtendienste**

Entsprechend den Bestimmungen der §§ 21 bis 25 MBG sind die Organe der nachrichtendienstlichen Abwehr (und Aufklärung)[49] berechtigt, bei Vorliegen der konkreten Voraussetzungen:

- **„offene“ Auskunftsverlangen** an jedermann zu stellen – diese sind dadurch charakterisiert, dass auf den amtlichen Charakter und auf die Freiwilligkeit der Mitwirkung hinzuweisen ist (§ 21)
- Auskünfte über sogenannte **Stammdaten** (Name, Teilnehmernummer) von den Betreibern öffentlicher Telekommunikationsdienste einzuholen (§ 22 Abs 2a)
- **„verdeckt“ Auskünfte** durch den Einsatz von verdeckten Ermittlern einzuholen (§ 21 iVm § 22 Abs 4)
- **Daten zu verarbeiten**, das heißt im Wesentlichen diese zu ermitteln (insb auch bei anderen Behörden), zu speichern, zu verwenden (§ 22 Abs 1)
- **„offen“ Bild- und Tonaufzeichnungen** herzustellen (§ 22 Abs 5)
- **„Observationen“** (Beobachtungen) durchzuführen (§ 22 Abs 3)
- **„verdeckt“ Bild- und Tonaufzeichnungen** herzustellen (§ 22 Abs 5 iVm Abs 4)
- Observationen und verdeckte Ermittlungen durch die Ausstellung von **Legendendokumenten** (täuschen über die wahre Identität der Organe) abzusichern (§ 22a)
- **Verlässlichkeitsprüfungen** durchzuführen (§§ 23 und 24 sowie VLE-VO des BMLV, BGBl. II Nr. 195/2001)
- **Datenübermittlungen** durchzuführen und Ressortvereinbarungen über Datenübermittlungen abzuschließen (§ 25 MBG und § 7 DSG 2000)

[49] Die nachrichtendienstlichen Aufklärung wird vom Heeres-Nachrichtenamt betrieben, das sich als strategischer Auslandsnachrichtendienst Österreichs und Teil des sicherheitspolitischen Frühwarnsystems der Republik und der EU versteht (vgl. EINSATZ 5/2007 – Magazin für Sicherheit und Wirtschaft, 20). Die Befugnisse der nachrichtendienstlichen Aufklärung sind zwar mit jenen der Abwehr identisch, haben aber unterschiedliche Voraussetzungen und dienen einer völlig anderen Aufgabe (§ 20 Abs 1 MBG). Die nachrichtendienstliche Aufklärung ist nicht Teil des militärischen Eigenschutzes (§ 2 Abs 1 MBG) und kann daher im ggstl. Zusammenhang vernachlässigt werden.

Hinzuweisen ist in diesem Zusammenhang, dass Observationen, jegliche Bild- und Tonaufzeichnung sowie verdeckte Ermittlungen **vorher dem Rechtschutzbeauftragten** zu melden sind und nur nach dessen ausdrücklicher **Zustimmung** durchgeführt werden dürfen. Im **Inland generell verboten** sind die Aufzeichnung von nicht in der Öffentlichkeit und nicht im Wahrnehmungsbereich eines „verdeckten“ Ermittlers gemachte Äußerungen oder Handlungen („großer Lauschangriff“). Ebenso **verboten** ist das „Abhören“ von Telefongesprächen und das „Abfangen“ und „Lesen“ von E-Mails oder sonstiger **Kommunikationsinhalte** auf dem Übertragungsweg, da in das Fernmeldegeheimnis[50] nicht eingegriffen werden darf.[51] Der **Einsatz von unmittelbarer Zwangsgewalt zur Durchsetzung der Befugnisse der Nachrichtendienste** ist selbst im Einsatz zur militärischen Landesverteidigung ausnahmslos **untersagt** (§ 16 Abs 1 MBG).

- **Keine Befugnisse zur Online-Durchsuchung**

Konkret interessiert im hier gegebenen Zusammenhang, ob eine der oa. Befugnisse als Rechtsgrundlage für eine „Online-Durchsuchung“ herangezogen werden könnte.

Die Befugnis zur Erhebung von **Stammdaten** (§ 22 Abs 2a MBG) bei Telekommunikationsanbietern deckt derartige Aktivitäten **nicht**, da es bei der Durchsuchung um gespeicherte Inhalte eines Computersystems geht und nicht um die Identifizierung eines Users.

Die in einem vernetzten Datenträger abgespeicherten Daten könnten als **Bild** (eines Dokumentes) angesehen und daher auch unbemerkt (verdeckt) **aufgezeichnet** (kopiert) werden (§ 22 Abs 5 iVm Abs 4 MBG). Damit ist aber noch nicht das Problem des Eindringens in das System gelöst, das – vor dem Hintergrund der entsprechenden Strafbestimmungen[52] – einer gesonderten Grundlage bedürfte.

In Frage käme noch die allgemeine Befugnis zur **Datenverarbeitung** (und damit auch Datenermittlung). § 22 Abs 1 MBG ermächtigt zur Datenverarbeitung, die nur dadurch beschränkt wird, dass sie ausschließlich zum Zwecke der mit nachrich-

[50] Art 10a StGG.

[51] § 22 Abs 5 MBG, letzter Satz.

[52] §§ 118a, 119a, 126c StGB.

tendienstlichen Abwehr (bzw. Aufklärung) verbundenen Aufgaben und Befugnisse erfolgen darf und iSd § 4 MBG, wie jede andere Befugnisausübung, verhältnismäßig sein muss. Diese Ermächtigung stellt eine **Generalermächtigung** dar, die nur **durch spezielle Befugnisse ergänzt** wird. Im Ergebnis sind alle Datenverarbeitungen erlaubt, sofern sich aus den speziellen Befugnisnormen (§ 22 Abs 2 – 8 MBG) nichts anderes ergibt.[53]

Auch hier stellt sich wiederum das Problem des Eindringens in ein Computersystem, dass bei verfassungskonformer enger Interpretation des § 22 Abs 1 MBG wohl nicht gedeckt sein dürfte. Wenn man – hier dürfte Konsens in der AG herrschen – davon ausgeht, dass das heimliche Eindringen in ein Computersystem einen noch schwereren Eingriff in das Grundrecht auf Privatsphäre darstellt als ein „großer Lauschangriff“, dann hätte der Gesetzgeber jedenfalls eine ausdrückliche Spezialbefugnis zu schaffen gehabt, um den Anforderungen der EMRK zu genügen.[54]

Zusammenfassend bleibt also festzustellen, dass es **dzt. im MBG keine Rechtsgrundlage für das heimliche Eindringen in ein Computersystem** durch die militärischen Nachrichtendienste gibt.

D. Telekommunikationsrecht[55]

- **Aufgaben des TKG 2003**

Sicherstellen der Versorgung mit elektronischer Kommunikation, d.h.

– erforderliche Regelungen betreffend die Infrastruktur
– erforderliche Regelungen zur Sicherstellung von Wettbewerb im Bereich des gewerblichen Bereitstellens von elektronischer Kommunikation

Es enthält KEINE Regelung oder Aufsicht über Content

---

[53] *Wiederin*, Privatsphäre und Überwachungsstaat, 169.

[54] *Sunday Times* I, EGMR 26.4.1979, Nr 6538/74, Z 49; *Silver*, EGMR 25.3.1983, Nr 5947/72, Z88; *Malone*, EGMR 2.8.19984, Nr 8691/79, Z66.

[55] Siehe Anlage, Seite 68 <BMVIT.Datenschutz im TKG 2003>

§ 1. (1) Zweck dieses Bundesgesetzes ist es, durch Förderung des Wettbewerbes im Bereich der elektronischen Kommunikation die Versorgung der Bevölkerung und der Wirtschaft mit zuverlässigen, preiswerten, hochwertigen und innovativen Kommunikationsdienstleistungen zu gewährleisten.

- **Datenschutz und Kommunikationsgeheimnis - Ausnahmen**

Regelungen betreffend Datenschutz und Kommunikationsgeheimnis sind in diesem Sinn lediglich ein Exkurs und beinhalten ausschließlich diejenigen Bestimmungen, die erforderlich sind zum Schutz von Kommunikation via elektronische Medien. Dieser Schutz unterliegt allerdings einigen Ausnahmen:

Kommunikationsgeheimnis

§ 93. (1) Dem Kommunikationsgeheimnis unterliegen die Inhaltsdaten, die Verkehrsdaten und die Standortdaten. Das Kommunikationsgeheimnis erstreckt sich auch auf die Daten erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Kommunikationsgeheimnisses ist jeder Betreiber und alle Personen, die an der Tätigkeit des Betreibers mitwirken, verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) 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 ist unzulässig. Dies gilt nicht für die Aufzeichnung und Rückverfolgung von Telefongesprächen im Rahmen der Entgegennahme von Notrufen und die Fälle der Fangschaltung sowie für eine technische Speicherung, die für die Weiterleitung einer Nachricht erforderlich ist.

(4) Werden mittels einer Funkanlage, einer Telekommunikationsendeinrichtung oder mittels einer sonstigen technischen Einrichtung Nachrichten unbeabsichtigt empfangen, die für diese Funkanlage, diese Telekommunikationsendeinrichtung oder den Anwender der sonstigen Einrichtung nicht bestimmt sind, so dürfen der Inhalt der Nachrichten sowie die Tatsache ihres Empfanges weder aufgezeichnet noch Unbefugten mitgeteilt oder für irgendwelche Zwecke verwertet werden. Aufgezeichnete Nachrichten sind zu löschen oder auf andere Art zu vernichten.

– Für Zwecke der **Strafrechtspflege**: § 92 (2) „Die Bestimmungen der Strafprozessordnung bleiben durch die Bestimmungen dieses Abschnittes unberührt.“ Gleichzeitig werden dem Betreiber öffentlicher Telekommunikationsdienste die Verpflichtung zum Bereitstellen von zur Überwachung der Telekommunikation erforderlichen Einrichtungen sowie zur Mitwirkung an der Überwachung auferlegt.

§ 92. (2) Die Bestimmungen der Strafprozessordnung (StPO), BGBl. Nr. 631/1975, bleiben durch die Bestimmungen dieses Abschnittes unberührt.

§ 94. (1) Der Anbieter ist nach Maßgabe einer gemäß Abs. 3 erlassenen Verordnung verpflichtet, alle Einrichtungen bereitzustellen, die zur Überwachung einer Telekommunikation nach den Bestimmungen der StPO erforderlich sind.

(2) Der Betreiber ist verpflichtet, an der Überwachung einer Telekommunikation nach den Bestimmungen der Strafprozessordnung im erforderlichen Ausmaß mitzuwirken.

– Ermittlung und Verarbeitung von Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten zum Zweck **der Besorgung eines Kommunikationsdienstes**

§ 96. (1) Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten dürfen nur für Zwecke der Besorgung eines Kommunikationsdienstes ermittelt oder verarbeitet werden.

– Übermittlung von Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten zum Zweck der Vermarktung von Kommunikationsdiensten oder der Bereitstellung von Diensten mit Zusatznutzen sowie sonstige Übermittlung ausschließlich mit **Zustimmung der Betroffenen**.

§ 96. (2) Die Übermittlung von im Abs. 1 genannten Daten darf nur erfolgen, soweit das für die Erbringung jenes Kommunikationsdienstes, für den diese Daten ermittelt und verarbeitet worden sind, durch den Betreiber erforderlich ist. Die Verwendung der Daten zum Zweck der Vermarktung von Kommunikationsdiensten oder der Bereitstellung von Diensten mit Zusatznutzen sowie sonstige Übermittlungen dürfen nur auf Grund einer jederzeit widerrufbaren Zustimmung der Betroffenen erfolgen. Diese Verwendung ist auf das erforderliche Maß und den zur Vermarktung erforderlichen Zeitraum zu beschränken. Die Anbieter dürfen die Bereitstellung ihrer Dienste nicht von einer solchen Zustimmung abhängig machen.

– Ermittlung und Verarbeitung von Stammdaten für Abschluss, Durchführung, Änderung oder Beendigung des **Vertrages mit dem Teilnehmer**, der **Entgeltverrechnung**, der Erstellung von **Teilnehmerverzeichnissen** und der Erteilung von **Auskünften an Notrufträger**

§ 97. (1) Stammdaten dürfen unbeschadet der §§ 90 Abs. 6 und 96 Abs. 2 von Betreibern nur für folgende Zwecke ermittelt und verarbeitet werden:

1. Abschluss, Durchführung, Änderung oder Beendigung des Vertrages mit dem Teilnehmer;
2. Verrechnung der Entgelte;

3. Erstellung von Teilnehmerverzeichnissen, auch gemäß § 18 und
4. Erteilung von Auskünften an Notrufträger.
(2) Stammdaten sind spätestens nach Beendigung der vertraglichen Beziehungen mit dem Teilnehmer vom Betreiber zu löschen. Ausnahmen sind nur soweit zulässig, als diese Daten noch benötigt werden, um Entgelte zu verrechnen oder einzubringen, Beschwerden zu bearbeiten oder sonstige gesetzliche Verpflichtungen zu erfüllen.

– Für Auskünfte über Stammdaten und Standortdaten an Betreiber von **Notrufdiensten**

§ 98. Betreiber haben Betreibern von Notrufdiensten auf deren Verlangen Auskünfte über Stammdaten im Sinn von § 92 Abs. 3 Z 3 lit. a bis d sowie über Standortdaten im Sinne des § 92 Abs. 3 Z 6 erteilen. In beiden Fällen ist Voraussetzung für die Zulässigkeit der Übermittlung ein Notfall, der nur durch Bekanntgabe dieser Informationen abgewehrt werden kann. Die Notwendigkeit der Informationsübermittlung ist vom Betreiber des Notrufdienstes zu dokumentieren und dem Betreiber unverzüglich, spätestens jedoch innerhalb von 24 Stunden nachzureichen. Der Betreiber darf die Übermittlung nicht von der vorherigen Darlegung der Notwendigkeit abhängig machen. Den Betreiber des Notrufdienstes trifft die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens.

– Verkehrsdaten dürfen gespeichert werden, soweit und solange dies für **Verrechnungszwecke** erforderlich ist. Eine darüber hinausgehende Speicherung ist ausschließlich in gesetzlich besonders geregelten Fällen zulässig. Diese Ausnahme wurde insbesondere im Hinblick auf die im Jahr 2003 bereits in Diskussion befindliche Vorratsdatenspeicherung in § 99 TKG 2003 aufgenommen.

§ 99. (1) Verkehrsdaten dürfen außer in den gesetzlich besonders geregelten Fällen nicht gespeichert werden und sind vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren.
(2) Sofern dies für Zwecke der Verrechnung von Entgelten, einschließlich der Entgelte für Zusammenschaltungen, erforderlich ist, hat der Betreiber Verkehrsdaten bis zum Ablauf jener Frist zu speichern, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht werden kann.

– Speicherung von Inhaltsdaten ist zulässig, sofern die Speicherung einen wesentlichen **Bestandteil des Kommunikationsdienstes** darstellt (Sprachboxen, SMS, e-mail-Postfächer usw.)

§ 101. (1) Inhaltsdaten dürfen - sofern die Speicherung nicht einen wesentlichen Bestandteil des Kommunikationsdienstes darstellt - grundsätzlich nicht gespeichert werden. Sofern aus technischen

Gründen eine kurzfristige Speicherung erforderlich ist, hat der Anbieter nach Wegfall dieser Gründe die gespeicherten Daten unverzüglich zu löschen.
(2) Der Anbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass Inhaltsdaten nicht oder nur in dem aus technischen Gründen erforderlichen Mindestausmaß gespeichert werden. Sofern die Speicherung des Inhaltes Dienstmerkmal ist, sind die Daten unmittelbar nach der Erbringung des Dienstes zu löschen.

– andere Standortdaten als Verkehrsdaten dürfen nach Anonymisierung oder nach **Einwilligung von Benutzer oder Teilnehmer** verarbeitet werden (Hintergrund dieser Regelung ist, dass Mobilfunknetze in der Lage sind Standortdaten zu verarbeiten, welche genauer sind als es für Zwecke der Nachrichtenübertragung erforderlich wäre und für die Erbringung von Diensten mit Zusatznutzen wie z.B. für Verkehrsinformationen verwendet werden)

§ 102. (1) Andere Standortdaten als Verkehrsdaten dürfen unbeschadet des § 98 nur verarbeitet werden, wenn sie
1. anonymisiert werden oder
2. die Benutzer oder Teilnehmer eine jederzeit widerrufbare Einwilligung gegeben haben.
(2) Selbst im Falle einer Einwilligung zur Verarbeitung von Daten gemäß Abs. 1 müssen die Benutzer oder Teilnehmer die Möglichkeit haben, diese Verarbeitung von Daten für jede Übertragung einfach und kostenlos zeitweise zu untersagen.

- **Zusammenfassung**

Die derzeit vorgesehenen Ausnahmen sind vorgesehen soweit dies erforderlich ist für

1. das Erbringen und die Verrechnung von Kommunikationsdiensten und Diensten mit Zusatznutzen, allenfalls nach Einwilligung von Benutzer oder Teilnehmer
2. das Erteilen von Auskünften im Zusammenhang mit Notrufen
3. Zwecke der Strafrechtspflege soweit dies in der Strafprozessordnung vorgesehen ist

- **Überlegungen zur Online-Durchsuchung**

Vornahme einer für den Benutzer nicht ersichtlichen Installation anderer Programme, z.B.

– Software, das den innerhalb eines Netzwerkes stattfindenden Datenverkehr aufzeichnet
– Software, die sämtliche Eingaben an einem Computer mitprotokolliert
– Software, die anderen via Internet Zugang zu fremden Computern gewährt

Welche Tätigkeiten werden am Computer vorgenommen und inwieweit handelt es sich dabei um elektronische Kommunikation?

– **E-mail**-Verkehr – ist elektronische Kommunikation, Überwachung unterliegt damit dem Regime des TKG 2003
– **Anlegen, Speichern von Dateien in verschiedensten Formaten** – stellt keine elektronische Kommunikation dar. Installation der Überwachungssoftware oder Überwachung von Speichervorgängen, die der User vornimmt, genießt damit nicht den Schutz des TKG 2003
– **Aufrufen von fremden Internetinhalten** – stellt nach der Definition von „Nachricht“ in § 92 Abs. 3 Z. 7 TKG 2003

> „…soweit die übertragenen Informationen mit einem identifizierbaren Teilnehmer oder Nutzer in Verbindung gebracht werden können…“

wohl elektronische Kommunikation dar und unterliegt damit dem Regime des TKG 2003. Die Verbindung ist zwar maschinenorientiert, aber es kann der Internetzugang meist mit einem Abonnenten in Verbindung gebracht werden.

E. Privatrecht

In der Arbeitsgruppe wurde in diesem Zusammenhang die Frage angesprochen, ob als Folgeschäden einer Online-Durchsuchung mit einer Kompromittierung von Signaturen mit der Konsequenz erheblicher Schadensrisken wegen ungültiger Rechtsgeschäfte zu rechnen wäre. Eine endgültige Klärung dieses Aspekts konnte nicht gefunden werden.

Zu bedenken sind auch Fragen der Zulässigkeit privatrechtlicher Notwehr und Selbsthilfe seitens Eingriffsbetroffener – darf RFS entfernt, manipuliert oder zur Täuschung verwendet werden?

Urheberrechtliche Gesichtspunkte.[56] Das österreichische Urheberrecht für Computerprogramme ist maßgeblich durch die RL 91/250/EWG über den Rechtsschutz von Computerprogrammen determiniert. Diese RL definiert in ihrem Art. 4 eine Reihe von zustimmungspflichtigen Handlungen, zu denen unter anderem die Bearbeitung und andere Umarbeitungen eines Computerprogramms zählen (Art. 4 lit. b). Eine Zustimmung des Rechteinhabers zu einer Bearbeitung oder anderen Umarbeitung ist allerdings nicht erforderlich, wenn sie für eine bestimmungsgemäße Benutzung des Computerprogramms einschließlich der Fehlerberichtigung durch den rechtmäßigen Erwerber notwendig ist (Art. 5 Abs. 1).

In Umsetzung dieser Richtlinienbestimmungen normiert § 40d Abs. 2 UrhG über „Freie Werknutzungen“, dass Computerprogramme (vervielfältigt und) bearbeitet werden dürfen, soweit dies für ihre bestimmungsgemäße Benutzung durch den zur Benutzung Berechtigten notwendig ist; hiezu gehört auch die Anpassung an dessen Bedürfnisse.

Grundsätzlich auch auf Computerprogramme anwendbar ist ferner die Bestimmung des § 41 UrhG über „Freie Werknutzungen im Interesse der Rechtspflege und der Verwaltung“: Demnach steht das Urheberrecht der Benutzung eines Werkes zu Zwecken der öffentlichen Sicherheit oder zur Sicherstellung des ordnungsgemäßen Ablaufs von Verwaltungsverfahren, parlamentarischen Verfahren oder Gerichtsverfahren nicht entgegen. Zu dieser Bestimmung, durch die Art. 5 Abs. 3 lit. e der RL 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft umgesetzt wurde, existiert allerdings keine Judikatur des OGH (bzw. des EuGH); lediglich zur Vorgängerbestimmung findet sich eine – für die vorliegende Problematik allerdings wenig erhellende – Entscheidung des OLG Wien aus dem Jahr 1991 (MR 1991, 240).

Eine abschließende Beurteilung der aufgeworfenen Fragen ist daher – auch weil aus den Fragestellungen nicht hervorgeht, welche Art von Computerprogrammen auf welche Weise verändert (bearbeitet) werden sollen und auf wessen Computer diese

[56] Siehe Anlage, Seite 99 <BMJ.Stellungnahme-Urheberrecht>.

Programme jeweils installiert sind – nicht möglich. Es kann lediglich festgehalten werden, dass § 41 UrhG als „urheberrechtlicher Rechtfertigungsgrund“ für Werknutzungen zu Zwecken der öffentlichen Sicherheit oder zur Sicherstellung des ordnungsgemäßen Ablaufs von Gerichtsverfahren (hier: gerichtliche Strafverfahren) grundsätzlich in Betracht kommt, während die anderen freien Werknutzungen für die angedachten Formen der Bearbeitung wohl ebenso ausscheiden wie eine Zulässigkeit nach dem jeweiligen Lizenzvertrag. Zu Frage 2 ist außerdem auszuführen, dass die zur Benutzung eines Computerprogramms berechtigte Person gemäß § 40d Abs. 3 Z 2 UrhG das Funktionieren des Programms beobachten, untersuchen oder testen darf, um die einem Programmelement zugrunde liegenden Ideen und Grundsätze zu ermitteln, wenn sie dies durch Handlungen zum Laden, Anzeigen, Ablaufen, Übertragen oder Speichern des Programms tut, zu denen sie berechtigt ist.

Gemäß § 4 Abs. 4 SigG[57] treten die Rechtswirkungen der Abs. 1 bis 3 (wonach die sichere elektronische Signatur das rechtliche Erfordernis der Schriftlichkeit, insbesondere der Schriftlichkeit im Sinne des § 886 ABGB erfüllt) nicht ein, wenn nachgewiesen wird, dass die Sicherheitsanforderungen des SigG und der auf seiner Grundlage ergangenen Verordnungen nicht eingehalten oder die zur Einhaltung dieser Sicherheitsanforderungen getroffenen Vorkehrungen kompromittiert wurden.

Als mögliche Verletzungen der Sicherheitsanforderungen sind in den Erläuterungen zu dieser Bestimmung (1999 BlgNR 20.GP) die Fälle erwähnt, in denen der private Schlüssel ausgespäht, der Chipspeicher gebrochen oder der Algorithmus mathematisch ausgeforscht wird. Als Kompromittierung der zur Einhaltung der Sicherheitsanforderungen getroffenen technischen Vorkehrungen nennen die Erläuterungen nachträgliche technische Eingriffe und Manipulationen.

„Kompromittierung“ ist in § 2 Z 14 SigG - eingefügt im Rahmen der parlamentarischen Behandlung - definiert als die Beeinträchtigung von Sicherheitsmaßnahmen oder Sicherheitstechnik, sodass das vom Zertifizierungsdiensteanbieter zugrunde gelegte Sicherheitsniveau nicht eingehalten werden kann.

Zu den Sicherheitsvorkehrungen zählen z. B. die beim Zertifizierungsdienstanbieter zum Einsatz gelangende Hardware oder die von ihm verwendeten Signaturprodukte, insbesondere die Signaturerstellungseinheiten samt den Signaturerstel-

[57] Siehe Anlage, Seite 101 <Stellungnahme BMJ – Abt. I 2>

lungsdaten. Zur Sicherheitstechnik gehören etwa kryptographische Algorithmen oder das Versiegeln eines Chips. Eine Kompromittierung liegt vor allem vor, wenn die Signaturerstellungsdaten (der private Signaturschlüssel) von Dritten erfahren werden. Denkbar wäre, dass die Signaturerstellungsdaten oder die Zugangsberechtigungen zu diesen ausgespäht oder in direkter oder indirekter Weise technisch ausgelesen werden, Signaturerstellungsdaten durch das Aufzeichnen von Sekundäreffekten, wie Stromverbrauch oder Ausführungszeit, ermittelt werden, der Chipspeicher gebrochen oder der Signaturalgorithmus mathematisch ausgeforscht wird. Weiters ist auch in einer missbräuchlichen Veränderung von Kommunikationsprotokollen eine Kompromittierung zu sehen. Wird einem Dritten eine fremde PIN bekannt und kann er sie einer bestimmten Person zuordnen, so wird bereits eine Kompromittierung vorliegen (*Brenn*, SigG, 61).

Vor diesem Hintergrund kann aus Sicht der Abt. I 2 nicht ausgeschlossen werden, dass es auch durch eine Online-Durchsuchung zu einer solchen Korrumpierung kommen könnte. Letztlich wird die Beantwortung dieser Frage aber davon abhängen, welche Daten dabei technisch ausgespäht werden (können).

Besitzstörung setzt Eigenmacht des Störers voraus. Eigenmacht liegt nicht vor bei behördlicher Anordnung (*Dittrich/Tades*, ABGB[36] § 339 E 58 ff). Im Zusammenhang mit behördlich oder gerichtlich angeordneten Online-Durchsuchung können Fragen der Besitzstörung demnach außer Acht gelassen werden.

IV. Verfassungsrechtliche Aspekte[58]

Bei der hoheitlich verfügten Online-Durchsuchung privater IT-Systeme (= „die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können“)[59] handelt es sich um schwerwiegende Eingriffe in grundrechtliche Freiheiten,

[58] Beitrag Funk

[59] BVerfG 27.02.2008, 1 BvR 370/07, 1 BvR 595/07. Wortlaut unter <BVerfG, Entscheidung 27.02.08>.

namentlich in die Rechte auf Geheimhaltung personenbezogener Daten (Datenschutz), auf Schutz der Privatsphäre und Gedankenfreiheit. Je nach Vorgangsweise sind auch der Schutz des Hausrechts und der Wohnung berührt.

Wenn dergleichen Maßnahmen im Zusammenhang mit und zu Zwecken der Überwachung von Kommunikation erfolgen, liegt auch ein Eingriff in das Fernmeldegeheimnis und die Kommunikationsfreiheit vor.

Berührt sind in jedem Falle auch Verfahrensgrundrechte, namentlich das Recht auf ein Verfahren vor dem gesetzlichen Richter, auf ein faires Verfahren in Strafsachen und auf eine wirksame Beschwerde vor einer nationalen Instanz.

Bei Schäden am Eigentum und am Vermögen kommt der grundrechtliche Schutz der Unverletzlichkeit des Eigentums zum Tragen.

In allen Fällen grundrechtlicher Berührungen werden nebst Eingriffsverboten und Eingriffsgrenzen auch staatliche Schutz- und Gewährleistungspflichten mobilisiert. Dieser Aspekt ist vor allem im Zusammenhang mit Vorsorgepflichten für wirksame Kontrollen von Bedeutung.

Das BVerfG hat in der obzitierten Entscheidung aus dem allgemeinen Persönlichkeitsrecht (Art 2 Abs 1 iVm Art 1 Abs 1 GG)[60] ein (spezielles) „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ abgeleitet. Dieses richterrechtlich entwickelte und insofern „neue“ Grundrecht schafft für die weitere Rechtsentwicklung und Diskussion einen festen verfassungsrechtlichen Bezugspunkt mit dogmatischer Signalfunktion und großer semantischer und pragmatischer Bedeutung. Auf die österreichische Verfassungsrechtslage ist dieses Produkt höchstgerichtlicher Judikatur nicht ohne weiteres zu übertragen. Es ist aber für eine vergleichende Orientierung relevant und hilfreich, weil die einzelgrundrechtlichen Garantien der österreichischen Verfassung ähnlich denen des Grundgesetzes gestaltet sind und im Ergebnis zu einer durchaus vergleichbaren Verdichtung auf induktiver Basis mit ähnlichen Ergebnissen führen: Der Sache nach ist ein grundrechtlicher Anspruch auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auch nach geltendem österreichischem Verfassungsrecht begründbar.

---

[60] Recht auf freie Entfaltung der Persönlichkeit (Art 2 Abs 1), Unantastbarkeit der Menschenwürde (Art 1 Abs 2).

Unmittelbare Parallelen bestehen hinsichtlich der allgemeinen Bedingungen für Grundrechtseingriffe und für damit verbundene staatliche Schutz- und Garantiepflichten. Sie werden dogmatisch durch die Stichworte „Gesetzesvorbehalt“, „Verhältnismäßigkeitsgrundsatz“ und „Wesensgehaltsperre“ markiert. Demnach sind Eingriffe nur zulässig, wenn sie gesetzlich vorgesehen, verhältnismäßig und mit den jeweils grundrechtsrelevanten Kernbereichsgarantien verträglich sind.

A. Gesetzesvorbehalt

In gesetzesstaatlichen Systemen bildet das formelle Gesetz die Grundlage für Eingriffsermächtigungen und deren Durchführung durch hoheitliche staatliche Verbandsfunktionen. Die – teils formell, teils materiell gestalteten – Gesetzesvorbehalte der geltenden Grundrechtsordnung stellen als notwendige (wenn auch nicht hinreichende) Rechtsbedingung darauf ab, dass Grundrechtseingriffe „gesetzlich vorgesehen“ sind. Dies wird als doppelte Bindung interpretiert: Einerseits als Auftrag an die Vollziehung, keine anderen als gesetzlich vorgesehene Maßnahmen zu verwirklichen, andererseits als Auftrag an die Gesetzgebung, Eingriffsermächtigungen an Hand ihrer Zwecke, Reichweite und Schranken sowie hinsichtlich der Zuständigkeiten und des Verfahrens so genau zu bestimmen, dass sprachliche und funktionale Unschärfen minimiert werden. Umgekehrt dürfen Unschärfen nicht dazu herangezogen werden, um eine Ausweitung von Eingriffsmöglichkeiten zu legitimieren.

Zur Sicherung der grundrechtlichen Schutzfunktionen sind gesetzliche Eingriffsermächtigungen grundsätzlich strikt und limitativ auszulegen. Die verfassungsrechtlichen Gebote der Spezialität und Nichterweiterung von Eingriffsermächtigungen haben eine Entsprechung in den strafrechtlichen und strafprozessualen Prinzipien der strikten Legalität und des Analogie- und Extensionsverbotes in Bezug auf materielle Straftatbestände und Vorgehensregeln zu Lasten verdächtiger, beschuldigter oder angeklagter Personen.

Wie schon in den Berichtsteilen zur straf(prozess)rechtlichen Rechtslage vorhin unter III.A. dargetan wurde, bieten bestehende Eingriffsermächtigungen, namentlich zur Durchführung von Hausdurchsuchungen und zur Beschlagnahme von Beweisge-

genständen, keine gesetzliche Grundlage für Fernzugriffe auf private IT-Systeme, wie sie bei Online-Durchsuchungen in Form heimlicher Infiltration solcher Systeme stattfinden.[61]

Die Grundsätze der Spezialität und Nichtextension gelten auch für Eingriffe in das Fernmeldegeheimnis (Freiheit und Vertraulichkeit der Telekommunikation). Es sind nur jene Maßnahmen zulässig, die durch bestehende gesetzliche Ermächtigungen – einzeln oder in Kombination – gestattet sind. Auch diesbezüglich sei auf die Ausführungen vorhin unter III.A. verwiesen: „Die Ermächtigung zur Überwachung von Nachrichten gestattet nur den Zugriff auf Nachrichten, die über ein Kommunikationsnetz usw. „ausgetauscht oder weitergeleitet werden“ (§ 134 Z 3 StPO). Sie betrifft also nur die im Übermittlungsvorgang befindlichen Nachrichten (einschließlich ihrer Speicherung bei den Übermittlungsdiensten). Nachrichten, die übermittelt wurden (und sich schon beim Empfänger befinden) oder möglicherweise übermittelt werden sollen (aber sich noch beim potenziellen Absender befinden), dürfen nach dieser Bestimmung nicht überwacht werden. Die optische und akustische Überwachung von Personen (§ 136 StPO) darf, wie der Name schon sagt, nur mit akustischen (Abhörgerät, Tonübertragung) oder mit optischen (Kameras) Mitteln erfolgen. Die geheime elektronische Überwachung eines Rechners ist durch diese Bestimmung nicht gedeckt.“

Wie sich aus den Beiträgen zum Sicherheitspolizeirecht (III.B.), zum Militärbefugnisrecht (III.C.) und zum Telekommunikationsrecht (III.D.) ergibt, finden sich auch sonst keine gesetzlichen Grundlagen, die Maßnahmen einer Online-Durchsuchung erlauben.

Aus der Sicht des grundrechtlichen Gesetzesvorbehaltes ist somit zweierlei festzuhalten: Die verfassungsrechtlich notwendige Bedingung einer speziellen gesetzlichen Ermächtigung für Vorgehensweisen der „Online-Durchsuchung“ ist nicht erfüllt. Vorhandene Eingriffsermächtigungen, speziell solche betreffend Hausdurchsuchungen, Beschlagnahme von Beweisgegenständen, Öffnung von Briefen, Überwachung von Nachrichten und die optische und akustische Überwachung von Personen, bieten keine tauglichen gesetzlichen Grundlagen für Online-Durchsuchungen.

---

[61] Siehe im Besonderen auch die in FN 30 enthaltene Feststellung.

B. Verhältnismäßigkeitsgrundsatz

Grundrechtseingriffe sind nur zulässig, wenn und soweit sie dem Grundsatz der Verhältnismäßigkeit entsprechen. Auch hier handelt es sich um eine notwendige, aber nicht hinreichende Bedingung für die verfassungsrechtliche Legitimierbarkeit von Eingriffsermächtigungen und tatsächlichen Eingriffen. Als Verfassungsgrundsatz geht das Verhältnismäßigkeitsprinzip im Wesentlichen auf richterliche und doktrinelle Rechtsfortbildung zurück. Der Grundsatz wurde und wird als Element und Facette des allgemeinen Sachlichkeitsgebotes angesehen, welches seinerseits dem Gleichheitssatz, dem Diskriminierungs- und Willkürverbot zugeordnet wird.

Der Grundsatz der Verhältnismäßigkeit verlangt, dass staatliche Maßnahmen und deren gesetzliche Grundlagen durch öffentliche Interessen legitimierbar sind, dass sie tatsächlich geeignet sind, die aus diesen Interessen abgeleiteten Ziele zu erreichen (instrumentelle Treffsicherheit) und dass dies in aufwands- und eingriffsoptimaler Weise geschieht.

Zur Legitimierbarkeit durch öffentliche Interessen. Die verfassungsrechtlich relevanten Elemente ergeben sich aus den materiell geprägten Gesetzesvorbehalten der EMRK. Im vorliegenden Zusammenhang sind insbesondere die Kriterien des Art 8 Abs 2 EMRK maßgeblich. Sie legen die Anforderungen und Grenzen für gesetzliche und exekutive Eingriffe in das Grundrecht auf Achtung des Privatlebens fest und bilden gleichermaßen die Kriterien für Eingriffe in das verfassungsgesetzlich gewährleistete Recht auf Schutz personenbezogener Daten.

Die dort als mögliche Legitimationsgrundlagen für Eingriffe genannten öffentlichen Interessen (nationale Sicherheit, öffentliche Ruhe und Ordnung, wirtschaftliches Wohl des Landes, Verteidigung der Ordnung, Verhinderung von strafbaren Handlungen, Schutz der Gesundheit und der Moral, Schutz der Rechte und Freiheiten anderer) sind ihrerseits nach Grundsätzen der Verhältnismäßigkeit zu gewichten und in ein komparatives Schema zu setzen, welches die Eingriffsintensität mit Interessenpräferenz in Beziehung setzt: Je schwerer und folgenreicher der Eingriff, desto höher die Anforderungen an die legitimierende Kraft öffentlicher Interessen. Schon hier gilt – wie in allen Facetten der Verhältnismäßigkeit – das Über- und Untermaßverbot.

Die in Art 8 Abs 2 EMRK (und in Gesetzesvorbehalten zu anderen Konventionsgrundrechten) aufgelisteten legitimationskräftigen öffentlichen Interessen werden durch das gemeinsame Erfordernis der Demokratiekonformität verbunden: Eingriffe sind sämtlich nur zulässig, soweit sie „in einer demokratischen Gesellschaft“ zur Erreichung der genannten Ziele notwendig sind.

Was bedeutet das für die Online-Durchsuchung? Eine Legitimierbarkeit durch öffentliche Interessen ist nicht ausgeschlossen, soweit eine angemessene Korrelation zwischen Maßnahmen und bedrohten Rechtsgütern besteht. Solche Maßnahmen dürfen nur für die Aufklärung und Verfolgung besonders schwerer Straftaten zur Verfügung gestellt werden.

In diese Richtung weist auch der 2. Leitsatz der Entscheidung des BVerfG: „Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.“[62]

„In einer demokratischen Gesellschaft notwendig“ können solche Maßnahmen sein, wenn sie durch starke öffentliche Interessen, wie die Bekämpfung und Verfolgung schwerer Kriminalität, die Erhaltung der Grundlagen oder den Bestandsschutz des Staates legitimiert werden.

Eingriffe in Grundrechte müssen, um dem Grundsatz der Verhältnismäßigkeit zu entsprechen, in der Lage sein, die Umsetzung der sie legitimierenden öffentlichen Interessen treffsicher zu gewährleisten. Damit ist die Frage der **Eignung** angesprochen. Ihre Beantwortung fällt in die Kompetenz der Informationstechnologie. Sie

[62] Nachweise bei FN 77. Bemerkenswert ist, dass das BVerfG über die Strafverfolgung hinaus die Online-Durchsuchung auch für präventive Zwecke nicht für ausgeschlossen hält.

zeigt hohe Risken eines technischen Fehlschlagens oder unbeherrschbarer Nebenwirkungen des Einsatzes von Strategien der Online-Durchsuchung. Zum gegenwärtigen Stand der Technik dürfte nicht gesichert sein, dass dieses Instrument in zuverlässiger, schadloser und treffsicherer Weise zur Anwendung gebracht werden kann. Nach Auffassung des Bundesverfassungsgerichts kann aber der heimliche Zugriff auf informationstechnische Systeme eine geeignete Ermittlungsmaßnahme darstellen.

Verhältnismäßigkeit im engeren Sinne erfordert eine Optimierung des Verhältnisses von Aufwand und Eingriff. Diesem Erfordernis wäre nicht entsprochen, wenn ein gleicher Erfolg mit weniger eingriffsintensiven Mitteln erreichbar wäre oder wenn die zum Einsatz gebrachten Mittel für die Erreichung des Erfolges zu schwach wären (Übermaß- und Untermaßverbot). Die Eingriffsintensität ist nicht an faktischen, sondern an rechtlichen Maßstäben zu messen. De facto wäre ein Fernzugriff für den Betroffenen nicht spürbar und somit weniger eingriffsintensiv als etwa der physische Zugriff und Beweismittel im Wege einer Hausdurchsuchung oder einer Beschlagnahme von Informationsträgern. Diese Sichtweise ist allerdings einer rechtlichen Qualifikation nicht angemessen. Aus grundrechtlicher Sicht ist der heimliche Fernzugriff, gerade weil er nicht spürbar und damit als solcher nicht erkennbar ist, für den Betroffenen der weitaus schwerere Eingriff als Zugriffe, die in konventioneller Weise erfolgen.

Dem Erfordernis der komparativen Minimierung der Eingriffsstärke entspricht das Postulat nach kompensatorischen Mechanismen des Rechtsschutzes und der Kontrolle. Je größer die Dichte und Wirksamkeit solcher Mechanismen ist, desto höher sind die Legitimierbarkeitschancen für solche Eingriffe unter dem Gesichtspunkt der Verhältnismäßigkeit.

Mit Fragen der Verhältnismäßigkeit haben im weitesten Sinne auch **technikbedingte Aspekte der Online-Durchsuchung** zu tun. Sie betreffen das Territorialitätsprinzip, den Schutz von Vertrauensträgern und die Bewältigung großer Datenmengen. Bei einem Zugriff auf Datenträger über Kommunikationsnetze ist – wegen der „Ortslosigkeit“ des Internet – nicht garantiert, dass hoheitliche Eingriffe auf den territorialen Wirkungsbereich des Staates beschränkt bleiben. Programmgesteuerte Durchsuchungen können die Bedeutung der ermittelten Daten nicht erkennen. Eine Beurteilung der Relevanz für Zwecke der Ermittlungszwecke kann nicht vom

Programm selbst geleistet werden – jedenfalls nicht auf rekursivem Weg. Die Bewertung muss durch Menschen erfolgen, die die solcherart erfassten Informationen verstehen und beurteilen können. Das Programm kann nicht unterscheiden, ob es sich um Informationen handelt, die bei Trägern speziell geschützter Berufsgeheimnisse, wie Journalisten, Rechtsanwälten und anderen Vertrauenspersonen, anfallen. Überdies kann die Leistungsfähigkeit solcher Verfahren sehr rasch an Grenzen stoßen, die sich aus der Notwendigkeit des (nicht maschinellen) Lesens großer Datenmengen ergeben.

Zusammenfassend zur Verhältnismäßigkeit: Der Grundsatz der Verhältnismäßigkeit bindet die Gesetzgebung und die Vollziehung. Er fordert die Vermeidung von Übermaß und Untermaß sowohl in den Zielen als auch auf der Ebene der Mittel, jeweils im komparativen Bezug auf eingriffslegitimierende öffentliche Interessen, Eignung und Minimalität der Eingriffe. Kompensatorische Legitimation kann durch wirksame Instrumente des Rechtsschutzes und der Rechtmäßigkeitsgewähr geschaffen werden. Ob im Sinne des Eignungsgebotes die Verhältnismäßigkeit gewährleistet werden kann, hängt wesentlich von den einschlägigen technologischen Gegebenheiten und Möglichkeiten ab. Die Bedingungen technischer Gefahrlosigkeit und Treffsicherheit können nicht als ausreichend sicher angesehen werden. Auch in der Relation von Aufwand und Ergebnis erscheint die Verhältnismäßigkeit zweifelhaft.

C. Wesensgehalt (Kernbereich) des Privaten

Das BVerfG hat aus dem allgemeinen Persönlichkeitsrecht ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme abgeleitet. In der bundesdeutschen Diskussion wurde verschiedentlich die Auffassung vertreten, dass heimliche Zugriffe auf die in solchen Systemen gespeicherten Informationen in einen eingriffsfesten Kernbereich des Privaten eingreifen und daher absolut unzulässig seien. Das BVerfG ist dieser Auffassung nicht gefolgt. Es hat in

seiner Entscheidung zum Nordrhein-Westfälischen Verfassungsschutzgesetz Bedingungen und Grenzen für Eingriffe in dieses Grundrecht angegeben.[63]

In Österreich stellen sich ähnliche Fragen, wenn auch in anderer verfassungsrechtlicher Terminologie und Systematik. Die Kernbereichsdiskussion hat ihre Entsprechung in der Frage der sog Wesensgehaltsperre. Sie wäre dort verletzt, wo Grundrechtseingriffe rechtlich oder faktisch zu einer gänzlichen oder großflächigen Aufhebung grundrechtlicher Schutzfunktionen führen.[64] Ob das bei Eingriffen in die Vertraulichkeit und Integrität informationstechnischer Systeme der Fall ist, kann – angesichts der Gesetzesvorbehalte bei den Grundrechten auf Achtung des Privatlebens und auf Geheimhaltung personenbezogener Daten – bezweifelt werden. Absolut gewährleistete Grundrechte finden sich in Art 3 EMRK.[65] Ein eingriffsfester Kern (unantastbarer Wesensgehalt) ist aber auch bei Grundrechten anerkannt, die nicht absolut gewährleistet sind, somit auch bei jenen Grundrechten, die im Dienste der Vertraulichkeit und Integrität informationstechnischer Systeme stehen.

Für die Online-Durchsuchung führt die Frage nach der Wesensgehaltsgarantie zurück zu den allgemeinen Bindungen, dh zum Gesetzesvorbehalt und zum Grundsatz der Verhältnismäßigkeit. Verletzungen dieser Bindungen können den Wesensgehalt der maßgebenden Grundrechte verletzen.

D. Datenschutzrechtliche Aspekte der Online-Durchsuchung im Besonderen [66]

- **Rechtsgrundlagen**

Europaweit gelten die Datenschutzkonvention des Europarates ETS 108 samt Zusatzprotokoll zu dieser Konvention, die Datenschutzregelungen enthalten, die in allen Bereichen gelten (also auch Polizei- und Justizbereich).

---

[63] Leitsätze unter VI.A.

[64] Beispiele: Abschaffung des Privateigentums an Sachkategorien, wie Grund und Boden oder bestimmten Produktionsmitteln. Aufhebung der Gewerbefreiheit in größeren Sparten.

[65] Verbot der Folter, der unmenschlichen oder erniedrigenden Strafe oder Behandlung.

[66] Siehe Anlage, Seite 7 <BKA-VD.Datenschutz und online-Durchsuchung>

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr („Datenschutzrichtlinie“) gilt nur für vergemeinschaftete Bereiche, Justiz und Inneres sind davon ausgenommen. Dasselbe gilt für die im TKG umgesetzte Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation). Der geplante Rahmenbeschluss über den Schutz personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit ist -sofern er noch im Jahr 2008 angenommen wird -auf rein nationale Sachverhalte nicht anwendbar.

Das Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 -DSG 2000), BGBl. Nr. 165/1999, zuletzt geändert durch BGBl I Nr 13/2005, setzt zwar die Datenschutzrichtlinie um, gilt aber darüber hinaus für alle Bereiche.

Besonders hervorzuheben ist der in Verfassungsrang stehende § 1 (Grundrecht auf Datenschutz). § 1 Abs. 1 und 2 lauten:

1. (1) 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 Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.
(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

Weiters enthält § 1 DSG 2000 Regelungen über die Betroffenenrechte (Auskunftserteilung, Richtigstellung und Löschung) und über den Rechtsschutz.

In Angelegenheiten der Gerichtsbarkeit sind überdies für den Datenschutz die Regelungen der §§ 83 – 85 GOG[67] maßgebend. Sie regeln die Zuständigkeiten und das Verfahren in Angelegenheiten der Auskunftserteilung, der Löschung und Richtigstellung, einschließlich des Rechtsschutzes vor den dafür zuständigen Gerichten.

- **Zulässigkeit von Eingriffen in das Grundrecht auf Datenschutz**

§ 1 Abs. 2 DSG 2000 sieht vor, dass Eingriffe in das Grundrecht auf Datenschutz entweder im lebenswichtigen Interesse oder mit Zustimmung des Betroffenen oder im überwiegenden Interesse eines anderen erfolgen dürfen. Das lebenswichtige Interesse ist eng auszulegen, d. h. etwa nur im Falle notfallmedizinisch indizierter Eingriffe. Ebenso stellt auch die Zustimmung nur beschränkt eine Eingriffsermächtigung dar, da hier insbesondere auf das – bereits in der Richtlinie 95/46/EG vorgesehene Zwangsverbot (vgl. § 4 Z 14 DSG 2000) bei Zustimmungserklärungen Rücksicht zu nehmen ist.

In der legistischen Praxis wird daher in der überwiegenden Anzahl von Fällen, in denen Eingriffe notwendig erscheinen, versucht werden müssen, Eingriffsermächtigungen auf das Vorliegen überwiegender berechtigter Interessen zurückzuführen.

§ 1 Abs. 2 DSG 2000 enthält einen **Gesetzesvorbehalt für Eingriffe durch staatliche Behörden**. Das Vorliegen einer gesetzlichen Grundlage – als formellem Kriterium – reicht aber allein nicht aus, den Eingriff zu legitimieren. Hiezu bedarf es zusätzlicher inhaltlicher (materieller) Voraussetzungen, die ebenfalls in § 1 Abs. 2 DSG 2000 benannt sind. Demnach dürfen Eingriffe durch staatliche Behörden nur erfolgen, soweit sie „**aus den in Art. 8 Abs. 2 [...] EMRK [...] genannten Gründen notwendig** sind“.

Eingriffe in das Grundrecht müssen zudem **verhältnismäßig** sein. D. h., der mit dem Eingriff verfolgte Zweck muss legitim sein, das Mittel muss zur Zielerreichung geeignet und erforderlich sein. Außerdem muss ein zwischen dem durch den Eingriff zu erreichenden Zweck und der Art des Eingriffs ein angemessenes Verhältnis bestehen. Als besondere Betonung der Verhältnismäßigkeit sieht § 1 Abs. 2 letzter Satz DSG 2000 das Gebot des **gelindesten Mittels** vor. Für die legistische Gestal-

[67] Gerichtsorganisationsgesetz, RGBl 1896/217.

tung von Eingriffsermächtigungen bedeutet dies, dass erstens unter mehreren geeigneten und erforderlichen Mittel nur jenes mit der geringsten Eingriffsintensität verfassungsrechtlich zulässig ist und zweitens auch dieses gelindeste Mittel insgesamt in einem angemessenen Verhältnis zum angestrebten Zweck stehen muss.

Besondere Kautelen sind hinsichtlich jener gesetzlichen Regelungen vorgesehen, die (auch) die Verwendung **sensibler Daten** (siehe die Definition sensibler Daten in § 4 Z 2 DSG 2000) vorsehen: Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind (= sensible Daten), nur zur Wahrung **wichtiger** öffentlicher Interessen vorsehen und müssen gleichzeitig **angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen** festlegen.

Die Ausgestaltung derartiger angemessener Garantien wird wohl auch mit der Intensität des Grundrechtseingriffes zu korrelieren haben. Dabei sind etwa Kombinationen von besonders strengen Sicherheitsmaßnahmen (z. B. lückenlose Protokollierung) mit besonderen Verschwiegenheitspflichten, ausdrücklichen Verwendungsbeschränkungen und -verboten, besonderen Informationsverpflichtungen und besonderen Rechtsschutzmechanismen denkbar.

- **Einfachgesetzliche Bestimmungen des DSG 2000**

Sofern nicht spezialgesetzliche Regelungen bestehen – die dem Grundrecht auf Datenschutz entsprechen müssen –, gelten die einfachgesetzlichen Regelungen des DSG 2000 (Grundsätze für die Verwendung von Daten, Ausübung von Betroffenenrechten etc.)

- **Online- Durchsuchung:**

Beim Instrument der Online-Durchsuchung würde es sich um einen schwerwiegenden Eingriff in das Grundrecht auf Datenschutz handeln, bei dem die zu verarbeitenden Daten offenbar auch nicht im vorhinein determiniert werden können und auch sensible Daten (z. B. Tagebücher, persönliche Korrespondenz) oder andere heikle Daten (z. B. Geschäfts- und Betriebsgeheimnisse) verarbeitet werden könnten, ohne dass der Betroffene davon Kenntnis hat. Dabei kann es sich auch um sensible Daten völlig unbeteiligter Dritter handeln. Überdies wäre dies offenbar im Regelfall

mit einem heimlichen Eindringen in die Räumlichkeiten des Computerbesitzers verbunden, wodurch ebenfalls in die Privatsphäre des Betroffenen eingegriffen würde.

Vor der allfälligen gesetzlichen Einführung eines derartigen Instruments wird besonders zu prüfen sein, ob dessen Einsatz dem Grundsatz der Verhältnismäßigkeit entspricht (Eignung zur Zielerreichung angesichts der in der Arbeitsgruppe angesprochenen Umgehungsmöglichkeiten, Grundsatz des gelindesten zum Ziel führenden Mittels).

V. Europäisches Gemeinschafts- und Unionsrecht

Ein gemeinschaftsrechtlicher Rahmen für Online-Durchsuchungen besteht weder de lege lata, noch ist in nächster Zeit mit einschlägigen Regelungen zu rechnen. Im Zusammenhang mit dem Vertrag von Lissabon wird über die Schaffung einer Europäischen Staatsanwaltschaft diskutiert.[68] Für ein europäisches Strafverfahrensrecht gibt es einige Ansätze. Sie betreffen Mindestrechte von Opfern und Beschuldigten, verfahrensrechtliche Mindeststandards, die Zulässigkeit von Beweismitteln auf gegenseitiger Basis und die Anerkennung von Entscheidungen, die solchen Standards entsprechen.

Zu beachten sind auch die Garantien der – nach dem Konzept des Vertrages von Lissabon künftig primärrechtlich verbindlichen – Charta der Grundrechte der EU, namentlich das Recht auf Achtung des Privat- und Familienlebens, einschließlich der Wohnung und der Kommunikation (Art 7), des Schutzes personenbezogener Daten (Art 8), der Gedankenfreiheit (Art 10), das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht im Falle der Verletzung von Rechten aus der Charta (Art 47) sowie die Verteidigungsrechte (Art 48).

---

[68] Gemäß Art 69e [86] AEUV (Vertrag über die Arbeitsweise der Europäischen Union) kann der Rat zur Bekämpfung von Straftaten zum Nachteil der finanziellen Interessen der Union nach einem besonderen Gesetzgebungsverfahren durch Verordnungen ausgehend von Eurojust eine Europäische Staatsanwaltschaft einsetzen.

Gemeinschaftsrechtliche Bezüge bestehen weiters im Zusammenhang mit der Datenschutzrichtlinie[69] und der Richtlinie 2006/24 EG über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden. Gegen diese RL hat Irland eine Nichtigkeitsklage beim EuGH mit der Begründung eingebracht, dass die richtige Rechtsform ein Rahmenbeschluss im Rahmen der 3. Säule hätte sein müssen. Die Entscheidung des EuGH ist noch nicht ergangen. Entsprechend Art 15 Abs 3 der RL hat Österreich die Umsetzung in Bezug auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-Email bis zum 15. März 2009 aufgeschoben. Ferner ist darauf hinzuweisen, dass der Rat am 8. November 2007 eine allgemeine Ausrichtung zu einem 3.Säule Rahmenbeschluss über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, erzielt hat.

VI. Vergleiche

Vorweg ist darauf hinzuweisen, dass Ausführungen in diesem Berichtsteil nur punktuelle Einblicke in die Rechtslage der genannten Staaten bieten und nicht den Anspruch erheben, damit die rechtlichen Rahmenbedingungen umfassend darzustellen oder Aussagen über ihre praktische Handhabung abzugeben.

In einigen Staaten sind solche Ermittlungsmaßnahmen im Rahmen nachrichtendienstlicher Befugnisse geregelt, auf die der Bericht im Hinblick auf seinen Arbeitsauftrag nicht eingeht.

[69] Siehe vorhin unter IV.D.1.

A. Deutschland[70]

1. Nach Ansicht des Bundesgerichtshofes (Beschluss vom 31.1.2007, GZ StB 18/06)[71] besteht im deutschen Strafprozessrecht derzeit keine Rechtsgrundlage zur Durchführung einer geheimen Online-Durchsuchung:

Die §§ 102 ff der dt. StPO über die Hausdurchsuchung erachtet der BGH als nicht anwendbar, weil das Bild der Strafprozessordnung von einer rechtmäßigen Durchsuchung dadurch geprägt sei, dass Ermittlungsbeamte am Ort der Durchsuchung körperlich anwesend sind und die Ermittlungen offen legen:

„...ist es den Ermittlungsbehörden - unabhängig davon, wonach gesucht wird - verboten, eine richterliche Durchsuchungsanordnung bewusst heimlich durchzuführen, um auf diese Weise dem Tatverdächtigen keine Hinweise auf die gegen ihn geführten Ermittlungen zu geben und den Erfolg weiterer Ermittlungen nicht zu gefährden. Dementsprechend versteht es sich, dass ein Richter keine Durchsuchung anordnen darf, die - wie die verdeckte Online-Durchsuchung - von vornherein darauf abzielt, bei ihrem Vollzug die gesetzlichen Schutzvorschriften des § 105 Abs. 2 und des § 106 Abs. 1 StPO außer Kraft zu setzen.“

Auch systematische Erwägungen würden gegen die Subsumtion der „Online-Durchsuchung“ unter die §§ 102 ff dt StPO sprechen, weil jene Vorschriften, die besonders grundrechtsintensive Ermittlungsmaßnahmen ohne Wissen des Betroffenen bzw. Dritter vorsehen (§§ 100a ff leg. cit.), unter hohen formellen unter materiellen Anforderungen stehen: Sie dürfen nur beim Verdacht bestimmter schwerer Straftaten angeordnet werden, wenn andere erfolgversprechende Aufklärungsmittel nicht vorhanden sind und sie nicht in den unantastbaren Kernbereich privater Lebensgestaltung eingreifen. Vergleichbar hohe Eingriffsschranken für die Anordnung einer Durchsuchung sieht aber § 102 dt StPO nicht vor, diese ist vielmehr zur Aufklärung jeder Straftat zulässig.

---

[70] Siehe Anlage, Seite 11 <Flendrovsky. Rechtslage in D> und Seite 86 <BMJ.Rechtslage EU.Schweiz>

[71] Volltext der Entscheidung unter http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2007&Sort=3&nr=38779& linked=bes&Blank=1&file=dokument.pdf.

Die §§ 100a ff dt. StPO selbst sehen eine Online-Durchsuchung nicht vor: Es handelt sich dabei insbesondere nicht um eine „Überwachung einer Telekommunikation“ (§ 100a leg. cit) oder Wohnraumüberwachung (§ 100c leg. cit.). Die Generalklausel des § 161 dt. StPO deckt nur Zwangsmaßnahmen mit geringer Eingriffsintensität.

Schließlich kann § 102 dt. StPO zur verdeckten Online-Durchsuchung auch dann nicht ermächtigen, wenn zusätzlich die für die Überwachung von Telekommunikation (§ 100 a StPO) und Wohnraum (§ 100 c StPO) normierten hohen Eingriffsvoraussetzungen - wie Verdacht einer Straftat von erheblicher Bedeutung, Subsidiarität gegenüber weniger belastenden Ermittlungsmaßnahmen - gegeben sind und der Grundsatz der Verhältnismäßigkeit „besonders“ beachtet wird. Es ist unzulässig, einzelne Elemente von Eingriffsermächtigungen zu kombinieren, um eine Grundlage für eine neue technisch mögliche Ermittlungsmaßnahme zu schaffen.

Innerhalb des Bundesgerichtshofes war die Zulässigkeit der Online-Durchsuchung umstritten. Zunächst ordnete mit Beschluss vom 21. Februar 2006 ein Ermittlungsrichter *„die Durchsuchung des von dem Beschuldigten […] benutzten Personalcomputers/Laptops, insbesondere der auf der Festplatte und im Arbeitsspeicher abgelegten Dateien“* an. Als Rechtsgrundlage legte er die Vorschriften der StPO zu Haus- und Wohnungsdurchsuchungen zugrunde. Am 25. November 2006 lehnte jedoch ein anderer Ermittlungsrichter den Antrag des auf Durchführung einer weiteren Online-Durchsuchung ab. Er begründete seine Entscheidung u. a. damit, dass eine solche Maßnahme ohne Wissen des Betroffenen stattfindet, während das Gesetz für eine herkömmliche Durchsuchung die Anwesenheit von Zeugen (vgl. § 105 Abs. 2 StPO) und des Inhabers (vgl. § 106 Abs. 1 StPO) des Durchsuchungsobjektes bzw. seines Vertreters vorsieht. Die gegen diesen Beschluss gerichtete Beschwerde des Generalbundesanwalts verwarf der 3. Strafsenat mit Beschluss vom 31. Januar 2007 (StB 18/06). Auch nach seiner Auffassung besteht für die Anordnung einer strafprozessualen Online-Durchsuchung keine Rechtsgrundlage. Einer solchen bedarf aber dieser „schwerwiegende Eingriff in das Recht auf informationelle Selbstbestimmung. Nach seiner Ansicht dürfen auch einzelne Elemente von Eingriffsermächtigungen nicht kombiniert werden, um eine Grundlage für eine neue technisch mögliche Ermittlungsmaßnahme zu schaffen. Dies widerspräche dem Grundsatz des Ge-

setzesvorbehaltes für Eingriffe in Grundrechte (Art. 20 Abs. 3 GG) sowie dem Grundsatz der Normenklarheit und Tatbestandsbestimmtheit von strafprozessualen Eingriffsnormen.

2. Noch aktueller ist die Diskussion um die Online-Durchsuchung für nachrichtendienstliche Zwecke.

a. In Nordrhein-Westfalen wurde dafür Ende 2006 mit § 5 Abs. 2 Nr. 11 des dortigen Verfassungsschutzgesetzes eine besondere gesetzliche Grundlage geschaffen. Diese war Gegenstand einer Prüfung durch das Bundesverfassungsgericht.[72] In der Entscheidung vom 27. 02. 2008 hat das BVerfG die genannte Bestimmung des VSG NRW als mit dem Grundgesetz unvereinbar und nichtig erklärt, in der Begründung jedoch Kriterien für eine verfassungskonforme Regelung aufgezeigt, die aber die konkrete Regelung nicht erfüllt hat, sodass auch von der Möglichkeit einer vorübergehenden weiteren Anwendung nicht Gebrauch gemacht wurde.[73]

b. In einer parlamentarischen Anfragebeantwortung hat das deutsche Bundesministerium des Inneren am 22. März 2007[74] eingeräumt, dass es schon derzeit eine Rechtsgrundlage zur Durchführung von Online-Durchsuchungen als vorliegend erachtet, und zwar in § 8 Abs. 2 und § 9 Abs. 1 des Bundesverfassungsschutzgesetzes. Diese Bestimmungen lauten:

„§ 8 Befugnisse des Bundesamtes für Verfassungsschutz

(1) Das Bundesamt für Verfassungsschutz darf die zur Erfüllung seiner Aufgaben erforderlichen Informationen einschließlich personenbezogener Daten erheben, verarbeiten und nutzen, soweit nicht die anzuwendenden Bestimmungen des Bundesdatenschutzgesetzes oder besondere Regelungen in diesem Gesetz entgegenstehen. Ein Ersuchen des Bundesamtes für Verfassungsschutz um Übermittlung perso-

---

[72] Siehe auch http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg07-082.html.

[73] Wortlaut der Entscheidung unter <BVerfG, Entscheidung 27.02.08>.

[74] Wortlaut der Anfragebeantwortung unter
http://dip21.bundestag.de/dip21/btd/16/048/1604803.pdf.

nenbezogener Daten darf nur diejenigen personenbezogenen Daten enthalten, die für die Erteilung der Auskunft unerlässlich sind. Schutzwürdige Interessen des Betroffenen dürfen nur in unvermeidbarem Umfang beeinträchtigt werden.

(2) Das Bundesamt für Verfassungsschutz darf Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung, wie den Einsatz von Vertrauensleuten und Gewährspersonen, Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen anwenden. Diese sind in einer Dienstvorschrift zu benennen, die auch die Zuständigkeit für die Anordnung solcher Informationsbeschaffungen regelt. Die Dienstvorschrift bedarf der Zustimmung des Bundesministeriums des Innern, der das Parlamentarische Kontrollgremium unterrichtet.

(3) Polizeiliche Befugnisse oder Weisungsbefugnisse stehen dem Bundesamt für Verfassungsschutz nicht zu; es darf die Polizei auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen, zu denen es selbst nicht befugt ist.

(4) Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist der Erhebungszweck anzugeben. Der Betroffene ist auf die Freiwilligkeit seiner Angaben hinzuweisen.

(5) Von mehreren geeigneten Maßnahmen hat das Bundesamt für Verfassungsschutz diejenige zu wählen, die den Betroffenen voraussichtlich am wenigsten beeinträchtigt. Eine Maßnahme darf keinen Nachteil herbeiführen, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg steht.

§ 9 Besondere Formen der Datenerhebung

(1) Das Bundesamt für Verfassungsschutz darf Informationen, insbesondere personenbezogene Daten, mit den Mitteln gemäß § 8 Abs. 2 erheben, wenn Tatsachen die Annahme rechtfertigen, daß (1.) auf diese Weise Erkenntnisse über Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 oder die zur Erforschung solcher Erkenntnisse erforderlichen Quellen gewonnen werden können oder (2.) dies zum Schutz der Mitarbeiter, Einrichtungen, Gegenstände und Quellen des Bundesamtes für Verfassungsschutz gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten erforderlich ist. Die Erhebung nach Satz 1 ist unzulässig, wenn die Erforschung des Sachverhalts auf andere, den Betroffenen weniger beeinträchtigende Weise möglich ist; eine geringere Beeinträchtigung ist in der Regel anzunehmen, wenn die Information aus allge-

mein zugänglichen Quellen oder durch eine Auskunft nach § 18 Abs. 3 gewonnen werden kann. Die Anwendung eines Mittels gemäß § 8 Abs. 2 darf nicht erkennbar außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhaltes stehen. Die Maßnahme ist unverzüglich zu beenden, wenn ihr Zweck erreicht ist oder sich Anhaltspunkte dafür ergeben, daß er nicht oder nicht auf diese Weise erreicht werden kann.

[...]

(3) Bei Erhebungen nach Absatz 2 und solchen nach Absatz 1, die in ihrer Art und Schwere einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses gleichkommen, wozu insbesondere das Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes mit dem verdeckten Einsatz technischer Mittel gehören, ist

1. der Eingriff nach seiner Beendigung dem Betroffenen mitzuteilen, sobald eine Gefährdung des Zweckes des Eingriffs ausgeschlossen werden kann, und
2. das Parlamentarische Kontrollgremium zu unterrichten.

[...]“

3. Dennoch wird über die Schaffung neuer Rechtsgrundlagen (eher für sicherheitspolizeiliche Zwecke) debattiert, bisher jedoch ohne wirklich konkretes Ergebnis.[75]

Die Bayerische Landesregierung erklärte am 16. Mai 2007, einen Gesetzentwurf zu Online-Durchsuchungen zu Strafverfolgungzwecken auf den parlamentarischen Weg zu bringen. Der bayerische Gesetzentwurf soll als Änderungsantrag im Rahmen der Stellungnahme des Bundesrats zu einem entsprechenden Gesetzentwurf der Bundesregierung eingebracht werden.[76]

Sofern das Recht einzelner Bundesländer Staatsorganen verdeckte Online-Maßnahmen erlaubt, ist dies Nachrichtendiensten vorbehalten. Nordrhein-Westfalen nimmt dabei eine Vorreiterrolle ein. Dort ist dem Verfassungsschutz seit dem 30. Dezember 2006 *„heimliches Beobachten und sonstiges Aufklären des Internets, wie*

---

[75] Siehe etwa http://www.spiegel.de/netzwelt/web/0,1518,502542,00.html.

[76] Siehe Anlage <BMI.20080220, Information zur geplanten Änderung des Bayerischen Verfassungsschutzgesetzes> <Anfragebeantwortung-Bayern> <080212_ministerrat-Bayern> <verfschg_e[1]>.

insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel“ zur Informationsbeschaffung erlaubt (siehe vorhin).

In der Entscheidung vom 27.02.2008 hat das BVerfG[77] zur Frage der Zulässigkeit der Online-Durchsuchung folgende Leitsätze aufgestellt:

1. Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.
2. Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.
3. Die heimliche Infiltration eines informationstechnischen Systems ist grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Das Gesetz, das zu einem solchen Eingriff ermächtigt, muss Vorkehrungen enthalten, um den Kernbereich privater Lebensgestaltung zu schützen.
4. Soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff an Art. 10 Abs. 1 GG zu messen.
5. Verschafft der Staat sich Kenntnis von Inhalten der Internetkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin nur dann ein Eingriff in Art. 10 Abs. 1 GG, wenn die staatliche Stelle nicht durch Kommunikationsbeteiligte zur Kenntnisnahme autorisiert ist. Nimmt der Staat im Internet öffentlich zugängliche Kommunikationsinhalte wahr oder beteiligt er sich an öffentlich zugänglichen Kommunikationsvorgängen, greift er grundsätzlich nicht in Grundrechte ein.

[77] 1 BvR 370/07, 1 BvR 595/07. Wortlaut der Entscheidung siehe Anlage <BVerfG, Entscheidung 27.02.08>.

B. Luxemburg

Luxemburg führt eine allgemeine Diskussion über die Problematik der TÜ betreffend „Skype“.

C. Niederlande

In den ***Niederlanden*** regelt die Strafprozessordnung ausdrücklich die Durchsuchung von Computern („*onderzoek van gegevens in geautomatiseerde werken*“), und zwar in den Artikeln 125i bis 125n.

Das Überwachen von vertraulicher Kommunikation mittels technischer Hilfsmittel ist in Artikel 126l geregelt. Die Eingriffsschwelle liegt bei Verdacht einer Straftat mit einer Strafdrohung von mindestens vier Jahren. Ist dafür zunächst erforderlich, in eine Wohnung einzudringen, so kann dies nur auf der Grundlage eines Verdachts einer Straftat mit einer Strafdrohung von mindestens 8 Jahren erfolgen.

Die Überwachung der Telekommunikation – dieser Begriff wird technologieneutral verwendet – findet sich in den Artikeln 126m bis 126 nb. Auch hier besteht die Eingriffsschwelle bei Verdacht einer Straftat mit einer Strafdrohung von mindestens vier Jahren.

Spezielle Regeln zu einer Online-Überwachung finden sich in der niederländischen Strafprozessordnung nicht. Allerdings werden in den ***Niederlanden*** derzeit Überlegungen im Hinblick auf Schaffung einer gesetzlichen Grundlage für die Online-Durchsuchung angestellt; es existiert ein entsprechendes Memorandum des Justizministeriums.

D. Portugal

Portugal diskutiert Online-Durchsuchung im Hinblick auf die Ratifizierung der Cybercrime-Konvention.

In den übrigen der genannten Staaten findet keine nennenswerte politische Diskussion statt.

E. Belgien

Die Überwachung der (Tele)Kommunikation ist in der belgischen Strafprozessordnung „technologieneutral“ ausformuliert und erfasst somit grundsätzlich auch die Kommunikation zwischen Computersystemen.

Die belgische StPO kennt die herkömmlichen Bestimmungen betreffend Telekommunikationsüberwachung, wobei die Standortbestimmung in Art 88bis geregelt ist, Inhaltsüberwachung in den Art 90ter bis 90decies. Dabei werden die Art 90ter bis 90decies auch bei Kommunikation im Wege der Datenübertragung zwischen Datenverarbeitungssystemen angewendet.

Art 88ter StPO enthält jedoch als Eigenart des belgischen Rechts eine Bestimmung einer Art „kleinen Online-Durchsuchung“, die die Durchsuchung eines (abgeschlossenen) Netzwerkes von Datenverarbeitungssystemen im Hinblick auf statische (d.h. nicht kommunikationsbezogene) Daten gestattet:

Abs 1 dieser Bestimmung lautet: *„Wenn der Untersuchungsrichter die Durchsuchung eines EDV-Systems oder eines Teils desselben anordnet, kann diese Durchsuchung auch auf ein EDV-System oder einen Teil desselben ausgedehnt werden, welches sich an einem anderen Ort befindet als dort, wo die Durchsuchung durchgeführt wird. […]“*

Gem Abs 2 darf die Ausdehnung der Durchsuchung nur so weit gehen, als diejenigen Personen, welche zur Benützung des von der Durchsuchungsanordnung erfassten EDV-Systems oder eines Teiles desselben auch zum weiteren EDV-System oder zu einem Teil desselben Zugang haben.

Gem Abs 3 ist die für das EDV-System verantwortliche Person zu informieren, außer deren Identität oder Adresse können nicht mit vernünftigen Mitteln ermittelt werden. Wenn sich die Daten nicht in Belgien befinden, dürfen sie lediglich kopiert werden.

F. Bulgarien

Online-Durchsuchung ist zulässig.

Nach Art 319d Abs 2 StGB ist die Verwendung von „Spionage-Computer-Programmen“ bzw eines Trojanischen Pferdes materiell strafbar. Andererseits soll Online-Durchsuchungs-Software „zwanglos“ unter die Legaldefinition des Art 2 des *Gesetzes über Sonderermittlungsinstrumente* subsumiert und gem Art 3 leg cit für die Verhinderung und Aufklärung von schweren Verbrechen verwendet werden dürfen.

Gem Art 13 ff leg cit ist dazu ein begründeter Antrag an das entscheidungsbefugte Stadtgericht Sofia, an von diesem autorisierte Bezirksgerichte oder – bei militärischem Einsatz – an das örtlich zuständige Militärgericht zu stellen.

Bei Gefahr im Verzug kann gem Art 15 eine entsprechende Anordnung auch vom Innenminister gegeben werden, wobei innerhalb von 24 Stunden eine richterliche Genehmigung einzuholen ist.

G. Dänemark

Das Kopieren von der Öffentlichkeit unzugänglichen Daten eines Datenverarbeitungssystems ist zulässig.

Nach § 791b Abs 1 der Dänischen StPO ist mit Hilfe von Software-Programmen oder anderen Hilfsmitteln (Kopieren von Daten) zulässig, wenn

- (Z 1) aufgrund bestimmter Umstände anzunehmen ist, dass das Datenverarbeitungssystem durch einen Verdächtigen dazu benützt wird, eine Straftat nach Z 3 vorzubereiten oder auszuführen;
- (Z 2) die Maßnahme für die Ermittlung unbedingt erforderlich sowie
- (Z 3) die Ermittlung eine Straftat nach *[Aufzählung verschiedener Verbrechen]* oder eine schwere Straftat betrifft, die mit mindestens sechsjähriger Freiheitsstrafe bedroht ist.

Die Maßnahme darf nicht unverhältnismäßig zur Bedeutung der Straftat sein und bedarf einer richterlichen Anordnung (Abs 2 und 3 leg cit). Nachträgliche Information des Inhabers ist erforderlich.

H. Italien

Gem Art 266ff StPO ist nach gerichtlicher Bewilligung, bei Gefahr im Verzug nach Anordnung der Staatsanwaltschaft und nachträglicher gerichtlicher Bewilligung, das *„Abfangen von Konversation und Kommunikation“* erlaubt. Da die Mittel zur Erreichung dieses Zweckes nicht beschränkt werden, kann die Überwachung von E-Mail-Verkehr oder Internet-Telefonie auch durch externen Zugriff auf Computersysteme erfolgen, was – soweit ersichtlich - zu Ermittlungszwecken in sog. Mafia-Verfahren jüngst auch in der Praxis erfolgte.

Eine klare gesetzliche Grundlage für Online-Durchsuchung fehlt jedoch.

Nicht kommunikationsbezogene Online-Durchsuchung wäre demnach unzulässig.

I. Litauen

Online-Durchsuchung ist zulässig gem Art 154 StPO (Überwachung, Aufzeichnung und Speicherung von mittels elektronischen Kommunikationsnetzwerken übermittelten Daten.)

Die Ermittlungsmaßnahme ist nur im Hinblick auf bestimmte natürliche und juristische Personen zulässig.

Es gibt mit Online-Durchsuchung jedoch keine praktische Erfahrung.

J. Rumänien

Online-Durchsuchung ist grundsätzlich zulässig und bedarf

- einer gerichtlichen Anordnung;
- eines begründeten Antrages;
- während der Durchführung einer detaillierten Dokumentation, da ansonsten die Ermittlungsergebnisse nicht im Gerichtsverfahren als Beweis zugelassen werden.

K. Slowenien

Gem Art 150 Abs 1 Z 3 StPO wird bei Verdacht einer Reihe schwerer Verbrechen neben anderen Überwachungsmaßnahmen (TÜ, Brieföffnung) allgemein auch die *„Kontrolle der Computersysteme von Banken und anderen juristischen Personen, die Finanzdienstleistungen oder andere unternehmerische Aktivitäten ausführen“* gestattet. Die slowenische StPO nimmt jedoch keinen expliziten Bezug auf Online-Durchsuchung.

L. Spanien

Online-Durchsuchung ist zulässig – Voraussetzungen:

- schweres Verbrechen;
- Online-Durchsuchung ist das gelindeste Mittel, um zuverlässig das Verbrechen aufzuklären;
- richterliche Genehmigung, welche immer zeitlich befristet sein muss;
- die Ermittlungsergebnisse müssen innerhalb angemessener Zeit dem Ermittlungsrichter vorgelegt werden;
- die eingesetzte Software darf den betreffenden PC nicht beschädigen;
- nach Beendigung der Online-Durchsuchung hat die Kriminalpolizei die eingesetzte Software vom betreffenden PC wieder zu entfernen.

M. Tschechische Republik

Online-Durchsuchung wird als nicht grundsätzlich unzulässig angesehen, da die tschechische StPO eine sehr allgemeine Bestimmung betreffend „Überwachung des Telekommunikationsverkehrs“ hat.

N. Vereinigtes Königreich

Online-Durchsuchung wird nach dem Police Act 1997 Part III als zulässig erachtet. Demnach wird dieses Gesetz als rechtliche Grundlage für auch in der Praxis durchgeführte Online-Durchsuchung gesehen. Diese bedarf

- der Anordnung durch einen höheren Polizeibeamten (zumindest Chief Constable);
- Die Maßnahme muss notwendig und verhältnismäßig sein;
- Die Maßnahme muss zur Aufklärung eines mit bei erstmaliger Begehung mehr als dreijähriger Freiheitsstrafe bedrohten Verbrechens dienen.

Eine richterliche Genehmigung ist nicht erforderlich, die Bestimmung ist sehr allgemein gehalten: (Section 93, subsection 1:)

„[…] ist anwendbar, wenn der anordnende Beamte glaubt, dass es notwendig ist, die gewählte Maßnahme zu ergreifen, da sie wahrscheinlich von substanzieller Bedeutung für die Verhinderung oder Aufklärung einer schweren Straftat ist.“
vgl: http://www.opsi.gov.uk/acts/acts1997/ukpga_19970050_en_6

O. Schweden

In Schweden[78] wurde im Jahre 2007, befristet von 2008 bis 2011, ein „Gesetz für Maßnahmen um gewisse besonders gefährliche Verbrechen zu verhindern“ erlassen. Damit wurden bislang der Strafrechtspflege vorbehaltene Maßnahmen, wie Tele-Abhörung (Telefon, und Internetüberwachung), Tele-Überwachung (Verwanzen), Kameraüberwachung und das Öffnen von Post, auf die vorbeugende Bekämpfung von Straftaten ausgedehnt. Die Maßnahmen können vom Gericht auf Antrag des Staatsanwalts bewilligt werden, wenn unter Betrachtung der Umstände der besondere Verdacht vorliegt, eine Person werde bestimmte schwere, gegen die staatliche Integrität und die Allgemeinheit gerichtete Straftaten begehen, wie Sabotage, gefährliche Brandstiftung, bewaffneter Aufstand, Hochverrat, Spionage, Terrorismus uam. Dazu

[78] Recherche Funk/Stern.

ist erforderlich, dass die Maßnahmen von besonderer Bedeutung sind, um solche Straftaten zu verhindern, und dass die Gründe für den Eingriff in geschützte Rechtsgüter andere Interessen überwiegen.

Im gerichtlichen Verfahren zur Bewilligung solcher Maßnahmen wird ein öffentlicher Anwalt bestellt, der die Interessen der von den Maßnahmen betroffenen Person(en) schützen soll. Besonders geschützt wird das Anwaltsgeheimnis. Sollte eine Kommunikation mit einem Anwalt abgehört werden, ist die Maßnahme umgehend abzubrechen. Von einer Maßnahme betroffene Personen, inklusive jener, die zwar selbst nicht des Verbrechens verdächtigt waren, deren Anschluss aber überwacht wurde, müssen umgehend nach Abschluss der Maßnahmen davon in Kenntnis gesetzt werden.

Die Kontrolle der Maßnahmen obliegt einer unabhängigen Überwachungsbehörde (Commission on Security and Integrity Protection), deren Mitglieder von der Regierung auf Vorschlag der im Reichstag vertretenen Parteien bestellt werden, unter dem Vorsitz einer rechtskundigen Person. Auf Antrag einer Person hat diese Kommission zu prüfen, ob diese Person geheimen Überwachungsmaßnahmen ausgesetzt war, und wenn ja, ob dies im Einklang mit den rechtlichen Vorschriften geschah. Auch von Amts wegen soll die Kommission Inspektionen und Untersuchungen durchführen.

P. Polen, Malta, Frankreich, Belgien, Estland, Finnland, Griechenland, Lettland, Ungarn, Slowakei

Keine Informationen.

Q. Schweiz

Der schweizerische Bundesrat legte im Juli 2006 sowie im Juni 2007 in leicht veränderter Form einen Vernehmlassungsentwurf des Eidgenössischen Justiz- und Polizeidepartements eines Gesetzes vor, mit dem das *„Bundesgesetz vom 21. März*

1997 über Massnahmen zur Wahrung der inneren Sicherheit (Besondere Mittel der Informationsbeschaffung -SR 120)“ geändert werden soll *(Entwurf „BWIS-II“).* Danach soll das geheime Durchsuchen eines Datenbearbeitungssystems zulässig sein, wenn es für das Erkennen und Abwehren einer konkreten Gefahr für die innere oder äußere Sicherheit erforderlich ist, die ausgeht von:

a. Terrorismus;
b. verbotenem politischen oder militärischen Nachrichtendienst;
c. verbotenem Handel mit Waffen oder radioaktiven Materialien sowie verbotenem Technologietransfer *(Art 13a leg cit).*

Art. 18m (neu) leg cit soll demnach lauten:

„Geheimes Durchsuchen eines Datenverarbeitungssystems

Lassen konkrete und aktuelle Tatsachen oder Vorkommnisse vermuten, dass ein mutmaßlicher Gefährder oder eine mutmaßliche Gefährderin ein ihm oder ihr zur Verfügung stehendes und gegen Zugriff besonders gesichertes Datenverarbeitungssystem benutzt, kann dieses vom Bundesamt durchsucht werden. Die Durchsuchung kann ohne Wissen des mutmaßlichen Gefährders oder der mutmaßlichen Gefährderin erfolgen.“

Dabei soll zunächst erforderlich sein, dass eine konkrete Gefährdung der Sicherheit der Schweiz vorliegt und herkömmliche Ermittlungsmaßnahmen versagen sowie die besondere Ermittlungsmaßnahme angemessen ist und nur soweit in die Grundrechte Betroffener eingreift wie nötig *(Art 18b (neu) leg cit)*

Berufsgeheimnisse sollen besonderem Schutz unterliegen *(Art 18c (neu) leg cit).*

Vorgesehen ist ein Genehmigungs- und Anordnungsverfahren, wobei über den Einsatz nach begründetem und ausgeführtem Antrag des Bundesamtes das Bundesverwaltungsgericht entscheiden soll *(Art 18d und e (neu) leg cit).*

Bei Gefahr im Verzug soll die Anordnung durch das Bundesamt zulässig sein, das Bundesverwaltungsgericht hätte nachträglich die Genehmigung zu erteilen. Würde diese verweigert, wäre der Einsatz einzustellen und allfällig erlangte Daten wären zu löschen *(Art 18f (neu) leg cit).*

Vorgesehen sind weiters Einstellungs-, Vernichtungs- sowie Informationsverpflichtungen *(Art 18 g bis i neu).*

Volltext des Entwurfs: http://www.admin.ch/ch/d/ff/2007/5139.pdf

VII. Rechtsschutz und Rechtmäßigkeitsgarantien

Für Österreich besteht Einigkeit darüber, dass die heimliche Infiltration informationstechnischer Systeme auf Zwecke der Strafverfolgung beschränkt bleiben und nicht auf den präventiven Bereich erstreckt werden soll. Eine Entgrenzung gegenüber der polizeilichen Prävention ergibt sich ohnehin aus der Struktur jener Organisations- und Absichtsdelikte, zu deren Aufklärung und Verfolgung die Online-Durchsuchung zur Verfügung gestellt wird. Die unvermeidliche Relativierung von Strafverfolgung und Sicherheitspolizei soll im Ergebnis möglichst klein gehalten werden.

Die unter III.3. deponierten Vorschläge und Forderungen (1. bis 3.)[79] sind an dieser Stelle in Erinnerung zu bringen:

1. Die geheime Überwachung sollte von einem höheren Richtergremium angeordnet werden. Die Genehmigung durch den (bisweilen jungen und unerfahrenen) Ermittlungsrichter der ersten Instanz kann nicht genügen (wobei in diesem Zusammenhang auch auf die Abschaffung der Ratskammer als Genehmigungsinstanz durch das StPRefG hinzuweisen ist). Jedenfalls sollte die Beschwerde gegen den Grundrechtseingriff an den OGH ermöglicht werden.
2. Die Kontrolle durch den Rechtsschutzbeauftragten sollte ausgebaut und verbessert werden. Dieser sollte im aktiven Berufsleben stehen und auch nach Maßgabe seiner bisherigen Berufslaufbahn unabhängig sein, vorzugsweise ein Rechtsanwalt oder ein Universitätslehrer im aktiven Dienst. Er sollte – selbstverständlich bei strikter Pflicht zur Geheimhaltung – den gesetzlichen Auftrag erhalten, vor allem die Rechte der Betroffenen zu wahren, die von den geheimen Maßnahmen nichts wissen und darum ihre Rechte nicht geltend machen können.

   Hegt man Bedenken, dass ein solcher Rechtsschutzbeauftragter zu viel Macht haben könnte, so ist darauf hinzuweisen, dass er keine Entscheidungen treffen soll, sondern – gleichsam als ein Abwesenheitskurator im Auftrag der Öffentlichkeit – die Kontradiktorietät im geheimen Ermittlungsverfahren wahrt (*audiatur et altera pars*).

[79] Siehe Anlage, Seite 72 <Fuchs, Online Überwachung 2-3 080214>; siehe vorhin FN 32.

3. Die Rechtsentscheidungen zu den geheimen Überwachungen (Beschlüsse, Anordnungen, Rechtsmittelentscheidungen) sind nach Beendigung der Maßnahme, jedenfalls aber nach Ablauf eines bestimmten fixen Zeitraumes ab ihrer Erlassung, anonymisiert zu veröffentlichen. Sie wären damit insbesondere der wissenschaftlichen Öffentlichkeit zugänglich, die sie diskutieren und evaluieren könnte.

Ebenfalls in Erinnerung zu bringen sind die Anforderungen an die technische Sicherung der Integrität der Daten, der Authentizität der Kommunikationspartner und der Verfügbarkeit der Kommunikationswege.[80] Darüber hinaus sind jene Rechtsschutzanforderungen zu beachten, die bereits im MRV enthalten sind, im besonderen auch die Rechtsmittellegitimation der DSK.

VIII. Forensischer Beweiswert[81]

Der Beweiswert von Informationen, die aus Online-Durchsuchungen gewonnen wurden, ist wesentlich von der Einhaltung und der Qualität der für solche Eingriffe maßgebenden Rechtsgrundlagen abhängig. Zu beachten ist, dass Systemveränderungen und Nebenwirkungen nicht mit letzter Sicherheit ausgeschlossen werden können (siehe II.B.).

IX. Sozio-politische Aspekte[82]

Das BVerfG hat ein „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ kreiert. In dieser richterrechtlichen Rechtsschöpfung kommt ein hohes Maß an Aufmerksamkeit für den gesellschaftspolitischen Stellenwert jener Entscheidungen zum Ausdruck, die mit der Einführung

[80] Siehe vorhin bei den FN 19, 20, 21.

[81] Formulierung von Funk auf Grund der Beratungen in der Arbeitsgruppe

[82] Formulierung von Funk auf Grund der Beratungen in der Arbeitsgruppe

einer Online-Durchsuchung zu tun haben. Die Sicherung der Vertraulichkeit und Integrität informationstechnischer Systeme ist ein hochrangiges gesellschaftspolitisches Anliegen. Eingriffsermächtigungen für Zwecke der Strafverfolgung und/oder der sicherheitspolizeilichen Prävention sind grundsätzlich geeignet, Vertrauen in die Vertraulichkeit und Integrität informationstechnischer Systeme zu beeinträchtigen – selbst wenn dies objektiv nicht gerechtfertigt wäre.

Andererseits gibt es fortschreitende Bestrebungen zur Förderung der Nutzung der Internet-Kommunikation in sämtlichen privaten und öffentlichen Lebensbereichen. Der Erfolg dieser Bestrebungen könnte in Frage gestellt, ja geradezu konterkariert werden, wenn mit staatlich verfügter Infiltration informationstechnischer System zu rechnen ist und es nicht gelingt, die Glaubwürdigkeit in Bezug auf Vertraulichkeit und Integrität des Internet zu gewährleisten.

X. Zusammenfassung der Ergebnisse

1. Die Bezeichnung „Online-Durchsuchung“ wird als Synonym für verschiedene Begriffe verwendet, und zwar
   - (im engsten Sinne) als „Suche nach verfahrensrelevanten Inhalten auf Datenträgern, die sich nicht im direkten Zugriff der Strafverfolgungsbehörden befinden, sondern nur über Kommunikationsnetze erreichbar sind“ (Anfragbeantwortung im dt Bundestag), weiters
   - als „heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können“ (BVerfG),
   - oder als „Installation von ‚Remote Forensic Software (RFS)“, sei es in Form unmittelbarer Installation durch Behördenorgane im physischen Zugriff auf das Kommunikationsgerät oder in Form einer remote-Installation, das ist die Einbringung durch Bereitstellen der zur Umsetzung der Maßnahme erforderlichen RFS-Komponenten mit einem aktivem, wenn auch unbewusstem Beitrag des Betroffenen zum Installationsvorgang.
2. Des Weiteren ist zwischen

– Online-Durchsuchung als digitaler Zugriff auf den Rechner einer Zielperson zum Zwecke des Auslesens der auf dem Rechner gespeicherten Daten;
– Online-Überwachung als fortlaufende Überwachung der konkreten Nutzung eines Rechners;
– Überwachung des Datenaustausches über das Internet (z.B.Internet-Telefonie, E-Mail-Verkehr, Internet-Chats, Online-Spiele, Abfrage von Datenbanken, Surfen im Internet) als besondere Form der Telekommunikation

zu unterscheiden.

Die Arbeitsgruppe verwendet den Begriff „Online-Durchsuchung“ mit dem Verständnis, dass damit alle Formen der heimlichen Durchsuchung oder Überwachung informationstechnischer Systeme erfasst sind.

3. „Remote-Forensic Software“ ist ein mit speziellen Funktionen für einen bestimmten Anlassfall ausgestattetes Computerprogramm, welches auf ein Kommunikationssystem zum Zwecke der Online-Durchsuchung eingebracht wird. „Remote“ deshalb, da die Software bei der Aktivierung oder Deaktivierung ferngesteuert werden kann.

4. Einbringung“ von „Remote-Forensic Software“ kann auf zwei Arten erfolgen:
   a) Durch Fernzugriff, das ist die Einbringung von „Remote-Forensic Software“ aus der Ferne, z.B. durch elektronische Übermittlung an das Zielsystem.
   b) Durch physischen Zugriff, das ist die Einbringung von „Remote-Forensic Software“ durch physischen Zutritt am Standort des Rechners.

5. „Deinstallation“ ist jene technische Maßnahme, mit der nach Ablauf des angeordneten Durchsuchungszeitraumes das ausgebrachte technische Hilfsmittel vom Rechner der Zielperson entfernt wird. Vollständige Deinstallation ist nicht mit Sicherheit zu erreichen. Die Deinstallation kann automatisch durch Zeitablauf oder manuell durch neuerlichen physischen Zugriff oder durch Fernzugriff erfolgen.

6. In der Durchführung ergeben sich folgende Varianten einer Online-Durchsuchung:
   – Physische Untersuchung des Gerätes im Rahmen einer offenen oder heimlichen Durchsuchung, Beschlagnahme technischer Geräte
   – Einsatz von Remote-Forensic Software
   – Nutzung elektromagnetischer Emissionen
   – Einbau eines Hardware Moduls im Zielrechner

7. Nach geltendem Strafprozessrecht passen zwar die vorhandenen Ermittlungsregelungen auf einen Teil der Computeranwendungen (E-Mail, VoIP), nicht jedoch die übrigen, jedenfalls in keinem Fall unter „Kommunikation“ bzw. „Nachrichtenübermittlung“ subsumierbaren Anwendungen (Textverarbeitung, Tabellen, Datenbanken etc.). Nicht nachrichten- bzw. kommunikationsbezogene Datenverarbeitung wäre keinesfalls verfassungskonform unter die Ermächtigung des § 135 StPO subsumierbar, weil es sich um keine „Äußerungsüberwachung im weiteren Sinn“ handelt.

8. Eine akustische Überwachung darf sich wiederum nur auf Äußerungen einer Person beziehen. Schon begrifflich wäre es daher ausgeschlossen, darunter auch die auf einem Speichermedium abgelegten Informationen zu subsumieren. Allerdings wäre es wohl zulässig, eine optische Überwachung so einzurichten, dass damit das Verhalten einer Person in Bezug auf deren Aktivitäten vor einem Bildschirm erfasst und überwacht werden kann (hochauflösbare Kamera, die eine Auswertung der Eingaben auf einer Tastatur ermöglicht).

9. Einen Graubereich stellt die offenbar in einem Fall praktizierte Anwendung einer Software dar, durch die der Bildschirminhalt („screenshots“) in Abständen von ungefähr einer Minute und die keylog-Daten übertragen und überwacht wurden. Selbst wenn man die Installation einer solchen Software durch § 135 Abs. 2 Z 3 iVm § 136 Abs. 2 StPO als gedeckt ansieht, so müsste doch deren Eingrenzung auf echte Kommunikationsvorgänge gefordert werden, weil die reine Überwachung

der schriftlichen oder bildlichen Darstellung von Gedankenvorgängen vom Begriff der Überwachung von Nachrichten nicht erfasst wird.

10. Im Sicherheitspolizeirecht findet sich keine Bestimmung, die auch nur annähernd eine taugliche Rechtsgrundlage für die Online-Durchsuchung abgäbe. Gleiches gilt für das Militärbefugnisrecht sowie für das Telekommunikationsrecht. Letzteres verweist diesbzgl auf die in der Strafprozessordnung vorgesehenen Möglichkeiten.

11. Vom Urheberrecht her gesehen dürfte es wegen der Freiheit von Werknutzungen im Interesse der Rechtspflege und der Verwaltung keine besonderen Probleme geben. Aus der Sicht des Signaturrechts ist durch den Einsatz von Remote-Forensic Software eine Kompromittierung“ im Sinne des § 2 Z 14 SigG nicht ausgeschlossen.

12. Vergleiche mit anderen europäischen Staaten zeigen ein uneinheitliches Spektrum. Juristische am weitesten strukturiert dürfte die Rechtslage in der BRD sein, wo das BVerfG in einem leading case klare Bedingungen und enge Grenzen für "die heimliche Infiltration eines informationstechnischen Systems, mittels de-rer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können" gesetzt hat.

13. Aus verfassungsrechtlicher Sicht sind eine Reihe von Grundrechten betroffen, die der Einführung einer Online-Durchsuchung Schranken setzen und staatliche Gewährleistungspflichten mobilisieren. Es bedarf jedenfalls spezieller gesetzlicher Ermächtigungen, die de lege lata im Wesentlichen fehlen. Vorhandene Eingriffsermächtigungen, speziell solche betreffend Hausdurchsuchungen, Beschlagnahme von Beweisgegenständen, Öffnung von Briefen, Überwachung von Nachrichten und die optische und akustische Überwachung von Personen, bieten keine tauglichen gesetzlichen Grundlagen für Online-Durchsuchungen. Solche Regelungen müssen den Grundsätzen der Verhältnismäßigkeit entsprechen und dürfen nicht gegen Wesensgehaltgarantien verstoßen. Wenngleich die Argumentation des

BVerfG mit der richterrechtlichen Entwicklung eines Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dogmatisch nicht Eins zu Eins auf die österreichische Grundrechtslage übertragbar ist, ergeben sich aus dieser Rechtsprechung beachtenswerte Perspektiven in Richtung Limitation solcher Eingriffe und Erforderlichkeit kompensatorischer Mechanismen, die einen effektiven Rechtsschutz, Kontrolle und Ersatz für Schäden verlangen. Ob die Eignung solcher Eingriffe im Sinne der Verhältnismäßigkeit der Zielerreichung gewährleistet ist, hängt wesentlich von den einschlägigen technologischen Gegebenheiten und Möglichkeiten ab, deren Gefahrlosigkeit und Treffsicherheit sowohl informationstechnisch als auch rechtlich zu gewährleisten sind. Vergleiche mit anderen europäischen Staaten zeigen ein uneinheitliches Spektrum. Juristisch am weitesten strukturiert dürfte die Rechtslage in der BRD sein, wo das BVerfG in einem leading case klare Bedingungen und enge Grenzen für „die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können“ gesetzt hat. Sollte die Entscheidung für gesetzliche Maßnahmen fallen, mit denen Online-Durchsuchungen erlaubt werden, so müssten flankierende Instrumente des Rechtsschutzes und der Kontrolle weiter entwickelt und zum Teil neue geschaffen werden,. dazu zählen insbesondere Kontrollen durch ein höheres Richtergremium, Verbesserungen beim kommissarischen Schutz durch Rechtsschutzbeauftragte sowie eine wissenschaftliche Kontrolle durch nachträgliche Veröffentlichung der maßgebenden Rechtsentscheidungen in anonymisierter Form. In diesem Zusammenhang ist auch die Bedeutung technischer Sicherheiten bei der Durchführung in Erinnerung zu bringen. Zu bedenken sind auch Auswirkungen auf die Authentizität und den Beweiswert von Daten, die im Wege von Online-Durchsuchungen gewonnen wurden. Die Authentizität und Integrität der Daten müssen sowohl in technischer als auch rechtlicher Hinsicht gesichert werden.

14. Ebenfalls zu berücksichtigen sind Auswirkungen auf das Vertrauen der Gesellschaft in die Sicherheit des Internet und mögliche Rückschläge auf die Nutzung der Möglichkeiten des Internet in allen Lebensbereichen. Andererseits kann ein

Ausbau des Ermittlungsinstrumentariums auch dem Sicherheitsbedürfnis der Bevölkerung entsprechen.