



FAKULTÄT FÜR **INFORMATIK**

Datenschutz gegen Verbrechensbekämpfung – am Beispiel der Novelle zum Sicherheitspolizeigesetz

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Magister

im Rahmen des Studiums

Wirtschaftsinformatik

eingereicht von

Thomas Rauchwerger

Matrikelnummer 0101209

an der

Fakultät für Informatik der Technischen Universität Wien

Betreuung:

Betreuer: Univ.Prof. Dipl.-Ing. Dr.techn. Hannes Werthner

Wien, 02.04.2010

(Unterschrift Verfasser/in)

(Unterschrift Betreuer/in)

Thomas Rauchwerger, Neulinggasse 39/4/6 1030 Wien

„Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.“

Abstract

Am 6. Dezember 2007 wurde im Nationalrat die Novelle zum Sicherheitspolizeigesetz beschlossen. Durch diese Novelle sind die Sicherheitsbehörden berechtigt, von Providern von öffentlichen Telekommunikationsdiensten Auskunft über IP-Adressen zu einer bestimmten Nachricht und den genauen Zeitpunkt der Übermittlung zu verlangen. Dies darf nur geschehen, wenn Tatsachen die Annahmen der konkreten Gefahrensituation rechtfertigen und sie diese Daten als Grundlage für die Erfüllung ihrer Aufgaben nach dem Sicherheitspolizeigesetz benötigen.

Durch die Novelle des Sicherheitspolizeigesetzes, die mit 01.01.2008 in Kraft getreten ist, ist die Kontrolle durch die Instanz der Justiz aufgehoben worden. Ohne richterlichen Befehl können Standortabfragen des Handy-Benutzers durchgeführt werden. Weiters können mit Hilfe von IMSI Catcher Gesprächsdaten des überwachten Handys aufgezeichnet werden. Es ist zwar weiterhin strafbar, dass eine Gesprächsaufzeichnung ohne richterlichen Befehl abgehört wird, aber es ist nicht mehr kontrollierbar. Somit ist die Tür für Datenmissbrauch sehr weit geöffnet. Die einzige Kontrollinstanz ist seit dieser Novelle nur mehr der Rechtsschutzbeauftragte des Bundesministeriums für Inneres. Die dritte Problematik der Novelle zum Sicherheitspolizeigesetz besteht darin, dass statische als auch dynamische IP-Adressen bei einer konkreten Gefahrensituation beim Provider ohne richterlichen Beschluss verlangt werden können.

Neben der Vorstellung der Änderungen durch diese Novelle, inkludiert diese Diplomarbeit eine generelle Übersicht der Gesetze in Österreich, in denen der Datenschutz eine Rolle spielt. Weiters wird ein Ausblick gegeben, in denen Richtlinien der EU präsentiert wird und deren Rolle für die nationalen Staaten spielt. Hierbei wird genauer die Richtlinie 2006/24/EG (Vorratsdatenspeicherung) beleuchtet, die in den letzten Monaten immer mehr in die Schlagzeilen geraten ist. Zusätzlich beinhaltet diese Arbeit einen Überblick über den Begriff der Online-Durchsuchung. Hierbei wird einerseits untersucht die Charakteristika einer Online-Durchsuchung und andererseits eine Zusammenfassung wie Sicherheitsbehörden sich zum Computersysteme Zugang verschaffen sowie dann die Daten auswerten.

Generell wird weiters in dieser Arbeit untersucht welche Sicherheitsbehörden in Österreich Überwachungsmethoden durchführen sowie eine Klassifizierung der Gleichen. In einem weiteren Kapitel werden noch die dahinter steckenden Technologien, wie z.B. IMSI-Catcher usw., beleuchtet, mit denen die Sicherheitsbehörden die Überwachungen durchführen. Hierbei werden auch Statistiken bezüglich Überwachungsmaßnahmen vorgestellt sowie eine Darstellung, ob durch die Novelle des SPG diese zugenommen haben. Als weiteren Aspekt dieser Arbeit wird auch ein Ausblick in anderen Ländern bezüglich Überwachungsmaßnahmen bzw. -methoden gewährt. Abschließend folgt ein Resümee der Arbeit, indem die Ergebnisse nochmals zusammenfassend werden sowie eine persönliche Stellungnahme zu diesem umfassenden Thema.

Grundsätzlich ist über die methodische Vorgehensweise zu sagen, dass der Hauptteil mittels Internet- bzw. Literaturrecherche vollzogen wird. Für einzelne Kapitel ist auch eine Zusammenarbeit mit Datenschutzexperten der grünen Parlamentspartei vollzogen worden.

On the 6 of december 2007 the Austrian governance determined a novelette to the "Sicherheitspolizeigesetz". According to this novelette the security agencies are allowed to demand IP-address to a certain message and to an exact point of time from public providers. This can only be executed when facts of danger episode are legitimated. Furthermore the provided data, like IP-addresses, and so on, must be the fundament of the completion of the purposes of "Sicherheitspolizeigesetz".

Because of the introduction of the "Sicherheitspolizeigesetz" novelette on 01.01.2008 the control-instance of the justice, especially the judges, was removed. Now it is possible to arrange location requests of mobile user without resolution of a judge. It is not furthermore prohibited that content of conversation will be recorded with IMSI-Catcher but this can not be controlled so easy anymore. Therefore data-misusage can not be strictly avoided. A further important issue of this novelette is that security agencies can demand static as well as dynamic IP-addresses from providers.

Beside of the introduction of the new novelette of the "Sicherheitspolizeigesetz", this paper includes an overview of the data protection laws in Austria. Furthermore this paper contains a general summary of the data protection guidelines of the European Union. Especially I want to elaborate on the guideline 2006/24/EG (data retention), which was very present in news in the nearly past. Additionally the paper will include the characteristics of the "Computer-surveillance". This contains on one hand how the security agencies will access to computer systems and on the other hand how the data will be evaluated. In another chapter there will be an overview of security agencies in Austria and a classification of supervisory measures generally.

Furthermore I will give in another chapter a summary of the supervisory technologies, which are now used from security agencies f.e.: IMSI-Catcher. Beside of this technologies there will be presented supervisory statistics. Here it should be checked if the supervisory measures or –methods have been increased or not. As a further aspect of this paper I will also present supervisory measures of different countries than Austria. At the end of the paper I will finish it with a résumé with personal statement to this comprehensive topic.

Generally the methodical approach of this paper is that the major components will be accomplished with literature and internet research. Furthermore cooperation for some chapters is planned with data protection experts of the Austrian green party.

Inhaltsverzeichnis

1	Einleitung	8
2	Datenschutz	10
2.1	Begriff	11
2.2	Definition	11
2.3	Rechtliche Grundlagen	12
2.3.1	Österreichische Gesetze	13
2.3.1.1	Datenschutzgesetz 2000 (DSG 2000)	13
2.3.1.2	Telekommunikationsgesetz 2003 (TKG 2003)	14
2.3.1.3	Sicherheitspolizeigesetz 2008 (SPG 2008)	16
2.3.2	Europäische Gesetze	17
2.3.2.1	Richtlinie 95/46/EG (Datenschutzrichtlinie)	17
2.3.2.2	Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation)	18
2.3.2.3	Richtlinie 2006/24/EG (Vorratsdatenspeicherung)	18
2.4	Datenschutzbehörden und Kontrollorgane in Österreich	21
2.4.1	Datenschutzkommission	21
2.4.1.1	Arbeit der Datenschutzkommission	21
2.4.2	Datenschutzrat	24
2.4.3	Rechtsschutzbeauftragter im Bundesministerium für Inneres	24
2.5	Datenschutzbehörden und Kontrollorgane in der EU	25
2.5.1	Europäischer Datenschutzbeauftragter	25
2.5.2	Art. 29 Datenschutzgruppe	25
3	Staatliche Überwachung in Österreich	27
3.1	Sicherheitsbehörden	27
3.2	Unterscheidung von Überwachungsmaßnahmen (Klassifikation)	28
3.2.1	Arten der Überwachungsmaßnahmen	28
3.2.2	Zielsetzung der Überwachungsmaßnahmen	29
3.2.3	Überwachung innerhalb des Wohnraumes vs außerhalb des Wohnraumes	29
3.2.4	Offizielle vs. inoffizielle Überwachung	29
3.3	Arten von Überwachungsmaßnahmen	29
3.3.1	Akustische Überwachung	30
3.3.1.1	Exkurs Lauschangriff in Österreich	32
3.3.2	Optische Überwachung	33
3.3.3	Überwachung durch Datenerfassung und -auswertung	33
4	SPG Novelle 2008	35
4.1	Einleitung und Gesetzestexte	35
4.2	Befugnisse des §53 Abs. 3a Z1 und § 53 Satz 2 SPG	38
4.3	Befugnis des §53 Abs. 3a Z2 SPG	39
4.3.1	Allgemein	39
4.3.2	Begriff „Nachricht“	40
4.3.3	Begriff einer „bestimmten“ Nachricht	42
4.3.4	Begriff „übermittelnde Daten“	42
4.3.5	Eingriff in das Fernmeldegeheimnis?	44
4.3.6	Eingriff in das Grundrecht auf Achtung der Privatsphäre?	46
4.3.7	Eingriff in das Grundrecht auf Datenschutz?	47
4.3.8	Eingriff in den Gleichheitssatz (Kostenersatz)?	48

4.3.9	Zusammenfassung	49
4.4	Befugnis des §53 Abs. 3a Z3 SPG	50
4.4.1	Kreis der auskunftspflichtigen Betreiber	50
4.4.2	Statische vs. dynamische IP-Adressen	51
4.5	Befugnisse des §53 Abs. 3b SPG	52
4.5.1	Voraussetzungen	52
4.5.1.1	Begriff der Gefahrensituation	52
4.5.1.2	Begriff der Hilfeleistung bzw. Abwehr dieser Gefahr	53
4.5.2	Auskunft über Standortdaten	53
4.5.3	Technologien zur Lokalisierung	54
4.6	Dokumentation des Auskunftsbegehrens	55
4.6.1	Allgemein	55
4.6.2	Standortdaten aus der Vergangenheit?	55
4.6.3	Qualität des Formulars	56
4.6.4	Rolle des Rechtsschutzbeauftragten im Bezug auf das SPG	57
4.7	Anzahl der Anfragen nach SPG Abs. 3a und 3b	58
5	Stand der Entwicklung von technischen Überwachungsmaßnahmen im Bereich Mobilfunk	60
5.1	IMSI-Catcher	60
5.1.1	Einleitung & Hintergrund	60
5.1.2	Exkurs Mobiltelefonie	61
5.1.2.1	GSM	61
5.1.2.1.1	Einleitung	61
5.1.2.1.2	Architektur	63
5.1.2.1.3	Adressierung von Geräten bzw. Benutzern	65
5.1.2.2	UMTS	67
5.1.2.2.1	Einleitung	67
5.1.2.2.2	Architektur	69
5.1.3	Funktionsumfang	71
5.1.3.1	Ermittlung der IMSI bzw. IMEI	72
5.1.3.2	Lokalisieren des mobilen Endgeräts	73
5.1.3.3	Abhören der Gespräche	74
5.1.4	Modelle bzw. IMSI-Catcher in Österreich im Einsatz?	75
5.1.5	Störungen durch den Einsatz von IMSI-Catchern?	76
5.1.6	Sicherheitsmaßnahmen	76
5.1.7	Rechtliche Beurteilung des Einsatz von IMSI-Catchern	78
5.2	Stille SMS	78
5.2.1	Funktionsweise	78
5.2.2	Sicherheitsmaßnahmen	79
5.2.3	Zusammenfassung	80
5.3	Spionage Software anhand eines Beispiels Flexispy	81
5.3.1	Funktionsweise	81
5.3.2	Sicherheitsmaßnahmen	82
5.3.3	Zusammenfassung	83
6	Exkurs: Online-Durchsuchung	84
6.1	Allgemein bzw. Begriffserklärung	84
6.2	Technische Gesichtspunkte der Online-Durchsuchung	85
6.2.1	Arten der Zugangsverschaffung zu einem Computersystem	85

6.2.1.1	Physische Angriffe	86
6.2.1.2	Social Engineering	86
6.2.1.3	Ausnützung technischer Sicherheitslücken	87
6.2.1.4	Backdoors.....	88
6.2.2	Arten der Ausnützung des Zugangs.....	89
6.2.3	Technische Sicherheitsmaßnahmen.....	89
6.2.4	Zusammenfassung bzw. Ausblick	92
7	Überwachungsmaßnahmen in anderen Ländern.....	94
7.1	Vereinigten Staaten von Amerika	94
7.1.1	Einleitung.....	94
7.1.2	Rechtliche Grundlagen	94
7.1.2.1	Der vierte Verfassungszusatz (Fourth Amendment)	95
7.1.3	Ausforschung von menschlicher Kommunikation.....	97
7.1.3.1	Abhören von Telefongesprächen	98
7.1.3.2	Pen Register und Trap and Trace.....	98
7.1.3.3	Lokalisierung von Mobiltelefonnutzern	99
7.1.4	Neue Formen der Überwachung	100
7.2	Deutschland.....	101
7.2.1	Rechtliche Grundlagen	101
7.2.2	Ausblick „Online-Durchsuchung“	104
7.3	Zusammenfassung.....	104
8	Resümee	106
	Literaturverzeichnis	108
	Abbildungsverzeichnis	117
	Tabellenverzeichnis	117
	Abkürzungsverzeichnis	118
	Anhang A: Auszug aus der EBRV zum SPG 2008	120
	Anhang B: Auskunftsverlangen gem. §53 Abs. 3a und 3b SPG Formular ..	121
	Anhang C: Telekommunikationsgesetz §113a (Deutschland): Speicherungspflichtige Daten.....	123

1 Einleitung

Diese Diplomarbeit behandelt Überwachungsmaßnahmen sowie -methoden des Staates, für welche die Informations- und Kommunikationstechnik (IKT) eine immer größere Rolle spielt. Durch z.B. die schnelle Entwicklung und Verbreitung des Internets & von Mobiltelefonen kann die Gesetzgebung dem technischen Fortschritt nur schwer folgen, und meistens erst auf bereits vorhandene Innovationen reagieren. Andererseits nützt der Staat den technischen Fortschritt, indem er Technologien, wie Wanzen, Richtmikrofone, Videokameras, Peilsender, Spionagesoftware und Ortungsgeräte einsetzt. Das offizielle Ziel der staatlichen Überwachungsmaßnahmen ist die Gewährleistung der Sicherheit der Gesellschaft, sowohl der Kriminalprävention als auch der Aufklärung der Straftaten. Zwar werden Spionage- und Überwachungsmaßnahmen schon seit langer Zeit von Staaten durchgeführt, aber in den letzten Jahren wird vermehrt das Argument zur Prävention von Terroraktivitäten angeführt. Deswegen sind die staatlichen Überwachungsaktivitäten weltweit stark angestiegen.

Somit hat sich das Spannungsfeld zwischen Freiheit und Sicherheit in den letzten Jahren stark verschärft. Durch Erlassen von Gesetzen, versucht der Staat die kollektive Sicherheit der Bürger zu gewährleisten, aber schränkt zeitgleich auch in manchen Fällen die individuelle Freiheit bzw. Privatsphäre jedes Individuum ein. *Diese Balance zwischen Freiheit und Sicherheit hat sich – insbesondere aufgrund internationaler Terrorismusbekämpfung – besonders in den letzten Jahren zu Gunsten der Sicherheit und zu Lasten der Freiheit entwickelt.* [KEC] Aufgrund dieser Entwicklung in den letzten Jahren, beleuchtet diese Arbeit jene drei – in der jüngsten Vergangenheit kontrovers diskutierten Überwachungsmaßnahmen: die SPG Novelle 2008, die Vorratsdatenspeicherung sowie die „Online-Durchsuchung“.

Durch die SPG Novelle 2008 wurde den österreichischen Sicherheitsbehörden neue umfangreiche Befugnisse im Zusammenhang mit der Überwachung des Internets als auch in der Ortung von Mobilfunkteilnehmer gewährt. Die Ausübung dieser Befugnisse können ohne richterliche Kontrolle vollzogen werden.

Das Konzept der Vorratsdatenspeicherung hat als Ziel, dass mittels Internet Access Provider flächendeckend und verdachtsunabhängig, Verkehrs- und Standortdaten für einen gewissen Zeitraum gespeichert werden müssen. Derzeit gibt es eine EU-Richtlinie bezüglich der Vorratsdatenspeicherung, die aber von Österreich noch nicht umgesetzt wurde.

Den dritten Schwerpunkt dieser Arbeit bildet die so genannte „Online-Durchsuchung“. Dieses Ermittlungsinstrument würde es den Sicherheitsbehörden erlauben, Computersysteme durch geheimes „Hacking“ zu überwachen. Diese Variante der Überwachungsmaßnahme wird derzeit sehr

heftig diskutiert, ist aber wie die Vorratsdatenspeicherung in Österreich noch nicht zugelassen.

Neben den 3 Hauptthemen dieser Arbeit wird der Begriff des Datenschutzes sowie die rechtlichen Grundlagen beleuchtet und die technischen staatlichen Überwachungstechnologien vorgestellt. Weiters wird ein Ausblick gegeben, wie in einem anderen Land Überwachungstechnologien bzw. -methoden eingesetzt werden. Hierfür wurden die Vereinigten Staaten von Amerika und Deutschland als Beispiele herangezogen.

Die Struktur dieser Arbeit ist wie folgt aufgebaut:

Nach dieser kurzen Einleitung zu diesem Thema folgt ein Kapitel über Datenschutz. Dies inkludiert sowohl die Begriffsbeschreibung, Gesetze als auch Institutionen in punkto Datenschutz. Neben den österreichischen Gesetzen wird auch auf die Datenschutzrichtlinie der EU näher eingegangen. Besonders wird hier die Richtlinie zur Vorratsdatenspeicherung beleuchtet. Im nächsten Kapitel wird die staatliche Überwachung in Österreich beschrieben, sowie eine generelle Klassifikation von Überwachungsmaßnahmen. Wie auch schon im Titel der Arbeit vermerkt, folgt im darauf folgenden Kapitel eine detaillierte Darstellung der Novelle zum Sicherheitspolizeigesetz. Neben dieser Darstellung des neuen Gesetzestexts wird im nächsten Kapitel der Stand der Technologien für die Umsetzung der staatlichen Überwachungsmaßnahmen präsentiert. In den beiden nächsten Kapiteln folgt dann ein Exkurs in die Online-Durchsuchung als auch eine Übersicht in Überwachungsmaßnahmen in den USA und Deutschland. Als Abschluss dieser Arbeit wird ein Resümee über die staatlichen Überwachungsmaßnahmen sowie deren Gesetze folgen.

Abschließend möchte ich darauf hinweisen, dass diese Arbeit den letzten state-of-the-art der verschiedenen Themen zum Zeitpunkt der Erstellung dieser Arbeit darstellt und unter diesem Gesichtspunkt gesehen werden muss. Durch die Schnelllebigkeit der Technologien und dadurch der resultierenden Gesetze muss nochmals festgehalten werden, dass diese Arbeit bzw. Problematik als schnell veraltet gehalten werden kann.

2 Datenschutz

Im diesem Kapitel möchte ich den Begriff und die Bedeutung des „Datenschutzes“ erklären. Weiters werden die rechtlichen Grundlagen bzw. Kontrollorgane des Datenschutzes in Österreich und in der Europäischen Union beleuchtet. Unter Datenschutz wird verstanden, dass personenbezogene Daten vor Missbrauch geschützt werden. Der Zweck des Datenschutzes ist es, jedem Menschen selbst die Entscheidung zu geben, wem, wann und welche Daten weitergegeben werden sollen. In Österreich ist der Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten verfassungsrechtlich als Grundrecht verankert.

Nun stellt sich die Frage, was unter „Daten“ überhaupt verstanden wird?

Unter „Daten“ wird nicht nur der Name, Geburtsdatum und Wohnadresse verstanden, sondern alle jene Informationen, die einem Menschen seine Identität gibt. Dies inkludiert z.B.: Stimm aufnehmen, Fingerabdrücke, Bilder, Videos usw. All jene Daten, die nicht personenbezogen oder allgemein verfügbar sind, fallen nicht unter den Grundrechtsschutz. *„Aber auch wenn ein Geheimhaltungsanspruch besteht, kann dieser unter bestimmten Voraussetzungen rechtmäßig eingeschränkt werden (das heißt: die Daten können von anderen als der betroffenen Person verarbeitet und übermittelt werden). Dies ist der Fall, wenn:*

- *die Verwendung der Daten im lebenswichtigen Interesse des Betroffenen,*
- *mit seiner Zustimmung oder*
- *zur Wahrung überwiegender berechtigter Interessen eines anderen (hierzu zählt auch ein öffentliches Interesse)*

erfolgt. [BKA]

Unter „öffentliches Interesse“ wird die Nationale Sicherheit, Verhinderung von strafbaren Handlungen, Schutz der Gesundheit, Schutz der Rechte und Freiheiten anderer verstanden. Wenn ein öffentliches Interesse besteht und der Staat hoheitlich agieren möchte, muss dies trotzdem durch ein Gesetz begründet sein. Wenn sensible Daten weitergegeben werden, dann sieht der Gesetzgeber vor, dass dies nur auf Grundlage eines Gesetzes passieren kann und weiters muss festgelegt werden, wie der Schutz des Geheimhaltungsinteressenten aussieht. Zusätzlich hat jeder ein Recht auf Auskunft über seine verwendete Daten als auch die Richtigstellung von „falschen“ Daten und die Löschung von unzulässigerweise verarbeiteten Daten.

2.1 Begriff

Der Begriff „data protection“ wird häufig im europäischen Rechtsraum verwendet. Im Vergleich dazu wird in Amerika oder Großbritannien eher von „data privacy“ gesprochen. Der Unterschied zwischen dem englischsprachigen Raum und Europa besteht darin, dass in Europa Datenschutz durch Gesetze (z.B. in Österreich verfassungsrechtlich) und in den Vereinigten Staaten eher durch gesellschaftliche Regeln bzw. Akzeptanz festgelegt ist. Hier 3 Beispiele von namhaften Autoren, wie Sie den Begriff Datenschutz definieren. [BBN]

H. R: Hansen, G. Neumann

„Als Datenschutz (engl.: data privacy; protection of data privacy) bezeichnet man die Gesamtheit der gesetzlichen und betrieblichen Massnahmen zum Schutz der Rechte von Personen vor Verletzung der Vertraulichkeit und zur Sicherheit des Informationshaushaltes.“

Carl August Zehnder

„Datenschutz (data protection) ist der Schutz der durch die Daten dargestellten Sachverhalte des realen Lebens vor jeder Art von Missbrauch, insbesondere bei Daten über Personen. Zum Datenschutz gehört die Abschirmung gegen Unberechtigte (Schutz der Privatsphäre, privacy), aber auch deren Verfügbarkeit für Berechtigte (Auskunftsrecht, Berichtigungsrecht).“

René Hugelshofer, Michael Anderes, Henk Goorhuis, Ruedi Niederer

„Der Datenschutz betrifft Personendaten. Er will die Betroffenen davor schützen, dass unnötige, unvollständige oder gar unrichtige Daten ein falsches Bild ihrer Person entstehen lassen. Durch falsche oder unvollständige Angaben kann Schaden entstehen. Datenschutzmassnahmen sollen auch verhindern, dass vertrauliche Daten (Spital, Bank, Arbeitgeber) verbreitet werden.“

2.2 Definition

Nachdem die ersten Datenschutzgesetze Anfang der 80er Jahre entstanden sind, ist die Bedeutung des Datenschutzes aufgrund der Vernetzung in unserer heutigen Gesellschaft gestiegen. Dies kann darauf zurückgeführt werden, dass aufgrund der Informations- und Kommunikationstechnik es immer einfacher geworden ist, Datenerfassung, Datenanalyse und Datenweitergabe zu vollziehen. Technologien, die heutzutage fast jeder Mensch verwendet, wie Internet, E-Mail, Mobiltelefon und Videokameras erleichtern die Erfassung und Weitergabe von personenbezogenen Daten. Neben staatlichen Behörden zeigen auch immer mehr private Unternehmen Interesse an personenbezogenen Daten. Bei den nächsten Beispielen möchte ich aufzeigen, wie vielfältig dieses Interesse an den Daten in unserer Gesellschaft schon ist. Sicherheitsorgane möchten durch Lauschangriffe, Rasterfahndung oder über andere Überwachungsmaßnahmen die Verbrechensbekämpfung optimieren. Finanzbehörden versuchen illegale Banktransaktionen aufzuzeigen, um Steuerdelikte aufdecken zu können. Auch private Unternehmen versuchen vermehrt durch Video- oder PC-Überwachung die Arbeitsleistung ihrer Arbeitnehmer effektiver zu gestalten. Wie Vorfälle in Deutschland z.B.

Videoüberwachungen bei der Fa. Lidl gezeigt haben, wurden diese Überwachungsmaßnahmen, ohne das Einverständnis der Arbeitnehmer, durchgeführt. Neben den eigenen Mitarbeiter, sind aber natürlich auch die Kunden ein wichtiges Ziel. Hier wird versucht, das Kaufverhalten der Kunden zu verstehen, als auch den Kunden zu binden. Ein weiteres Beispiel für das Interesse von Unternehmen, das nicht immer im Einklang mit dem Datenschutz steht, ist der Versuch im Internet Bewegungsprofile zu erstellen. Wie der Vorfall um Google Chrome gezeigt hat, könnten so die Daten der Bewegungsprofile leicht in die falschen Hände gelangen. Wie schon oben erwähnt, ist die Bedeutung des Datenschutzes noch nie so wichtig gewesen wie in der heutigen Zeit, da wie die Beispiele der jüngsten Vergangenheit gezeigt haben, die Anzahl der Interessenten von personenbezogenen Daten extrem angestiegen ist.

2.3 Rechtliche Grundlagen

In Österreich ist der Datenschutz verfassungsrechtlich im Datenschutzgesetz 2000 (DSG 2000) verankert. Neben dem DSG 2000 ist der Schutz von personenbezogenen Daten auch in weiteren einfachen Gesetzen festgelegt. In der nachfolgenden Auflistung sind die wichtigsten Rechtsgrundlagen in punkto Datenschutz in Österreich als auch der EU aufgelistet.

- **Österreich - verfassungsrechtliche Grundlagen**
 - §§ 1ff Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999
- **Österreich - einfachgesetzliche Grundlagen**
 - §§ 4ff Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999
 - Bundesstatistikgesetz 2000, BGBl. I Nr. 163/1999
 - E-Government-Gesetz (E-GovG), BGBl. I Nr. 10/2004
 - Gentechnikgesetz (GTG), BGBl. Nr. 510/1994
 - Gesundheitstelematikgesetz (GTelG), BGBl. I Nr. 179/2004
 - Meldegesetz 1991 (MeldeG), BGBl. Nr. 9/1992
 - § 4 Abs. 3 Rundfunkgebührengesetz, BGBl. I Nr. 159/1999
 - Sicherheitspolizeigesetz (SPG), BGBl. Nr. 566/1991
 - Telekommunikationsgesetz 2003 (TKG 2003), BGBl. I Nr. 70/2003
 - § 3 Wählerevidenzgesetz 1973, BGBl. Nr. 601/1973
- **Österreich - Grundlagen auf Verordnungsebene**
 - Datenschutzangemessenheitsverordnung, BGBl. II Nr. 521/1999
 - Datenverarbeitungsregisterverordnung 2002 (DVRV 2002), BGBl. II Nr. 24/2002
 - Standard- und Musterverordnung 2004 (StMV 2004), BGBl. II Nr. 312/2004

- **EU**

- *Datenschutzrichtlinie (RL 95/46/EG)*
- *Datenschutzrichtlinie für elektronische Kommunikation "Telekom-Datenschutzrichtlinie" (RL 2002/58/EG)*
- *Vorratsdatenspeicherungs-Richtlinie (RL 2006/24/EG)*
- *Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr*

- **Europarat**

- *Verträge des Europarates zur Datenschutzkonvention*
- *Empfehlungen und Resolutionen des Europarates [BKA]*

2.3.1 Österreichische Gesetze

In den nächsten Kapiteln werden nicht alle relevanten Gesetze im Bereich Datenschutz behandelt. Es wird nur ein Überblick über die wichtigsten Gesetze in Österreich gewährt.

2.3.1.1 Datenschutzgesetz 2000 (DSG 2000)

In Österreich wurde am 18. Oktober 1978 das Bundesgesetz über den Schutz personenbezogener Daten erlassen (Inkrafttredatum: 1980). Dieses erste Gesetz über Datenschutz war 20 Jahre in Österreich gültig und musste dann aufgrund der europäischen Datenschutzrichtlinie (RL 95/46/EG) von 1995, im Jahre 2000 revidiert werden. Somit ist das Datenschutzgesetz von 1978 heute außer Kraft. Das heute noch gültige Datenschutzgesetz 2000, BGBl. I Nr. 165/1999 (DSG 2000), trat mit 1.1.2000 in Kraft und wurde im Jahre 2005 nochmals grundlegend novelliert. In diesem Kapitel möchte ich nun auf die wichtigsten Paragraphen des DSG 2000 eingehen:

Gleich im §1 wird im DSG 2000 festgehalten, dass jedermann Anspruch auf die Geheimhaltung personenbezogener Daten hat.

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. [I4J1]

Für die Erlassung gesetzlicher Datenschutzbestimmungen sind sowohl der Bundes- als auch der Landesgesetzgeber berechtigt (DSG 2000 §2). Die Entscheidung wer von beiden zur Gesetzgebung berufen ist, obliegt darin, ob die Verwendung automationsunterstützt oder manuell durchgeführt wird.

Im Gesetz werden weiters die genauen Definitionen in punkto Daten beschrieben (DSG 2000 §4):

- **Personenbezogene Daten** sind Angaben zu Personen, deren Identität bestimmt oder zumindest bestimmbar sind.

z.B. Name, SV-Nr., Adressen

- **Nur indirekt Personenbezogen** sind Daten bei denen der Personenbezug der Daten vom Auftraggeber, Dienstleister oder Empfänger mit rechtlich zulässigen Mitteln nicht bestimmt werden kann.
- **Sensible Daten** sind gesetzlich definiert: Daten über rassische oder ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder Sexualleben.
- **Zustimmung** ist die gültige, ohne Zwang abgegebene Willenserklärung der betroffenen Person zur konkreten Verwendung der Daten "in Kenntnis der Sachlage". Diese kann schriftlich, mündlich oder auch schlüssig abgegeben werden (keine Formvorschrift). [14J1]

Im §6 sind Datenschutzgrundsätze definiert, die festschreiben, wie die Datenverarbeitung erfolgen muss. Die Datenverarbeitung muss nach 6 Prinzipien erfolgen, um den Datenschutzgrundsätzen zu entsprechen.

Neben der Zulässigkeit der Datenverwendung und Datenübermittlung, Nichtverletzung der schutzwürdigen Geheimhaltungsinteressen (§7) werden weiters auch einige Rechte für die Betroffenen im DSG 2000 festgeschrieben. Wie schon im §1 beschrieben, wird das Recht auf Geheimhaltung festgehalten. Weiters wird im §26 das Recht auf Auskunft erlassen. Der Auftraggeber muss dem Betroffenen Auskunft über seine zu verarbeitenden Daten mitteilen. Dies muss innerhalb von 8 Wochen passieren, oder zumindest eine Begründung geben, wieso dies nicht möglich war. Falls dem Auskunftsrecht nicht Folge geleistet wird, kann der Betroffene, eine formlose Beschwerde bei der Datenschutzkommission einreichen. Im darauf folgenden §27 wird dem Betroffenen das Recht auf Richtigstellung bzw. Löschen der Daten gewährt. Die Daten müssen korrigiert oder gelöscht werden, wenn die Verarbeitung der Daten unzulässig bzw. die Daten nicht der Wahrheit entsprechen.

2.3.1.2 Telekommunikationsgesetz 2003 (TKG 2003)

Aufgrund der Datenschutzrichtlinie für elektronische Kommunikation der Europäischen Union wurde das Telekommunikationsgesetz von 1997 massiv erweitert, und im Jahre 2003 wurde das neue Telekommunikationsgesetz 2003 erlassen. Ein Unterschied zu dem vorherigen Gesetz ist, dass der Anwendungsbereich ausgeweitet wurde. Das neue Gesetz ist auch anwendbar auf Unternehmen, die öffentliche Kommunikationsnetze und -dienste bereitstellen. Gleich im §1 wird der Zweck bzw. die Zielsetzung dieses Gesetzes deklariert. Das Gesetz soll gewährleisten, dass durch die Förderung

des Wettbewerbes im Bereich der elektronischen Kommunikation die Bevölkerung und die Wirtschaft mit zuverlässigen, preiswerten, hochwertigen und innovativen Kommunikationsdienstleistungen versorgt werden. Eine weitere wichtige Zielsetzung dieses Bundesgesetzes ist der Schutz der Nutzer in Kommunikationsnetzen und -diensten. Deswegen wurde eine Vielzahl von Regelungen erlassen. Da für die weitere Arbeit die Begriffe Inhaltsdaten, Stammdaten, Verkehrsdaten und Standortdaten von beträchtlicher Relevanz sind, möchte ich diese hier näher erläutern.

Inhaltsdaten werden in §87 Abs. 3 Ziffer 6 TKG beschrieben. Diese stellen Informationen bzw. Nachrichten dar, die mittels Telekommunikation ausgetauscht werden. Hier sind z.B. Inhalte von Telefongesprächen bzw. E-Mails anzuführen.

Unter *Stammdaten* (in Deutschland wird der Begriff Bestandsdaten [KEC] verwendet) versteht der Gesetzgeber, die personenbezogenen Daten eines Teilnehmers, die auf Dauer vom Vertragspartner zugeordnet bzw. gespeichert werden. Diese Daten werden bei der Erstellung, Änderung bzw. Beendigung eines Vertragsverhältnisses mit dem Dienstleister erhoben. Beispiele hierfür sind der Name, Anschrift, Geburtsdatum oder Bankverbindung. Stammdaten werden im TKG §92 Abs. 3 Ziffer 3 definiert.

Verkehrsdaten werden im TKG §92 Abs. 3 Ziffer 4 normiert. Hierbei handelt es sich um jene Daten, die zur Weiterleitung einer Nachricht bzw. Erbringung einer Telekommunikationsdienstes verarbeitet werden. Beispiele hierfür wären die Rufnummer eines mobilen Endgeräts, Beginn und Ende der Kommunikation bzw. IP-Adressen.

Standortdaten sind jene Verkehrsdaten, die den geografischen Standort einer Telekommunikationsendeinrichtung angeben. Der Begriff wird im TKG §92 Abs. 3 Ziffer 6 erklärt. Die zugewiesene Funkzelle eines Mobiltelefons kann hier als Beispiel für Standortdaten angeführt werden. [14J2]

Im §93 TKG wird das Kommunikationsgeheimnis bezüglich dieser Datenkategorien festgehalten. Wie im Abs. 1 nachzulesen ist, fallen unter das Kommunikationsgeheimnis Inhaltsdaten, Verkehrsdaten und Standortdaten. Weiters ist im Abs. 3 festgehalten: „*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.* [14J2]

Neben der bereits erwähnten Datenschutzrichtlinie für elektronische Kommunikation, wurden weitere vier Richtlinien der europäischen Union umgesetzt:

1. Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, ABl. Nr. L 108 vom 24. April 2002, S 33,
2. Richtlinie 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und -dienste, ABl. Nr. L 108 vom 24. April 2002, S 21,
3. Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten , ABl. Nr. L 108 vom 24. April 2002, S 51,
4. Richtlinie 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung, ABl. Nr. L 108 vom 24. April 2002, S 7

2.3.1.3 *Sicherheitspolizeigesetz 2008 (SPG 2008)*

Das Sicherheitspolizeigesetz wurde 1991 in Österreich erlassen und regelt die Organisation der Sicherheitsverwaltung sowie die Aufrechterhaltung der öffentlichen Sicherheit, Ordnung und Ruhe. Somit stellt dieses Gesetz die Grundlage der Sicherheitsverwaltung und deren Organe in Österreich dar. Das Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (offizielle Titel) wurde speziell in den letzten Jahren öfters novelliert. Im Jahre 2005 musste aufgrund der Zusammenlegung von Bundesgendarmerie, Bundessicherheitswachekorps und dem Kriminalbeamtenkorps zur Bundespolizei dieses Gesetz von Grund auf novelliert werden. Eine weitere grundlegende Novelle wurde Ende des Jahres 2007 (Inkrafttredatum: 1.1.2008) beschlossen. Das BMI legte im September 2007 einen Ministerialentwurf bezüglich Änderungen des Sicherheitspolizeigesetzes, des Grenzkontrollgesetzes und des Polizeikooperationsgesetzes vor. Dieser Ministerialentwurf enthielt einerseits die nunmehr neu geregelten Lokalisierungsbefugnisse (genauere Details siehe Kapitel 4.1 Einleitung und Gesetzestexte) im § 53 Abs. 3b SPG sowie andererseits eine kleine Änderung im Bezug auf die „kleine passive Rufdatenrückerfassung“ (Ermittlung des Anrufenden anhand der angerufenen Teilnehmernummer). Hier war vorgesehen, dass im § 53 Abs. 3a Satz 2 SPG, das Tatbestandsmerkmal des „Gesprächs“ auf den Begriff „Kommunikation“ ausgetauscht wird. Hintergrund dieser vorgesehenen Änderung war wahrscheinlich, dass eine Ausdehnung des Anwendungsbereichs auf neuere Technologien (Internet, Voice over IP, usw.) beabsichtigt war. Im Oktober 2007 wurde dann nach zahlreichen Stellungnahmen [PAR1]in Bezug auf den Ministerialentwurf die Regierungsvorlage zur Novelle des SPG vorgelegt. Diese Regierungsvorlage enthielt dann nicht mehr die Änderung des § 53 Abs. 3a Satz 2 SPG bezüglich der Ausdehnung des Begriffs „Gesprächs“ auf „Kommunikation“. Ansonsten enthielt die Regierungsvorlage fast genau die gleichen Punkte wie es dann in der Novelle umgesetzt wurde. Einzige Ausnahme hierbei war, dass in der Regierungsvorlage nur in Bezug auf

Standortdaten eine Auskunftspflicht ausgewiesen war. In der Umsetzung jedoch wurde explizit die IMSI vorgesehen.

Am letzten Sitzungstag 06.12 des Jahres 2007 im Parlament wurde dann diese Regierungsvorlage als letzter Tagesordnungspunkt anberaumt. Die Diskussion über die Novelle zum SPG wurde dann um 22:34 begonnen. Hierbei wurde von den Abgeordneten Rudolf Parnigoni (SPÖ) und Günter Kößl (ÖVP) der Abänderungsantrag [PAR2] zur Novelle zum SPG eingebracht. Dieser inkludiert die Neufassung des § 53 Abs. 3a und 3b SPG (genauere Details siehe Kapitel 4.1 Einleitung und Gesetzestexte). Die Novelle wurde um 23:50 von den Regierungsparteien SPÖ und ÖVP beschlossen und als BGBl. I 114/7 kundgemacht. Somit traten dann am 1.1.2008 die geänderten Fassungen des §53 Abs. 3 a und 3b in Österreich in Kraft. (Siehe nähere Details zur Geschichte der Novelle [SPG]). Die Gesetzestexte, Befugnisse sowie Erörterungen der Novelle des SPG werden im Kapitel 3 Staatliche Überwachung in Österreich beschrieben.

2.3.2 Europäische Gesetze

Auch in der Charta der Grundrechte der Europäischen Union wurde im Artikel 8 festgelegt, dass jede Person Recht auf den Schutz der Sie betreffenden personenbezogenen Daten hat [EUC]. Neben dieser Charta gibt es eine Reihe an Richtlinien, die sich mit dem Datenschutz befassen. Diese werde ich in den nächsten Sub-Kapiteln beleuchten.

2.3.2.1 Richtlinie 95/46/EG (Datenschutzrichtlinie)

1995 wurde die Richtlinie 95/46/EG (Datenschutzrichtlinie) zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom Europäischen Parlament und Europäische Rat beschlossen. Die Zielsetzung der Europäischen Union war es, dass Mindeststandards für den Schutz der Privatsphäre von natürlichen Personen bei der Verarbeitung von personenbezogenen Daten geschaffen werden. Durch diese Richtlinie wurden alle Mitgliedsstaaten aufgefordert, ihre nationalen Gesetze dahingehend anzupassen. Einzige Ausnahmen hierbei waren die gemeinsame Außen- und Sicherheitspolitik sowie den Bereich der justiziellen und polizeilichen Zusammenarbeit. Weiters wurde festgelegt, wie die Übermittlung von personenbezogenen Daten zu Drittländern, also nicht EU-Mitglieder, auszusehen hat. Die Übermittlung der personenbezogenen Daten ist nur dann zulässig, wenn das Drittland ein „angemessenes Schutzniveau“ garantieren kann (definiert in Artikel 25). Wer ein „angemessenes Schutzniveau“ gewährleisten kann, entscheidet die Europäische Kommission, die wiederum von der Artikel-29-Datenschutzgruppe beraten wird. Wie schon oben beschrieben, wurde die Richtlinie 95/46/EG (Datenschutzrichtlinie) durch das Datenschutzgesetz von 2000 in Österreich umgesetzt.

2.3.2.2 Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation)

2002 wurde von der Europäischen Union die Datenschutzrichtlinie für elektronische Kommunikation erlassen, um verbindliche Mindeststandards für den Datenschutz im Bereich Telekommunikation festzulegen. Die Zielsetzung der Ergänzung zur Richtlinie 95/46/EG (Datenschutzrichtlinie) war einerseits der Schutz der Grundrechte und die Privatsphäre der Bewohner der Mitgliedsstaaten, aber auch andererseits die Gewährleistung des freien Datenverkehrs zwischen den EU-Ländern. Die Europäische Union verpflichtete somit ihre Mitgliedsländer telekommunikationsspezifischen Normen zum Datenschutz zu erlassen. Die Richtlinie enthält zum Beispiel Regelungen bezüglich dem Abhören von Telefongesprächen, Abfangen von E-Mail Verkehr, automatischen Anrufweiterschaltungen, Einzelgebührennachweis sowie Möglichkeiten der Anzeige und Unterdrückung von Telefonnummern. Die Datenschutzrichtlinie für elektronische Kommunikation wurde von Österreich im Jahre 2003 mit dem Telekommunikationsgesetz 2003 (BGBl. I Nr. 70/2003) umgesetzt.

2.3.2.3 Richtlinie 2006/24/EG (Vorratsdatenspeicherung)

Diese Richtlinie der europäischen Union sieht vor, dass die verschiedenen nationalen Standards bezüglich Telekommunikationsdaten auf Vorrat vereinheitlicht werden. Die Zielsetzung hierfür ist, dass durch diese Harmonisierung eine Erleichterung der Ermittlung und Verfolgung von schweren Straftaten geschieht. Die Richtlinie bezieht sich darauf, dass Verkehrs- bzw. Standortdaten auf Vorrat gespeichert werden. Dies inkludiert aber keine Inhaltsdaten. Die Dauer der Speicherung der Daten ist mit mindestens 6 Monaten bis höchstens 2 Jahren ab dem Zeitpunkt der Kommunikation festgeschrieben. Diese Richtlinie ist eine Erweiterung der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) und sollte wie diese in nationales Recht umgesetzt werden. Diese Richtlinie ist derzeit sehr umstritten, da Befürworter es als geeignetes Mittel für Verbrechens- und Terrorismusbekämpfung sehen, aber die Gegner es als schweren Eingriff gegen das Recht auf Privatsphäre bezeichnen. Derzeit ist in Österreich nur die Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) im Telekommunikationsgesetz 2003 umgesetzt worden.

Um diese Richtlinie näher zu beleuchten, werde ich in der nächsten Tabelle die Kategorien der Daten auflisten, die laut EU auf Vorrat gespeichert werden sollen (Artikel 5):

Beschreibung	Festnetz bzw. Mobilfunk	Internetzugang, Internet-Telefonie und E-Mail
1. Identifikation eines Absenders einer Nachricht	a. Rufnummer des anrufenden Anschluss b. Name und Anschrift des Teilnehmers	a. Zugewiesene Benutzerkennung b. Rufnummer bzw. Benutzerkennung c. der Name und die Anschrift des Teilnehmers bzw. registrierten Benutzers, dem eine Internetprotokoll-Adresse (IP-Adresse), Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war
2. Identifikation eines Empfängers einer Nachricht	a. Die gewählte Rufnummer bzw. bei Rufweiter- und Rufumleitung, jene Rufnummer an die weitergeleitet wurde b. Name und Anschrift des Teilnehmers	a. Bei Internet-Telefonie: Benutzerkennung oder Rufnummer des Empfängers b. Namen und Anschrift der Teilnehmer bzw. Benutzererkennung des Empfängers
3. Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung	a. Datum und Zeit des Beginns bzw. Ende der Nachrichtenübermittlung	a. Datum und Uhrzeit der An- und Abmeldung des Internetzugangs. Dies muss passieren auf der Grundlage, dass eine statische bzw. dynamische IP-Adresse, Benutzerkennung sowie die Zeitzone gespeichert werden müssen. b. Datum und Uhrzeit der An- und Abmeldung der Internet-Telefonie bzw. E-Mail-Dienstes. Hier muss auch die Zeitzone gespeichert

		werden.
4. Art der Nachrichten-übermittlung	a. Der in Anspruch genommene Telefondienst wird hier protokolliert.	a. Hierbei wird der verwendete Internetdienst gespeichert.
5. Identifikation einer Endeinrichtung	a. Festnetz: Rufnummer des anrufenden und angerufenen Teilnehmers b. Mobilfunk i. die Rufnummern des anrufenden und des angerufenen Anschlusses, ii. die internationale Mobilteilnehmerkennung (IMSI) des anrufenden Anschlusses, iii. die internationale Mobilfunkgeräte-kennung (IMEI) des anrufenden Anschlusses, iv. die IMSI des angerufenen Anschlusses, v. die IMEI des angerufenen Anschlusses, vi. vorbezahlte anonyme Dienste: Datum und Uhrzeit der ersten Aktivierung + Kennung des Standorts der ersten Aktivierung	a. Wählanschluss: Rufnummer des angerufenen Dienstes b. DSL: digitale Teilnehmeranschluss bzw. Endpunkt der Kommunikation
6. Bestimmung des Standorts von mobilen Endgeräten	a. Standortkennung bei Beginn der Verbindung b. Daten zur geographischen Ortung von Funkzellen im Konnex zur Standortkennung während des Zeitraums der Verbindung	

Tabelle 1: Kategorien der Vorratsspeicherung

Wie schon erwähnt ist diese Richtlinie noch nicht in Österreich umgesetzt. Eigentlich hätte die Umsetzung der Richtlinie bis September 2007 laut EU in den einzelnen Staaten durchgeführt werden sollen. Österreich hat noch auf die Entscheidung des Europäischen Gerichtshofs (EuGH) bezüglich einer Klage von Irland gewartet. Da diese aber abgelehnt wurde, wurde 2008 dann das Ludwig-Boltzmann-Institut für Menschenrechte mit der Beauftragung einer Gesetzesvorlage zur Vorratsdatenspeicherung beauftragt. Diese wurde im September 2009 an das Infrastrukturministerium übergeben. Diese Gesetzesvorlage sieht vor, dass nur die Mindestanforderungen umgesetzt werden sollten. Seitens des Innenministeriums, im speziellen durch die Innenministerin Maria Fekter, wurden aber die Bedenken geäußert, dass diese Vorlage *"wenig praktikabel"* ist. Weiters wurde angemerkt, dass diese Vorlage *"an den Bedürfnissen der Polizeiarbeit vorbeigehe."* [FTZ3] Der derzeitige Plan sieht vor, dass die Vorratsdatenspeicherung-Richtlinie im Frühjahr 2010 umgesetzt wird, aber durch die unterschiedlichen Meinungen im Infrastruktur- bzw. Innenministerium ist der genaue Inhalt der Richtlinie, die eine Novelle des TKG 2003 bedeutet, noch nicht bestimmt.

2.4 Datenschutzbehörden und Kontrollorgane in Österreich

Die Datenschutzkommission (DSK) bildet nur den Rechtsschutz für den öffentlichen Bereich. Dies heißt, dass der Rechtsschutz nur für den öffentlichen Auftraggeber (z.B. Behörden) gilt (§5 Abs. 2 DSG 2000). Ein weiteres Beispiel für die Zuständigkeit der Datenschutzkommission wäre, wenn der Auftraggeber die gesetzlich übertragenen Aufgaben erfüllt (ebenso §5 Abs. 2 DSG 2000). Ansonsten – also im privaten Bereich – muss bei einer Verletzung gegen Datenschutzbestimmungen Klage vor einem österreichischen Gericht eingebracht werden (§ 32 DSG 2000). Wenn also Bedenken vorhanden sind, dass ein Auftraggeber im privaten Bereich gegen Datenschutzbestimmungen verstoßen hat, dann muss vor einem Landesgericht Klage eingebracht werden (§ 32 Abs. 4 DSG 2000). Als mögliche zusätzliche Instanz kann bei Datenschutzverletzungen in der Europäischen Union der Europäische Datenschutzbeauftragte herangezogen werden.

2.4.1 Datenschutzkommission

Die Datenschutzkommission (abgekürzt: DSK) wurde 1980 mit dem Inkrafttreten des Datenschutzgesetz (DSG), BGBl. Nr. 565/1978 gegründet. Somit ist die österreichische DSK eine der ältesten Datenschutzbehörden in Europa. Neben den oben erwähnten Rechtsschutz für öffentliche Auftraggeber möchte ich im nächsten Kapitel noch ihre weiteren Befugnisse darstellen.

2.4.1.1 Arbeit der Datenschutzkommission

Der DSK obliegt die Führung des Datenverarbeitungsregisters. Es dient zur Transparenz aller der in Österreich durchgeführten Datenverarbeitungen. *„Das Datenverarbeitungsregister ist ein öffentliches, allen zugängliches, teilweise elektronisch geführtes Register, in das alle meldepflichtigen Datenanwendungen aufgrund einer Meldung des jeweiligen Auftraggebers*

eingetragen werden. Gemäß § 3 Abs. 2 DVRV 2002 besteht das Datenverarbeitungsregister aus:

- den registrierten Meldungen über Auftraggeber und Datenanwendungen,*
- einem gesonderten Verzeichnis der Informationsverbundsysteme und*
- den Registrierungsakten.“ [DSK]*

Das Datenverarbeitungsregister wurde mit dem §16 Abs. 1 DSG 2000, also mit Wirksamkeit 01.01.2000, eingeführt und obliegt der Verantwortlichkeit der DSK. Vor der Einführung des neuen DSG von 2000, oblag die Führung des Datenverarbeitungsregisters beim Österreichischen Statistischen Zentralamt (heute als Bundesanstalt Statistik Österreich bekannt). Anlässlich der letzten Zählung des Datenverarbeitungsregisters im Jahre 2007 wurden insgesamt 80.000 Auftraggeber gezählt. Jeder Auftraggeber inkludiert meistens mehrere Datenanwendungen.

Zu einer weiteren Arbeit oder Befugnis der DSK zählt die Durchführung des Auskunftsrechts nach § 26 DSG 2000. Das Auskunftsrecht obliegt sowohl im öffentlichen als auch im privaten Bereich. Somit hat jeder Betroffene das grundlegende Recht auf die Einsicht der ihn betreffenden Datenströme. Dieses zentrale Recht nach Auskunft ist meistens die Grundlage für eine Beschwerde bei der DSK, da die Einsicht in die tatsächlich verwendeten Daten die Basis bilden für die Durchsetzung der Rechte der Betroffenen, z.B. Löschung oder Richtigstellung von Daten, Widerspruch usw.. Der Betroffene muss schriftlich ein Auskunftsbegehren an die DSK richten.

Wie schon oben erwähnt ist ein weiteres Betätigungsfeld der Datenschutzkommission die Entscheidung über Beschwerden. Wenn der berechnigte Verdacht besteht, dass Datenschutzverletzungen oder Verletzungen von Pflichten des Auftraggebers oder Dienstleisters nach DSG 2000 bestehen, können Betroffene eine Beschwerde bei der DSK einbringen. Bei einer Beschwerde beim DSK stehen 2 Möglichkeiten zur Verfügung:

1. Der Betroffene hat die Möglichkeit, ein förmliches Verfahren nach §31 DSG 2000 einzubringen. In diesem Verfahren wird über Beschwerden wegen Rechtsverletzungen durch Bescheid geurteilt, der nach den sonstigen Regeln des Verwaltungsrechts durchsetzbar ist. Folgende Gründe können zu einer Durchführung eines so genannten förmlichen Verfahrens führen:

- Der Betroffene bringt Beschwerde gegen Auftraggeber des öffentlichen und des privaten Bereichs über behauptete Verletzungen des Rechtes auf Auskunft gemäß § 1 Abs. 3 Z 1 und § 26 DSG 2000 ein.
- Die Beschwerde wird gegen Auftraggeber des öffentlichen Bereichs über behauptete Verletzungen des Rechtes auf Geheimhaltung nach §1 Abs. 1 und 2 und § 7 DSG 2000 oder des Rechtes auf Richtigstellung oder auf Löschung nach §1 Abs. 3 Z 2 und §27 DSG 2000 eingebracht.

- Wenn Ansprüche wegen Verletzung dieser Rechte durch Auftraggeber des privaten Bereiches bestehen, dann können diese nur durch Klage bei Gericht geltend gemacht werden (§ 1 Abs. 5 und § 32 DSG 2000).

2. Als zweite Variante besteht das „Ombudsmann-Verfahren“ gemäß §30 DSG 2000. In diesem so genannten nicht förmlichen Verfahren können Verletzungen von Pflichten des Auftraggebers oder Dienstleisters aufgezeigt werden, ohne den hohen finanziellen Risiko wie bei Variante 1 bei einem förmlichen Verfahren. Die DSK übernimmt hier die Funktion eines Ombudsmanns („Mediators“) und kann Empfehlungen zur Beseitigung von Datenschutzverletzungen herausgeben. Bei diesem Verfahren gibt es jedoch nicht die Möglichkeit einer rechtlich durchsetzbaren Entscheidung.

Weiters hat die DSK Kontrollbefugnis bei berechtigtem Verdacht auf Datenschutzverletzungen auch außerhalb der Beschwerdeverfahren nach §30 und §31. Dies inkludiert, dass die DSK alle notwendigen Unterlagen vom Auftraggeber oder Dienstleister verlangen kann, als auch Einsicht in die Datenanwendungen. Somit muss der Auftraggeber oder Dienstleister der Datenanwendung alles Notwendige zur Aufklärung der DSK zur Verfügung stellen.

Neben den bereits angeführten Arbeiten der DSK, zählt weiters die Mitarbeit in wichtigen Gremien der Europäischen Union. Hierzu zählt die Teilnahme an der Artikel-29-Datenschutzgruppe, Schengen, Europol, Zollinformationssystem (ZIS), Eurodac (europäische Datenbank zur Speicherung von Fingerabdrücken) und Eurojust (Einheit für justizielle Zusammenarbeit der Europäischen Union).

Die DSK ist weiters Stammzahlenregisterbehörde gemäß §7 des E-Government-Gesetz BGBl. Nr. 10/2004 idgf. Zu den Aufgaben der Stammzahlenregisterbehörde gehören:

- Vergabe von Stammzahlen und bereichsspezifischen Personenkennzeichen (bPK) (§ 10 Abs. 2 E-GovG),
- Ausstellung von Ersatz-Stammzahlen (§ 6 Abs. 5 E-GovG),
- Führung der Ergänzungsregister (§ 6 Abs. 4 E-GovG),
- Festlegung und Publikation der mathematischen Verfahren zur Bildung der Stammzahlen, Ersatzstammzahlen und bPK (§ 6 Abs. 6 E-GovG) und (§ 9 Abs. 3 E-GovG),
- Eintragung von Vollmachtsverhältnissen auf die Bürgerkarte des Vertreters (§ 5 E-GovG).

Abschließend ist über die Arbeit der DSK zu vermerken, dass diese Behörde Stellungnahmen veröffentlicht, wenn neue Entwürfe von Gesetzen oder rechtskräftige Rechtsvorschriften in punkto Datenschutz diskutiert werden. Diese Stellungnahmen sind unter der URL: <http://www.dsk.gv.at/site/6185/default.aspx> abrufbar.

2.4.2 Datenschutzrat

Der Datenschutzrat (abgekürzt: DSR) ist ein Beirat der Bundes- als auch der Landesregierungen für rechtspolitische Fragen in Zusammenhang mit Datenschutz. Dieser Beirat der Bundes- und Landesregierungen ist im Bundeskanzleramt eingerichtet und wurde mit dem DSG 2000 in den §35 (1), §40, §41, §42, §43 und §44 als Kontrollorgan festgelegt. Der Datenschutzrat wurde zwar schon im Jahre 1978 gebildet, dieser hatte aber damals nicht den gleichen Aufgabenbereich wie heute. Die Einrichtung des DSR hat die Zielsetzung, die Entwicklung des Datenschutzes zu beobachten und Verbesserungsvorschläge zu unterbreiten. Somit kann zusammenfassend gesagt werden, dass die Hauptaufgaben der DSR sowohl die Beratung der Bundes- und Landesregierungen in punkto Datenschutzgesetze als auch Stellungnahmen, Anregungen und Bedenken zu Gesetzesentwürfen sind.

Der DSR setzt sich zusammen aus Vertreter aller gewählten Parteien, der Länder, des Gemeinbundes, des Städtebundes, der Bundeskammer für Arbeiter und Angestellte, des Wirtschaftsbundes und eines Vertreters des Bundes, der vom Bundeskanzler ernannt wird. Diese Vertreter der verschiedensten Interessensgemeinschaften führen die Aufgabe des Kontrollorgans ehrenamtlich aus.

2.4.3 Rechtsschutzbeauftragter im Bundesministerium für Inneres

Mit der Sicherheitspolizeigesetz-Novelle von 2000 (nicht 2008!) wurde die Institution des Rechtsschutzbeauftragten im Bundesministerium für Inneres eingerichtet. Dieses besteht aus dem Rechtsschutzbeauftragten und 2 Stellvertretern. Der Rechtsschutzbeauftragte wird für 5 Jahre vom Bundespräsidenten auf Vorschlag der Bundesregierung bestellt. Als Voraussetzung muss der Rechtsschutzbeauftragte bzw. die 2 Stellvertreter ein Studium der Rechtswissenschaften und 5 Jahre Berufserfahrung vorweisen. Die Aufgaben des Rechtsschutzbeauftragten sind im SPG §91 a bis d und Grenzkontrollgesetz §12 Abs. 1 geregelt. Zu den Aufgaben des Rechtsschutzbeauftragten zählt:

1.) Die öffentlichen Sicherheitsorgane müssen den Rechtsschutzbeauftragten von jeder Ermittlung von personenbezogenen Daten in punkto verdeckter Ermittlung gegen kriminelle Verbindungen (SPG § 54 Abs. 3-5) in Kenntnis setzen. Dazu zählen Einsätze von Bild- oder Tonaufzeichnungsgeräten bei Fahndungen gegen kriminelle Verbindungen oder durch Verarbeiten von Daten, die andere mittels Einsatz von Bild- und Tonaufzeichnungsgeräte übermitteln. Hierbei muss zum Beispiel dem Rechtsschutzbeauftragten die Möglichkeit gegeben werden, die Ermittlungen überwachen zu können und die Einsicht aller notwendigen Unterlagen.

2.) Wenn öffentliche Sicherheitsorgane Bild- oder Videoaufzeichnung von öffentlichen Orten beabsichtigen, weil gefährliche Angriffe gegen die nationale Sicherheit (z.B. Staatsbesuche, usw.) oder Leben, Gesundheit oder Eigentum von Menschen zu befürchten sind (SPG §54 Abs. 6-7), muss der

Bundesminister für Inneres verständigt werden. Dieser gibt dem Rechtsschutzbeauftragten 3 Tage Zeit, um eine Stellungnahme abzugeben.

3.) Falls durch Verwendung von personenbezogenen Daten Rechte von Betroffenen verletzt wurden, müssen diese umgehend verständigt werden, oder wenn dies aus rechtlichen Gründen nicht möglich ist, muss der Rechtsschutzbeauftragte eine Beschwerde bei der DSK erheben.

4.) Weiters zählt zu seinen Aufgaben die Überwachung der Richtigstellungs- bzw. Löschungsbestimmungen, wenn Daten unsachgemäß aufbewahrt oder unrichtig sind.

5.) Der Rechtsschutzbeauftragte muss jedes Jahr bis spätestens 31. März dem Bundesminister für Inneres einen Bericht über seine Tätigkeiten vorlegen. Der Bundesminister für Inneres leitet den Bericht an den ständigen Unterausschuss des Ausschusses für Inneres zwecks Überprüfung weiter.

2.5 Datenschutzbehörden und Kontrollorgane in der EU

2.5.1 Europäischer Datenschutzbeauftragter

Der Europäische Datenschutzbeauftragte (EDPS European Data Protection Supervisor) wird vom Europäischen Parlament und des Rats für 5 Jahre gewählt. Durch die Ernennung eines Europäischen Datenschutzbeauftragten wurde der Datenschutz aufgewertet, da es nun eine zentrale Stelle für diesen Bereich auch nach außen gibt. Diese Stelle ist sowohl unabhängig als auch weisungsfrei. Zu den Aufgaben des EDPS zählt die Kontrolle der europäischen Organe in punkto Datenschutzfragen als auch eine beratende Funktion für die europäischen Institutionen. Weiters muss der EDPS die aktuellen Entwicklungen beobachten und bewerten, damit er seine beratende Funktion wahrnehmen kann. Neben diesen Aufgaben, übernimmt der EDPS die Koordination mit den nationalen Datenschutzbehörden [EUJ].

Falls durch EU-Behörden oder Institutionen Datenschutzverletzungen passieren, kann jeder einzelner Bürger Beschwerde beim EDPS einbringen. Dieser muss dann binnen 6 Monaten ein Urteil bezüglich dieser Beschwerde fällen. Der Zuständigkeitsbereich des EDPS beruht nur auf Beschwerden gegen EU-Behörden bzw. europäischen Institutionen. Der EDPS ist keine weitere Instanz über den nationalen Datenschutzbehörden. Somit sind in Österreich weiterhin bei Beschwerden über Auftraggeber im privaten oder öffentlichen Bereich die DSK bzw. die jeweiligen Gerichte zuständig und nicht der EDPS.

2.5.2 Art. 29 Datenschutzgruppe

Diese Gruppe wurde mit dem Beschluss der Richtlinie 95/46/EG (Datenschutzrichtlinie) im Artikel 29 gegründet. Sie besteht aus jeweils einem Vertreter der nationalen Kontrollstellen, einem Vertreter der europäischen Organe bzw. Institutionen sowie einem Vertreter der Europäischen

Kommission. Die Zielsetzung für diese Datenschutzgruppe ist es, Sachverständigenbeiträge bezüglich Fragen des Datenschutzes für die Mitgliedsstaaten durchzuführen. Weiters soll die Datenschutzgruppe die einheitliche Anwendung der allgemeinen Grundsätze bezüglich Datenschutzes fördern. Ein weiteres wichtiges Ziel der Datenschutzgruppe ist es, die Europäische Kommission bezüglich der Rechten und Freiheiten der natürlichen Personen in punkto Verarbeitung der personenbezogenen Daten zu beraten und Empfehlungen diesbezüglich auszuarbeiten. Neben diesen Empfehlungen wird auch jedes Jahr ein Bericht veröffentlicht, der den Status des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten aufzeigt. Weiters sind alle Aufgaben bzw. Ziele der Art. 29 Datenschutzgruppe in den Art. 30 der Richtlinie 95/46/EG sowie in Artikel 14 der Richtlinie 97/66/EG dokumentiert.

3 Staatliche Überwachung in Österreich

In diesem Kapitel werden relevanten Sicherheitsbehörden in Österreich, Klassifikation von Überwachungsmaßnahmen sowie die Arten der Überwachungsmaßnahmen erörtert. Zuerst möchte ich die befugten Sicherheitsbehörden mit Überwachungskompetenzen beleuchten.

3.1 Sicherheitsbehörden

Unter der staatlichen Überwachung versteht man die fortgesetzte Überprüfung von Personen, Sachen und Vorgängen durch die Sicherheitsbehörden. In Österreich sind folgende Sicherheitsbehörden mit Überwachungskompetenzen ausgestattet:

- Sicherheitspolizei
- Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT)
- Abwehramt (AbwA)

Die Sicherheitspolizei hat als Zielsetzung die Aufrechterhaltung der öffentlichen Sicherheit, Ruhe und Ordnung (§3 SPG). Die Struktur und Befugnisse der Sicherheitsbehörden (und im speziellen der Sicherheitspolizei) sind im SPG definiert. Die Organe der Sicherheitspolizei bestehen aus der Bundespolizei, der Gemeindewachkörper und der rechtskundigen Dienste. Die Organe der Sicherheitspolizei sind unterstellt dem Bundesministerium für Inneres. Damit ist das Bundesministerium für Inneres die oberste Sicherheitsbehörde (§4 SPG). Jene Organisationseinheiten im Bundesministerium für Inneres, die Angelegenheiten der Sicherheitsverwaltung durchführen, bilden die Generaldirektion für die öffentliche Sicherheit. (§6 SPG).

Eine weitere wichtige Säule der Sicherheitsverwaltung in Österreich bildet das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT), das den zivilen österreichischen Inlandsgeheimdienst darstellt. Vor 2002 gab es kein zentrales Bundesamt für die Terrorabwehr in Österreich, sondern nur eine Sondereinheit im Bundesministerium für Inneres genannt EBT (Einsatzgruppe zur Bekämpfung des Terrorismus). Aufgrund der Zunahme der Terroranschläge weltweit und im speziellen die Ereignisse um den 11. September 2001 wurde 2002 die Neustrukturierung der österreichischen Terrorabwehr beschlossen. Als Ergebnis wurde das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) im Bundesministerium für Inneres eingerichtet. In diesem neuen Bundesamt wurde die Staatspolizei sowie die Sondereinheiten EDOK (Einsatzgruppe zur Bekämpfung der organisierten Kriminalität) und EBT zusammengefasst. Die Gesetzesgrundlage für das neu eingerichtete Bundesamt bildet das SPG.

Das BVT arbeitet eng mit den beiden Nachrichtendiensten des Bundesheeres zusammen, da natürlich diese gewonnen Informationen für das BVT auch sehr wichtig sind. Die beiden Nachrichtendienste sind das Heeresnachrichtenamt (HNA) und das Abwehramt (AbwA), die dem Bundesministerium für

Landesverteidigung unterstellt sind. Das HNaA ist der Auslandsnachrichtendienst, der Informationen über militärische Vorgänge beschafft und auswertet. Das HNaA wurde in der oben angeführten Auflistung nicht erwähnt, da dieser Nachrichtendienst keine rechtliche Befugnis hat, im Inland zu agieren.

Genau diese Aufgabe obliegt dem AbwA, dem militärischen Inlandsnachrichtendienst des österreichischen Bundesheeres. Der AbwA soll Angriffe auf militärische Einrichtungen im Inland verhindern bzw. aufklären und ist für den militärischen Schutz in Österreich zuständig. Im Gegensatz zum HNaA ist somit der AbwA im Inland tätig, und übernimmt Überwachungsmaßnahmen im militärischen Bereich. Durch das Militärbefugnisgesetz (MBG) von 2001 ist das AbwA ermächtigt, im Inland verdeckt zu ermitteln bzw. Überwachungsmaßnahmen, wie Lauschangriff oder Videoüberwachung durchzuführen, wenn „Zwecke der nachrichtendienstlichen Aufklärung“ erfüllt werden. Wie schon oben erwähnt, werden natürlich Ergebnisse der Überwachungsmaßnahmen an das BVT weitergeleitet, wenn diese für die Terrorismusbekämpfung relevant sind. Beispiele für geheime Überwachungsmaßnahmen des AbwA sind im Jahre 2009 in den Schlagzeilen aufgetaucht. So wurden z.B: Nationalratsabgeordnete im Juni 2009 bei einer Diskussionsveranstaltung zum Thema "Wohin bringt uns der Eurofighter? Österreichs Verteidigungspolitik in der EU – regional und international" überwacht. Im November wurde zusätzlich veröffentlicht, dass das AbwA die Subversiv Messe in Linz im Mai dieses Jahre überwacht hat. Bei dieser Messe handelt es sich um Fachmesse für Gegenkultur und Widerstandstechnologie, die das Interesse der Geheimagenten des AbwA erweckte. Beide geheimen Überwachungsmaßnahmen wurden durch Mitarbeiter des Magazins „Profil“ aufgedeckt.

3.2 Unterscheidung von Überwachungsmaßnahmen (Klassifikation)

3.2.1 Arten der Überwachungsmaßnahmen

Überwachungsmaßnahmen können auch nach der Art der eingesetzten Technologien unterschieden werden. Laut [GÖD] kann man diese in 3 Klassen einteilen:

- Akustische Überwachung
- Optische Überwachung
- Überwachung durch elektronische Datenerfassung und –auswertung

Diese 3 Arten bzw. Klassen werden näher im Kapitel 3.3 Arten von Überwachungsmaßnahmen beleuchtet.

3.2.2 Zielsetzung der Überwachungsmaßnahmen

Bezüglich der Zielsetzung der Überwachungsmaßnahmen kann man zwischen der präventiven und der repressiven Überwachung unterscheiden. Unter der repressiven Überwachung versteht man jene Überwachung, die innerhalb eines Strafverfahrens zwecks Beweissicherung angewendet wird. Im Gegensatz dazu gibt es die präventive Überwachung, die angewendet wird, bevor die eigentliche Straftat begangen wird, um diese zu verhindern. Die meisten Sicherheitsbehörden setzen natürlich beide Zielsetzungen ein, wobei natürlich der Schwerpunkt je nach Sicherheitsbehörde unterschiedlich ist.

3.2.3 Überwachung innerhalb des Wohnraumes vs außerhalb des Wohnraumes

Weiters kann man unterscheiden, ob Überwachungen an öffentlichen Örtlichkeiten (bzw. auch in allgemein zugänglichen Büro- und Geschäftsräumen) oder aber in Wohnungen vollzogen werden. Wohnungen haben hier eine Sonderstellung, da dies für jeden Berechtigten die Stätte seines Lebens und Wirkens (Privatsphäre) darstellt. Diese Unterscheidung wird auch die Begrifflichkeiten „Kleiner“ bzw. „Großer“ Lauschangriff verwendet (siehe Kapitel 3.3.1.1 Exkurs Lauschangriff in Österreich).

3.2.4 Offizielle vs. inoffizielle Überwachung

Der Unterschied hier liegt darin, ob die Überwachungsmaßnahme rechtlich legitimiert (durch ein Gesetz) ist oder nicht. Einerseits kann eine inoffizielle Überwachung sein, wenn Behörden nicht genehmigte bzw. gesetzeswidrige Überwachungsmaßnahmen durchführen. Andererseits gibt es auch inoffizielle Überwachungen im privaten Bereich. Hier spricht man dann von inoffiziellen Überwachungen, wenn z. B. privatwirtschaftliche Unternehmen Industriespionage betreiben oder Privatdetektive verdeckte Überwachungsmaßnahmen nachgehen, die rechtlich nicht legitimiert sind.

3.3 Arten von Überwachungsmaßnahmen

Aufgrund des enormen Fortschritts in der Technik, der speziell in den letzten Jahren vollzogen wurde, gibt es eine Vielzahl an Technologien, die für Überwachungsmaßnahmen genutzt werden. Wie bereits erwähnt, kann man diese Technologien in 3 Hauptklassen einordnen. Diese lauten Akustische Überwachung, Optische Überwachung und Überwachung durch Datenerfassung und –auswertung. Die einzelnen Möglichkeiten (Technologien) in den Arten der Überwachungsmaßnahmen sind in der nächsten Tabelle aufgelistet.

Art der Überwachung:	Möglichkeiten/Technologien:
Akustische Überwachung	Übertragung durch Schall

	Mikrofone („Wanzen“), Richtmikrofone
	Infrarot-Laser zum Abtasten von Körperschwingungen
	Abhören von analogen Funkgeräten bzw. Türsprechanlagen
	Abhören von Telefon- und Mobiltelefongesprächen
Optische Überwachung	Fotoapparate
	Mini-Kameras (Körper bzw. Gegenständen angebracht)
	Stationäre bzw. mobile Video-Kameras
	Computerprogramme (Analyse von Bilder bzw. Videos)
Datenerfassung und -auswertung	Überprüfung von Telefon- und Internetverbindungsdaten („Vorratsdatenspeicherung“)
	Erstellung von Bewegungsprofilen (Ortung Mobiltelefons bzw. GPS-Geräten)
	Überprüfung/Analyse von finanziellen Daten (Kreditkarten)
	Überwachung von Daten aus Funknetzwerken (WLAN, Bluetooth, RFID)
	Überwachung von Internet-Foren und Websites (rechtswidrige Inhalte)

Tabelle 2: Überblick Arten von Überwachung

In den nächsten Subkapiteln werden die einzelnen Möglichkeiten pro Art der Überwachung erläutert.

3.3.1 Akustische Überwachung

Das Ziel der akustischen Überwachung ist es, die verbale Kommunikation zwischen Menschen an öffentlichen oder nicht-öffentlichen Orten mit technischen Mitteln abzuhören bzw. aufzuzeichnen. Hierbei ist die einfachste Methode zur Überwachung von akustischen Signalen die Übertragung durch den Luftschall. Unter Luftschall wird im engeren Sinn der Frequenzbereich des menschlichen Gehörs gesehen. Der Frequenzbereich des menschlichen Gehörs liegt zwischen 16 Hz und 20 kHz. Dieses Abhören von Gesprächen passiert ohne elektronische Übertragungswege und stellt somit die „klassische“ Methode des Abhörens dar, die schon seit Jahrhunderten angewandt wird. Bei dieser Methode bestehen aber die Nachteile, dass einerseits eine bestimmte Nähe zum Überwachungsobjekt vorhanden sein muss und andererseits Störfaktoren, wie andere Geräusche, vorhanden sind.

Als Meilenstein für die akustische Überwachung kann die Erfindung des Mikrofons gesehen werden. Hierbei ist es möglich, akustische Signale über größere Distanzen zu übertragen, ohne größere Störeinflüsse zu haben. Die Entwicklung des Mikrofons ging Hand in Hand mit der Erfindung des Telefons.

Ein Mikrofon stellt einen Schallwandler dar, der den Luftschall in elektrische Spannungsänderungen (so genannten Mikrofonsignal) umwandelt. Da die Technologie in diesem Sektor schnell vorangeschritten ist, werden heute sehr kleine Mikrofone (auch genannt „Wanzen“) für Überwachungsaktivitäten eingesetzt. Da diese Mikrofone sehr klein sind können sie fast überall unbemerkt angebracht werden und können somit ideal für eine heimliche Wohnraumüberwachung oder für ein Mitschneiden einer Observation verwendet werden. Um das aufgenommen akustische Signale zum Empfänger zu übertragen, gibt es verschiedene Möglichkeiten der Übertragung: Kabel- (auch über Trägerfrequenzanlagen), Funk- und optoelektronische Verbindungen ((Lichtwellenleiter wie z. B. Glasfaserkabel). Somit kann man eine Unterscheidung zwischen Drahtlosen bzw. Drahtgebundenen Mikrofonsystemen durchführen. Drahtlose Mikrofonsysteme werden dadurch eher bei Observationen eingesetzt, wo die Räumlichkeiten nicht in der Gewalt des Abhörers sich befinden (wie z.B: Wohnraumüberwachung) oder die Überwachung sich über mehrere Örtlichkeiten erstreckt (Verfolgung). Hierbei werden als Funkfrequenz UHF- bzw. VHF-Frequenzen eingesetzt. Drahtgebundene Mikrofonsysteme werden somit eher dann eingesetzt, wenn eine dauerhafte Installation des Mikrofonsystems notwendig ist bzw. die Räumlichkeiten sich in der Gewalt des Abhörers befinden. Eine spezielle Art des Mikrofons stellt das Richtmikrofon dar. Dieses spezielle Mikrofon nimmt primär den frontal eintreffenden Schall auf. Dadurch dass der Schall aus anderen Richtungen nur gedämpft aufgenommen wird, können Richtmikrofone die Sprachverständlichkeit bei einer lauten Umgebung verbessern. Aufgrund der Abschirmwirkung aus anderen Richtungen, wird das Richtmikrofon im speziellen für das Abhören von Gesprächen aus größeren Entfernungen (bis zu 100 Meter) eingesetzt. Jedoch kann es auch hier aufgrund von Störfaktoren, die den Schall blockieren, zu Problemen beim Abhören kommen.

Eine weitere Möglichkeit der akustischen Überwachung besteht darin, Schallwellen aufgrund von Schwingungen der Objekte in ihrer Nähe zu rekonstruieren. Damit ist gemeint, dass jede Schallwelle die Körper in ihrer unmittelbaren Umgebung auch in Schwingungen versetzt. Diese Art von Schwingungen der Körper wird auch „Körperschall“ genannt. Ein Beispiel für diese Art der Überwachung wäre, dass mit Hilfe eines Lasermikrofons eine Wohnraumüberwachung durchgeführt wird. Der Infrarot-Laser des Lasermikrofons wird auf das Fenster, der zu observierenden Wohnung, gerichtet. Der Infrarot-Laser registriert die Schwingungen der Fensterscheibe und kann somit diese wieder in Schallsignale umwandeln und die Schallinformation rekonstruieren.

Neben dem Abhören von analogen Funkgeräten wie z.B. Schnurlos-Telefonen oder Walki-Talkies oder dem Abhören von Türsprechanlagen, ist die Überwachung von Telefonen und Mobiltelefonen in den letzten Fokus der staatlichen Sicherheitsbehörden gerückt. Um Telefongespräche im Festnetz abzuhören, werden die Glasfaserleitungen bzw. Multiplexanschlüsse angezapft. Dies ist effektiver als so genannte „Wanzen“, da nur die Gespräche am Telefon mitgeschnitten werden und nicht noch weitere Geräusche. Der Vorteil darin

liegt, dass somit ein Abhören auf Anschlusskennung möglich ist und eine genauere Analyse der Sprachmerkmale möglich ist.

Aufgrund des fulminanten Anstiegs der Mobilfunk-Telefone (Mobiltelefons) und dem Abstieg an Festnetz-Anschlüssen, ist natürlich das Interesse der Sicherheitsbehörde bezüglich der Überwachung von Mobiltelefonen enorm. Hierfür werden so genannte IMSI-Catcher („International Mobile Subscriber Identity“ - netzinterne Teilnehmerkennung) eingesetzt, um Mobiltelefon-abzuhören bzw. aufzuzeichnen. Die Funktionsweise des IMSI-Catcher beruht auf einer Schwachstelle des GSM-Netzes. Zwar authentifiziert sich das Mobiltelefon gegenüber dem Mobilfunknetz, aber nicht das Mobilfunknetz gegenüber dem Mobiltelefon. Der IMSI-Catcher simuliert hierbei ein Mobilfunknetz (Funkzelle) und hier melden sich die Mobiltelefone in dieser neuen Funkzelle an. Somit bekommt der IMSI-Catcher die International Mobile Subscriber Identities der Mobiltelefons, die sich in seiner Funkzelle angemeldet haben. Neben der Ortung des Mobiltelefon-Benutzers ist es auch möglich mit dem IMSI-Catcher Gespräche abzuhören und mitzuschneiden. Die genauere Funktionsweise bzw. Einsatzmöglichkeiten des IMSI-Catcher werden im Kapitel 5.1 IMSI-Catcher näher erläutert.

3.3.1.1 *Exkurs Lauschangriff in Österreich*

In diesem Exkurs möchte ich näher auf den Lauschangriff eingehen, da dieser auf akustische als auch optische Überwachung auf Personen mit Hilfe von technischen Mitteln abzielt. Der Lauschangriff wurde 1997 mit dem §149d StPO eingeführt und wurde somit als neue Form der Beweisgewinnung für die Strafverfolgungsbehörden eingeführt. Unter dem Begriff Lauschangriff versteht man, dass die Polizei und Staatsanwaltschaft befugt sind, Wohnungen als intimsten Bereich des Menschen zu überwachen. In anderen Ländern, wie z.B.: Deutschland wurde unterschieden zwischen „kleinen Lauschangriff“ und dem „großen Lauschangriff“. Der Unterschied besteht darin, dass beim „kleinen Lauschangriff“ außerhalb von Wohnungen überwacht werden durften, d.h. öffentliche Einrichtungen oder allgemein zugänglich Büro- oder Geschäftsbereiche. Im Gegensatz zu diesen Ländern, wurde in Österreich gleich der „große Lauschangriff“ unter dem Titel „Lauschangriff“ eingeführt. In Österreich ist als Kontrollinstanz für die Rechtmäßigkeit des Lauschangriffs der Rechtsschutzbeauftragte im Bundesministerium für Inneres. Aufgrund von Bedenken gegen den Eingriff der Privatsphäre wurde der Lauschangriff in Österreich nur unter Probe eingeführt. Die erste große Aktion in punkto Lauschangriff war 1999 die „Operation Spring“, in der mit Hilfe von akustischen und optischen Überwachungsmaßnahmen Observationen durchgeführt wurden, um gegen den Drogenhandel aktiv zu werden. Die zu dieser Zeit größte kriminalpolizeiliche Operation, rief massiven Widerstand, gegen die Methoden des Lauschangriffs hervor. Aufgrund der schlechten Qualität der akustischen und optischen Aufzeichnungen, wurde die Rechtmäßigkeit als Beweislage von diversen Datenschutzverbänden als auch Menschenrechtsorganisationen in Frage gestellt. Trotz dieser massiven Bedenken ist zur heutigen Zeit, der Lauschangriff als Instrument zur Verbrechensbekämpfung unumstritten.

3.3.2 Optische Überwachung

Optische Überwachungsmaßnahmen sind aufgrund der Entwicklung der Technologien in diesem Bereich auf dem Vormarsch. Mussten früher hauptsächlich Personen zur Observierung von Objekten eingesetzt werden, übernehmen dies heute Video- bzw. Fotokameras. Die Zielsetzung für die optische Überwachung ist es durch Fotos oder Videos Informationen über die überwachten Objekte zu gewinnen. Im speziellen ist durch die Miniaturisierung der Videokameras die Möglichkeit geschaffen worden, dass diese Überwachungsmaßnahmen unbemerkt installiert werden können. Dies kann einerseits geschehen, dass Observationen mit Mini-Kameras an der Kleidung durchgeführt werden oder dass diese in Alltagsgegenständen bei der zu observierenden Person eingebaut werden. Weiters ist auf dem Vormarsch das Installieren von stationären Kameras an öffentlichen Orten. Diese werden z.B: in U-Bahnen, bei U-Bahn Stationen oder an stark frequentierten Plätzen eingesetzt, um die öffentliche Sicherheit zu gewähren. Neben diesen stationären Kameras werden aber auch oft mobile Kameras eingesetzt, die z.B: an Fahrzeugen oder Hubschraubern montiert sind. Mit diesen optischen Überwachungstechnologien kann natürlich das menschliche Auge nicht mithalten. Mit den heutzutage eingesetzten Videokameras können Spektralbereiche des Lichtes erfasst werden, die für das menschliche Auge nicht erkennbar wären. Beispiele hierfür wären Wärmebildkameras, die einen menschlichen Körper in einem Versteck ausfindig machen können, oder Infrarot-Kameras, die auch bei Dunkelheit eingesetzt werden können. Zunehmend werden auch Computerprogramme für die Analyse von Bildern bzw. Videos eingesetzt. Hierbei wird versucht, abgebildete Objekte zu erkennen bzw. zu identifizieren. Ein Beispiel hierfür wären Biometrie-Systeme.

3.3.3 Überwachung durch Datenerfassung und -auswertung

Die dritte Art, Kommunikation und Interaktion zwischen Menschen zu überwachen, ist die Datenerfassung und deren Analyse. Da die Kommunikation zwischen Menschen immer häufiger auf elektronischen Weg ausgetauscht wird, ist diese Art der Kommunikation immer mehr Ziel der Überwachungsmaßnahmen. Da die technische Entwicklung in der Informationstechnologie immer schneller vorangeht, ist es für den Gesetzgeber besonders schwer mitzuhalten, da teilweise rechtliche Grauzonen herrschen. Beispiele für diese neuen Betätigungsfelder der Sicherheitsbehörden wären die Überwachung von Internetforen und privaten Internetseiten in Bezug auf rechtswidrige Inhalte, wie z.B.: Kinderpornografie oder Rechtsextremismus). Wie schon im Kapitel 3.3.1 Akustische Überwachung angemerkt, ist ein weiteres Ergebnis der Überwachungsmaßnahmen das Erstellen von Bewegungsprofilen. Diese können aufgrund von Mobiltelefons, die sich automatisch in neue Mobilfunkzellen einwählen, erstellt werden. Bewegungsprofile lassen sich aber nicht nur durch Mobiltelefons erschließen, sondern auch durch GPS-Empfänger, die in vielen Geräten eingebaut sind, anfertigen. Neben diesen Feldern der Datenerfassung und -auswertung ist

speziell in den letzten Jahren, das Schlagwort „Vorratsdatenspeicherung“ gefallen. Diese Richtlinie (siehe Kapitel 2.3.2.3 Richtlinie 2006/24/EG (Vorratsdatenspeicherung)) sieht vor die Erfassung der Verbindungsdaten von Telefonanschlüssen, Internetanschlüssen, E-Mail Verkehr und Internet-Telefonie. Hierbei sollten nur Verkehrs bzw. Standortdaten gespeichert werden, jedoch keine Inhaltsdaten.

Immer häufiger sind auch finanzielle Daten Teil der Überwachung. Das Ziel hierfür ist, durch die Überprüfung von Kontobewegungen von Kreditkarteninhabern, zum Beispiel Konsumenten von Kinderpornographie, zu entlarven. Neben diesen Daten werden in einigen Ländern der Europäischen Union so genannte „Kontenabrufverfahren“ eingesetzt. Durch dieses Verfahren wird ermöglicht, dass Kontostammdaten abgerufen werden können, und somit Rückschlüsse auf die Vermögensverhältnisse der Person bzw. Firma gezogen werden können.

Ein weiteres Feld der Datenerfassung ist das Abfangen von Daten aus Funknetzwerken, wie Wireless Local Area Network (WLAN) oder Radio Frequency Identification (RFID). Die übertragenen Daten in diesen Funknetzwerken werden zwar meistens verschlüsselt, aber die Daten können trotzdem abgefangen, gespeichert und später entschlüsselt werden.

Aufgrund der steigenden Anzahl an Straftaten die einerseits im Internet geplant bzw. durchgeführt werden, wird die generelle Überwachung des Netzes gefordert. Dies spiegelt sich in jenem Maße nieder, dass die Sicherheitsbehörden fordern, Computer durch Einsatz von Spionagesoftware heimlich zu überwachen. Dies hätte zur Folge, dass E-Mails bzw. Dokumente von einem Rechner gelesen oder manipuliert werden könnten oder jeglicher Datenaustausch überwacht werden könnte.

4 SPG Novelle 2008

4.1 Einleitung und Gesetzestexte

Durch diese Novelle von 2008 sind die Sicherheitsbehörden berechtigt, von Providern von öffentlichen Telekommunikationsdiensten Auskunft über IP-Adressen zu einer bestimmten Nachricht und den genauen Zeitpunkt der Übermittlung zu verlangen. Dies darf nur geschehen, wenn Tatsachen die Annahmen der konkreten Gefahrensituation rechtfertigen und sie diese Daten als Grundlage für die Erfüllung ihrer Aufgaben nach dem Sicherheitspolizeigesetz benötigen. Weiters wurde dadurch ermöglicht, dass ohne richterlichen Beschluss, Standortabfragen eines Mobiltelefonbenutzers durchgeführt werden können. Gesprächsaufzeichnung müssen aber weiterhin von einem Richter beantragt werden. Standortabfragen und Gesprächsaufzeichnung werden über so genannte IMSI-Catcher durchgeführt. Deswegen wurde im §53 Zulässigkeit der Verarbeitung Absatz 3a neu geregelt und um einen weiteren Absatz 3b ergänzt (bisherige Absatz 3b wurde zu 3c). Hier eine genaue Gegenüberstellung der alten Fassung mit dem neuen Gesetzestext der Novelle von 2007 (114/2007):

SPG §53 Abs.3 vor Novelle 114/2007:

„(3a) Die Sicherheitsbehörden sind berechtigt,

- von den Betreibern öffentlicher Telekommunikationsdienste

Auskunft über

Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses zu verlangen, wenn sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen.

Die Bezeichnung dieses Anschlusses 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 des Zeitpunktes und der passiven Teilnehmernummer erfolgen.

Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen.“

SPG §53 Abs.3 (Novelle 114/2007):

(3a) Die Sicherheitsbehörden sind berechtigt,

- von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 - TKG 2003, BGBl. I Nr. 70) und

- sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz - ECG, BGBl. I Nr. 152/2001)

Auskunft zu verlangen über

1. Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses, (Z1)¹

2. Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung sowie (Z2)

3. Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war (Z3)

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. (Satz 2)

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. II Nr. 322/2004, zu erteilen.[WKO] [I4J4]

¹Z1 bedeutet Zeile 1. Dies ist relevant, da ich später immer auf die einzelnen Zeilen verweise.

Bevor im nächsten Kapitel die einzelnen Befugnisse des § 53 erörtert werden, müssen die Voraussetzungen beleuchtet werden. Als Voraussetzung für die Befugnisse sind hier anzusehen, dass „bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen“ sowie, dass Sicherheitsbehörden „diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen“. Bei der ersten Voraussetzung ist anzumerken, dass eine „konkrete Gefahrensituation“ vorherrschen muss. Somit ist wie in § 16 Abs. 1 SPG nicht die „allgemeine Gefahr“ gemeint. Ob bestimmte Tatsachen die Annahme einer derartigen Gefahrensituation rechtfertigen, ist im Einzelfall zu hinterfragen. Namhafte Autoren kritisieren generell die Feststellung „Annahme“ einer „konkreten Gefahrensituation“ als Widerspruch in sich [KUN]. In dem Erlass vom BMI bezüglich der SPG-Novelle ist zu lesen, dass solche Tatsachen bzw. Hinweise auf sicherheitspolizeiliche Aufgaben schließen lassen. Hierbei werden als Beispiele Selbstmordankündigungen in Intern-Foren sowie Hinweise auf strafbare Handlung im Bereich der Kinderpornographie angeführt.

Bei der zweiten Voraussetzung, dass die an die Sicherheitsbehörden zu übermittelnden Daten eine „wesentliche Voraussetzung“ für die Erfüllung einer der Aufgaben nach dem SPG darstellen, ist festzuhalten, dass hierbei der Grundsatz der allgemeinen Verhältnismäßigkeit (§ 29 SPG) sowie der Vorrang nicht eingreifender Mittel (§ 28a Abs. 3 SPG) betont wird [DHO].

Die Befugnisse des §53 SPG erstrecken sich sowohl auf die Erfüllung der ersten allgemeinen Hilfeleistungspflicht (§19 SPG), der Aufrechterhaltung der öffentlichen Sicherheit §20 bis § 26 SPG), der Aufrechterhaltung der öffentlichen Ordnung (§27 SPG) als auch im Bezug des Rahmen des besonderen Überwachungsdienstes (§ 27a SPG) [HKE]. Der nächste wichtige Punkt ist die Auskunftspflicht. Hier wird in der SPG Novelle festgehalten, dass von der Auskunftspflicht Betreiber öffentlicher Telekommunikationsdienste sowie sonstige Dienstanbieter nach §3 Z2 ECG betroffen sind. *Betreiber eines öffentlichen Kommunikationsdienstes nach § 92 Abs. 3 Z1 TKG 2003 ist, wer einer breiten Öffentlichkeit eine gewerbliche Dienstleistung anbietet, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze besteht* [ZAN]. Da in der Novelle von Telekommunikationsdienst gesprochen wird und nicht von Kommunikationsdienst, kann angenommen werden, dass der Bereich des Rundfunks ausgenommen wird. Somit können zu den öffentlichen Telekommunikationsdiensten insbesondere die Internet Access Provider sowie Telefon- bzw. Mobilfunkanbieter gezählt werden.

Neben den Betreibern öffentlicher Telekommunikationsdienste sind in der SPG-Novelle sonstige Dienstanbieter angeführt. Diese sind entweder natürliche oder juristische Personen, die einen Dienst der Informationsgesellschaft anbieten. Hierzu zählen unter anderem Internet Access Provider (§ 13 ECG), Suchmaschinen Betreiber (§14 ECG) oder Hosting Provider (16 ECG). Im E-Commerce Gesetz ist geregelt, dass ein Dienst der Informationsgesellschaft in der Regel gegen Entgelt zu verstehen ist (§3 ECG). Dies ist so zu verstehen, dass eine Ertragsabsicht bei Dienst vorliegen muss. Beispiele hierfür wären

einerseits eine Website eines Unternehmens oder eine private Website mit Werbeeinblendungen.

4.2 Befugnisse des §53 Abs. 3a Z1 und § 53 Satz 2 SPG

Die Z1 setzt fest, dass die Auskunft über „Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses“ verlangt werden kann. Diese Regelung ist keine Erneuerung sondern ist auch schon vor der Novelle im SPG gestanden. Im §3 des TKG 2003 wird der Begriff des Teilnehmeranschluss genau definiert. Der Teilnehmeranschluss ist als die „physische Verbindung“ zu verstehen, mit der der Netzanschluss in den Räumlichkeiten des Teilnehmers an den Hauptverteilerknoten bzw. gleichwertige Einrichtungen im festen öffentlichen Telefonnetz verbunden ist. Diese Informationen über den Inhaber des Teilnehmeranschlusses können die Betreiber der öffentlichen Telekommunikationsdienste bieten. Damit die Erfüllung der allgemeinen Hilfeleistungspflicht bzw. Abwehr von gefährlichen Angriffen nachgekommen wird, muss nicht unbedingt die Anschlusskennung bekannt sein, sondern es reicht gegenüber dem Auskunftspflichtigen den möglichst genauen Zeitraum sowie die passive Teilnehmernummer zu nennen. Hier spricht man dann von der so genannten „kleinen passiven Rufdatenrück Erfassung“ [POW]. Somit ist es möglich, die Identität des Betroffenen zu ermitteln, indem die vom Betroffenen angerufene Teilnehmernummer sowie den möglichst genauen Gesprächszeitraum bekannt gegeben wird. Hier muss nun aber hinterfragt werden, wie der Begriff „von einem Anschluss aus geführtes Gespräch“ ausgelegt werden kann. Ist hier nur der Bereich der klassischen Sprachtelefonie erfasst, oder auch Voice over IP?

Wie im EBRV zu §92 TKG 2003 [I4J2] nachzulesen ist, wird unter der Teilnehmernummer die reine Teilnehmernummer im Telefonbereich verstanden. Bei Voice over IP-Adressen oder verwendeten statischen IP-Adressen wird nicht von Teilnehmernummer sondern von „sonstigen Kontaktinformationen“ gesprochen. Würde man IP-Adressen als Teilnehmernummern auslegen, würde dies in der Novelle als redundant angesehen werden. In der Z3 als auch Z1 würde man von IP-Adressen sprechen. Somit kann festgehalten werden, dass die Befugnis des §53 Abs. 3a Satz 2 SPG sich ausschließlich auf den klassischen Telefonbereich und nicht auf Voice over IP Dienste, wie z.B.: Skype bezieht. Abschließend ist zum Thema „kleine passive Rufdatenrück Erfassung“ zu bemerken, dass dies schon in der alten Fassung des SPG möglich war und aufgrund der erhobenen Unterlagen es sich im Größenbereich von 1000 Abfragen pro Jahr handelt (Bemerkungen zum Abänderungsantrag von Hrn. Parnigoni und Hrn. Kößl).

Im Vergleich zur alten Fassung gab es noch eine weitere Änderung im Bezug auf §53 Abs. 3a Satz 2. Bei der alten Fassung wurde noch die Bezeichnung eines „Zeitpunktes“ gefordert. In der neuen Fassung war nur mehr die Rede von einem „möglichst genauen Zeitpunkt“. Bezüglich dieser Änderung wurde aber festgehalten, dass der Zeitraum nicht mehr als eine Stunde sein darf [TVO].

4.3 Befugnis des §53 Abs. 3a Z2 SPG

Hier ist einleitend zu sagen, dass mit dem §53 Abs. 3a Z2 SPG die Befugnis geschaffen wurde, dass Auskunft über die (statische oder dynamische) IP-Adresse (und den Übermittlungszeitpunkt) „zu einer bestimmten Nachricht“ verlangt werden kann. Durch die Z3 ist es somit den Behörden möglich, aufgrund der erlangten IP-Adresse zum Übermittlungszeitpunkt auch die Identität des Betroffenen zu ermitteln.

4.3.1 Allgemein

Mit der Befugnis des §53 Abs. 3a Z2 ist es den Behörden möglich, IP-Adresse zu einer bestimmten Nachricht sowie deren Übermittlungszeitpunkt zu verlangen. Dies geschieht ohne, dass der Auskunftspflichtige einen Kostenersatz stellen darf sowie der Betroffene darüber informiert werden muss. Hierbei muss dieser Paragraph auf etwaige Verletzungen gegenüber vorhandenem Recht untersucht werden. In den späteren Kapiteln wird untersucht, ob aufgrund des Eingriffs das geschützte Recht auf Achtung des Privat- und Familienleben, das Grundrecht auf Datenschutz (§1 DSG2000), Eingriff in das Fernmeldegeheimnis (Art 10a StGG) sowie die Verletzung des Gleichheitssatzes in Bezug auf den fehlenden Kostenersatz verletzt wird. Neben diesen Punkten möchte ich hier auch die einzelnen Begriffe, wie „Nachricht“, „Bestimmbarkeit der Nachricht“, „zu übermittelnde Daten“ usw. beleuchten.

Bevor diese Punkte untersucht werden, muss natürlich die Frage nach dem Zweck des §53 Abs. 3a Z2 gestellt werden. Eine Möglichkeit wäre, dass der Gesetzgeber aufgrund dieser Befugnis versuchen will, die Auskunft über die Absender IP-Adressen einer Mail zu bekommen. Da dies die häufigste Form der Kommunikation ist, wäre dies ein denkbar möglicher Zweck. Beispiele hierfür wären, dass per E-Mail eine Bombendrohung eingegangen ist, oder ein Bekennerschreiben einer terroristischen Organisation eingelangt ist. Wenn dies der Beweggrund des Gesetzgebers war, dann wirft dies aber eine berechtigte Kritik auf: In nahezu jeder E-Mail wird bereits die IP-Adresse des Absenders mitgeschickt. Beim Erhalt einer E-Mail fügt der Mail Server einen „Received Header“ ein, indem er angibt, von welchem Computersystem er die E-Mail erhalten hat. Dies geschieht nur bei E-Mail Server die das Simple Mail Transfer Protokoll (SMTP) verwenden [RFC1]. Wird jedoch nicht SMTP sondern Hypertext Transfer Protocol (HTTP) verwendet (z.B.: Webmail Service), dann gibt es keinen Standard, dass IP-Adressen des Absenders in einem Received Header angewandt wird. In der Regel verwenden aber auch namhafte Webmail Provider, wie Hotmail oder Yahoo auch die IP-Adresse des Absenders in einem Mail-Header. Hier gibt es zum Beispiel neben dem Received Header Format auch den Header X-Originating-IP, wie es zum Beispiel Hotmail einsetzt. Laut [ZAN] nehmen derzeit gmail sowie die Business Webmail der Telekom Austria keine Mail-Header auf. Wenn aber dies nicht der Zweck für die Novelle sein kann, ist zu hinterfragen, wieso der Gesetzgeber diesen Passus geschaffen

hat. In den nächsten Unterkapiteln wird untersucht ob vielleicht ein anderer Kernbereich intendiert wurde.

4.3.2 Begriff „Nachricht“

Da dem Nachrichtenbegriff eine zentrale Bedeutung in diesem Paragraph 53 zukommt, möchte ich ihn hier näher beleuchten. Hierbei wurde vom Gesetzgeber der nicht näher beschriebene Begriff der „Nachricht“ gewählt. Es stellt sich natürlich hier die Frage, wo die Grenze für eine Nachricht gezogen wird. Bei den folgenden Aufzählungen ist die Frage, ob hier der Gesetzgeber dies auch als „Nachricht“ ansieht: http-Requests (Aufrufen von Websites), Postings auf Message-Boards, Eingaben in Suchmaschinen, ein Video bei youtube.com, Einträge auf Blogs oder Profile bei Communities wie xing.com oder studivz.net. Um hier eine klare Definition zu verwenden, wäre es besser gewesen den Nachrichtenbegriff des TK2003 §92 Abs3 Z10 zu nehmen: den der „elektronischen Post“ [I4J2].

Leider gibt es zwar keine genaue Definition des Nachrichtenbegriffs aber es gibt die Einschränkung in der Novelle, dass es zu der Nachricht eine IP-Adresse geben muss. Dies bedeutet, dass z.B.: eine von einem MS gesendete SMS nicht zu diesem Nachrichtenbegriff laut Z2 zählt da hier nicht das Internetprotokoll verwendet wird. Neben dieser Einschränkung ist auch im Z2 vermerkt, dass es einen Übermittlungszeitpunkt geben muss. Damit ist festzuhalten, dass nur eine bereits übermittelte Information eine Nachricht laut Z2 darstellt. Somit können 3 Fragen bezüglich des nicht näher beschriebenen Begriffs der Nachricht aufgeworfen werden:

- Muss eine Kommunikation zwischen zwei Menschen vorliegen?
- Ist eine Voraussetzung, dass die Nachricht einer beschränkten Anzahl von Empfängern zur Verfügung gestellt wird?
- Muss eine Nachricht einen Gedankeninhalt inkludieren?

Wie schon oben angeführt, stellt sich die Frage, wie der Begriff der Nachricht in punkto Web-Surfen zu verstehen ist. Hier schickt der Anwender eine URL an den Web-Server. Somit besteht keine Mensch zu Mensch-Kommunikation (Web-Server ist keine natürliche Person) und die URL enthält keinen Gedankeninhalt. Der Web-Server übermittelt die Web-Seite zwar sehr wohl mit einem Gedankeninhalt, aber die Seite ist nicht auf eine beschränkte Anzahl von Empfängern limitiert und es besteht weiters keine Kommunikation zwischen 2 Menschen.

Um näher den Begriff der Nachricht zu verstehen, macht es Sinn, diesen Begriff bei anderen Gesetzen wie im TKG oder der StGB zu beleuchten. Diese können zwar nicht eins zu eins übernommen werden, aber es hilft vielleicht zu verstehen, welchen Inhalt der Gesetzgeber gemeint haben könnte.

Im §92 TKG 2003 wird die Begriffsdefinition der Nachricht von der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) hingewiesen. Bei dieser Richtlinie wird der Begriff „Communication“ für

Nachricht verwendet. Hierbei umfasst der Nachrichtenbegriff nicht nur Inhaltsdaten sondern jegliche Form der Information [ZSC]. Weiters ist in der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) und somit auch im TKG 2003 es nicht erforderlich, dass die Nachricht zwischen natürlichen Personen ausgetauscht werden muss. Falls der Gesetzgeber aber den Begriff aus TKG übernehmen wollte, ist dies aus meiner Sicht sehr bedenklich. Somit würde es den Sicherheitsbehörden möglich sein, den Begriff auf die bereits oben ausgeführten Dienste (http-Requests, usw.) auszuüben. Man hätte hier die Möglichkeit festzustellen, wer zu einem bestimmten Zeitpunkt eine Web-Seite aufgerufen hat, welches Foto auf eine Plattform geladen hat oder ob ein bestimmtes Buch gekauft wurde. Da die Daten als sensibel anzusehen sind, weil man Rückschlüsse auf politische Überzeugungen, religiöses Bekenntnis bzw. das Sexualleben des Betroffenen gezogen werden können, ist dies als besonders problematisch anzusehen.

In einem anderen Gesetz StGB wurde der Begriff auch im Jahre 2002 eingeführt. In der EBRV [StG] ist nachzulesen, dass unter Nachricht „die Vermittlung von Gedankeninhalt“ beschrieben wird. Wie man hier sieht, ist der Begriff Nachricht in den Gesetzen TKG und StGB unterschiedlich beschrieben und da keine genaue Erläuterung in der Novelle angeführt wurde ist es fraglich, ob der Gesetzgeber sich an einem bestehenden Gesetz orientiert hat oder einen Begriff schaffen wollte. Wie oben schon erwähnt, wäre die Möglichkeit bestanden, dass der Gesetzgeber den Begriff „elektronische Post“ verwendet, wie es z.B.: auch die Wirtschaftskammer Österreich aufgrund eines Gutachtens von Hrn. Mag. Pilz befürworten würde. Somit wäre es eine Einschränkung auf Dienste E-Mail bzw. verschickte SMS aus dem Internet. Dies wurde vom Gesetzgeber ausdrücklich nicht gewählt, sondern der Begriff „Nachricht“. Abschließend möchte ich einen Vorschlag aus dem Buch [ZAN] aufgreifen der den Begriff einer Nachricht einschränken würde:

Zusammenfassend lässt sich der hier vorgeschlagene Nachrichtenbegriff des §53 Abs. 3a Z2 SPG mit fünf Tatbestandsmerkmalen umschreiben:

- *eine Mitteilung einer Gedankenerklärung,*
- *die von einem Menschen*
- *an einen endlichen Kreis anderer Menschen*
- *unter Verwendung des Internet Protocol*
- *bereits übermittelt wurde.*

Auch dieser Vorschlag würde die Abgrenzung bei Problemfällen schwer machen. Wenn z.B.: eine Nachricht bei einem Webmail-Dienst als Entwurf gespeichert ist, ist dies nach dieser Beschreibung nicht als Nachricht zu sehen, da keine Übermittlung an eine andere Person stattgefunden hat. Wenn aber eine dritte Person Zugang zu den Entwürfen hätte, würde dies als Nachricht anzusehen sein. Trotz dieser Grenzfälle finde ich den gerade beschriebenen Ansatz sehr interessant, da es den Begriff Nachricht sehr einschränken würde. Abschließend ist nochmals anzumerken, dass der Gesetzgeber den Nachrichtenbegriff ohne genaue Definition verfasst hat und

daher festzuhalten ist, dass dies aus den oben genannten Punkten als sehr problematisch zu betrachten ist.

4.3.3 Begriff einer „bestimmten“ Nachricht

Im Z2 des SPG ist ausdrücklich von der Auskunft von einer „bestimmten“ Nachricht die Rede. Hierbei muss hingewiesen werden, dass das Wort „bestimmt“ näher untersucht werden muss. Mit dem Wort „bestimmt“ ist die eindeutige Identifizierung der Nachricht gemeint. Wenn aber das Wort „bestimmbar“ verwendet werden würde, dann hieße dies, dass die Identifizierbarkeit aufgrund von Aufwendung weiterer Mittel abhängig wäre [DWP]. Wenn der Gesetzgeber mit bestimmt als „bestimmbar“ auslegen wollte, dann würde dies die Befugnis massiv erweitern, wie das nächste Beispiel zeigen wird. Wenn bei den Sicherheitsbehörden eine Warnung bezüglich eines Bombenattentats von einem ausländischen Geheimdienst vorliegen würde, dann würde Auskunft bezüglich einer Nachricht mit dem Wort „Bombe“ verlangt werden. Da die Nachricht den Sicherheitsbehörden nicht eindeutig bekannt ist, muss man hier von „bestimmbar“ sprechen (Wort Bombe in einem E-Mail). Dies hätte zur Folge, dass der Provider zur Erfüllung einer derartigen Auskunftspflicht alle gespeicherten Nachrichten seiner User durchsuchen müsste. Für die Auslegung auf „bestimmbar“ spricht, dass das BMI einen Erlass zur SPG Novelle veröffentlicht hat, und hierbei die Bestimmung „anhand relevanter Abfragekriterien (etwa Nickname, Chat und Zeitraum)“ als ausreichend befindet [VKO]. Dies würde aber inkludieren, dass der Gesetzgeber bei der Auslegung des Z2 schon an die Verarbeitung von Vorratsdaten und somit schon die Umsetzung der Richtlinie 2006/24/EG (Vorratsdatenspeicherung) gedacht hatte.

Abschließend ist festzuhalten, dass Z2 vorsieht, dass Auskunft bezüglich „einer bestimmten“ Nachricht gegeben werden muss und somit eine individualisierte Nachricht gemeint ist. Meiner Meinung nach ist aufgrund des verwendeten Wortes „bestimmt“ zwar der §53 Abs. 3a Z2 restriktiv zu betrachten, wobei aber erneut Zweifel bleiben, wie der Gesetzgeber diese Annahme auslegt.

4.3.4 Begriff „übermittelnde Daten“

Im Z2 SPG wird weiters geregelt, dass die IP-Adresse zu einer bestimmten Nachricht sowie der Zeitpunkt der Übermittlung beauskunftet werden kann. Hierbei ist festzuhalten, dass der verwendete Begriff der IP-Adresse keine genaue Formulierung ausweist, denn es ist nicht klar, ob zB die IP-Adresse des Absenders oder des Empfänger bei einer E-Mail Kommunikation gemeint ist. Um dies genauer zu beleuchten, ist hier das Internet Protocol von Relevanz. Da das Internet Protocol ein paket-basierendes Protokoll ist, gibt es für jedes Datenpaket bei einer Kommunikation im Internet eine Absender sowie eine Empfänger IP-Adresse [RFC2]. Falls der Gesetzesgeber die Absender IP-Adresse gemeint hat, würde dafür sprechen, dass zB Bombendroher, die mittels einer E-Mail die Tat ankündigen, ausgeforscht werden können. Da aber auch immer angeführt wird, dass die Novelle zum SPG auch gegen die

zunehmende organisierte Kriminalität bzw. internationalen Terrorismus verwendet wird, ist auch die Empfänger IP-Adresse von erheblicher Relevanz. Wenn z.B. eine „österreichische Terrorzelle“ Instruktionen von Dritten aus dem Ausland bekäme, würde auch die IP-Adresse des Empfängers für die Sicherheitsbehörden interessant sein. Wenn man aber nun die E-Mail Kommunikation sich näher ansieht, besteht aber nicht nur 1 Absender und 1 Empfänger IP-Adresse sondern eine Vielzahl davon. Dies geschieht dadurch, da die Nachricht über eine Vielzahl von Mail-Servern an den Empfänger weitergeleitet wird. Wie in Kapitel 4.3.1 Allgemein beschrieben, werden Received Header verwendet, in denen die IP-Adresse des Computersystems, die die Nachricht verschickt hat, übermittelt wird. Somit gibt es auch eine Vielzahl an Received Headers mit zahlreichen IP-Adressen von den Mail-Servern, die die Nachricht nur weiterleiten. Hier stellt sich natürlich die Frage, ob der Gesetzgeber die Auskunftspflicht auch auf diese IP-Adressen (von den Mail-Servern, die diese Nachricht nur weiterleiten) anwenden darf? Da im Gesetzestext nur von einer „IP-Adresse zu einer bestimmten Nachricht“ die Rede ist, läge die Interpretation nahe, dass die Auskunftspflicht nur auf eine „einzige“ IP-Adresse besteht. Da der Empfänger einer Nachricht passiv bei der Kommunikation teilnimmt, spricht einiges dafür, dass der Gesetzgeber die IP-Adresse des Absenders gemeint hat. Zu diesem Ergebnis kommt auch der Grundrecht- bzw. Verfassungsexperte Hr. Gerhard Kunnert in seinen Ausführungen in dem Titel „Der sicherheitspolizeiliche Griff nach Telekommunikationsdaten [KUN].

Neben der gerade beschriebenen Datenkategorie der IP-Adresse zu einer bestimmten Nachricht, muss noch der „Zeitpunkt der Übermittlung“ beleuchtet werden. Wie auch schon in den letzten Kapiteln beschrieben, stellt diese Definition keine exakte Deklaration dar und birgt somit zahlreiche Interpretationen. Wenn man sich z.B.: die E-Mail Kommunikation näher ansieht, stellt man fest, dass es zahlreiche Zeitpunkte der Übermittlung gibt. Neben dem Versendungs- und Empfangszeitpunkt, werden wie beschrieben in den Received Header der Zeitpunkt der Weiterleitung der E-Mail am Server gespeichert. Neben diesen Zeitpunkten gibt es noch einen Date-Header [RFC3], der vom Mail-Client des Absenders in die E-Mail aufgenommen wird. Somit können folgende Übermittlungszeitpunkte zusammengefasst werden:

- Date-Header vom Absender E-Mail
- Der erste Received-Header¹: Es ist jener Zeitpunkt, an dem die E-Mail an den SMTP-Server des Absender übertragen wurde
- Zusätzliche Received Header von zwischengeschalteten Mail-Servern
- Der letzte Received-Header: Dieser gibt den Zeitpunkt der E-Mail beim SMTP-Server des Empfängers an.
- Der Zeitpunkt bzw. die Zeitpunkte, in dem das E-Mail vom Empfänger auf seinem Mail-Client abgefragt wird.

Neben diesen Punkten gibt es noch weitere Probleme in Zusammenhang mit dem Zeitpunkt. Einerseits kann bei schlecht gewarteten Mail-Server eine inkorrekte Systemzeit auftreten oder andererseits wird nun vermehrt Greylisting

¹ Der Mail Server fügt den Received Header immer am Anfang hinzu. Somit ist der erste Received Header am Ende der Liste der Mail-Headers. 43

als Maßnahme gegen SPAM verwendet. Mit diesem Verfahren werden alle E-Mails beim ersten Zustellversuch abgelehnt. Erst nach einem Timeout wird ein weiterer Versuch der Zustellung erlaubt. Somit würde es auch zu Differenzen bis zu einigen Minuten in den Received-Headern kommen.

Somit stellt sich abschließend wieder die Frage, wie der Gesetzgeber den Begriff des Übermittlungszeitpunkts in der Novelle gemeint hat? Geht man von der Annahme aus, dass bei dem Begriff der IP-Adresse, die des Absenders gemeint war, liegt es nahe, dass auch beim Übermittlungszeitpunkt jener gemeint ist, indem der Absender die Nachricht versendet hat (Date-Header). Falls aber wie oben erörtert, der Begriff der IP-Adresse nicht auf den Absender begrenzt war, dann bleibt es gänzlich offen, welchen Zeitpunkt der Übermittlung der §53 Abs. 3 Z2 SPG bezeichnen könnte.

4.3.5 Eingriff in das Fernmeldegeheimnis?

Im Art. 10a Staatsgesetzbuch (StGG) wurde das Fernmeldegeheimnis in Anlehnung an das Briefgeheimnis geregelt [I4J3]. Dieser Artikel schützt ausschließlich Nachrichten, die für eine konkrete Person gerichtet sind. Hingegen Nachrichten, die für die Öffentlichkeit bestimmt sind, werden von diesem Artikel nicht geschützt. Dies bedeutet, dass an eine öffentliche Mailing-Liste gesendete Nachricht bzw. ein Eintrag in einem öffentlichen Blog nicht von diesem Artikel geschützt werden. Der Artikel schützt das Fernmeldegeheimnis im besonderen Maße und ein Eingriff darf somit nur mit Hilfe eines richterlichen Beschlusses vollzogen werden. Der Schutz des Fernmeldegeheimnisses bezieht sich auf Inhaltsdaten, da das Briefgeheimnis nur den Schutz von Inhaltsdaten vorsieht. Ob auch Verkehrsdaten von der Regelung betroffen sind, ist auch bei Verfassungsexperten sehr umstritten. In Deutschland, wo nahezu der gleiche Gesetzestext bezüglich des Fernmeldegeheimnisses vorhanden ist, hat der Bundesverfassungsgerichtshof entschieden, dass neben Inhaltsdaten auch die näheren Umstände des Fernmeldevorgangs zum Schutzbereich gehören (Verkehrsdaten). [REP]

Gemäß §53 Abs. 3 Z2 SPG ist geregelt, dass Auskunft über eine IP-Adresse erteilt werden kann. Hierbei ist zu beachten, dass davon die Vertraulichkeit eines Stammdatums (bei einer statischen IP-Adresse) oder eines Verkehrsdatum (bei einer dynamischen IP-Adresse) betroffen sind. Wenn man sich nun die Frage stellt, ob die Vertraulichkeit einer Information verletzt wurde, muss der gesamte Kommunikationsprozess betrachtet werden. Dies bedeutet dass sowohl das Auskunftsbegehren der Sicherheitsbehörde als deren Auskunft vom Provider relevant sind. Somit kann festgehalten werden, dass die Ausübung der Befugnis nach §53 Abs. 3 Z2 SPG die Vertraulichkeit von Inhaltsdaten dann verletzt, wenn die Nachricht aufgrund von „Inhaltsdaten“ bestimmt wird. Ein weiterer wichtiger Punkt ist, dass der Art 10a StGG die Inhaltsdaten nur auf Kommunikationsweg schützt. Dies bedeutet zB dass wenn eine Bombendrohung bei den Sicherheitsbehörden eingelegt ist und Inhaltsdaten von dieser E-Mail verwendet wird, dass kein Eingriff nach Art. 10a StGG vorliegt. Bei dem Begriff Kommunikationsweg, stellt sich die Frage, was

alles zu diesem Begriff zählt. Hier ist die Betrachtung des Briefgeheimnisses aufgrund der Nähe zum Fernmeldegeheimnis sehr wichtig. Das Briefgeheimnis schützt Briefe bis zum Zeitpunkt der Öffnung durch den Empfänger [WKH]. Dies inkludiert, dass alle Briefe in einem Postkasten unter den Schutz des Art. 10 StGG fallen. Wenn man diese Regelung auf das Fernmeldegeheimnis umlegt, bedeutet dies, dass noch nicht abgerufene E-Mails bzw. noch nicht abgehörte Mailbox Nachrichten sich noch am Kommunikationsweg befinden und somit unter den Schutz des Fernmeldegeheimnisses fallen würden. Würden Sicherheitsbehörden noch nicht abgerufene E-Mails bzw. noch nicht abgehörte Mailbox Nachrichten aufgrund von Inhaltsdaten bestimmen wollen, würde dies einen Eingriff in das Fernmeldegeheimnis darstellen.

Mit den nun angeführten Überlegungen lässt sich nun zusammenfassend sagen, dass es 2 Arten gibt, mit denen die Ausübung der Befugnis des §53 Abs. 3a Z2 SPG gibt. Hier spielt wie gesagt eine zentrale Rolle, wie die Behörde die Nachricht „bestimmt“. Bei der ersten Möglichkeit, wird die Nachricht aufgrund von Inhaltsdaten bestimmt. Die Sicherheitsbehörde verwendet hierbei Schlüsselworte, wie z.B. Bombe. Wenn die Sicherheitsbehörde eine Auskunft darüber verlangt, der Provider dem Auskunftsbegehren nachkommt und die Absender-IP-Adresse der Nachricht (mit dem Schlüsselwort) nachkommt, dann wird die Vertraulichkeit der Tatsache verletzt, dass eine bestimmte Person eine Nachricht mit dem Inhalt versendet hat. *Da das Fernmeldegeheimnis auch eine Nachrichtenübermittlung schützt, wenn die übertragenen Inhaltsdaten (die Schlüsselwörter bzw. der gesamte Inhalt der Nachricht) als solche bereits bekannt waren, stellt eine Ausübung der Befugnis des § 53 Abs. 3a Z2 SPG unter Bestimmung einer Nachricht mit derartigen Inhaltsdaten einen Eingriff in Art 10a StGG dar. Da dieser Eingriff ohne einen richterlichen Beschluss erfolgt, liegt diesfalls eine Verletzung des Grundrechts auf Wahrung des Fernmeldegeheimnisses vor* [ZAN]

Bei der zweiten Art weiß die Behörde von einer bestimmbaren Nachricht, kennt aber jedoch nicht den Inhalt. Hierbei würde die Sicherheitsbehörde aufgrund von Stamm- oder Verkehrsdaten, wie z.B.: Absender E-Mail Adresse oder Übermittlungszeitpunkt die Nachricht bestimmen wollen. Wenn dadurch die Absender IP-Adresse herausgegeben würde, könnte dies aber keine Aufschlüsse zum Inhalt der Nachricht führen. Somit würde kein Eingriff in den Art. 10a StGG führen.

Abschließend ist nochmals festzuhalten, dass wenn eine bestimmte Nachricht durch Inhaltsdaten „bestimmt“ wird, ein Eingriff in das Grundrecht auf Wahrung des Fernmeldegeheimnisses besteht. Dies wird auch von namhaften Verfassungsexperten [REP], [ZAN] unterstützt, die die Befugnis §53 Abs. 3a Z2 als verfassungswidrig ansehen, da die Kontrollinstanz der Richter fehlt. Aus diesem Grund wurde auch im ersten Quartal 2008 eine Verfassungsklage (Individualanträge) von Frau Marie Ringler (Landtagsabgeordnete der Wiener Grünen), Internet-Provider Silver Server, der Mobilfunk T-Mobile und der

Gratis-WLAN-Hotspot-Betreiber Freewave eingebracht. Die Ergebnisse der Individualanträge sind im Kapitel 8 Resümee ersichtlicht.

4.3.6 Eingriff in das Grundrecht auf Achtung der Privatsphäre?

Durch die Befugnis des §53 Abs. 3a Z2 SPG wird es den Sicherheitsbehörden ermöglicht, eine Ermittlung von wem (bzw. an wen) eine bestimmte Nachricht gesendet wird, durchzuführen. Hierbei ist auch die Europäische Menschenrechtskonvention (EMRK) von Bedeutung. Im Art. 8 des EMRK wird geregelt, dass jede Person ein Recht auf „Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz“ hat. Bezüglich dieser Auslegung sind drei Gerichtsurteile des Europäischen Gerichtshofs für Menschenrechte (EGMR) interessant. Im Verfahren *Klass and Other vs Germany* [KLA] wurde 1978 entschieden, dass Telefonkommunikation sowohl vom Begriff des Privatlebens als auch von jenem der Korrespondenz erfasst ist. Im zweiten Fall *Copland vs the United Kingdom* [COP] wurde 2007 festgestellt, dass dies im gleichen Maße auch für die E-Mail Kommunikation als auch die Verwendung des Internets gilt. In einem weiteren Verfahren *Malone vs the United Kingdom* [MAL] wurde vom EGMR entschieden, dass nicht nur Inhaltshalten sondern auch Verkehrsdaten unter dem Schutz des Art. 8 EMRK stehen. Dies wurde dann auch im Fall *Copland vs the United Kingdom* [COP] in Bezug auf Verkehrsdaten der Internet- und E-Mail-Nutzung bestätigt. Wenn man nun den §53 Abs. 3a Z2 SPG auch unter restriktiver Auslegung hernimmt, würde man zu dem Ergebnis kommen können, dass hier ein Eingriff in Art. 8 EMRK besteht.

Somit ist zu prüfen, wann ein Eingriff gemäß Art. 8 EMRK zulässig ist. Hierbei ist festgelegt, dass ein Eingriff gemäß Art. 8 EMRK nur dann zulässig ist, wenn er gesetzlich vorgesehen ist und in einer demokratischen Gesellschaft notwendig bzw. verhältnismäßig ist. Mit „gesetzlich vorgesehen“ versteht man, dass die gesetzliche Grundlage für den Betroffenen zugänglich ist und darüber hinaus präzise formuliert ist. Das in der Präambel der EMRK genannte Prinzip der Rechtsstaatlichkeit („rule of law“) wird so ausgelegt, dass die gesetzliche Grundlage von einer bestimmten Qualität sein muss [VKH]. Da der §53 Abs. 3a Z2 SPG eine geheime Überwachung darstellt, kann der Maßstab an die „gesetzliche Vorhersehbarkeit“ nicht sehr streng ausgelegt werden, da sonst die geheime Überwachungsmaßnahme unterlaufen werden würde. Somit steht der §53 Abs. 3a Z2 SPG nicht im Widerspruch zum Art. 8 EMRK. Daher ist zu untersuchen, ob der Paragraph in der Novelle einen notwendigen bzw. verhältnismäßigen Eingriff in einer demokratischen Gesellschaft darstellt.

Diesbezüglich ist festzuhalten, dass die Ausübung der Befugnis gemäß §53 Abs. 3a SPG immer das gelindeste Mittel darstellen muss. In diesem Paragraphen steht, dass die Ausübung der Befugnis nur dann zulässig ist, wenn die an die Sicherheitsbehörden zu übermittelnden Daten eine „wesentliche Voraussetzung“ für die Erfüllung einer der Aufgaben nach dem SPG darstellen. Somit wird geregelt, dass ein Auskunftsbeghehen nur dann rechtmäßig ist, wenn die Informationen nicht auf einem anderen Weg beschaffen werden können. Dies ist weiters im §28a Abs. 2 und 3 deklariert,

der besagt, dass z.B. die Befugnis des §53 Abs. 3a Z2 SPG nur dann ausgeübt werden darf, wenn das SPG keine gelindere Mittel vorsieht. Zusammenfassend zu dem Eingriff in eine demokratische Gesellschaft kann man vermerken, dass das Problem besteht, dass nicht immer das gelinderte Mittel eingesetzt wird, sondern der einfache Weg (über den §53 Abs. 3a SPG) von den Sicherheitsbehörden gewählt wird.

Ein weiterer wichtiger Punkt in der Judikatur des EGMR ist in diesem Bezug die Gefahr aus Missbrauch. *Der Gesetzgeber hat angemessene und wirksame Garantien gegen Missbrauch („adequate and effective guarantees against abuse“) vorzusehen. Die Beurteilung dieser Garantien hängt von den Umständen des Falles ab. Insbesondere Art, Umfang und Dauer der möglichen Maßnahmen, die für ihre Anordnung erforderlichen Gründe, die für die Zulassung, Ausführung und Kontrolle zuständigen Behörden und die Art der im nationalen Recht vorgesehenen Rechtsbehelfe sind zu berücksichtigen.*[ZAN]

Bezüglich der Missbrauchsgefahr sind meiner Meinung nach 2 Punkte von wesentlicher Bedeutung. Einerseits ist es als bedenklich zu bewerten, dass für die Zulassung und die Ausführung der Befugnis die identische Behörde zuständig ist. Weiters ist hier zu vermerken, dass der Rechtsschutzbeauftragte im Innenministerium (siehe Kapitel 2.4.3 Rechtsschutzbeauftragter im Bundesministerium für Inneres) als Kontrollorgan unzureichend ausgestattet ist, um Missbrauch zu verhindern. Der zweite wichtige Punkt in diesem Zusammenhang ist, dass der Betroffene zu keinem Zeitpunkt über das Auskunftsbeghären zu informieren ist. Weiters ist laut §91d Abs.3 SPG der Rechtsschutzbeauftragte lediglich befugt – und damit nicht verpflichtet – den Betroffenen bezüglich etwaige Verletzungen bezüglich personenbezogenen Daten zu informieren. Abschließend kann festgehalten werden, dass der Gesetzgeber seinen Verpflichtungen, angemessene und wirksame Garantien gegen Missbrauch zu installieren, nicht ausreichend nachgekommen ist und mit den beiden oben beschriebenen Punkte Lücken für etwaigen Missbrauch geschaffen hat.

4.3.7 Eingriff in das Grundrecht auf Datenschutz?

Wie schon im Kapitel 2.3.1.1 Datenschutzgesetz 2000 (DSG 2000) beschrieben, ist in Österreich im §1 Abs.1 Satz 1 DSG 2000 das Grundrecht auf Geheimhaltung verfassungsrechtlich geschützt. Hierbei ist hinzuweisen, dass der Gesetzesgeber bei Eingriffen in das Grundrecht durch eine staatliche Sicherheitsbehörde direkt auf den Art. 8 Abs. 2 EMRK verwiesen hat. Durch die Auskunftspflicht werden die IP-Adresse und der Übermittlungszeitpunkt zu einer bestimmten Nachricht an die Sicherheitsbehörde übermittelt. Somit kann durch die Z3 der Novelle ein Bezug zu einer konkreten Person hergestellt werden und die Identität des Betroffenen bestimmt werden. Der konkrete Personenbezug wird zwar aufgrund eines rechtmäßigen Gesetzes vollzogen, es ist aber in Frage zu stellen, ob dieser Personenbezug auch immer nur für den Zweck der nationalen Sicherheit, der öffentlichen Ruhe und Ordnung, des wirtschaftlichen Wohl des Landes, der Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutze der Gesundheit und der

Moral oder zum Schutz der Rechte und Freiheiten anderer eingesetzt wird (wie in Art. 8 Abs. 2 EMRK deklariert), angewandt wird. Zusammenfassend ist zu sagen, dass in Hinblick auf EMRK und DSGVO 2000 die neu geschaffene Novelle zumindest sehr fragwürdig erscheint.

4.3.8 Eingriff in den Gleichheitssatz (Kostenersatz)?

Grundlegend ist einmal zu erwähnen, dass der Gesetzgeber einen Kostenersatz für die Erfüllung der Auskunft für den §53 3b SPG (siehe Kapitel 4.1 Einleitung und Gesetzestexte) vorsieht, aber nicht für den §53 3a SPG. In diesem Kapitel möchte ich prüfen, ob nicht dies einen Eingriff in den Gleichheitssatz darstellt. Hierbei von Bedeutung erscheint die Erkenntnis von 27.02. 2003, indem der VfGH den nicht gewährten Kostenersatz für die Verpflichtung zur Bereitstellung von Überwachungseinrichtungen laut §89 Abs. TK 1997 wieder aufhob [VfGH]. Begründung hierfür war, dass dies als Verstoß gegen den Gleichheitssatz vom VfGH angesehen wurde. Der VfGH führte in Bezug auf den Kostenersatz an, dass die entstehenden Kosten einerseits kalkulierbar und wirtschaftlich zumutbar sein sollten. Als drittes Kriterium führte der VfGH an, dass die zu erbringenden Leistungen, auch im Sinne des Auskunftspflichtigen sein sollte und zu seinem Schutz dienlich sein soll. Diese 3 Kriterien müssen nun in Bezug auf den §53 Abs. 3a geprüft werden.

Da die Auskunftsbegehren nicht automatisiert sondern weitestgehend manuell von technischen Experten durchgeführt werden müssen, ist davon auszugehen, dass dies erhebliche Kosten verursacht. Etwaige automatisierte technische Schnittstellen sind derzeit nach meinem Wissensstand noch nicht realisiert. Da die Novelle dies auch für Sonstige Diensteanbieter laut ECG vorsieht, ist dies dort besonders problematisch. Da wie in den letzten Kapiteln beschrieben, die Gesetzesbegriffe als nicht ausreichend beschrieben zu interpretieren sind, lassen sich die Kosten kaum abgrenzen, geschweige als kalkulierbar zu bezeichnen.

Bezüglich dem zweiten Kriterium der wirtschaftlichen Zumutbarkeit kann man vermerken, dass dies auch wieder für Sonstige Diensteanbieter laut ECG ein Problem darstellen wird. Viele sonstige Diensteanbieter haben nur unentgeltliche Verträge mit ihren Usern und besitzen als einzige Einnahmequelle Online-Werbungen. Hierbei stellt sich die Frage, wie diese Unternehmen die entstehenden Mehrkosten durch die Auskunftspflicht bewerkstelligen sollen. Die Benutzer werden wahrscheinlich nicht gewillt sein, für einen kostenlosen Dienst, jetzt einen Betrag ohne Mehrwert für Sie zu zahlen.

Bezüglich des Punktes, dass die Auskunftspflicht im Sinne bzw. zum Schutz für den Provider sein muss, ist festzuhalten, dass kein eigenes Interesse des Providers besteht. Durch die Auskunftspflicht wird der Provider nicht mehr geschützt, sondern der Dienst des Providers wird nur zwecks der Tatbegehung benutzt. Wie schon in der Einleitung dieses Kapitels erwähnt, ist es interessant, dass der Gesetzgeber für die Erfüllung der Auskunftspflicht einen

Kostenersatz nach §7 Z4 Überwachungskostenverordnung (ÜKVO) [ÜVO] für den §53 Abs. 3b SPG vorsieht, dies aber für den §53 3a SPG ausschließt. Wenn man diese zwei Absätze vergleicht, kommt man darauf, dass einerseits für den §53 Abs. 3a mehr Kosten entstehen würden und andererseits auch ein größerer Kreis an betroffenen Provider, nämlich sonstige Diensteanbieter, besteht. Somit ist die Differenzierung zwischen den beiden Absätzen unverständlich.

Zusammenfassend kann festgehalten werden, dass für die Pflicht zur Auskunftserteilung erhebliche und schwer kalkulierbare Kosten entstehen und somit die wirtschaftliche Zumutbarkeit nicht gegeben ist. Weiters trägt die Beauskunftung nicht zum Schutz des Providers dar. Neben den angeführten Punkten und der nicht verständlichen bzw. begründeten Differenzierung ist es fraglich, ob der §53 Abs. 3a Z2 SPG mangels Berücksichtigung des Verhältnismäßigkeitsgrundsatzes standhalten würde. Dies würde somit einen Verstoß gegen den Gleichheitssatz laut VfGH darstellen.

4.3.9 Zusammenfassung

Da die Novelle Eingriffe in die Grundrechte eines Menschen ermöglicht, muss genau darauf geachtet werden, ob die Novelle inhaltlich ausreichend Regelungen schafft. Somit spricht man bei dem SPG von einem „eingriffsnahe Gesetz“ [BEK]. In diesem Kapitel möchte ich nochmals die einzelnen Ergebnisse der letzten Kapitel zusammenfassen. Leider ist es nicht ersichtlich, wie der Gesetzgeber den Begriff der Nachricht auslegt. Dies kann sich von E-Mails und über das Internet versendete SMS bis hin zu jeder Information, die mittels Telekommunikationseinrichtungen ausgetauscht bzw. weitergeleitet werden, erstrecken. Weiters ist fraglich, wie der Gesetzgeber den Begriff der „bestimmten“ Nachricht auslegt. Meiner Meinung nach wird hier von eindeutig bestimmten Nachrichten ausgegangen und nicht von bestimmbar Nachrichten via Abfragekriterien. Der nächste Punkt, indem der Gesetzgeber nicht ausreichend Klarheit geschaffen hat, ist der Begriff der IP-Adresse. Es kann zwar davon ausgegangen werden, dass hier die IP-Adresse des Absenders gemeint ist, aber es wäre auch denkbar, dass jegliche IP-Adressen in einer Kommunikation abgefragt werden können. Wie auch in der Frage des Zeitpunkts der Übermittlung, kann festgehalten werden, dass der Gesetzgeber sich äußert unbestimmter Gesetzesbegriffe bedient. Neben diesen nicht ausreichend formulierten Gesetzesbegriffen, ist zusammenfassend zu sagen, dass der §53 Abs. 3a Z2 SPG Eingriffe in diverse Grundrechte darstellt. Es besteht zumindest der berechtigte Verdacht, dass der §53 Abs. 3a Z2 SPG gegen das Fernmeldegeheimnis, die Achtung auf Privatsphäre, das Grundrecht auf Datenschutz sowie gegen den Gleichheitssatz verstößt. Abschließend ist noch anzumerken, dass dieser Grundrechtseingriff keiner richterlichen Kontrolle obliegt.

4.4 Befugnis des §53 Abs. 3a Z3 SPG

Wie schon in den oberen Kapiteln beschrieben, müssen Betreiber öffentlicher Telekommunikationsdienste sowie Diensteanbieter laut ECG dem Ansuchen nach Auskunft über „Namen und Anschrift eines Benutzers“ nachkommen, „dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war. Bezüglich dem Z3 möchten ich 2 Punkte näher beleuchten: 1.) dem Kreis der auskunftspflichtigen Betreiber sowie 2.) einen kurzen Exkurs bezüglich statischen und dynamischen IP-Adressen.

4.4.1 Kreis der auskunftspflichtigen Betreiber

Die Voraussetzung für die Erfüllung der Auskunftspflicht nach Z3 besteht für den Auskunftspflichtigen darin, dass es ihm möglich ist, zu ermitteln, wem zu einem bestimmten Zeit eine bestimmte IP-Adresse zugewiesen war. Aufgrund dieser Voraussetzung kann festgehalten werden, dass dies nur jenen Providern möglich ist, die selbst nur die IP-Adresse zuweisen – d.h. Internet Access Providern. Dies wird in den nächsten Absätzen nun beleuchtet.

Grundsätzlich wird von den Internet Access Providern eine IP-Adresse immer einem Internetanschluss bzw. der Netzwerkkarte eines Computersystems zugewiesen, und nicht dem Inhaber des Anschlusses. Dies ist von Bedeutung, da der Internetanschluss nicht nur von dem Inhaber des Internetanschluss genutzt wird, sondern mit oder ohne Einwilligung von Dritten benutzt werden kann. Wenn man die Zuweisung der IP-Adresse technisch betrachtet, wird dies meistens unter der Verwendung des Dynamic Host Configuration (DHCP) vollzogen. Hierbei können „dynamische“ und „statische“ IP-Adressen vergeben werden. Wenn zwischen dem Nutzer und dem Betreiber vertraglich vereinbart ist, dass eine „statische“ IP-Adresse zugewiesen wird, dann verpflichtet sich der Betreiber immer eine bestimmte IP-Adresse zuzuweisen. Dem Nutzer obliegt meistens die Konfiguration der IP-Adresse auf seinem Computersystem. Im Gegenzug dazu wird bei sogenannten „dynamischen“ IP-Adressen, bei der Herstellung der Verbindung des Internets eine andere IP-Adresse vom DHCP vergeben. Zwar kann somit festgehalten werden, dass Internet Access Provider stets die Information haben, welchem Internetanschluss ihrer Kunden welche IP-Adresse zugeordnet ist, aber es stellt sich die Frage wie es mit den sonstigen Diensteanbietern gemäß ECG aussieht. Wenn zum Beispiel ein Hosting Provider (sonstige Diensteanbieter) ein Message Board für seine Nutzer anbietet, dann könnte er nach einer Registrierung mit Name und Anschrift diese mit der vom Benutzer verwendeten IP-Adresse speichern. Dies würde zwar bedeuten, dass der Hosting Provider zwar bei einem Eintrag ins Message Board, den Zeitpunkt, Name und Adresse des Registrierten sowie die zugewiesene IP-Adresse beauskunften könnte, dies aber nicht klärt, ob der Registrierte mit dem Ersteller des Message Board Eintrags gleichzusetzen ist. Diesbezüglich kann man auch als Beispiel die Verwendung eines Proxy-Servers heranziehen. Die Funktion eines Proxy-Servers kann man wie folgt zusammenfassen. Der Proxy-Server fungiert als Stellvertreter bei der Kommunikation im Internet mit anderen Systemen. Dies bringt den Vorteil, dass die Performance als auch die Sicherheit für eine größere Anzahl an Nutzern gewährleistet wird. Wenn man nun das Beispiel mit dem Hosting-

Provider mit einem Message Board hernimmt, würde nur die IP-Adresse des Proxy-Servers gespeichert werden und nicht die des eigentlichen Benutzers. Der Hosting Provider kann auch nicht unterscheiden, ob es nun die IP-Adresse des Proxy-Servers ist oder die des Benutzers. Der Hosting-Provider würde somit nur wissen, dass die IP-Adresse vom Benutzer verwendet wird, jedoch nicht von wem die IP-Adresse zugewiesen wurde. Da im SPG nur von der Zuweisung und nicht von der Verwendung die Rede ist, kann nochmals festgehalten werden, dass sich die Auskunftspflicht nur auf Internet Access Provider, d.h. jene Provider die tatsächlich die Zuweisung der IP-Adressen vollziehen, beschränkt. Hierbei ist noch zu erwähnen, dass Unternehmen auch als Internet Access Provider für ihre Dienstnehmer auftreten können. Zwar stellen diese Unternehmen keine Betreiber eines öffentlichen Telekommunikationsdienstes dar, weil diese nicht öffentlich zugänglich sind, trotzdem fallen sie unter die Auskunftspflicht, da sie unter sonstige Dienstanbieter laut ECG eingeordnet werden können. Da aber die meisten Unternehmen in ihrem Firmennetzwerk „private“ IP-Adressen verwenden und somit nur im Internet alle Dienstnehmer mit derselben „öffentlichen“ IP-Adresse auftreten, würde nur diese unter die Auskunftspflicht fallen. Deswegen würde ich dies eher einer geringeren Bedeutung zumäßen.

4.4.2 Statische vs. dynamische IP-Adressen

Wie schon im Kapitel 2.3.1.2 Telekommunikationsgesetz 2003 (TKG 2003) vermerkt, fallen IP-Adressen unter den Begriff der Verkehrsdaten laut §92 Abs. 3 Z4 TKG 2003. Die Begründung hierfür ist, dass sie zum Zweck der Weiterleitung einer Nachricht verarbeitet werden müssen. Unter Experten ist jedoch strittig, ob IP-Adressen auch unter den Begriff der Stammdaten fallen können. Dies ist jedoch von erheblicher Relevanz, da nur Verkehrsdaten unter der Vertraulichkeit des Telekommunikationsgeheimnisses bzw. der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) fallen. Meiner Meinung nach würde aber eine IP-Adresse nur unter Stammdaten subsumiert werden können, wenn zwischen dem Kunden und dem Anbieter vertraglich eine konkrete IP-Adresse definiert worden ist, d.h. eine „statische IP-Adresse“. Andererseits sind aber dauerhaft zugewiesene, aber nicht vertraglich bestimmte IP-Adressen, bzw. „dynamische“ IP-Adressen als Verkehrsdaten zu beurteilen. Dies untermauert die EBRV zur TKG 2003 die als Beispiel eine E-Mail Adresse nicht aber eine IP-Adresse als Beispiel für Stammdaten. Wenn man jetzt „statische“ IP-Adressen von einem bestimmten Kunden zu einem bestimmten Zeitraum laut §53 Abs. 3a Z3 SPG abfragen würde, dann ist die Ausübung der Befugnis unzulässig, da nicht das gelindeste Mittel seitens der Sicherheitsbehörden (§28a Abs. 2 und 3) eingesetzt wurde. „Statische“ IP-Adressen sind in einer sogenannten WHOIS-Datenbank (z.B. für Europa die RIPE NCC (Réseaux Européens Network Coordination Centre) gespeichert und für Dritte ersichtlich. Somit müsste dieser Weg von den Sicherheitsbehörden beschritten werden und nicht über den Betreiber mittel Auskunftsbegehren. Bei „dynamischen“ IP-Adressen stellt sich überhaupt die Frage, wie sich die Beauskunftung nach §53 Abs. 3a Z3 SPG in Bezug auf das

Telekommunikationsgeheimnis bzw. der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) vereinbaren lässt.

4.5 Befugnisse des §53 Abs. 3b SPG

Hier ist einleitend zu erwähnen, dass mit dem §53 Abs. 3b SPG Befugnisse geschaffen wurden, dass unter gewissen Voraussetzungen die Sicherheitsbehörden berechtigt sind, Auskunft von Betreibern von öffentlichen Telekommunikationsdiensten zu verlangen. Hierbei zählen Standortdaten, die IMSI des Betroffenen sowie technische Mittel zur Lokalisierung. Weiters ist im §53 Abs. 3b SPG festgehalten, dass die Sicherheitsbehörde für die rechtliche Zulässigkeit und Dokumentation für den Betreiber zuständig ist. Abschließend ist in diesem Absatz festgeschrieben, dass ein Ersatz für Kosten für den Betreiber gegeben werden muss, zum Unterschied zu den Befugnissen in §53 Abs. 3a SPG.

4.5.1 Voraussetzungen

4.5.1.1 Begriff der Gefahrensituation

Im §53 Abs. 3b SPG gilt als Voraussetzung, dass eine Annahme einer Gefahr für das Leben bzw. die Gesundheit eines Menschen besteht. Hierbei ist festzuhalten, dass die bloße Gefahr für das Eigentum (z.B.: Diebstahl bzw. Raub) oder sonstige Rechtsgüter nicht ausreichend ist. Der Gesetzestext bezieht sich ausschließlich auf die Gefahr für das Leben bzw. Gesundheit eines Menschen. Da im Gesetzestext die Formulierung „ist aufgrund bestimmter Tatsachen anzunehmen“ verwendet wird, ist anzunehmen, dass die Meldung einer Gefahr für das Leben bzw. Gesundheit einer dritten Person von einem Beteiligten zulässig ist. Beispiele hierfür wären, dass eine Dritte Person meldet, dass eine Person Selbstmord begehen möchte oder von einer Lawine verschüttet wurde. Wie auch schon im Kapitel 4.3.6 Eingriff in das Grundrecht auf Achtung der Privatsphäre? dargestellt, muss diese Befugnis vor Missbrauch geschützt werden. Da aber im SPG durch den §29 SPG der Grundsatz der Verhältnismäßigkeit gepflegt ist, stellt diese Bestimmung Schutz gegen Missbrauch dar.

Bei diesem Gefahrenbegriff versteht der Gesetzgeber nicht den Begriff der allgemeinen Gefahr bzw. des gefährlichen Angriffs. Um dies nochmals zu veranschaulichen möchte ich hier 2 Beispiele anführen. Wenn zum Beispiel verzweifelte Eltern bei der Sicherheitsbehörde anrufen, da ihr Kind entführt wurde, dann dürfte das Mobiltelefon des Entführungsofers durch technische Überwachungsmaßnahmen (siehe Kapitel 5 Stand der Entwicklung von technischen Überwachungsmaßnahmen im Bereich Mobilfunk) geortet werden. Da aber nur „gefährdete Menschen“ lokalisiert werden dürfen, wäre es nicht rechtmäßig, den Entführer zu orten. Hierbei ist weiters festzuhalten, dass nach Beendigung der Gefahr für das Leben bzw. Gesundheit §53 Abs. 3b SPG nicht angewendet werden darf. Dies hieße für dieses Beispiel, dass wenn das Entführungsoffer die Freiheit erlangt, und das Mobiltelefon beim Entführer

bleiben würde, das Mobiltelefon nicht lokalisiert werden dürfte. Als zweites Beispiel wäre denkbar, dass verzweifelte Eltern die Sicherheitsbehörden verständigen, da die Annahme besteht, dass ihr Kind Selbstmord begehen könnte. Hierbei ist auch von einer „gefährdeten Person“ auszugehen, und somit wäre die Lokalisierung des Suizidgefährdeten rechtmäßig.

Wie auch schon in den vorangegangenen Kapiteln vermerkt, ist auch hier zu hinterfragen, ob nicht eine ausführliche Beschreibung des Begriffs der Gefahr für Leben und Gesundheit besser gewesen wäre. Dies möchte ich wieder mit einem Beispiel untermauern: Wenn zum Beispiel verzweifelte Eltern anrufen, und melden, dass ihr Kind raucht bzw. Alkohol zu sich führt, dann besteht sehr wohl die Gefahr für Leben bzw. Gesundheit der gefährdeten Person. Diesbezüglich müssten dann die Sicherheitsbehörden zwecks Abwehr der Gefahr das Mobiltelefon des „Gefährdeten“ orten. Da dies aber nicht in den sicherheitspolizeilichen Aufgaben (siehe Kapitel 4.5.1.2 Begriff der Hilfeleistung bzw. Abwehr dieser Gefahr) fällt, ist es fraglich, wie wirklich die Sicherheitsbehörden im realen Fall reagieren würden.

4.5.1.2 Begriff der Hilfeleistung bzw. Abwehr dieser Gefahr

Im Gesetzestext des SPG wird ausdrücklich als Voraussetzung für die Befugnisausübung eine „Hilfeleistung bzw. Abwehr dieser Gefahr“ hingewiesen. Interessant ist, dass der Gesetzgeber nicht den Wortlaut von §53 Abs. 3a Satz 2 SPG „der Erfüllung der ersten allgemeinen Hilfeleistungspflicht“ gewählt hat, sondern den globalen Begriff der „Hilfeleistung“. Da aber die Ausübung sicherheitsbehördlicher Befugnisse des SPG immer an sicherheitspolizeiliche Aufgaben gebunden ist, kann angenommen werden, dass hier kein wesentlicher Unterschied zwischen den beiden Begriffen besteht und keine neue Befugnis geschaffen wurde. Ähnlich ist es bei dem Begriff der „Abwehr dieser Gefahr“. Zwar gab es vor der Novelle, nur den Begriff der „Gefahrabwehr“, aber man kann auch hier annehmen, dass durch den neuen Begriff keine neue Aufgabe für die Sicherheitsbehörden besteht.

Somit ist auch in diesem Absatz festzuhalten, dass neue Begriffe ohne nähere Erläuterung bzw. nicht gut ausformulierte Begriffe verwendet wurden, die natürlich für Interpretationen Spielraum bieten.

4.5.2 Auskunft über Standortdaten

Da in dem Gesetzestext nicht näher auf den Begriff der Standortdaten eingegangen wird, möchte ich auf das Telekommunikationsgesetz 2003 (TKG 2003) §92 Abs. 3 Z6 referenzieren. Hierbei ist die Rede davon, dass *Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben* [14J2] als „Standortdaten“ angesehen werden. Neben dieser Bestimmung im TKG 2003 gibt es sonst keine andere Bestimmung in der österreichischen Rechtsordnung, die den Begriff der Standortdaten erklärt. Somit kann ausgegangen werden, dass der

Begriff im SPG sich nach dem TKG 2003 richtet. Der Betreiber wird somit von den Sicherheitsbehörden angewiesen, dass die Funkzelle (Cell-ID), indem sich das Endgerät befindet, ermittelt werden soll. Aufgrund dieser Basis kann die geografische Lage des Endgeräts bzw. der Person massiv eingeschränkt werden.

Jedoch muss festgehalten werden, dass der geschaffene Passus in der Novelle 2008 nicht die erste Bestimmung ist, dass Standortdaten beauskunftet werden. Im § 98 TKG 2003 ist festgeschrieben, dass Betreiber von Notrufdiensten Auskünfte über die Standortdaten eines Endgeräts erteilen müssen, damit ein Notfall abgewehrt werden kann. Hierbei ist der Betreiber des Notrufdienstes angewiesen, die Notwendigkeit der Informationsübermittlung zu dokumentieren. Dies sollte sofort, aber spätestens 24 Stunden nach Erteilung erfolgen. Weiters trägt der Betreiber des Notrufdienstes die Verantwortung über die rechtmäßige Weitergabe der Standortdaten. Da es schon den Passus im TKG 2003 bezüglich Notrufe gibt, stellt sich die Frage, wieso der Gesetzgeber zusätzlich eine Ergänzung schafft. Hintergrund hierbei könnte sein, dass Standortdaten eines Mobiltelefons bekannt gegeben werden müssen, ohne dass zuvor ein Notruf der „gefährdeten Person“ eingegangen ist. Bei näherer Betrachtung geht aber auch das TKG von einem Notfall aus und nicht von einem Notruf der „gefährdeten Person“. Oft wird für die Begründung der Schaffung der neuen Absätze im SPG verwendet, dass Lawinenopfer selbst nicht mehr anrufen können.

Abschließend möchte ich in diesem Kapitel vermerken, dass Standortdaten gemäß §93 Abs. 1 TKG 2003 dem Kommunikationsgeheimnis unterliegen [14J2]. Weiters verbietet der Abs. 3 das Mithören, Abhören, Aufzeichnen bzw. sonstige Überwachungen der Nachrichten sowie der damit verbundenen Standort- bzw. Verkehrsdaten, ohne dass alle Beteiligten eingewilligt haben. Im §53 Abs. 3b SPG wurde veranlasst, dass Betreiber öffentlicher Telekommunikationsdienste den Sicherheitsbehörden Auskunft über Standortdaten des Endgeräts einer gefährdeten Person geben sollen.

4.5.3 Technologien zur Lokalisierung

Im Gesetzestext wird die Formulierung bezüglich eingesetzter Technologien zur Lokalisierung von Endgeräten neutral gehalten. In der EBRV ist hingegen zu lesen, dass der Gesetzgeber auf den Einsatz von IMSI-Catcher (siehe Kapitel 5.1 IMSI-Catcher) ausgeht. In dieser EBRV steht unter „finanziellen Auswirkungen“, dass sich die Neuanschaffung eines neuen IMSI-Catchers bei ca. 600.000 Euro beziffern lässt. Neben der einmaligen Anschaffung eines neuen IMSI-Catcher ist in der EBRV angeführt, dass weitere laufende Kosten anfallen. Hierbei sind erhöhte Personalkosten als auch Sachaufwände aufgeführt. Insgesamt werden diese Mehraufwände auf 402.901 Euro pro Jahr geschätzt. (nähere Details siehe Anhang A: Auszug aus der EBRV zum SPG 2008). Neben diesen laufenden Kosten werden noch andererseits die Lizenzkosten für die ViCLAS-Datenbank angeführt. ViCLAS steht für „Violent Crime Linkage Analysis System“ und wird als kriminalpolizeiliches Informations-

und Analysesystem zur Bekämpfung von schwerer Gewaltkriminalität eingesetzt. Diese Datenbank gibt den Sicherheitsbehörden sehr schnell die Möglichkeit, differenziert auf geklärte und ungeklärte Straftaten zuzugreifen. Dies ermöglicht den Sicherheitsbehörden einfacher und effizienter Serien in Bezug auf Verbrechensdelikte zu erkennen.

Abschließend ist zu der EBRV zu vermerken, dass andere Technologien als wie den Einsatz von IMSI-Catchers nicht erwähnt werden.

4.6 Dokumentation des Auskunftsbegehens

4.6.1 Allgemein

Im §53 Abs. 3b Satz 2 SPG ist geregelt, dass die Dokumentation des Auskunftsbegehens dem Betreiber unverzüglich, jedoch spätestens innerhalb von 24 Stunden, zu erteilen ist. Die rechtliche Zulässigkeit obliegt in den Händen der Sicherheitsbehörden und nicht beim Betreiber. Hierbei lehnt sich die Novelle an die Bestimmung des §98 TKG 2003 an [I4J2]. Es wurde aber nicht genau der Wortlaut übernommen, sondern der Begriff der „Dokumentation des Auskunftsbegehens“ verwendet (im Vergleich zu §98 TKG 2003 war die Rede von der „Notwendigkeit der Informationsübermittlung zu dokumentieren“) [KUN]. Die Dokumentation des Auskunftsbegehens hat als Zielsetzung, dass der Betreiber nachvollziehen kann, zur Abwehr welcher Gefahr die Standortdaten übermittelt werden sollen. Aus diesem Grund sollten dem Betreiber die Dokumentation des Auskunftsbegehens so rasch als möglich übermittelt werden. Diese Bestimmung soll den Missbrauch gegen nicht rechtmäßige Standortabfragen vorbeugen.

Hierbei ist aber festzuhalten, dass wie auch im §98 TKG 2003 der Betreiber die Übermittlung der Daten nicht von der Dokumentation der Sicherheitsbehörde abhängig machen kann. Dies bedeutet, dass der Betreiber nicht das Recht hat, ein Auskunftsverlangen aufgrund von mangelhafter Qualität der Dokumentation zu verweigern. Dies wird auch dadurch deutlich, dass den Sicherheitsbehörden eine Nachfrist von 24 Stunden bezüglich der Dokumentation zugestanden wurde.

4.6.2 Standortdaten aus der Vergangenheit?

Der §53 Abs. 3b SPG ermöglicht den Sicherheitsbehörden die Standortdaten vom Betreiber ermitteln zu lassen. Die Frage, die sich hier stellt ist, ob dies auch für Standortdaten aus der Vergangenheit rechtmäßig ist. Grundsätzlich steht in dem Absatz keine ausdrückliche Einschränkung auf Standortdaten aus der Gegenwart, jedoch wird im Gesetztext der Begriff des „mitgeführte Endeinrichtung des Gefährdeten“ verwendet. Somit könnte man interpretieren, dass der Gesetzgeber keine Auskunftspflicht für Standortdaten aus der Vergangenheit bereitstellen wollte. Jedoch kann nicht hundertprozentig ausgeschlossen werden, dass auch im Bedarfsfall eine Auskunftspflicht bei Standortdaten in der Vergangenheit besteht.

Standortdaten aus der Vergangenheit können aber von beträchtlicher Relevanz sein. Wenn man wieder das Beispiel eines Lawinenopfer hernimmt, dann könnte es möglich sein, dass das Mobiltelefon nicht mehr in einem betriebsbereiten Zustand ist, und somit wären Standortdaten aus der unmittelbaren Vergangenheit (wo das Mobiltelefon noch in einem betriebsbereiten Zustand war) hilfreich. Die derzeitige Rechtslage (noch keine Umsetzung der Richtlinie 2006/24/EG (Vorratsdatenspeicherung)) lässt jedoch die Speicherung von Standortdaten nur in einem sehr begrenzten Umfang zu. Dies ist im §102 TKG 2003 geregelt. Daher ist festzuhalten, dass wie gesagt, nur in bestimmten Ausnahmefällen die Speicherung von Standortdaten zulässig ist.

Abfragen auf Standortdaten aus der Vergangenheit sind sicherheitstechnisch viel höher einzustufen, da sonst die Sicherheitsbehörden aufgrund dieser Daten exakte Bewegungsprofile des Betroffenen erstellen könnten. Aufgrund von Regelmäßigkeiten könnten gewisse Standortdaten aus der Vergangenheit auch auf den momentanen Standort des Betroffenen geschlossen werden, ohne dass für den jetzigen Zeitpunkt eine Standortabfrage durchgeführt wird.

Abschließend ist festzuhalten, dass die Abfrage von aktuellen Standortdaten durch die Novelle eindeutig gedeckt ist. Anders sieht es bei Abfragen von Standortdaten aus der Vergangenheit aus. Hierbei ist die Rechtslage nicht ausreichend beschreiben. Weiters ist in diesem Zusammenhang die Art der Umsetzung der Richtlinie 2006/24/EG (Vorratsdatenspeicherung) in weiterer Zukunft sehr interessant.

4.6.3 Qualität des Formulars

Wenn die Sicherheitsbehörden eine Auskunft gemäß §53 SPG bei dem zuständigen Telekommunikationsanbieter stellen, wird ein entsprechendes Formular (siehe Anhang B: Auskunftsverlangen gem. §53 Abs. 3a und 3b SPG Formular) übermittelt. In diesem Formular wird der Provider verpflichtet, die gewünschten Daten auf eine bestimmte Weise (telefonisch, per E-Mail oder via Fax) zu senden.

Wenn man sich das Formular näher ansieht, dann mangelt es dem Formular an einer Bezeichnung als Bescheid. Durch das Formular gewinnt man eher den Eindruck, dass der Provider um eine Auskunftserteilung „ersucht“. Die Sicherheitsbehörde geht nicht näher auf die Bestimmung ein, sondern verweist lediglich auf die Befugnisse des §53 Abs. 3a bzw. Abs. 3b SPG. *„Nach der Judikatur des VfGH sind die Wortwahl und die sprachliche Fassung ein Indiz für die Beurteilung des Behördenwillens. Einem Schreiben, in dem sich lediglich Hinweise auf gesetzliche Bestimmungen finden und der Gesetzestext wortwörtlich wiederholt wird, ohne dass ihn die Behörde konkretisiert oder interpretiert, wurde vom VfGH die Bescheidqualität nicht zuerkannt [ZAN].* Diese Behauptungen werden auch von [ZAN] damit begründet, dass es zu diesem Thema drei VfGH Urteile gibt – VfGH 10.3. 194, B295/83; 13.10.1977, B 382/76; 1.3.1990, B953/89. Somit könnte man

argumentieren, dass das Formular zur Auskunftserteilung keine Bescheidqualität hat.

Da es sich nun nicht um einen Bescheid handelt, kann man die Frage stellen, ob die Übermittlung des Formulars einen Akt unmittelbarer verwaltungsbehördlicher Befehls- und Zwangsgewalt darstellt. Da aber wie oben angemerkt, das Formular eher einem Ersuchen gleich kommt und somit keinen Befehlscharakter darstellt, kann es auch nicht als Akt unmittelbarer verwaltungsbehördlicher Befehls- oder Zwangsgewalt qualifiziert werden. Somit kann man dieses Formular unter die schlichte Hoheitsverwaltung einordnen. Dies steht auch im Einklang mit den Grundsätzen des SPG. Wie schon im Kapitel 4.3.6 Eingriff in das Grundrecht auf Achtung der Privatsphäre? angemerkt, soll die Zwangsausübung für die Erfüllung sicherheitspolizeilicher Aufgaben nur dann zur Anwendung kommen, wenn es kein anderes gelinderes Mittel gibt. Da ein Ersuchen ein gelinderes Mittel als ein Bescheid oder einen Befehl darstellt, wurde diese Form für dieses Formular gewählt.

4.6.4 Rolle des Rechtsschutzbeauftragten im Bezug auf das SPG

Um Personen zu schützen, die von geheimen Ermittlungsmaßnahmen betroffen sind, wurde die Institution eines Rechtsschutzbeauftragten geschaffen. Diese Einrichtung gibt es nicht nur für die Bestimmungen des SPG (definiert im §91 [I4J4]), sondern auch für die StPO und dem Militärbefugnisgesetz. Da bei geheimen Überwachungsmaßnahmen der Betroffene nichts von den Ermittlungen wissen kann, soll der Rechtsschutzbeauftragte die Rechte stellvertretend für ihn wahrnehmen bzw. hüten [VOG]. Dem Rechtsschutzbeauftragten obliegt das Recht, eine Beschwerde bei der DSK vorzubringen, wenn er bemerkt, dass durch das Verwenden von personenbezogenen Daten Rechte eines Betroffenen verletzt werden. Weiters hat der Rechtsschutzbeauftragte in diesem Fall die Befugnis, den Betroffenen zu informieren. Hierbei ist aber festzuhalten, dass durch den § 91d Abs. 3 SPG [I4J4] der Rechtsschutzbeauftragte sowohl zur Beschwerde bei der DSK als auch bei der Information beim Betroffenen jeweils „befugt, aber nicht „verpflichtet“ ist. Ob nun die Rechte des Betroffenen wirklich verletzt wurden, ist eine Rechtsfrage. Hier kommt es zwangsläufig zu unterschiedlichen Meinungen. Der Betroffene würde zu der Auffassung gelangen, wenn er von der geheimen Ermittlungsmaßnahme gewusst hätte, dass seine Rechte verletzt wurden, wobei hingegen der Rechtsschutzbeauftragte dies als unbedenklich einstufen würde.

Wichtig ist auch im Zusammenhang mit dem SPG festzuhalten, dass es schon vor der Novelle die Institution des Rechtsschutzbeauftragten im Bundesministerium gegeben hat, aber vor der Novelle noch zusätzlich die Kontrollinstanz der Richter vorhanden war. Somit stellt nun die einzige Kontrollfunktion der Rechtsschutzbeauftragte dar. Dies ist aus meiner Sicht als bedenklich zu beurteilen, da nun gewisse Sicherheitsbehörden als auch der Rechtsschutzbeauftragte dem Bundesministerium für Inneres unterstehen.

Weiters darf nicht außer Acht gelassen werden, dass eine Überlastung des Rechtsschutzbeauftragten direkte Auswirkungen auf die Qualität bzw. Wirksamkeit der einzigen Kontrollinstanz mit sich bringen würde. Besonders wenn die Beanspruchung durch sehr viele Fälle gegeben ist, besteht die Gefahr, dass diese weniger konsequent verfolgt werden, als wie für den Betroffenen notwendig.

4.7 Anzahl der Anfragen nach SPG Abs. 3a und 3b

Mit 01.01.2008 ist die Novelle zum SPG in Kraft getreten. Da die Kontrollinstanz durch die Richter weggefallen ist, stellt sich die Frage, ob nicht die Auskunftsverlangen nach § 53 zugenommen haben. Hierbei ist ganz klar zu sagen, dass dies sehr wohl der Fall ist. Um dies zu untermauern möchte ich verschiedene Statistiken präsentieren. T-Mobile-Justiziar Klaus Steinmaurer gab bekannt, dass im Jänner 2008 doppelt so viele Standortpeilungen von Sicherheitsbehörden (63 mal) nur bei T-mobile durchgeführt wurden, wie im Vergleichsmonat Jänner 2007 bei T-mobile [FTZ]. Auch die Arbeiterkammer kam auf das Ergebnis, dass die Mobiltelefonortung massiv im Vergleich zu 2007 zugekommen hat. Arbeiterkammer Konsumentenschützerin Daniela Zimmer bezifferte die Zunahme der Handyortung im Vergleichszeitraum Jänner und Februar zum Vorjahr bei ca. 70 % [ORF]. Weiters war die Frage nach dem Umgang der Sicherheitsbehörden mit dem novellierten Gesetz, Teil einer parlamentarischen Anfrage. Der Abgeordnete Alexander Zach (ehemals Liberales Forum – 2008 im Klub der SPÖ) stellte im Juni 2008 eine Anfrage bezüglich der Zahlen der Mobiltelefonlokalisierungen und Ausforschungen von Internetusern. Der damalige Innenminister Günther Platter beantwortete diese Anfrage, dass im Zeitraum zwischen 01.01.2008 und 30.04.2008 258 Handybenutzer lokalisiert bzw. 3863 Internetuser ausgeforscht wurden [FTZ2]. Die Frage die sich hier stellt ist, ob die Zahlen vom Innenministerium stimmen, da wenn man allein die Zahlen von T-mobile hochrechnet auf 4 Monate, man auf einen höheren Wert kommt. Aber wenn man auch den Zahlen vom Innenministerium Glauben schenkt, würde dies bedeuteten, dass in Österreich im Durchschnitt täglich 2 Handybenutzer lokalisiert und 32 Internetuser ausgeforscht werden! Diese Statistiken aus unabhängigen Quellen als auch vom Innenminister selbst zeigen auf, dass die Zahlen massiv zugenommen haben. Einen wichtigen Punkt, der bei den vorgestellten Statistiken aber nicht berücksichtigt wurde, ist die Vergleichszahl zwischen Anträgen und Bewilligungen. Diese Zahlen gibt es seit der Novelle ja nicht mehr, da ja die Kontrollinstanz der Richter weggefallen ist. Da die Sicherheitsbehörden den Rechtsschutzbeauftragte des Innenministeriums nur bezüglich Dokumentation kontaktieren müssen, kann davon ausgegangen werden, dass die Höhe der Anträge mit der Höhe der Bewilligungen übereinstimmt. Um die wichtige Kontrollinstanz von unabhängigen Richtern zu untermauern, möchte ich in der nächsten Abbildung eine Gegenüberstellung von Anträgen und Bewilligungen vom Zeitraum 2003 bis 2006 präsentieren:

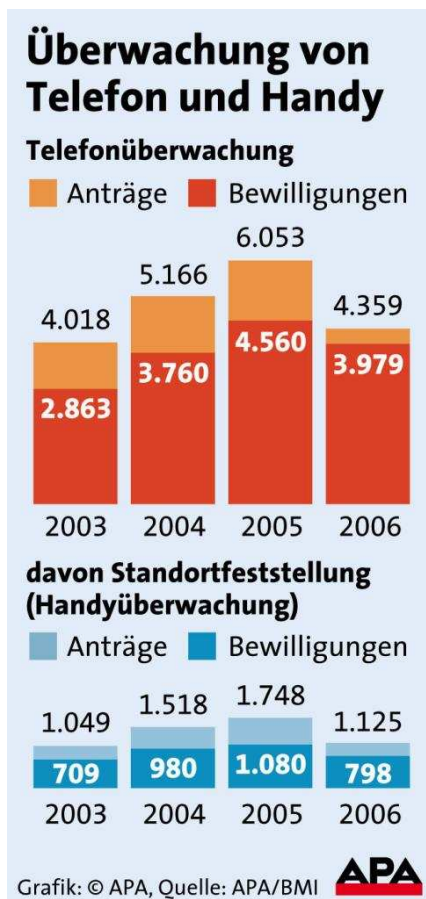


Abbildung 1: Überwachung von Telefon und Handy 2003 – 2006 [APA]

Die letzte Statistik bezüglich der Anzahl an Auskunftsverlangen gibt es durch die Anfrage von Nationalratsabgeordneten Peter Pilz von November 2008. Hierbei wurde ein Fragekatalog mit 60 detaillierten Fragen an die Frau Innenminister Maria Fekter gestellt [PAR4]. Weiters wurde in diesem Fragenkatalog versucht, die Begriffsbestimmung im SPG zu klären. Anfang 2009 wurden die Fragen von der Innenministerin beantwortet. Der Zeitraum der Statistiken erstreckt sich von 01.01.2008 bis 30.09.2008. Bezüglich §53 Abs. 3a Z1 gab es in diesem Zeitraum 4665 Auskunftsverlangen. Weiters gab es für §53 Abs. 3a Z2 39 und für §53 Abs. 3a Z3 1.308 Auskunftsverlangen. Bezüglich der Standortdaten von Mobilfunkteilnehmer (§53 Abs. 3b) wurde die Antwort gegeben, dass insgesamt im besagten Zeitraum 695 Auskunftsverlangen von den Mobilfunkbetreiber geholt wurden. Bezüglich den nicht sehr ausführlich gewährten Begriffsbestimmungen wurde als Antwort gegeben, dass die Begriffsbestimmungen im Gesetz ausdrücklich und abschließend angeführt sind und keine weiteren „Leitlinien“ benötigen [PAR5].

5 Stand der Entwicklung von technischen Überwachungsmaßnahmen im Bereich Mobilfunk

In diesem Kapitel möchte ich näher auf den aktuellen Stand der Entwicklung von technischen Überwachungsmaßnahmen eingehen. Neben den bereits erwähnten Überwachungsarten, wie der Einsatz von IMSI-Catcher oder der Einsatz von Trojaner, werden in diesem Kapitel noch weitere aktuelle Überwachungsgeräte bzw. Überwachungssoftware in Bezug auf dem derzeit aktuellen technischen Stand beleuchtet. Weiters soll in den folgenden Subkapiteln jeweils auch die Abwehr bzw. Schutzmöglichkeit vor diesen Überwachungsarten untersucht werden.

5.1 IMSI-Catcher

5.1.1 Einleitung & Hintergrund

Aufgrund der Entwicklung und der rasanten Verbreitung von mobilen Telekommunikationsgeräten, standen die staatlichen Strafverfolgungsbehörden bzw. Nachrichtendienste vor einer neuen großen Herausforderung. Zwar waren die Abhörmethoden bei Festnetze schon sehr ausgereift, aber durch die Einführung von mobilen Telekommunikationsgeräten war der Bezugspunkt bzw. die eindeutige Kennung nicht mehr ohne weiteres feststellbar. *„Solange observierte Personen das herkömmliche Telefonnetz (Festnetz) für ihre Kommunikation benutzen, lässt sich die für die Veranlassung einer Abhörmaßnahme oder die Ermittlung der Verbindungsdaten erforderliche Nummer des verwendeten Endgeräts unmittelbar aus dem Standort ableiten.“* [FOX] Wenn somit der Standort des „Verdächtigten“ bekannt war, wurden aufgrund eines richterlichen Beschluss und mit Mitwirkung des Netzbetreibers die Anschlusskennung bzw. Verbindungsdaten ausgewertet. Weiters war aufgrund der Einschränkung des Standortes leicht möglich Wanzen oder andere Abhörgeräte zu installieren. Dies änderte sich schlagartig mit dem rasanten Aufstieg des Mobiltelefons.

Im Gegensatz zu Festnetzanschlüssen ist es bei mobilen Kommunikationsendgeräten nicht mehr möglich einen Konnex zwischen dem Aufenthaltsort eines Mobiltelefonbenutzers und der Anschlusskennung herzustellen. Auch der Name des Mobiltelefonnutzers ist nicht zwangsläufig wichtig, da bei pre-paid Mobiltelefonen keine Verträge abgeschlossen werden und somit keine Authentifizierung vorherrscht.

1997 wurde erstmals in den Medien berichtet, dass es eine Möglichkeit gab, die Endgeräteerkennung eines Mobiltelefons zu bestimmen und somit das Mobiltelefon auch zu lokalisieren: der IMSI-Catcher (IMSI steht für International

Mobile Subscriber Identifier siehe Kapitel 5.1.2.1.3 Adressierung von Geräten bzw. Benutzern). Dieses Gerät wurde ursprünglich als Test- und Messsystem in der Firma Rohde & Schwarz eingesetzt. Dieses wurde dann von der Firma Rohde & Schwarz für den Zweck der Bestimmung der Endgeräteerkennung eines Mobiltelefons weiterentwickelt und im Dezember 1996 den staatlichen Ermittlungsbehörden bzw. Mobilfunkanbietern in Deutschland vorgestellt. Bevor ich nun näher auf den Funktionsumfang und die Ziele eines Einsatzes eines IMSI-Catcher eingehen werde, möchte ich noch einen Exkurs über Mobiltelefonie, indem die Netzwerkgenerationen GSM bzw. UMTS näher beleuchtet werden, durchführen. Dies ist notwendig, um die Funktionalität eines IMSI-Catchers genau beschreiben zu können.

5.1.2 Exkurs Mobiltelefonie

Mobiltelefonie hat das tägliche Leben dermaßen verändert, dass es aus der heutigen privaten als auch der beruflichen Welt nicht mehr wegzudenken ist. Somit kann man behaupten, dass die Mobiltelefonie die bekannteste Netzwerktechnologie ist. Durch diese Netzwerktechnologie wird es ermöglicht, dass man jederzeit bzw. überall eine Sprachverbindung mit einem anderen Mobilfunkteilnehmer oder einem Festnetzteilnehmer aufnehmen kann. 1992 wurde einerseits durch die Digitalisierung der Mobilfunk-Endgeräte und andererseits durch die Miniaturisierung der Bauteile die Preise enorm gesenkt und somit der Konsummarkt für die breite Masse erschlossen. Durch den Mobiltelefon-Standard, der sich fast weltweit etabliert hat, konnten Mobiltelefone für einen sehr großen Markt produziert werden, was in weiterer Folge wieder zu einem Preisverfall führte. Nicht nur der stetige Preisverfall kam den Endkunden zu gute, sondern auch die Möglichkeit länderübergreifend mobil zu telefonieren. Dies war aufgrund von Abkommen zwischen den Mobilfunkbetreibern möglich. *Der Begriff Mobilfunk wird oft in Verbindung mit Mobiltelefonie gebracht, so dass sich die Bezeichnung PLMN (Public Land Mobile Network) in der englischsprachigen Literatur eingebürgert hat.* [STM] Die Mobilfunktechnologie kann man in insgesamt 4 Generationen einteilen, die in der nächsten Tabelle beschrieben wird.

Art der Technologie-Generation	Beschreibung
1. Mobilfunk-Generation	Analoge Netze, wie A-,B- und C-Netze: In Österreich wurde nur das analoge C-Netz (unter dem Namen D-Netz) 1990 von der Mobilkom eingeführt. Dieses wurde dann 2002 abgeschaltet, da das GSM-Netz (2. Generation) diese Art von Netz abgelöst hat. A- und B-Netze gab es z.B in Deutschland in den 70er Jahren, die aber nicht von der breiten Maße genutzt wurden (Preis!): zwischen 10.000 – 30.000 Benutzern
2. Mobilfunk-Generation	Digitale GSM-Netze, D-Netz (1992 GSM-Standard

	900 MHz) und E-Netze (1994 GSM-Standard Erweiterung 1800 MHz und DES 1800 MHz (Digital Cellular System 1800)). Ein Mobiltelefon, das diese beiden Standards unterstützt, wird Dual-Band Mobiltelefon genannt. Mit diesem Dual-Band Mobiltelefon konnte man in die meisten Länder der Welt telefonieren, ausser den USA und Japan. In diesen Ländern hatte man das Problem, dass noch ein Analog-System (genannt Advanced Mobile Phone Service) oder eine inkompatible GSM-Variante verwendet wurde: GSM 1900. Damit man in Europa und in den USA flächendeckend telefonieren konnte, braucht man ein Triband-Mobiltelefon, dass alle 3 GSM-Varianten mit folgenden Frequenzen beherrschte: 900, 1800 und 1900 MHz. In Österreich wurde das GSM-Netz 1993 (unter der Bezeichnung E-Netz) eingeführt.
3. Mobilfunk-Generation	UMTS-Netze (Universale Mobile Telecommunications System) Durch die verbesserten Datenraten war vermehrt der Fokus auf den Zugang zu Internet-Diensten. Die ersten UMTS Netze wurden in Österreich 2002 eingeführt.
4. Mobilfunk-Generation	LTE-Netze (Long Term Evolution) Hierbei werden neue Standards im Bereich der Datenübertragung (Multiple Input Multiple oder Orthogonal Frequency Division Multiplexing Access) eingesetzt, mit denen man 100 MBit's im Download- sowie 50 Mbit's im Upload-Bereich erreichen könnte. Diese Netze sind aber erst in der Testphase und werden frühestens 2010 pilotiert werden. In Österreich besteht generell die Frage, ob dieser Technologiesprung vollzogen wird, da eine Vergabe von neuen Frequenzbänder erforderlich sei

Tabelle 3: Mobilfunk-Generationen

Da für den IMSI-Catcher nur die 2. und 3. Generation (GSM & UMTS) relevant sind, werden nur diese Technologie-Standards in den nächsten Kapiteln beleuchtet.

5.1.2.1 GSM

5.1.2.1.1 Einleitung

GSM steht für Global System for Mobile Communication und 1982 wurde als erster Schritt eine Arbeitsgruppe Group Special Mobile gegründet. Diese Arbeitsgruppe hatte als Ziel einen europäischen digitalen Mobilfunk zu entwickeln. In den weiteren Jahren wurde diese Arbeitsgruppe 1989 in die europäische Normungsgruppe ETSI (European Telecommunications Standards Institute) als Technical Committee aufgenommen. Als der Standard GSM dann schon etabliert war, wurde der Standard der TSG GERAN (Technical Specification Group GSM EDGE Access Network) überführt und wird dort auch weiter spezifiziert. Diese Gruppe untersteht wiederum der 3GPP (3rd Generation Partnership Project), die auch den Standard UMTS spezifiziert. Die Zielsetzung von GSM wurde daraufhin ausgelegt, dass viele Millionen Kunden pro Netzwerk versorgt werden können. Dies war natürlich ein Meilenstein in der Mobiltelefonie, da dies bei analogen Netzen nicht der Fall war. Der Fokus bei GSM wurde dezidiert auf den Massenmarkt ausgelegt, wobei keine Einschränkung auf die Anzahl der Mobilfunkbetreiber besteht. Dies ist derzeit in den meisten europäischen Ländern der Fall, wo mehrere Mobilfunkbetreiber dieselbe Fläche abdecken. Für die Mobilfunkbetreiber war natürlich die Zielsetzung eine vollständige Flächenabdeckung innerhalb des Landes zu erreichen, um den Teilnehmern zu ermöglichen, innerhalb des ganzen Landes mobil telefonieren zu können. Da die Teilnehmer mobil sind und innerhalb des Netzes Funkzellen wechseln können, muss die Gesprächsverbindung von einer Basisstation zur nächsten Basisstation übergeben werden. Diesen Prozess ist in der Spezifikation als Handover vermerkt. Falls der Teilnehmer das Netz verlässt und sich in einem anderen Netz anmeldet, ist er weiterhin unter seiner Nummer erreichbar und kann auch aktiv telefonieren. Dies passiert auf so genannte Roaming-Abkommen zwischen den Netzbetreibern, die somit das mobile Telefonieren über Ländergrenzen und die Abrechnung der Kosten ermöglichen.

Neben dem mobilen Telefonieren bieten GSM Netze eine weitere Anzahl an zusätzlichen Diensten an. Der Teilnehmer kann einem anderen Teilnehmer Text/Bild/Ton Kurznachrichten schicken (SMS – Short Message Service; MMS Multimedia Message Service; EMS – Enhanced Message Service). Neben diesen Services wurde speziell in den letzten paar Jahren es immer populärer, Internetinhalte auf den Mobilfunkgeräten, mit Hilfe von Datendiensten abzurufen. Hierfür werden verschiedene Technologien, wie WAP (Wireless Application Protocol), GPRS (General Packet Radio Service) oder EDGE (Enhanced Data Rates for GSM Evolution) verwendet.

5.1.2.1.2 Architektur

Da die Architektur des GSM-Netzes für den Einsatz des IMSI-Catcher relevant ist, möchte ich in diesem Subkapitel noch einen kleinen Überblick darüber geben. Das GSM Netz ist in 3 Subsystemen aufgegliedert:

- dem Betriebssubsystem (engl. Operation and Maintenance Subsystem OMSS)

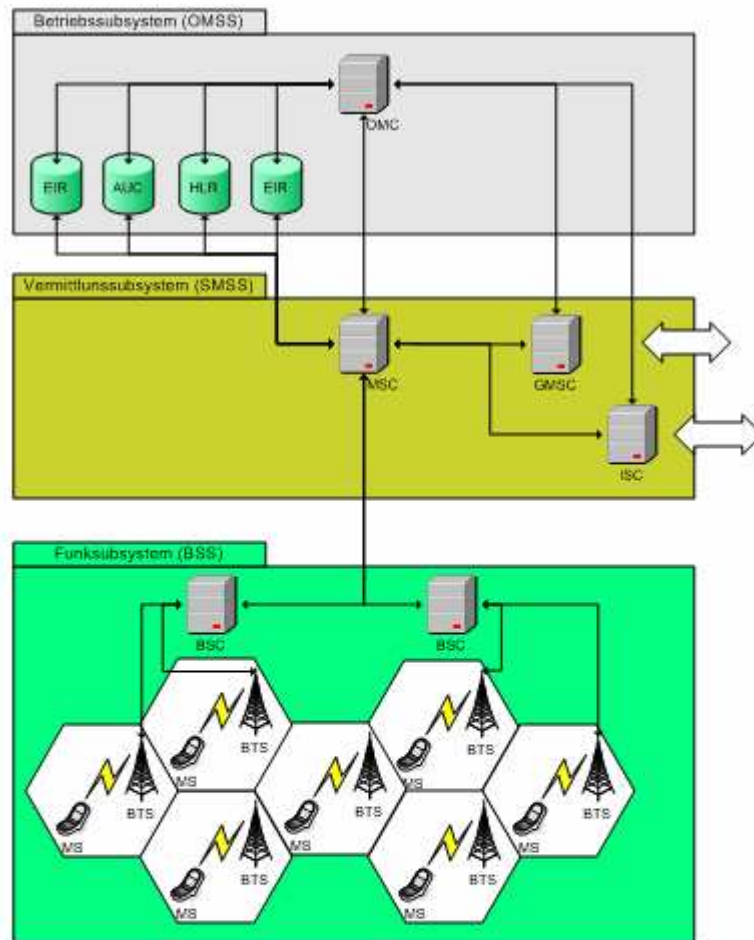
- dem Vermittlungssubsystem (engl. Mobile Switching and Management Subsystem SMSS)
- dem Funksubsystem (engl. Base Station Subsystem, BSS)

Das Betriebssubsystem hat als Aufgabe die Administration und Kontrolle des Netzwerkes. Hierbei ist der Kern dieses Subsystem das OMC (Operation and Maintenance Center). Die wichtigsten Aufgaben dieses Center sind die Verwaltung Kundendaten, Gebührenverrechnung, Statistiken sowie die Konfiguration als auch die Sicherheit des Netzes. Insgesamt gibt es noch vier weitere Datenbanken im Betriebssubsystem. Eine dieser Datenbank stellt die AUC (Authentication Center) dar, die vertrauliche Daten und die Schlüssel des Kunden speichern. Diese Daten werden somit herangezogen, wenn sich der Benutzer authentifiziert. In der zweiten Datenbank, genannt EIR (Equipment Identify Register) werden die Seriennummer der Endgeräte gespeichert. Weitere Datenbanken sind die HLR (Home Location Register) und VLR (Visitor Location Register). Im HLR werden Informationen über die Teilnehmer des Funknetzeigentümers gespeichert. Hingegen im VLR werden Informationen über alle Teilnehmer gespeichert, die sich in diesem Netz aufhalten.

Das Vermittlungssubsystem hat die Aufgabe die Nutzdaten innerhalb des Netzes weiterzuleiten und stellt somit das Bindeglied zwischen dem Betriebssubsystem und dem Funksubsystem dar. Weiters stellt es eine Anbindung an andere Netze zur Verfügung. Die wichtigste/n Komponente bzw. Komponenten stellen die MSC (Mobile Switching Center) in diesem Subsystem dar. Wie gerade erwähnt, kann es in einem Netzwerk auch mehrere MSC geben, die so genannte Areas abdecken. MSC bewerkstelligen einerseits die Verbindung zu anderen Netzen und andererseits den Netzwerkverkehr innerhalb der Funksubsysteme. Weiters übernimmt der MSC die Lokalisierung der Benutzer. Hierbei werden wiederum die Datenbanken HLR und VLR genutzt. Weitere Komponenten des Vermittlungssubsystem sind die GMSC (Gateway Mobile Switching Center) und ISC (International Switching Center). Das GMSC ermöglicht es, dass Kunden des Netzes auch mit Teilnehmer von Festnetzen oder anderen Mobilfunkbetreiber kommunizieren können. Das ISC hingegen ist für den Datenverkehr mit anderen Ländern zuständig.

Das Funksubsystem besteht aus insgesamt 3 Komponenten: MS (Mobile Stations), BTS (Base Transceiver Station) und BSC (Base Station Controller). Mit MS ist in der GSM Terminologie das mobile Endgerät gemeint. Der BTS besteht aus einem Sender- und Empfängersystem und ein paar zusätzlichen Komponenten. Als wichtigste Aufgabe des BTS zählt das Abarbeiten des Protokolls zur Datenübertragung der Funkschnittstelle. Somit wickelt das BTS die Kommunikation zwischen MS und dem GSM Netz ab. Die BTS ist nur für ihren Bereich bzw. Zelle zuständig, d.h. für alle MS in diesem Bereich. Der BSC kontrolliert wiederum mehrere BTS und gewährleistet die Weiterleitung der Daten. Weiters ist der BSC dafür zuständig, dass das Weiterreichen in eine andere Zelle (wie oben schon beschrieben: genannt Handover) funktioniert. Die Kommunikation zwischen BTS und BSC funktioniert entweder leitungsgebunden (z.B.: Glasfaser) oder wird über Richtfunkstrecken vollzogen. Um das

Zusammenspiel der 3 Subsysteme nochmals besser zu veranschaulichen, hier eine Übersicht aller Komponenten bzw. Datenbanken in einem GSM-Netz:



Legende:

Komponenten:

MS	Mobile Stations
BTS	Base Transceiver Station
BSC	Base Station Center
MSC	Mobile Switching Center
ISC	International Switching Center
GMSC	Gateway Mobile Switching Center
OMC	Operation & Maintenance Center

Datenbanken:

EIR	Equipment Identifier Register
AUC	Authentication Center
HLR	Home Location Register
VLR	Visitor Location Register

Abbildung 2: Architektur eines GSM-Netz

[BWA]

5.1.2.1.3 Adressierung von Geräten bzw. Benutzern

Im GSM Netz werden einerseits die Geräte (MS) und andererseits die Mobilfunkbenutzer unterschiedlich identifiziert. Die Mobilfunkbenutzer werden anhand einer Chipkarte, genannt SIM-Karte (Subscriber Identifier Module), erkannt. Diese Chipkarten werden vom Mobilfunkbetreiber an den

Mobilfunkbenutzer ausgegeben und in den MS eingesetzt. Folgende Daten werden auf der SIM-Karte gespeichert:

- Veränderbarer Pin (Geheimnummer) zum Schutz vor unbefugter Benutzung
- Speicher von Telefonbuch bzw. Notizen
- Speicher von SMS Nachrichten
- Speicher der zuletzt gerufenen Telefonnummern
- Speicher von geheimen Nummern und Algorithmen: Diese dienen zur Verschlüsselung und Signalisierungsdaten. Beispiele hierfür sind die eindeutige Benutzernummer oder technische Daten des Mobilfunkbetreibers, wie z.B.: die zugeordneten Frequenzen

Wie gerade oben beschrieben, gibt es eine eindeutige Benutzerkennung für jeden Mobilfunkteilnehmer. Diese eindeutige Benutzerkennung wird IMSI (International Mobile Subscriber Identity) genannt und kann auch nicht vom Benutzer geändert werden. Die IMSI ermöglicht es jeden Mobilfunkteilnehmer auch in fremde Netze sich zu identifizieren. Somit können Telefonate nur dann durchgeführt werden, wenn die SIM-Karte (und somit auch die IMSI gelesen werden kann) im MS eingelegt ist. Einzige Ausnahme in gewissen Netzen sind hierbei Notrufe, die auch ohne SIM-Karte getätigt werden können. Die Länge der IMSI ist immer 15 Zeichen und ist, wie in der nächsten Tabelle ersichtlich, aufgebaut:

Bezeichnung	Länge	Beispiele für Österreich
Mobile Country Code (MCC)	1-3	232
Mobile Network Code (MNC)	4-5	01 = A1, 03 = T-Mobile, 05 = Orange
Mobile Station Identification Number (MSIN)	6-15	3321256545 muss immer eindeutig sein

Tabelle 4: Aufbau einer IMSI

Wie bei der Benutzerkennung gibt es eine eigene eindeutige Kennung der MS: die IMEI (International Mobile Station Equipment Identity). Wie auch bei der IMSI kann die IMEI nicht vom Benutzer verändert werden. Diese Kennung wird bei der Herstellung des MS vergeben und ist weltweit eine eindeutige Nummer. Vom Mobilfunkbetreiber wird die IMEI in der EIR gespeichert und ist wie folgt aufgebaut. Die ersten 6 Ziffern bilden den TAC (Type Approval Code). Hierbei bilden die ersten zwei Ziffern die zulassende Stelle und die letzten 4 Ziffern den Zulassungscode. Da der TAC eindeutig ist kann auch nur dieser Code zur Identifizierung der MS herangezogen werden. Nach dem TAC bilden die nächsten zwei Zeichen den FAC (Final Assembly Code). Dieser bildet den Herstellercode der MS. Bei neueren Versionen von MS entfällt der FAC und der TAC ist 8 Ziffern lang. Die nächsten 6 Ziffern stellen die Seriennummer (Abk. SNR) dar. An der letzten Stelle bildet eine Prüfziffer, genannt CN (check digit)

[3GP1].

IMEIs werden im GSM Netz in der EIR-Datenbank gespeichert. Hierbei gibt es mindestens 3 Kategorien, in die sie eingeteilt sein kann:

- White List: Diese speichert alle Gerätenummern der registrierten MS
- Black List: In dieser Liste sind alle MS, die als gestohlen oder verloren gemeldet wurden und vom Teilnehmer gesperrt wurden. Diese Liste wird unter allen Mobilfunkbetreibern ausgetauscht, damit das gesperrte Gerät in keinem Netz mehr betrieben werden kann.
- Grey List: Diese optionale Liste wird dafür verwendet gewisse Services zu sperren. Dies ist z. B.: bei MS mit Funktionsstörungen notwendig.

Neben den eindeutigen Nummern der Benutzerkennung (IMSI) und der MS (IMEI) gibt es einige weitere wichtige Nummern, die für das Verständnis des GSM-Netzes relevant sind.

Die MSISDN (Mobile Subscriber Integrated Services Digital Network) stellt die eigentliche Telefonnummer der MS dar. Die Telefonnummer ist eindeutig, aber es kann eingerichtet werden, dass ein MS mehrere MSISDN's zugewiesen bekommt. Die MSISDN wird in der HLR gespeichert und wird bei einem Gespräch auf die IMSI abgebildet. Die MSISDN besteht aus der Ländervorwahl (z.B: Österreich +43), Provider (z.B: Österreich 664, 676, 699, usw.) und der eindeutigen Nummer beim Provider (7 bzw. 8 Stellen in Österreich). Interessant bei dieser Nummer ist, dass sie Bestandteil des ISDN-Nummernplans ist und deswegen auch den Bestandteil im Namen hat.

Die TMSI (Temporary Mobile Subscriber Identity) ist eine lokale bzw temporär vergebene Nummer, die anstatt der IMSI übermittelt wird. Diese Nummer wird bei jedem Handover neu vergeben und auf der SIM-Karte gespeichert, um so die Anonymität des Teilnehmers zu gewähren und die Erstellung von Bewegungsprofilen zu erschweren.

Eine weitere wichtige Nummer im GSM-Netz ist die MSRN (Mobile Station Roaming Number). Jene Nummer wird temporär vergeben, wenn der Teilnehmer das eigene Netz verlässt und zu einem fremden Netz wechselt. Diese Nummer ist für die Gesprächspartner nicht ersichtlich, sondern wird nur zwischen den Providern ausgetauscht.

Zum Abschluss möchte ich noch folgende zwei Nummern beleuchten: LAI () und CI (): Diese beiden Nummern bewerkstelligen die eindeutige internationale Identifikation einer Funkzelle. Diese beiden Nummern werden ständig von der BTS an die MS in ihrer Reichweite (Funkzelle) gesendet. Am MS kann somit festgestellt werden, in welcher Funkzelle es sich gerade befindet.

5.1.2.2 UMTS

5.1.2.2.1 Einleitung

Zur dritten Mobilfunkgeneration zählt der Standard UMTS (Universale Mobile Telecommunications System). Die Einführung eines neuen Standards nach GSM

ging darauf zurück, dass die Datenübertragungsraten bei GSM nicht ausreichend für gewisse Dienste waren. Deswegen wurde in den 90er Jahren von der ITU (International Telecommunication Union) ein Aufruf gestartet, dass ein neuer Mobilfunkstandard bis 2000 gefunden wird. Die Zahl 2000 im Namen wurde genommen, da als Start des Mobilfunkstandards das Jahr 2000 geplant war. Unter dem Namen IMT2000 (International Mobile Telecommunication 2000) sollten Vorschläge für die dritte Mobilfunkgeneration eingereicht werden. Die Standardisierung von UMTS wurde von 3GPP (3rd Generation Partnership Project), das wiederum aus 5 Standardisierungsgremien (darunter ETSI European Telecommunications Standards Institute) besteht, übernommen. Wie schon oben beschrieben, ist auch das 3GPP für die Weiterentwicklung von GSM zuständig.

Bei der Architektur des neuen Mobilfunkstandards wurde Wert darauf gelegt, dass die verschiedensten Nutzungsszenarien der Teilnehmer bedacht werden. Hierzu zählen multimediale Dienste, die durch neue satelliten- und erdgestützte Sendeanlagen angeboten werden können. Wie schon erwähnt, war die enorme Verbesserung der Datenrate der Meilenstein (bis zu max. 2 MBit/s), um ganz neue Möglichkeiten von Mobilfunkanwendungen, wie z.B. der Videotelefonie, anzubieten. Bei GSM war der Bereich Multimedia aufgrund der Einschränkung der Datenrate (zwischen 9 – 14 kbit/s) nicht im Vordergrund und konnte erst mit UMTS voll ausgenutzt werden.

Hier eine kurze Auflistung, für welche Bereiche bzw. Anwendungen UMTS eingesetzt wird:

- Zwischenmenschliche Kommunikation: Dies inkludiert sowohl Audio- als auch Videotelefonie. Wenn beide Teilnehmer UMTS Mobiltelefone mit Kamera besitzen, besteht der Vorteil auch den Gesprächspartner zu sehen und nicht nur zu hören.
- Nachrichtendienste: Neben den herkömmlichen Diensten, wie SMS, MMS usw., wurden auch neue Bereiche, wie Video-Sprachmail, Instant-Messaging oder Unified Messaging, erschaffen. Hierbei ist erwähnenswert, dass UMTS sowohl paket- als auch leitungsvermittelte Übertragung ermöglicht.
- Informationsverteilung: Hierzu zählen das Browsing im World Wide Web, Informationsdienste bzw. öffentliche Dienste. Speziell die Abfrage von Finanzdaten wird hierbei sehr stark genutzt. Dazu zählen Onlinebanking, Abfragen von Börsenkursen, Micro- und Macropayment und Beratungsdienste. Weiters unterstützt UMTS den Zugang zu anderen Netzwerken, wie ISDN bzw. TCP/IP. Somit unterstützt UMTS asymmetrischen Datenverkehr, dies bedeutet z.B. hohe Übertragungsraten im Downlink und niedrige Übertragungsraten im Uplink Bereich, wie es bei einem Nutzer des Internets auftritt. Somit besteht der Vorteil, dass gleichzeitig Daten übertragen werden können und auf das Internet zugegriffen werden kann.
- Roaming und Handover: Diese zwei Funktionen müssen auch zwischen verschiedenen Anbietern bzw. Funkzugängen funktionieren. D. h. z.B: das ein Handover auch mit einem GSM-Mobiltelefon aus der zweiten Mobilfunk Generation möglich sein muss.

- Standortbezogene Dienste: Anwendungen, wie persönliche Navigation, Abfrage von lokalen Informationen, und Fahrerunterstützung, helfen dem Benutzer des UMTS-Mobiltelefons bei etwaigen Problemen. Hierbei wird auch immer öfters von VHE (Virtual Home Environment) gesprochen. Dies ermöglicht dem Benutzer die Speicherung seiner benutzerspezifischen Konfiguration, um diese auch in anderen Netzen zu nutzen. Somit unabhängig von der Position des Benutzers, ist dieser in der Lage seine Dienste zu benutzen.
- Unterhaltung: Wie schon oben erwähnt, besteht bei UMTS der Vorteil der Nutzung von Multimedialinhalten, die über das Internet heruntergeladen werden. Dieser Bereich erstreckt sich von der Nutzung von interaktivem Fernsehen, Download von E-Books, Spiele, Videoclips bis hin zu Music-on-Demand.

5.1.2.2.2 Architektur

Die Architektur von UMTS kann grob in drei Subsysteme bzw. Domänen eingeteilt werden:

- Endgeräte-Domäne (engl. User Equipment Domain)
- Zugangsnetz-Domäne (engl. Access Network Domain)
- Kernnetz-Domäne (engl. Core Network Domain)

Die Endgeräte-Domäne besteht aus der Mobilen Einheit (MS) und dem UMTS Teilnehmeridentitätsmodul, genannt USIM (UMTS Subscriber Identity Module). Physikalisch gesehen ist das USIM ein Bestandteil der SIM-Karte und enthält alle Informationen bzw. Funktionen, um die Verschlüsselung über die Kommunikationsschnittstelle und die Authentifizierung der Mobilen Einheit gegenüber dem Netz durchzuführen.

Die Zugangsnetz-Domäne hat als Aufgabe, den Teilnehmern den Zugang zum UMTS-Netz zu ermöglichen bzw. den Zugang zu den Transportnetzen zu erstellen. Die Realisierung des Zugangsnetzes wird durch ein UMTS Terrestrial Radion Access Network (UTRAN) oder einer GSM BSS bewerkstelligt. Unter eines GSM BSS versteht man eine Kombination aus GSM und GPRS. Die Komponenten des Zugangsnetz sind das Funknetzsystem (RNS Radio Network Subsystem), Funknetzsteuerung (RNC Radio Network Controller), Node B und den Zellen. Die Bestandteile des RNS sind genau eine RNC und mehrere Node B. Die Aufgabe des RNC ist die Verwaltung des Funkbetriebsmittels und die Koordination der Node B's. Ein Node B übernimmt die Implementation der Funkübertragung in den zugeordneten Zellen, wobei sie mehrere Zellen bedienen kann. Wie auch bei GSM ist das Sende- und Empfangsgebiet in Zellen eingeteilt. Der Unterschied zu GSM besteht aber, dass sich Zellen überdecken können. Die Kategorisierung der Zellen wird aufgrund der geographischen Ausdehnung der Versorgung vollzogen. Hier die Einteilung der Zellen:

- Pikozellen: Diese Zellen haben eine Größe bis zu 60 Metern und sind normalerweise innerhalb von Gebäuden. Die Pikozellen werden an stark frequentierten Orten, so genannte Hot-Spots, wie Bahnhöfe, Flughäfen, Firmenzentralen, usw.
- Mikrozellen: Die Größe hierbei geht bis zu mehreren Kilometern und deckt Bereiche von Städte bzw. Vorstädte ab.
- Makrozellen: Diese Zellen sind für das ländliche Gebiet vorgesehen und erstrecken sich über einige 10 Kilometer.
- Satelliten: Diese decken noch größere Zellen ab.

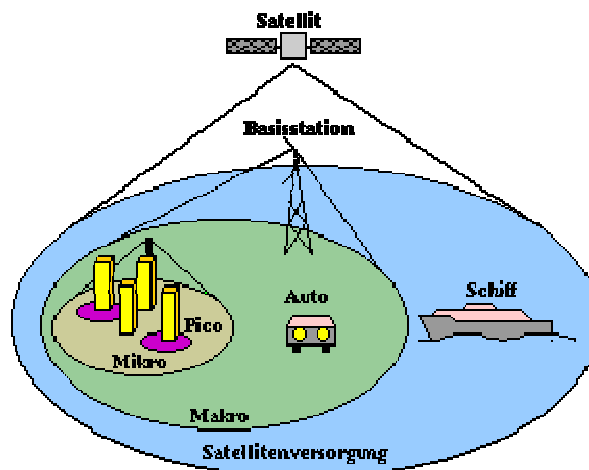


Abbildung 3: UMTS Zellen [FLM]

Angesprochen wurde in diesem Kapitel die Verbesserung der Datenrate auf max. 2 Mbit/s. Diese ist aber nur in Pikozellen möglich, wenn der Teilnehmer sich nicht schneller als 10 km/h bewegt und die Zellenauslastung optimal ist. Somit kann festgehalten werden, dass der aktuelle Standort, Entfernung zur Basisstation, Bewegungsgeschwindigkeit des Teilnehmers und die Zellenauslastung Einflussfaktoren für die Datenübertragungsrate bei UMTS sind.

Die Kernnetz-Domäne kann man als Plattform bezeichnen, die aus verschiedenen Transportnetzen bestehen kann. Transportnetze können hierbei GSM, Internet oder ISDN sein. Diese Transportnetze können mittels so genannten Interworking Units verbunden sein. Zu den Komponenten der Kernnetz-Domäne zählen das Mobile Switching Center (MSC), Home Location Register (HLR), Visitor Location Register (VLR), Equipment Identity Register (EIR), Authentication Center (AUC), Serving GPRS Support Node (SGSN), Gateway GPRS Support Node (GGSN) und Gateway Mobile Switching Center (GMSC). Da die meisten Begriffe schon im Kapitel 5.1.2.1.2 GSM Architektur erklärt wurden, möchte ich hier nur mehr auf die Begriffe SGSN und GGSN eingehen. Der SGSN hat als Aufgabe ein bestimmtes geographisches Versorgungsgebiet und leitet in diesem alle Datenpakete zu einem MS bzw. vom MS gesendete, weiter. Weiters übernimmt der SGSN das Sitzungsmanagement, Mobilitätsmanagement sowie die Verbindung zu anderen funktionalen Komponenten im UMTS-Netz.

Mit dem GGSN wird die Anbindung des Kernnetzes an externe Datennetze ermöglicht. Beispiele hierfür sind die Anbindung an einem Internet Service Provider (ISP) bzw. eine Anbindung an einem privaten Datennetz (Intranet). Der GGSN übernimmt im Kernnetz alle Datenpakete in die Richtung eines externen Datennetzes und leitet alle eingehenden Datenpakete an den zuständigen SGSN weiter. Hierbei ist auch eine Filterung der Pakete möglich.

In der nächsten Abbildung ist die Architektur eines UMTS-Netzes nochmals graphisch dargestellt:

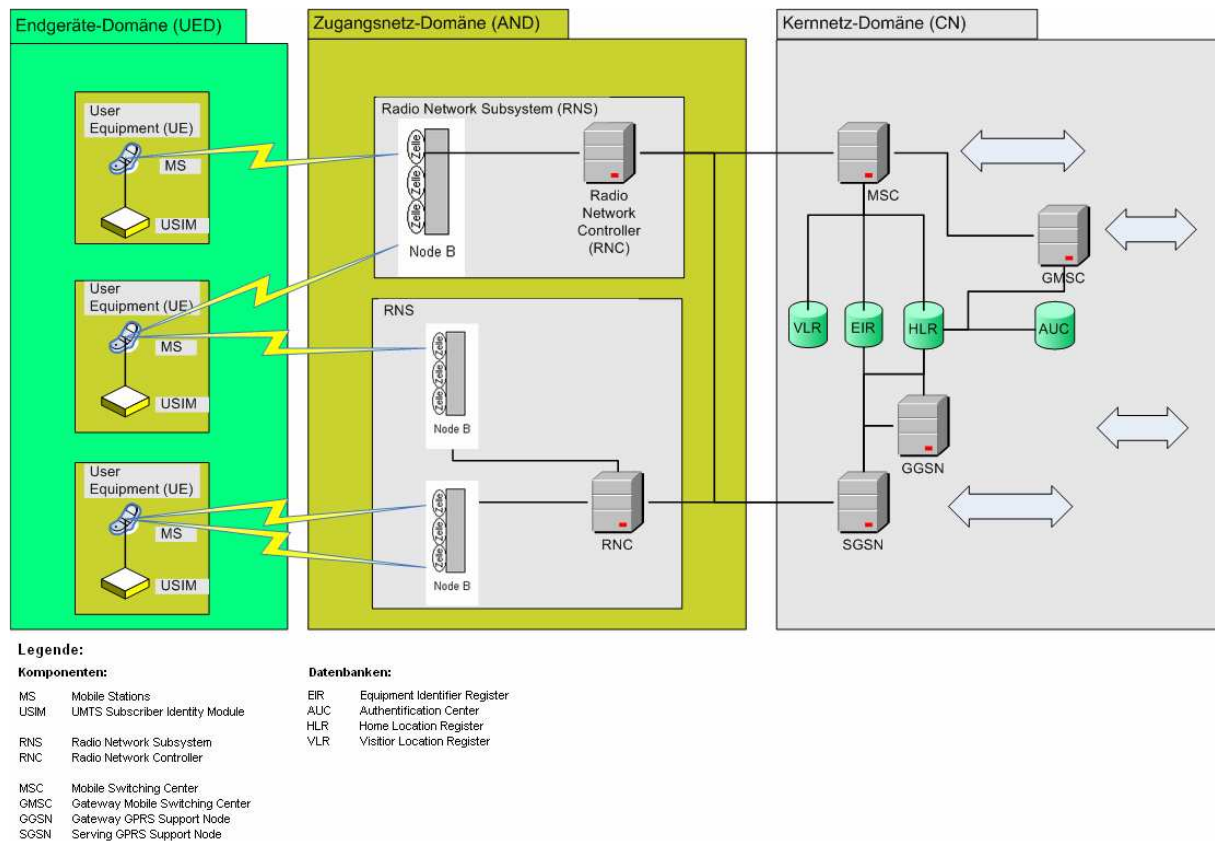


Abbildung 4: Architektur eines UMTS-Netz

[BWA]

5.1.3 Funktionsumfang

Der IMSI-Catcher an sich besteht aus einem Laptop mit spezieller Ergänzungssoftware, einer leistungsfähigen Antenne, mehreren Messgeräten und einem oder mehreren Mobiltelefonen zum Abhören der Gespräche. Hier eine Abbildung eines IMSI-Catchers, wie er in Deutschland vom Verfassungsschutz eingesetzt wird bzw. wurde.

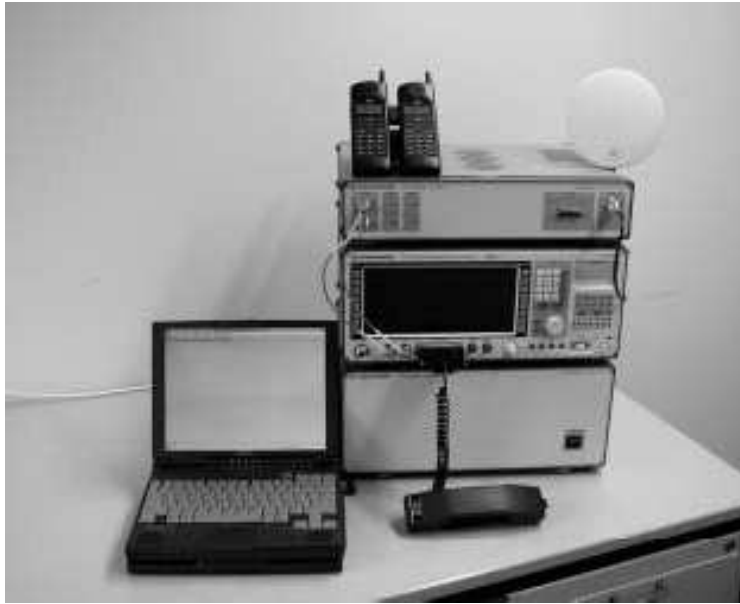


Abbildung 5: IMSI-Catcher Anlage [WZI]

Der IMSI-Catcher arbeitet grundsätzlich in 2 Betriebsmodi: Fangen und Abhören. Geräte, die Gespräche Fangen oder auch zusätzlich Abhören sind grundlegend gleich aufgebaut, wobei bei jenen Geräten, die Gespräche auch Abhören, zusätzlich Software bzw. ein nachgeschaltetes Mobiltelefon verwendet wird. Somit können folgende Funktionen bzw. Einsatzgebiete bei einem IMSI-Catcher festgehalten werden: die Ermittlung der IMSI, die Ermittlung der IMEI, das Lokalisieren des mobilen Endgeräts und das Abhören der Gespräche. In den nächsten Unterkapiteln wird auf die einzelnen Funktionen näher eingegangen.

5.1.3.1 Ermittlung der IMSI bzw. IMEI

Wenn die Sicherheitsbehörden die IMSI bzw. IMEI ermitteln möchten, dann wird wie oben beschrieben ein IMSI-Catcher im Fangmodus verwendet. *Zur Ermittlung der IMSI simuliert ein IMSI-Catcher die Basisstation einer regulären Funkzelle eines Mobilfunknetzes.*[FOX] Da die simulierte Basisstation (IMSI-Catcher) mit einer stärkeren Leistung als die anderen Basisstationen (BTS) arbeitet, melden sich alle Mobiltelefone bei der neuen vom IMSI-Catcher generierten Funkzelle an und nicht bei den eigentlichen Basisstationen. Hierbei melden sich aber nur eingeschaltete Mobiltelefone im Standby Modus an, d.h. Mobiltelefone die gerade ein aktives Gespräch haben, können vom IMSI-Catcher nicht erfasst werden. Im Detail funktioniert dies wie folgt: Der IMSI-Catcher schickt zuerst eine neue LAI aus. Durch diese werden die Mobiltelefone dazu gebracht mit dem Mobilfunknetz Kontakt aufzunehmen. Dies wird in der Mobiltelefonie Location Update Prozedur genannt. Nun wenn das Mobiltelefon in der Funkzelle zugeordnet ist, schickt die simulierte Basisstation (IMSI-Catcher) einen Identity Request an alle ihm zugeordneten Mobiltelefonen. Diese

antworten wiederum mit einem Identity Response, der die IMSI, TMSI bzw. IMEI inkludiert. Hierbei ist festzuhalten, dass der IMSI-Catcher nicht nur die TMSI erfährt, sondern auch das Mobiltelefon dazu zwingt die eindeutige IMSI preiszugeben. Die oben beschriebene Vorgehensweise des IMSI-Catchers beruht auf einer Schwachstelle der GSM Spezifikation. Das Mobiltelefon muss sich zwar bei der Basisstation authentifizieren, aber nicht die Basisstation beim Mobiltelefon. Aufgrund der einseitigen Authentifizierung ist diese Überwachungsart für Sicherheitsbehörden leicht möglich. In der Literatur wird diese Art des Angriffs als Maskerade-Angriff bezeichnet.

Nicht nur die IMSI kann durch den IMSI Catcher ermittelt werden, sondern auch die eindeutige Gerätekennung IMEI. Da oft Benutzer mehrere SIM-Karten bei einem Mobiltelefon verwenden, und diese mehrmals wechseln, kann die Bestimmung der eindeutigen Gerätekennung für Sicherheitsbehörden von Bedeutung sein. Durch den oben beschriebenen Prozess des Identity Request bzw. Response kann die IMEI des Gerätes an den IMSI-Catcher übermittelt werden.

5.1.3.2 *Lokalisieren des mobilen Endgeräts*

Gewisse Modelle (siehe Kapitel 5.1.4 Modelle bzw. IMSI-Catcher in Österreich im Einsatz?) erlauben neben der Ermittlung der IMSI bzw. IMEI eine Ortung des Mobiltelefons. Somit kann mit dem IMSI-Catcher die Feststellung des Aufenthaltsorts des Mobiltelefons ermöglicht bzw. eingeschränkt werden. Dies hilft den Sicherheitsbehörden, da die der Aufenthaltsort der observierenden Person eingegrenzt werden kann, und anschließend ein polizeilicher Zugriff vollzogen werden kann. Der Basisstation eines Netzbetreibers, in diesem Fall der IMSI-Catcher, ist jedoch der Standort des Mobiltelefon-Benutzers nur sehr grob bekannt, da die Zelle in einem Netz über mehrere Kilometer sich erstrecken kann. Wenn der IMSI-Catcher aber eine „neue“ Zelle erstellt, wird nur eine geringe Ausdehnung als bei einer normalen Zelle geschickt. Somit kann der Aufenthaltsort eines eingeschalteten Mobiltelefons stark eingeschränkt bzw. indirekt „geortet“ werden. Voraussetzungen für diese „indirekte“ Lokalisierung des mobilen Endgeräts sind wie folgt:

- Das Mobilfunknetz sowie die IMSI sind den Sicherheitsbehörden bekannt.
- Das Mobiltelefon derzeit keine aktive Verbindung hat und somit im Stand-by Modus ist
- Der IMSI-Catcher hat das zu observierende Mobiltelefon bereits „gefangen“ (Mobiltelefon hat sich gegeben über dem IMSI-Catcher authentifiziert).

Zusätzlich werden von Sicherheitsbehörden technische Equipments eingesetzt, um Mobiltelefons zu orten. Diese Messgeräte, die meistens in einem Auto von Sicherheitsbehörden eingesetzt werden, führen 3 Ortungen von verschiedenen Standorten durch, um den Aufenthaltsort des Mobiltelefon-Benutzers exakt zu bestimmen.

5.1.3.3 Abhören der Gespräche

Die ersten Modelle des IMSI-Catchers, die von der Firma Rohde & Schwarz entwickelt wurden, ermöglichten nur die Ermittlung der IMSI bzw. IMEI in ihrem Einzugsbereich. Neuere Modelle des IMSI-Catchers sind in der Lage, abgehende Gespräche von „gefangenen“ Mobiltelefonen („Fangmodus“) mitzuschneiden. Dies ist aufgrund einer Erweiterung der Betriebssoftware des IMSI-Catchers möglich. Bei dieser Funktion der vermeintlichen „Basisstation“, gibt sich der IMSI-Catcher gegenüber der nächsten erreichbaren Basisstation des Netzbetreibers als Mobiltelefon aus. Über die nächste erreichbare Basisstation des Netzbetreibers wird der Verbindungsaufbau vollzogen und leitet die von dem „gefangenen“ Mobiltelefon ausgehenden Datenpakete zwischen den beiden Basisstationen weiter und wieder zurück. *„Der IMSI-Catcher realisiert damit einen sogenannten „Man-in-the-middle“-Angriff.“* [FOX] Diese Variante des Angriffs des IMSI-Catcher soll besser mit Hilfe der nächsten Abbildung verdeutlicht werden.

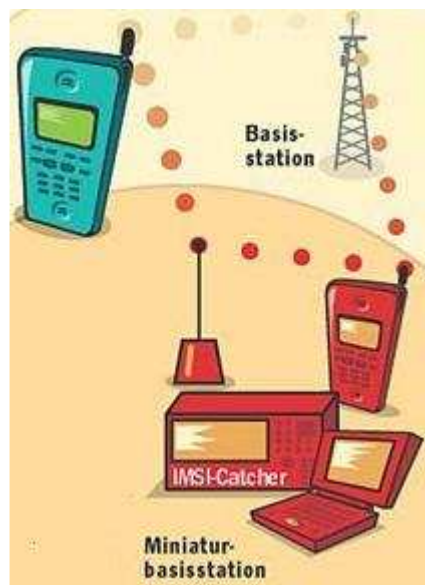


Abbildung 6: IMSI-Catcher Abhören von Gesprächen [WZI]

Damit die Übertragung der Inhaltsdaten überhaupt „belauscht“ werden kann, muss der IMSI-Catcher den Verschlüsselungsmodus am Mobiltelefon ausschalten. Normalerweise wird die Übertragung zwischen dem Mobiltelefon und der Basisstation mit einem geheimen Schlüssel versehen. Dieser Schlüssel ist nur der „echten“ Basisstation bekannt. Da aber in manchen Ländern der Welt die Verschlüsselung unzulässig bzw. genehmigungspflichtig ist, wurde im GSM-Standard die Verschlüsselung der Inhaltsdaten zwischen Mobiltelefon und Basisstation nur optional eingeführt. Somit kann der IMSI-Catcher aufgrund der Unterdrückung der Verschlüsselung bei der Funkübertragung, Gespräche abhören bzw. mitschneiden. Wie schon oben angemerkt, können IMSI-Catcher der neuen Generation somit ein abgehendes Gespräch des „observierten“ Mobiltelefons abhören.

5.1.4 Modelle bzw. IMSI-Catcher in Österreich im Einsatz?

Wie schon im Kapitel 5.1.1 Einleitung & Hintergrund angemerkt, entwickelte die Firma Rohde & Schwarz Test- und Messsystem. Im Dezember 1996 wurde dann das erste Modell GA090 eines IMSI-Catcher (siehe Abbildung 5: IMSI-Catcher Anlage [WZI]) den deutschen Sicherheitsbehörden vorgestellt. Dieses erste Modell GA 090 hatte als einzige Funktion das Orten eines Mobiltelefons. Dies inkludiert die Bestimmung der IMSI, IMEI und die Position des Endgeräts, jedoch nicht das Abhören der abgehenden Gespräche. Das Nachfolger Modell GA900 wurde bereits 1997 vorgestellt und mit diesem Modell ist auch das Abhören von abgehenden Gesprächen möglich. Bei beiden Modellen war der Funktionsumfang auf GSM Mobiltelefon ausgerichtet. Als natürlich die 3. Generation der Mobiltelefone 2001/2002 auf den Markt kam, benötigten die Sicherheitsbehörden auch einen IMSI-Catcher, der auch UMTS-fähige Mobiltelefone orten bzw. abhören kann. Mit dem Modell GA 900 konnten zwar nicht Gespräche mit UMTS Mobiltelefone abgehört werden, aber mit einem Störsender konnten die Funkzellen auf GSM „herunter geschaltet“ werden. Hier war dann die Überwachung möglich. Da aber die Firma Rohde & Schwarz weiter auf diesem Markt tätig blieb, kam 2008 ein neues Modell GA 2G heraus, dass auch diese Lücke für die Sicherheitsbehörden schloss. Neben der Firma Rohde & Schwarz gibt es auch ein paar andere Hersteller von IMSI-Catcher, wie z.B. den GSM Interceptor der Firma Spy World [SPY] oder der GSM Interceptor buatan Israel [GSI]. Diese beiden sowie ein IMSI-Catcher aus dem Dokument [WAL] von Hrn. Walker sind in den nächsten Abbildungen ersichtlicht.



Abbildung 7: 3 alternative IMSI-Catcher Modelle

Jedoch muss festgehalten werden, dass im deutschsprachigen Raum die Firma Rohde & Schwarz sicher ein Monopol Stellung in punkto IMSI-Catchern vorweist.

Nun stellt sich die Fragen, wie viele IMSI-Catcher wirklich in Österreich von den Sicherheitsbehörden verwendet werden. Da die IMSI-Catcher für geheime Ermittlungsmaßnahmen verwendet werden, gibt es natürlich auch keine genaue Auflistung. Hier muss ich mich auf meine einzige Quelle [USS] stützen, da natürlich von den Sicherheitsbehörden versucht wird die Anzahl der IMSI-Catcher geheim zu halten. Hier wird angeführt, dass insgesamt 4 IMSI-Catcher vorhanden sind. Die Sonderheit Observation (SEO) besitzt insgesamt 3 IMSI-Catcher:

- 1x veralteten GA 090 (der voraussichtlich nicht mehr im Einsatz ist)
- 1x GA 900
- 1x GA 2G

Weiters soll die BVT einen weiteren IMSI-Catcher im Einsatz haben (Modell unbekannt).

5.1.5 Störungen durch den Einsatz von IMSI-Catchern?

Durch den Einsatz von IMSI-Catchern befürchten Provider, wie z.B. T-mobile usw., bzw. Datenschützer, dass Störungen im Zuge der Durchführung der Lokalisierung passieren. Nun möchte ich die Bedenken bezüglich diesen Störungen des Netzes näher beleuchten. Wie schon im Kapitel 5.1.3.1 Ermittlung der IMSI bzw. IMEI erwähnt, sendet der IMSI-Catcher („neue“ Basisstation) mit einer höheren Leistung als die im Umfeld befindlichen Basisstationen. Dies führt zu dem Ergebnis, dass in diesem Einzugsbereich jegliche Mobiltelefone bei dem IMSI-Catcher anmelden. Aufgrund des Wechsels zu der „neuen“ Basisstation befürchten die Provider, dass für ein paar Minuten keine Notrufe vom „gefangenen“ Handy getätigt werden können. Da sehr viele Mobiltelefone sich gleichzeitig an der „neuen“ Basisstation anmelden, ist es auch nicht 100% widerlegt, dass aufgrund von Problemen erneute Authentifizierungsversuche benötigt werden. Somit würde sich die Zeit, indem keine Notrufe getätigt werden können, noch verzögern. Neben diesen Wartezeiten für den Kunden, bestätigt auch der Leiter des Technischen Sicherheitsmanagement bei T-Mobile Gerhard Kramarz-von Kohout (Stand 2001) die Befürchtung, dass es nicht ausgeschlossen werden kann, dass es zu Gesprächsabbrüchen bei Mobilfunkteilnehmer während des Einsatzes des IMSI-Catchers kommen kann [KOH]. Dies kann natürlich auch zu ungewollten Konsequenzen für die Mobilfunkbetreiber führen, da natürlich die Qualitätsstandards für die Endkunden nicht gehalten werden können, und somit auch zivilrechtliche Prozesse nach sich ziehen könnten. Neben diesen Bedenken sieht Herr Kohout als weiteres Problem die Verletzung der Privatsphäre. Einerseits werden bei Fehlversuchen ganze Gespräche von Unbescholtenen mitgeschnitten und andererseits werden auch bei Verdächtigten, Gespräche mit dritten aufgezeichnet, die mit dem eigentlichen Verbrechen nichts zu tun haben.

5.1.6 Sicherheitsmaßnahmen

Bezüglich der Lokalisierung eines Mobiltelefons durch einen IMSI-Catcher können sich Benutzer nur in geringem Maße schützen. Der IMSI-Catcher kann nur Mobiltelefone orten, die eingeschaltet sind. Damit man nie von einem IMSI-Catcher erfasst werden könnte, müsste das Mobiltelefon immer ausgeschaltet bleiben und somit würde der Nutzen eines Mobiltelefons nicht mehr vorhanden sein.

Im Bezug auf das Abhören von Gesprächen sieht es einwenig anders aus. Aufgrund der fehlenden gegenseitigen Authentifizierung zwischen Mobiltelefon und Basisstation sowie der Einsatz von nicht sehr sicheren Verschlüsselungs-Algorithmen (sehr kurze Schlüssellänge bei A3 Algorithmus (Benutzer) sowie A5 Algorithmus (Gespräch) [KRY]), ist der GSM Standard in punkto Sicherheit nicht sehr vertrauenswürdig. Anfang 2000 wurde die so genannte „Top Sec“ Initiative gegründet, um zu gewährleisten, dass Gespräche wirklich abhörsicher sind. Diese Initiative wurde von Siemens Forschern gestartet und 2001 gab es das erste Krypto Mobiltelefon, das am Markt erhältlich war. Diese Neuheit auf dem Sektor der Kryptographie wurde aus einem Siemens S35 entwickelt, genannt TopSec GSM, das auf Knopfdruck eine gesicherte und abhörsichere Verbindung zwischen den Gesprächspartnern ermöglicht. Einzige Voraussetzung hierfür ist, dass beide Gesprächspartner über ein TopSec Mobiltelefon verfügen [FMK]. Um die Verschlüsselung zu aktivieren, drückt man eine vorprogrammierte Taste oder auch Softkey genannt. Der gravierende Unterschied bei dieser Technologie liegt darin, dass eigentlich eine Sprachübertragung nur simuliert wird und nach Eingabe des Softkeys in den Datenmodus von GSM gewechselt wird. Bezüglich der Verschlüsselung wurden sowohl asymmetrische als auch symmetrische Verschlüsselungsalgorithmen mit besseren Schlüssellängen verwendet, die wiederum bei jeder Verbindung neu generiert werden. Für die Authentifizierung des Verbindungsaufbaus wird ein asymmetrischer Verschlüsselungsalgorithmus mit einer Schlüssellänge von 1024 Bit verwendet. Für die Verschlüsselung des Gesprächs wird ein symmetrischer Algorithmus mit 128 Bit herangezogen [RSC]. Bei dieser Art der Verbindungs- und Sprach-Kryptographie stellen die große Schlüssellänge und das Wechseln der Schlüssel erhebliche Sicherheitsfaktoren dar. Durch die oben beschriebenen Verschlüsselungskomponenten, kann gewährleistet werden, dass eine echte Verschlüsselung von Handy zu Handy oder von Handy zu Provider durchgeführt wird. Die Sicherheitsfaktoren für die sichere Verbindung des Produkts TopSec GSM sind die Länge des asymmetrischen Schlüssels, das Löschen des erzeugten Schlüssels nach Beendigung des Gesprächs sowie die Authentifizierungssoftware. Das größte Problem für die Durchsetzung am Markt ist derzeit sicher noch der Preis, der mit rund 2000 Euro nicht für die breite Masse erschwinglich ist. Somit könnte man zu dem Schluss kommen, dass das TopSec GSM ein hohes Sicherheitsniveau zur Verfügung stellt, das ohne Probleme gewährleistet, vertrauliche Themen am Handy zu besprechen, ohne dass IMSI-Catcher diese abhören können. Hierbei gibt es nur eine „kleine“ Sicherheitslücke: Die Initiative wurde zwar von Siemens-Spezialisten ins Leben gerufen, aber die Firma Rohde & Schwarz (!) übernahm im Mai 2001 den Verschlüsselungs-Bereich von der Firma Siemens. Die Firma Rohde & Schwarz preist dieses Top-Sec als absolut abhörsicher an [RSC], es ist aber jedoch zu bezweifeln, dass das eigene mitentwickelte Mobiltelefon der Firma Rohde & Schwarz nicht von den eigenen IMSI-Catchern abgehört werden kann.

Abschließend möchte ich noch erwähnen, dass es natürlich auch andere Krypto-Handys am Markt gibt. Die Firma Crypto AG entwickelte ein Modell namens „Secure GSM“. Hierbei wird ein externer Aufsatz verwendet, der den

Verschlüsselungschip enthält. Ein ähnliches Produkt vertreibt auch die Firma General Dynamics in den USA, wo ein Aufsatz auf Motorola Mobiltelefone verwendet wird.

Eine weitere interessante Software-Lösung bietet z.B. die Firma SecurStar an. Das Produkt PhoneCrypt ermöglicht laut Hersteller jedem Mobiltelefon Benutzer, dass das Abhören (auch durch IMSI-Catchern oder anderen Handy-Trojanern) unmöglich gemacht wird [PHC]. Dies begründet der Hersteller damit, dass eine sichere Verbindung zwischen den Endkunden aufgrund von Verschlüsselungsalgorithmen aufgebaut wird. Die verwendeten, nachstehenden Verschlüsselungsalgorithmen werden auch im militärischen Bereich eingesetzt: 4096 Bit RSA und AES 256 bit Verschlüsselung; Diffie-Helman(DH) Schlüsselaustausch; MD5 und SHA512 Hash zur Sicherung der Sprachintegrität. Aber auch bei dieser Sicherheitslösung bleibt ein Restfunke Misstrauen, dass es vor dem Einsatz gegen IMSI-Catcher schützt, da immer darauf verwiesen wird, dass das Militär bzw. Sicherheitsbehörden dieses Produkt auch verwenden. Neben diesem Misstrauen, ist natürlich auch der Kaufpreis für eine einzelne Person ein erhebliches Problem: 900 Euro.

5.1.7 Rechtliche Beurteilung des Einsatz von IMSI-Catchern

Wie bereits schon mehrfach erwähnt, sieht die EGMR in Bereichen, in denen Missbrauch im Einzelfall besonders leicht möglich ist vor, dass die Kontrolle einem Richter übertragen werden soll. Durch die Novelle ist die einzige Kontrollinstanz vor Missbrauch der Rechtsschutzbeauftragte des Bundesministeriums für Inneres und kein Richter wird mehr benötigt. Somit kann festgehalten werden, dass die Kontrolle eines IMSI-Catchers Einsatzes nicht mehr unter der Kontrolle eines Richters besteht sondern derselben Zuständigkeit des Innenministerium. Damit verstößt dies eindeutig gegen die Judikatur des EGMR („adequate and effective guarantees against abuse“), da die Missbrauchsgefahr durch Rechtsschutzbeauftragten des Innenministeriums nicht gänzlich abgedeckt werden kann. Dies beruht auf 2 wesentlichen Punkten. Einerseits die nicht absolute Unabhängigkeit (wie bei der Kontrollinstanz der Richter) sowie die zunehmende Anzahl an Anträgen.

In den nächsten Kapiteln möchte ich untersuchen, ob es noch andere bzw. gleichwertige Technologien gibt, mit Hilfe derer man Mobiltelefone lokalisieren kann, ohne dass der Betrieb gestört wird.

5.2 Stille SMS

5.2.1 Funktionsweise

Neben dem Einsatz von IMSI-Catcher zur Lokalisierung eines Endgeräts, gibt es auch die Möglichkeit des Versenden einer „Stillen SMS“ (auch bekannt unter „Stealth ping“). Diese Art der Überwachung birgt den Vorteil, dass man sich nicht in der Nähe des Endgeräts aufhalten muss, sondern bequem von einem PC die Überwachung durchführen kann. Unter „Stillen SMS“ versteht man

Kurznachrichten, welche am angeschriebenen Endgerät nicht angezeigt werden bzw. als SMS am Endgerät erkannt werden, aber der Empfang der „Stillen SMS“ wird gegenüber dem Netz quittiert. Diese Art der Kurznachricht war ursprünglich gedacht, um die Erreichbarkeit eines Mobiltelefons zu testen. Somit könnte man es vergleichen, wie den Ping-Befehl in einem Netzwerk. Da durch den Empfang am Endgerät Verbindungsdaten beim Mobilfunkanbieter generiert werden, können diese zum Zweck der Standortbestimmung ausgewertet werden und an die Sicherheitsbehörden weitergeleitet werden. Wie auch beim Einsatz eines IMSI-Catchers kann die Funktion einer „Stillen SMS“ nur auf ein Mobiltelefon angewendet werden, das eingeschaltet ist. Aufgrund dieser Möglichkeit der Überwachung, lassen sich relativ einfach Bewegungsprofile von Mobiltelefonie-Benutzern erstellen. Wie schon oben angemerkt, kann der Versand von „Stillen SMS“ in einer beliebigen Menge durch Free- bzw. Shareware Tools einfach durchgeführt werden. SMS Blaster, MyPhoneExplorer oder SmartSMS sind zB Free- bzw. Shareware Programme, die diese Funktion einer „Stillen SMS“ unterstützen. Das Produkt HushSMS unterstützt dieses Feature für Windows Mobile Phones [HUS]. Da diese Art der Lokalisierung eines Endgerätes keine Störungen auf den Betrieb (im speziellen auf die Verwendung eines Notrufs) eines Mobiltelefons darstellt, kann angemerkt werden, dass diese Art der Überwachung den gleichen Nutzen für die Sicherheitsbehörden in punkto Lokalisierung eines mobilen Endgeräts bringt. Da aber in der EBRV zu der Novelle SPG die Anschaffung eines IMSI-Catchers enthält, darf berechtigter Weise vermutet werden, dass auch die Gespräche zwischen zwei Teilnehmern im Visier der Sicherheitsbehörden steht.

5.2.2 Sicherheitsmaßnahmen

Da Stille SMS nicht am Display bzw. Menü SMS aufscheinen, wollte ich in Erfahrung zu bringen, ob es auf einem anderen Weg feststellbar ist, ob man bemerken kann, wenn man eine Stille SMS empfangen bzw. quittiert hat. Um Stille SMS verschicken zu können, habe ich die Freeware Software MyPhoneExplorer herunter geladen und am PC installiert [FJS]. Nachdem die Installation abgeschlossen war, ist als weitere Voraussetzung, um Stille SMS verschicken zu können, die Herstellung einer Verbindung zwischen PC und eines Mobiltelefons. Mein Firmentelefon wurde via USB an den PC angeschlossen und somit konnte ich meine erste Stille SMS an mein privates Mobiltelefon schicken. Wie in der nächsten Abbildung ersichtlich, wählt man das Feature „Neue Nachricht verfassen“ mit der Option „Ping SMS senden“ aus. Nachdem die gewünschte Rufnummer eingegeben wurde, wird der „Stealth Ping“ über das angebundene Mobiltelefon verschickt.

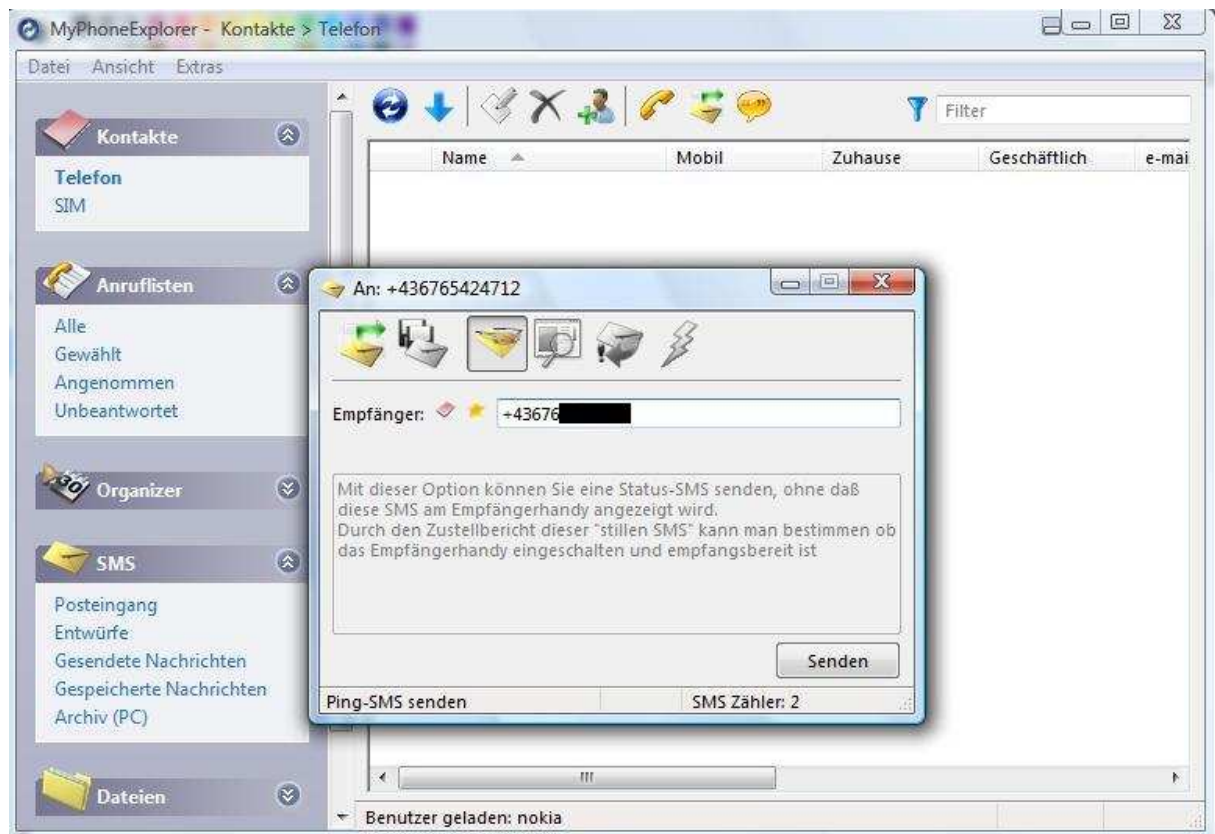


Abbildung 8: Test Stille SMS

Die Stille SMS wird am Mobiltelefon nicht angezeigt. Ich habe nun versucht rauszufinden ob man trotzdem als Benutzer bemerkt, dass eine Stille SMS empfangen wurde. Mit meinem Blackberry 8800 war es mir nicht möglich nachzuweisen, dass eine Stille SMS empfangen wurde. Ich ermittelte die Datenbankgröße der SMS Nachrichten vor und nach Erhalt der Stillen SMS, aber die Größe ergab keinen Unterschied (Optionen / Status / Menü Datenbankgrößen / SMS Messages). Auch bei einem weiteren Versuch bei dem Mobiltelefon meiner Freundin konnte ich den Empfang einer Stillen SMS nicht nachvollziehen. Beim Modell Nokia 6080 dachte ich, dass zumindest der SMS Counter für empfangene SMS hoch zählen wird. Auch hierbei veränderte sich die Anzahl nicht zwischen vor und nach dem Erhalt der Stillen SMS. Somit kann festgehalten werden, dass meiner Meinung nach der Benutzer es nicht nachvollziehen kann, ob und wie viele Stille SMS empfangen bzw. quittiert wurden.

5.2.3 Zusammenfassung

Es kann somit festgehalten werden, dass mit „Stillen SMS“ die Lokalisierung von Mobiltelefonen auch gewährleistet werden kann. Weiters ist die Handhabung von Stillen SMS gegenüber IMSI-Catchern einfacher sowie die finanzielle Belastung geringer (600.000 EUR 1x IMSI-Catcher). Hier stellt sich aber dann natürlich die Frage, wieso im EBRV explizit nur an eine Anschaffung eines IMSI-Catchers gedacht wurde (siehe Abbildung 13: Finanziellen Auswirkungen Novelle SPG 2008) [PAR3]. Es kann die Vermutung angestellt

werden, dass es dem Gesetzesgeber bzw. den Sicherheitsbehörden nicht nur um die Lokalisierung eines Endgeräts gegangen ist, sondern auch um die Überwachung der Telefongespräche. Diese sind natürlich nur mit einem IMSI-Catcher und nicht mit Stillen SMS möglich. Da aber angenommen werden kann, dass nicht nur IMSI-Catcher und Stille SMS im Einsatz sind, möchte ich gerne noch eine dritte Möglichkeit der Überwachung im Bereich der Mobiltelefonie im nächsten Kapitel beleuchten.

5.3 Spionage Software anhand eines Beispiels Flexispy

5.3.1 Funktionsweise

In diesem Kapitel möchte ich noch eine Software vorstellen, mit der es möglich ist, die gewünschte Person abzuhören, jegliche Gespräche als auch Kurzmitteilungen zu dokumentieren, sowie den Mobilfunk-Nutzer zu lokalisieren. Ein Beispiel für eine Software ist das Produkt Flexispy von einer Firma Flexispy aus Thailand (Bangkok). Es gibt 2 Produkte der Firma Flexispy, die jeweils kostenpflichtig sind. Die Pro Version beträgt 150 Euro pro Monat und die Light Version kommt auf 100 Euro pro Monat [FXS]. Um die Features von Flexispy zu nutzen, muss man eine Software auf das Mobiltelefon des „Opfers“ installieren. Remote soll es nicht möglich sein, die Software zu installieren. Laut Hersteller funktioniert Flexispy nur bei Geräten, die ein Symbian oder Windows-Mobile Betriebssystem haben. Neben dem zu überwachenden Mobiltelefon, muss der „Überwacher“ noch die Version von Flexispy bestellen. Wenn das Geld überwiesen worden ist, dann bekommt der Besteller per E-Mail einen Produktkey. Nun muss der „Überwacher“ mit dem zu überwachenden Mobiltelefon ins Internet einsteigen und auf die Hersteller Seite einloggen. Nachdem der davor erworbene Produktkey eingegeben wurde, wird das Spionage-Programm auf das Mobiltelefon geladen (Größe beträgt je nach Modell 200 KB bis 800 KB).

Wie schon oben beschrieben, bietet Flexispy neben der gesamten Protokollierung der Gespräche, Kurzmitteilungen usw. auch das Feature, dass jene Person, die das Mobiltelefon mit sich hat, abzuhören. Wie ist dies aber nur möglich? Nachdem die Installation der Spionage-Software abgeschlossen ist, kann man per Optionsmenü eine Rufnummer angeben, von der aus Abhöranrufe stattfinden können. Wenn nun der „Überwacher“ mit dieser Rufnummer anruft, dann wird der Anruf sofort ohne Rufton übernommen und der Lautsprecher wird am Mobiltelefon aktiviert. Bei gewissen Mobiltelefon-Modellen blinkt kurz das Display, aber sonst werden danach alle Geräusche im Umkreis des Geräts an das Mobiltelefon des „Überwachers“ übertragen.

Flexispy zeichnet alle abgehenden und angenommenen Gespräche, gesendete und empfangene Kurzmitteilungen sowie gesendete und empfangene E-Mails auf. Diese werden dann an Flexispy geschickt und sind auf der Homepage von Flexispy nach einem Login abrufbar. Auf dieser Seite sind dann auch Detaildaten wie Anrufzeit, Anrufdauer sowie Namen des Adressbuchs ersichtlich (siehe Abbildung 9: Flexispy Protokollierung Anruftdaten).

SMS	Email	Location	System	Search
IMEI: 353248010175626				
Client Time: 02.08.07 05:44:44				
Server Time: 02/08/07 15:24:35				
Event Type: VOICE				
Direction: OUT				
Duration: 0:00:00				
Phone Number: 01775				
Contact Name: Bärlü, Babsi				
back				

Abbildung 9: Flexispy Protokollierung Anrufdaten [XON]

Flexispy bietet zusätzlich einen Export der gelisteten Daten in folgenden Formaten an: RTF, CSV oder XML Format. Weiters ist es auch mit Flexispy möglich, nachzuvollziehen wo die Gespräche stattgefunden haben, denn auch die Cell-ID wird mitprotokolliert, wie in der Abbildung 10: Flexispy Protokollierung Cell-ID ersichtlich. Mit etwas Aufwand und Internetrecherche kann dann der Überwacher möglicherweise eruieren, wo die Basisstation steht und somit das Gespräch getätigt wurde.

SMS	Email	Location	System	Search
IMEI: 353248010175626				
Client Time: 06.08.07 04:31:40				
Server Time: 06/08/07 14:11:30				
Event Type: LOC				
Location:				
Cell ID: 3413608				
Cell Name: 3413608				
ID: 01				
Network Info: Name: T-Mobile D				
Country Code: 262				
Area Code: 34591				

Abbildung 10: Flexispy Protokollierung Cell-ID [XON]

5.3.2 Sicherheitsmaßnahmen

Wie schon im vorigen Kapitel angemerkt, läuft die Flexispy nicht auf dem Mobiltelefon. Betroffen sind laut Hersteller, nur Smartphones auf denen ein Symbian- oder Windows-Mobile Betriebssystem installiert ist. Auch wenn das Mobiltelefon ein angegebenes Betriebssystem verwendet, kann aufgrund von bestimmten Verhalten leicht festgestellt werden, ob Flexispy installiert ist oder nicht. Zunächst benötigt Flexispy eine Internetverbindung, damit die protokollierten Daten übertragen werden. Dies bedeutet, dass wenn nach jedem Telefongespräch bzw. SMS Versand oder Empfang das Mobiltelefon eine Verbindung zum Internet aufbaut, ist die Wahrscheinlichkeit sehr hoch, dass Flexispy installiert ist. Weiters müsste es jedem Benutzer auch auf der Endabrechnung bemerken, dass die Internetverbindungen übermäßig

angestiegen sind (bei Flaterate-Verträgen wird dies nicht gleich auffallen). Weiters kann jeder mit einem Symbian-Betriebssystem leicht überprüfen, ob Flexispy auf dem Mobiltelefon als Anwendung vorhanden ist. Unter dem Programm-Manager ist Flexispy unter dem Namen „RBackupPro“ aufzufinden. Symbian hat die Software unter diesem Namen zertifiziert. Falls diese Software nicht vom Benutzer selbst installiert wurde, dann sollte sie so schnell wie möglich deinstalliert werden. Wie auch schon im Kapitel 5.1.6 Sicherheitsmaßnahmen angemerkt, wirbt die Software PhoneCrypt damit, dass eine sichere Verbindung zwischen zwei Endkunden hergestellt werden kann und dass Handy-Trojaner wie Flexispy nicht wie gewünscht ihren Schaden anrichten können.

5.3.3 Zusammenfassung

Es kann davon ausgegangen werden, dass auch die Sicherheitsbehörden ähnliche Handy-Trojaner wie Flexispy kennt bzw. auch einsetzen wird. Neben dem Einsatz von IMSI-Catchern und Stille SMS stellt diese Art der Überwachungsmaßnahme die dritte große Säule im Bereich von Mobilfunk dar. Die Frage, die hier von Relevanz ist, ob es ethisch gerechtfertigt werden kann, dass staatliche Sicherheitsbehörden „schadhafte“ Software verwenden und dies als legal gelten würde. Bei Verbrechern, die diese Art von Software für ihren persönlichen Nutzen verwenden, werden eingesperrt, aber Sicherheitsbehörden nutzen die gleiche Software bzw. Technologie, um die Verbrecher zu jagen. Dieser Zwiespalt ist aus meiner Sicht eher als problematisch einzustufen.

6 Exkurs: Online-Durchsuchung

In diesem Kapitel möchte ich nun die heftig diskutierte Thematik der „Online-Durchsuchung“ beleuchten. Vorweg einmal der Begriff der Online-Durchsuchung existiert nicht in der österreichischen Rechtsordnung, aber wie die nächsten Subkapitel zeigen werden, gibt es schon eine fertige Studie von BMJ bzw. BMI über dieses Thema. Eine innerministerielle Arbeitsgruppe von BMJ und BMI, genannt „Online-Durchsuchung“ hat sich mit diesem Themenbereich in 5 Sitzungen befasst und einen Schlussbericht am 09.04.2008 dem Ministerrat geliefert. Dies könnte aus meiner Sicht bedeuten, dass diese Art der Überwachung nicht mehr all zu lange auf sich warten lässt. In den weiteren Subkapiteln möchte ich näher auf den Begriff, Arten sowie mögliche Sicherheitsmaßnahmen gegen Online-Durchsuchung eingehen.

6.1 Allgemein bzw. Begriffserklärung

Da es derzeit noch keine rechtliche verbindliche Definition für den Begriff der „Online-Durchsuchung“ besteht, gibt es verschiedene Terminologien dafür. In der Literatur oder im WWW ist auch meist die Rede von „Online-Zugriff“ oder auch „Online-Überwachung“. Ich habe den Begriff der Online-Durchsuchung gewählt, da diese Terminologie am meisten anzufinden ist. Um diese Begriffe voneinander trennen zu können, möchte ich eine Abgrenzung der Begriffe aus einem Abschlussbericht bezüglich des Themas Online-Durchsuchung vom BMJ/BMI zitieren [BJI]: *In der informationstechnisch-juristischen Fachdiskussion ist verschiedentlich von „Online-Zugriff“ als Oberbegriff für Online-Durchsuchung und Online-Überwachung die Rede.*

Weiters werden im nächsten Absatz des 2. Kapitels des Schlussberichts näher die einzelnen Begriffe erklärt:

- *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. [BJI]*

Nun stellt sich mal die Frage, was im Detail unter dem Begriff Online-Durchsuchung verstanden wird.

Im Abschlussbericht des BMJ bzw. BMI ist folgendes über die Durchführung der „Online Durchsuchung“ nachzulesen: *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“* [BJI]. Das Hauptziel lässt sich somit zusammenfassen, dass eine geheime Zugangsverschaffung zu einem Computersystem zwecks Überwachung geschaffen wird.

Da es noch keine rechtliche Grundlage für die Online-Durchsuchung in Österreich gibt, wird erst der Gesetzgeber den Begriff genau bestimmen. Trotzdem möchte ich noch eine Begriffserklärung aus dem Buch [ZAN] vorstellen:

Unseres Erachtens weisen Maßnahmen der Online-Durchsuchung vor allem folgende grundlegende Charakteristika auf:

- *Zugangsverschaffung: Die Behörde verschafft sich, ohne den Betroffenen zu informieren, Zugang zu einem Computersystem*
- *Ausnützung des Zugangs: Nach Verschaffung des Zugangs werden Daten erhoben, die in dem Computersystem gespeichert sind oder von diesem verarbeitet (zB versendet) werden.*
- *Es müssen entweder die Zugangsverschaffung, die Ausnützung des Zugangs oder beide über ein öffentliches Kommunikationsnetz erfolgen.*

Wenn man diese Interpretation hernimmt und im speziellen das dritte Merkmal, dann ist das folgende Beispiel sehr interessant. Wenn z.B. durch eine Ermittlungsmaßnahme Spyware vor Ort auf einem Computersystem installiert wird und die von der Software gespeicherten Daten dann wieder „physisch“ abgeholt werden, würde dies keine Online-Durchsuchung darstellen. Die Begründung hierfür wäre, da sowohl die Zugangsverschaffung als auch die Ausnützung des Zugriffs „offline“ durchgeführt wird. Da es derzeit noch keine rechtliche Grundlage für die Online-Durchsuchung in Österreich gibt, wird erst der Gesetzgeber den Begriff genau bestimmen und somit jegliche Ungereimtheiten beseitigen.

6.2 Technische Gesichtspunkte der Online-Durchsuchung

Wie in den vorherigen Charakteristika von [ZAN] beschrieben, möchte ich auch in diesem Kapitel zwischen den Arten der Zugangsverschaffung zu einem Computersystem und Arten der Ausnützung eines solchen Zugangs unterscheiden. In einem weiteren Kapitel möchte ich noch technische Gegenmaßnahmen vorstellen, die ein Betroffener gegen eine Online-Durchsuchung vorsehen könnte.

6.2.1 Arten der Zugangsverschaffung zu einem Computersystem

Der widerrechtliche Zugriff auf ein Computersystem, meist auch Hacking genannt, wird im StGB 118a definiert: *„Wer sich in der Absicht, 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, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen Zugang verschafft, indem er spezifische Sicherheitsvorkehrungen im Computersystem verletzt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen“ [14J5]. Die in ständiger Entwicklung befindlichen Methoden sollen nun hier vorgestellt werden. Die Angriffsmethoden erstrecken sich über die Bereiche des physischen Angriffs, Social Engineering, Ausnutzung technischer Sicherheitslücken bis hin zum Einsatz von Backdoors in verschiedenen Software Produkten.

6.2.1.1 Physische Angriffe

Meistens werden Computersysteme mit Sicherheitssoftware ausgestattet, um Eindringlinge zu verhindern, aber der physische Zugriff wird vernachlässigt. Oft stellt die Eingangstüre zur Wohnung die einzige physische Sicherheitsvorkehrung dar. Jedoch kann auch durch den physischen Zugriff bewerkstelligt werden, dass Trojaner bzw. Key-Logger installiert werden. Durch die Erlangung der Daten aus dem Einsatz der Spionage-Software können nützliche Daten für weitere Angriffe gefunden werden. Neben Software Lösungen besteht auch die Möglichkeit das Sicherheitsbehörden einen USB-Stick am Computersystem anstecken und somit den Zugriff auf die Daten versuchen. Ein Beispiel für so ein Spionage-Tool auf einem USB-Stick ist Gonzor Payload. Mit dieser Software am USB-Stick ist es möglich Windows- und Browserpasswörter sowie den Verlauf von besuchten Seiten im WWW auszulesen. Weiters bietet das Spionage-Tool die Möglichkeit, das Computersystem remote via winvnc zu steuern.

Neben dieser Variante des Angriffs wir nun immer öfters die Möglichkeit des Social Engineerings verwendet, um Zugriff auf das gewünschte System zu bekommen, dass im nächsten Kapitel vorgestellt wird.

6.2.1.2 Social Engineering

Unter dem Begriff „Social Engineering“ werden Angriffe auf Computersysteme verstanden, bei denen ein Angreifer die bei einer Großzahl an Menschen vorhandene Toleranz ausnützt, dritten Personen ein gewisses Maß an Vertrauen entgegenzubringen [GRS]. Bei Social Engineering Angriffen ist das Ziel, die getäuschte Person dahin zu leiten, eine bestimmte Handlung zu setzen, damit dem Angreifer der Zugriff zum Computersystem gewährt wird. Um dies besser zu veranschaulichen, werde ich nun einige Beispiele des Social Engineering darstellen. Ein Beispiel für Social Engineering wäre den Verdächtigen zur Ausführung eines Trojaner zu bewegen. Dem Verdächtigen könnte die Software mittels Website oder E-Mail angeboten werden und der verdächtige Anwender würde glauben, dass dies eine nützliche Software wäre,

ohne die schädlichen Funktionen zu kennen. Eine weitere denkbare Übermittlungsform wäre, den Trojaner in einer Online-Tauschbörse anzubieten. Hierbei wäre aber die Gefahr, dass nicht nur der Verdächtige sondern auch andere Benutzer betroffen wären. Die Schwierigkeit bei diesem Angriff liegt aber generell, den Verdächtigen zur Ausführung der präparierten Software zu überzeugen.

Eine weitere Möglichkeit des Social Engineerings ist im Rahmen des so genannten Phishings. Hierbei werden E-Mails mit gefälschten Absender bzw. Inhalt geschickt, indem dem Empfänger aufgefordert wird, Passwörter oder andere Zugangsdaten preiszugeben. Wenn an ausgewählte Personen bzw. Personengruppen Phishing-Mails geschickt werden, dann spricht man in der Literatur von Spear Phishing [MIC]. Da Sicherheitsbehörden nicht massenhaft Phishing-Mails verschicken werden, sondern eher nur an den verdächtigten Personenkreis, kann daher davon ausgegangen werden, dass Spear-Phishing eingesetzt wird, um Zugangsdaten zu erlangen. Die Problematik ist aber hier für die Sicherheitsbehörden, dass die Wahrscheinlichkeit sehr hoch ist, dass der Angriff entdeckt wird. Somit ist dieser Angriffsvariante eher geringe Relevanz zuzuordnen.

Neben diesen Varianten des Social Engineerings wäre es auch denkbar, den Verdächtigen dahin zu bringen, einen präparierten Datenträger, wie USB-Stick oder DVD, an seinem Computersystem anzustecken bzw. einzulegen. Hierbei könnte als Vorwand z.B. ein Werbegeschenk dienen, damit der Betroffene dazu bewogen wird, den Datenträger in seinem Computersystem zu benutzen. Wenn nun der Datenträger mit dem Computersystem verbunden ist oder eingelegt wurde, dann könnte mittels Auto-Start-Funktion die Ausführung von beliebiger Software (z.B. ein Trojaner, sonstiger Spyware usw.) ermöglicht werden. Damit könnte auch eine Zugangsverschaffung für Sicherheitsbehörden geschaffen werden.

6.2.1.3 Ausnützung technischer Sicherheitslücken

Damit technische Sicherheitslücken bei Computersystemen ausgenutzt werden können, sind große Sachkenntnisse bei den Sicherheitsbehörden erforderlich. Grundsätzlich können hierbei 2 verschiedene Sicherheitslücken unterschieden werden: Host-basierte und Netzwerk-basierte Sicherheitslücken.

Unter Host-basierte Sicherheitslücken versteht man, dass aufgrund von Software-Fehlern diese Sicherheitslücken geöffnet werden. Wie schon erwähnt ist dies aber schwerer als andere Formen der Zugangsverschaffung, da der Überwacher einiges an Know-How benötigt und dies generell nur mit erhöhtem Aufwand möglich ist. Häufig entstehen diese Sicherheitslücken dadurch, dass der Software andere bzw. mehr Eingabedaten geliefert werden, als diese erwartet. So ein klassisches Beispiel für eine Entstehung einer Sicherheitslücke wird auch in der Fachliteratur als „Buffer Overflow“ bezeichnet. Weitere Beispiele für diese Art des Angriffs wären Integer Overflow, Format String Bugs sowie Double-free Bugs [MNC]. Neben diesen Beispielen für Host-basierte

Sicherheitslücken wäre es auch denkbar, dass Sicherheitslücken in Browser Software ausgenutzt werden. Wenn die zu überwachende Person dazu gebracht wird eine präparierte Web-Seite aufzurufen, könnte eine Sicherheitslücke eines Plugin (wie z.B. Quicktime, Flash Player, usw.) oder eines ActiveX Control ausgenutzt werden.

Die zweite Art bei der Ausnutzung sind netzwerk-basierte Sicherheitslücken. Diese entstehen durch Fehler bzw. Unzulänglichkeiten eines Netzwerkprotokolls. Ein Beispiel hierfür wären die unverschlüsselten Netzwerkprotokolle HTTP, FTP oder POP3. Diese Netzwerkprotokolle können nicht sicherstellen, dass die Identität des Kommunikationspartners verifiziert wird. Somit bildet diese Sicherheitslücke die Grundlage einer so genannten „Man-in-the-middle Attacke. Unter dieser Attacke versteht man, dass es einem Dritten (in diesem Fall der Sicherheitsbehörde) gelingt, sich zwischen den beiden Kommunikationspartner zu setzen und somit einerseits die Vertraulichkeit und andererseits auch die Integrität der transferierten Daten zu beeinträchtigen. Um dies nochmals besser zu veranschaulichen möchte ich ein reales Beispiel präsentieren. Der Verdächtige ist gewohnt seine Software per HTTP auf seinen Computer herunterzuladen. Wenn nun die Sicherheitsbehörde es schafft den HTTP-request abzufangen, könnte sie eine präparierte Version der Software ausbringen. Um generell solchen Problemen vorzubeugen, wäre es ratsam bei jeder Art der Kommunikation digitale Signaturen zu verwenden. Somit kann zumindest sichergestellt werden, dass die Integrität der Daten gewährleistet wird.

6.2.1.4 Backdoors

Neben den bereits vorgestellten Varianten, wäre es auch denkbar, dass Sicherheitsbehörden Software-Hersteller dazu verpflichten, Hintertüren, so genannte „Backdoors“, einzubauen, um sich so Zugang zu einem Computersystem zu verschaffen. Unter Backdoors versteht man in der Fachliteratur folgendes: *„Als Hintertür (Backdoor) bezeichnet man einen geheimen, in der Regel nicht autorisierten Zugang zu einem IT-System oder Softwaremodul“* [KUC]. Grundsätzlich können bei Backdoors 2 Arten unterschieden werden. Entweder kann die Benutzeridentifikation, -authentifikation und -autorisierung nicht vollständig oder fehlerhaft durchgeführt werden, oder es wird ein Umgehen der Benutzeridentifikation, -authentifikation und -autorisierung als zusätzlich Funktion ermöglicht.

Grundsätzlich ist hier einmal zu vermerken, dass schwerwiegende verfassungsrechtliche Bedenken bezüglich dieser Vorgehensweise bestehen. Indem Software-Hersteller Hintertüren für Sicherheitsbehörden ermöglichen und ihnen den Schlüssel zur Verfügung stellen, würden auch rechtliche bzw. wirtschaftliche Probleme für die Software-Hersteller entstehen. Falls Schäden bei einer Ausnutzung des Zugangs durch die Sicherheitsbehörden verursacht werden, könnte auch der Software-Hersteller für die Bereitstellung des Backdoors verantwortlich gemacht werden.

Neben den rechtlichen Bedenken müsste es auch eine globale Gesetzgebung geben, denn sonst könnten Benutzer die gewünschten Produkte bei ausländischen Software-Herstellern ohne Backdoors beziehen. Somit kann abschließend festgehalten werden, dass diese Art der Zugangsverschaffung sehr unwahrscheinlich ist und nur schwer umzusetzen wäre, da eine globale Lösung nicht zu erwarten sein wird.

6.2.2 Arten der Ausnützung des Zugangs

Wie im letzten Kapitel vorgestellt, können die Sicherheitsbehörden nachdem sie sich zu dem Computersystem des Verdächtigen Zugang verschafft haben, die eigentliche Online-Durchsuchung durchführen. Grundlegend kann man hier unterscheiden, ob eine regelmäßige manuelle Durchsuchung oder eine automatisierte Durchsuchung durch Spyware erfolgt. Bei einer manuellen Durchsuchung wäre der Vorteil, dass hier eine höhere Flexibilität herrscht, aber der große Nachteil daran wäre, dass dies nur mit hohen Sachkenntnissen sowie erhöhten Personen- und Zeitaufwand durchführbar wäre. Darüber hinaus würde bei dieser Variante auch eine sehr hohe Fehler- bzw. Missbrauchsgefahr bestehen. Bei einem Einsatz von automatisierter Spyware-Software wäre der Vorteil, dass sehr einfach alle Funktionen des Systems überwacht werden könnten. Z.B. könnten hierbei von Sicherheitsbehörden Keylogger zum Einsatz gebracht werden, die jegliche Tastenanschläge mitprotokollieren würden. Dadurch kann dann ganz einfach festgestellt werden, welche E-Mails geschrieben werden oder das Surf-Verhalten des Verdächtigen überwacht werden. Ebenso könnten Sicherheitsbehörden ein Programm installieren, das regelmäßig Screenshots macht bzw. Screen Videos des Computersystems erstellt, das mittels Streaming zu den Sicherheitsbehörden übertragen wird. Eine weitere Möglichkeit der Ausnützung des Zugangs wäre, dass eine angeschlossene Webcam aktiviert wird und die aufgenommenen Bilder in Echtzeit überträgt. Wie die bereits dargestellten Beispiele gibt es hier eine sehr große Bandbreite an Möglichkeiten für die Ausnützung des Zugangs durch die Sicherheitsbehörden, wenn einmal die Zugangsverschaffung zum Computersystem bewerkstelligt wurde.

6.2.3 Technische Sicherheitsmaßnahmen

In diesem Kapitel möchte ich aufzeigen, welche technischen Sicherheitsmaßnahmen in Bezug auf die Online-Durchsuchung getroffen werden können. In diesem Abschnitt werden nur technische Sicherheitsmaßnahmen erörtert. Administrative bzw. physische Sicherheitsmaßnahmen werden nicht beleuchtet. Grundsätzlich kann man die technischen Sicherheitsmaßnahmen in 3 Gruppen einteilen:

- Präventive Sicherheitsmaßnahmen
- Detektive Sicherheitsmaßnahmen
- Korrektive Sicherheitsmaßnahmen

Präventive Sicherheitsmaßnahmen zielen darauf ab, dass entweder die Zugangsverschaffung zum Computersystem oder die Installation der Spyware

verhindert wird. Damit Sicherheitslücken in installierten Diensten des Systems nicht unmittelbar von den Sicherheitsbehörden ausgenutzt werden können, ist eine Einrichtung einer Firewall zu empfehlen. Durch den Einsatz von einer Firewall wird ermöglicht, dass eine Filterung des Netzwerkverkehrs anhand von Verkehrsdaten, die in einem IP-Datenpaket enthalten sind, durchgeführt wird. Mit Verkehrsdaten ist hier Quell- und Ziel-IP-Adresse bzw. auch Port gemeint. Eine weitere wichtige Sicherheitsmaßnahme besteht darin, dass Sicherheitsupdates möglichst gleich nach Erscheinung eingespielt werden. Bei Betriebssystemen bzw. auch Anwendungssoftware wird vermehrt eine Auto-Update-Funktion zur Verfügung gestellt, die die manuelle Installation durch den Benutzer obsolet macht. Leider gibt es aber keine Auto-Update-Funktion z.B. für Browser-Plugins (Flash Player usw.). Somit ist jedem Benutzer zu raten, dass die Sicherheitsupdates immer zeitnah am Erscheinungsdatum eingespielt werden, da damit die Ausnützung einer technischen Sicherheitslücke für die Sicherheitsbehörden enorm erschwert wird. Neben den bereits vorgestellten Varianten ist die Installation von Anti-Malware Software eine Sicherheitsmaßnahme. Unter Malware Software wird Malicious Software verstanden, dass nichts anderes bedeutet wie böswillige Software. Darunter fallen Trojaner, Spyware, Viren, Würmer usw. Durch den Einsatz von Anti-Malware Software könnte verhindert werden, dass eine Installation einer Spyware-Software durchgeführt werden könnte. Hierbei können zwei verschiedene Versionen von Anti-Malware Software unterschieden werden: signatur-basierte Anti-Malware bzw. Malware mit heuristischen Verfahren.

Bei signatur-basierter Anti-Malware Software wird auf bereits bekannte Malware Software angewandt und somit kann aber nicht verhindert werden, dass komplett neue Malware Software installiert wird. Hier setzen genaue heuristische Verfahren an. Hier wird in den Dateien nach auffälligem Programmcode gesucht. Weiters wird bei der Analyse untersucht, ob diese typische Befehle bzw. Zugriffe inkludiert, die auf böswillige Software schließen lässt. Wie schon bereits erwähnt, bieten heuristische Verfahren den Vorteil, dass somit auch neuartige Malware, die von Sicherheitsbehörden eingesetzt wird, zu identifizieren und zu entfernen. Der Nachteil an heuristische Verfahren bei Anti-Malware Software ist aber, dass das Programm auch bei nicht-„böser“ Software Fehlalarme liefert.

Einen weiteren wichtigen Punkt bei den technischen Sicherheitsmaßnahmen bildet eine restriktive Konfiguration des Computersystems. Hierzu zählt einerseits die Vergabe von sicheren bzw. schwer „knackbaren“ Passwörtern. Dies beschränkt sich aber nicht nur auf das Passwort für den Benutzer im Betriebssystem. Es ist weiters auch wichtig ein Passwort auf BIOS Ebene zu vergeben. Wenn nämlich die Sicherheitsbehörden einen physischen Angriff mittels Boot-CD probieren, könnte dies mittels einem BIOS-Boot-Passwort verhindert werden. Nun würde den Sicherheitsbehörden nur noch die Möglichkeit überbleiben, die Festplatte auszubauen und dann die Spyware von einem anderen Computersystem auf die Festplatte des Verdächtigen zu installieren. Um zu bewerkstelligen, dass dies auch nicht durchgeführt werden soll, könnte man mit einer Festplatten Verschlüsselung arbeiten. Beispiel für

eine derartige Verschlüsselungssoftware wäre TrueCrypt, mit der man Festplatten inklusive Systempartitionen verschlüsseln kann. Falls die verwendete Verschlüsselungssoftware keine Sicherheitslücken aufweist, kann das Risiko eines Angriffs mittels Spyware fast ausgeschlossen werden. Wie aber z.B. das Beispiel TrueCrypt zeigt, wurde Anfang 2008 eine Sicherheitslücke gefunden, indem die Schlüssel im Speicher während des Ruhezustands verbleiben und ein Angreifer diese auslesen kann. Somit könnten auch Partitionen bzw. Festplatten entschlüsselt werden und die Installation einer Spyware durchgeführt werden. Neben diesen Punkten der präventiven Sicherheitsmaßnahmen sollten weiters Anwender-Programme nicht mit administrativen Rechten ausgeführt werden. Dies hat den folgenden Sinn, dass wenn z.B. die Sicherheitsbehörde zwar eine Sicherheitslücke in einem Anwenderprogramm findet, sie aber nicht alle Berechtigungen auf dem System hat. Somit würde die Installation der Spyware entgegen gewirkt werden.

Als nächsten Punkt möchte ich auf die detektiven Sicherheitsmaßnahmen eingehen. Unter diesem Begriff versteht man, dass Software eingesetzt wird, um die heimliche Überwachung aufzudecken und somit das Ziel des Angreifers vereitelt werden kann. Bezüglich dieser Maßnahmen können zwei Arten von Systemen unterschieden werden: host-basierte und netzwerk-basierte Systeme. Die Charakteristika eines host-basierten Systems lassen sich dadurch beschreiben, dass der gesamte Zustand eines Computersystems überwacht wird. Beispiele für derartige host-basierte Systeme wären Virens Scanner bzw. Intrusion Detection Systeme (IDS). Bei Intrusion Detection Systeme werden alle Vorgänge auf einem spezifischen Rechner überwacht und mittels Log Dateien protokolliert, welche in weiterer Folge auf bestimmte Angriffs- oder Einbruchsmuster untersucht werden. Diese Art von IDS bietet den Vorteil, dass die Auswirkungen von Angriffen auf einen bestimmten Rechner genau ersichtlich sind und darauf sofort reagiert werden kann und z.B. eine korrektive Sicherheitsmaßnahme eingeleitet werden kann.

Im Gegensatz dazu beschränken sich netzwerk-basierte Systeme auf die Analyse des Netzwerkverkehrs. Diese Systeme werden auch Extrusion Detection Systeme (EDS) genannt. Ein Netzwerk-basiertes System ist auf einem oder auch mehreren ausschließlich dafür eingesetzten Computersystemen installiert, welche den gesamten Verkehr analysieren und Angriffe auf alle im Netzwerk vorhandenen Rechner orten können. Der Einsatz eines derartigen Systems auf mehreren Hosts erschwert einem Angreifer sie zu lokalisieren und gestaltet den Angriff komplizierter. Bei beiden Arten von Systemen (host- bzw. netzwerk-basiert) kann wie bei der Anti-Malware Software auch zwischen Signatur-basierten Systemen bzw. Anomalie-basierten Systemen unterschieden werden. Das Signatur-basierte System achtet auf jene Angriffe, die durch eine eindeutige Zeichenfolge im Netzwerkverkehr erkennbar ist. Dabei erkennt es diese Patterns bekannter Angriffsmethoden und vergleicht diese mit dem laufenden Netzwerkverkehr. Diese Methode ist nur sehr effektiv bei der Erkennung von bekannten Angriffstechniken, erfordert aber wie ein Virens Scanner laufende Updates um gegen neue Arten von Angriffen schützen zu können.

Bei der Anomalie-basierten Erkennung wird der Eindringling durch sein unübliches Verhalten im Netzwerk identifiziert. Da die Sicherheitsbehörden eher nicht bekannte Muster für den Angriff bei Verdächtigen wählen werden, ist somit die Anomalie-basierte Variante im Einsatz gegen Eindringlinge zu empfehlen.

Wenn der Angriff entdeckt wurde und somit die detektive Sicherheitsmaßnahme erfolgreich war, kommt die korrektive Sicherheitsmaßnahme in Betracht. Um die Sicherheit eines Computersystems zu erhöhen, muss aber nicht erst ein Anlass für eine korrektive Sicherheitsmaßnahme bestehen, sondern könnte dies regelmäßig durchgeführt werden. Ein Beispiel hierfür ist die Verwendung einer Live-CD, mit dem das Betriebssystem von einer CD-ROM bzw. DVD gestartet wird. Jegliche Datenänderungen geschehen nur im Arbeitsspeicher und nach einem Neustart des Computersystems werden alle Daten im Arbeitsspeicher gelöscht. Somit würde die Zugangsverschaffung zu einem Computersystem nur bis zu dem nächsten Neustart eines Rechners wirken und die Sicherheitsbehörde müsste einen erneuten Versuch unternehmen. Einziger Nachteil dieser Variante besteht darin, dass die CD-Rom bzw. DVD leicht bei einem physischen Angriff ausgetauscht werden kann und auf diesem Wege die Spyware auf das Computersystem gelangen würde. Weitere Möglichkeiten sind Backup-Tools, die jederzeit den „gesunden“ Computerzustand wieder herstellen können. Beispiele für solche Software wären Norton Ghost oder Acronis.

6.2.4 Zusammenfassung bzw. Ausblick

Grundsätzlich ist zu sagen, dass die Entwicklung von Angriffsmethoden sowie Sicherheitsmaßnahmen ein stetiger Prozess ist. Der viel zitierte „Bundestrojaner“ in den Medien, der für alle Zeit den Zugang zu allen Computersystemen gewährt, den wird es niemals geben. Somit kann festgehalten werden, dass sowohl Angriffsmethoden als auch etwaige Spyware Software immer weiterentwickelt werden müssen. Die Wahrscheinlichkeit ist sehr hoch, wenn mal ein Angriff erkannt wurde, dass bei nochmaligem Versuch schon eine Signatur entwickelt wurde, die diesen Angriff bemerkt und den Zugang verwehren wird.

Die Frage, die sich bei diesem Thema aber stellt ist, ob es nicht auch technische Alternativen zur Online-Durchsuchung gibt. Hierbei können 2 Maßnahmen hervorgehoben werden. Einerseits könnten Hardware Keylogger von den Sicherheitsbehörden eingesetzt werden. Dabei handelt es sich um einen ca. 2 cm großen Adapter, der zwischen dem Anschluss der Tastatur und dem Computer angebracht wird (siehe Abbildung 11: Hardware Key-Logger). Somit wird ermöglicht, dass jeder Tastenanschlag mit Einbezug des Zeitpunktes) mitprotokolliert wird. Hierbei handelt es sich nicht um eine Online-Durchsuchung, da die Sicherheitsbehörden zwecks Installation und Abholung der Daten jeweils Zugang zum Computer in der Wohnung des Verdächtigen verschaffen müssen. Wie in den letzten Kapiteln beschrieben, fehlt für die

Bezeichnung als Online-Durchsuchung die Einbeziehung eines öffentlichen Kommunikationsnetzes.



Abbildung 11: Hardware Key-Logger [WKL]

Eine zweite Variante wäre entsprechende Geräte einzusetzen, die in der Lage sind elektromagnetische Abstrahlungen aufzufangen bzw. auszuwerten. Es wäre durch die elektromagnetische Abstrahlung eines Monitors möglich, die dargestellten Bilder zu rekonstruieren. Echte Gegenmaßnahmen wären hierbei sehr kostspielig und nur für die wenigsten Personen durchführbar.

Wie in der Einleitung dieses Kapitels schon bemerkt, gibt es den Begriff der Online Durchsuchung nicht in der österreichischen Rechtsordnung. Da aber beide zuständigen Ministerien eine Arbeitsgruppe gebildet haben und schon einen Abschlussbericht vorgelegt haben, ist davon auszugehen, dass in der näheren Zukunft, Verdächtige mittels Online-Durchsuchung überwacht werden.

7 Überwachungsmaßnahmen in anderen Ländern

In diesem Kapitel möchte ich noch einen kurzen Überblick über Überwachungsmaßnahmen sowie -technologien in anderen Ländern geben. Hierbei wurden die Vereinigten Staaten von Amerika und Deutschland als Vergleich zu Österreich herangezogen. Diese Auswahl wurde daher getroffen, dass einerseits die rechtlichen als auch technologischen Anwendungen in den USA sich deutlich von Österreich unterscheiden. Andererseits wurde aber auch Deutschland gewählt, da hier die Rechtsprechung als auch die verwendeten Technologien sehr verwandt zu Österreich sind. Diese Gegenüberstellung soll helfen, ein Bild darüber zu gewinnen, wie das SPG im speziellen sowie andere Gesetze in Österreich im internationalen Vergleich gesehen werden kann.

7.1 Vereinigten Staaten von Amerika

7.1.1 Einleitung

In den USA wird unter sicherheitsbehördlicher Überwachung die meist heimliche Beobachtung bzw. Kontrolle einer Person, ihrer Bewegung und Verhaltensweisen, Sachen und Wohnung sowie der Kommunikation mit anderen Menschen und der Aufzeichnungen von gespeicherten Daten verstanden. Für die Überwachung von Personen bzw. Wohnungen ist in der Rechtsprechung von der physical surveillance, bei Kommunikation von communication surveillance und bei gespeicherten Daten von transactional surveillance die Rede. Im nächsten Kapitel wird versucht, die rechtlichen Grundlagen polizeilicher Überwachungsmaßnahmen zu skizzieren. Hier muss gleich erwähnt werden, dass aufgrund der Anschläge vom 11. September 2001 eine Vielzahl an Änderungen und somit neuen Befugnissen geschaffen wurde (z.B. USA Patriot Act 2001 oder Homeland Security Act 2002). In einem darauf folgenden Sub-Kapitel wird im speziellen auf den vierten Verfassungsgrundsatz eingegangen, der den Maßstab für Überwachungsmaßnahmen seitens der Sicherheitsbehörden darstellt. Danach wird ein Überblick gewährt, wie in den USA menschliche Kommunikation überwacht bzw. ausgeforscht werden kann. Hier wird in einem weiteren Sub-Kapitel speziell auf die Lokalisierung von Mobiltelefonnutzern auch eingegangen. Als letzten Punkt möchte ich noch neue Formen der Überwachungen in den USA beleuchten, die in Österreich noch nicht angewendet werden.

7.1.2 Rechtliche Grundlagen

In den USA herrscht ein recht zersplittertes Gebilde in punkto Polizeibehörden vor. Diese existieren auf lokaler, bundesstaatlicher und auf Distriktebene. Neben diesen Sicherheitsbehörden bildet eine große Anzahl an Geheimdiensten das Bild der Sicherheitskräfte ab, die für den Schutz der nationalen Sicherheit arbeiten. Bezüglich eines Polizeirechts nach österreichischem Verständnis mit einem Gefahrenabwehrrecht, gibt es in dieser Form nicht in den USA, sondern nur auf lokaler Ebene. Festzuhalten ist hier, dass in den USA die

Rechtmäßigkeit von gefahrenabwehrenden Maßnahmen von einem Strafgericht beurteilt wird. Dies kann aber als formelles Recht ausgelegt werden, da nur rund ein Drittel über ein umfassendes Strafprozessrecht verfügen, wobei auch hier in nur einigen Bundesstaaten alle polizeilichen Eingriffsbefugnisse abgedeckt werden. *Letztendlich sind daher 52 unterschiedliche Ausformungen des Strafprozessrechts in den USA vorzufinden. Auf der Ebene des Bundes -...- können allein sechs verschiedenen Ebenen von Rechtsquellen identifiziert werden, durch die polizeiliche Maßnahmen im Bereich der Strafverfolgung determiniert werden können: (1) die Verfassung der Vereinigten Staaten mit den in der Bill of Rights verankerten Grundrechten, (2) Bundesgesetz, (3) die Strafprozessordnung des Bundes, (4) die Prozessordnungen der Bezirksgerichte, (5) Entscheidungen der Bundesgerichte im Rahmen ihrer Auslegungsbefugnisse des common law und - ... - und (6) Dienstvorschriften des Department of Justice und anderen im Bereich des Bundesrechts zuständigen Behörden [ARC].* Zu den einzelnen vorgestellten Formen der Überwachung (physical oder transactional surveillance) im Kapitel 7.1.1 Einleitung herrscht somit eine vielfältige Judikatur der verschiedenen Gerichte und Instanzen, die für Außenstehende als nicht einfach zu durchblicken bzw. wenig konsistent angesehen werden kann.

Wie gerade oben angeführt, stellt die Bundesverfassung und der ihr vorangestellte Katalog an Grundrechten (Bill of Rights) den rechtlichen Ausgangspunkt bei der Frage nach der Zulässigkeit einer sicherheitsbehördlichen Maßnahme. Falls eine Frage in der Bundesverfassung vollständig geregelt ist, gehen die Grundrechte in der Bundesverfassung jedem bundes- oder einzelstaatlichen Gesetz vor. Wenn aber für den Betroffenen ein höherer Schutzstandard durch ein einfaches Recht auf Bundes- bzw. Landesebene als in der Bundesverfassung gewährt wird, kann auch dem einfachen Recht Vorrang gegeben werden. Durch die Vielfalt an Gesetzen und verschiedenen Lokalitäten der rechtlichen Grundlagen, möchte ich mich im nächsten Kapitel nur den verfassungsrechtlichen Rahmenbedingungen mit Blick auf die Bundesverfassung spezialisieren. Im Detail heißt dies, eine Übersicht über den vierten Verfassungszusatz zu gewähren, der den rechtlichen Maßstab für sicherheitsbehördliche Überwachungsmaßnahmen darstellt.

7.1.2.1 Der vierte Verfassungszusatz (Fourth Amendment)

Der vierte Verfassungszusatz stellt die Rahmenbedingung für jede polizeiliche Überwachungsmaßnahme in den USA. Dieser auch zur Bill of Rights gehörende Verfassungszusatz wurde 1791 festgeschrieben. Folgende beide Anwendungsbereiche für den vierten Verfassungszusatz sind deklariert: Es fallen nur solche sicherheitsbehördlichen Eingriffshandlungen darunter, die sich als „search“ und „seizure“ bezeichnen lassen. Unter dem Begriff „search“ wird in den USA die Durchsuchung von Personen, Sachen oder auch Wohnungen sowie die Fahndung nach Personen verstanden. Hingegen die Wegnahme von Sachen die Beeinträchtigung von Eigentum sowie die Festnahme einer Person wird unter dem Begriff „seizure“ subsumiert. Um diese beiden Begriffe auf die österreichische Rechtsordnung umlegen zu können, ist einerseits die StPO und

andererseits das SPG von Relevanz. Bei beiden Begriffen kann eine weite Spanne an Maßnahmen abgedeckt werden, die in diesen beiden Gesetzen definiert ist. Weiters muss festgehalten werden, dass diese Norm nur dann greift, wenn eine Maßnahme gegen Personen, Häuser, Schriftstücke oder Privateigentum gerichtet ist. Wichtig ist hierbei, dass in der amerikanischen Rechtsordnung immer auch die Ausdrücke der Angemessenheit (reasonableness) und ein hinreichender Verdacht (probable cause) verwendet werden. Eine Überwachungsmaßnahme ist nur dann zulässig (reasonable), wenn eine (verfassungs-)rechtliche Rechtfertigung vorliegt. Die Angemessenheit der Überwachungsmaßnahme ist eng mit dem nächsten Punkt „hinreichender Verdacht (probable cause)“ verknüpft. Unter probable cause wird in der amerikanischen Rechtsprechung verstanden, dass bei objektiver Betrachtung der Fakten eines Falles, der Polizeibeamte eine gerechtfertigte Maßnahme (Search oder Seizure) durchführt, die auch ein umsichtiger Mensch zum Zeitpunkt der Entscheidung getätigt hätte. Hierbei ist nicht gemeint, dass der Polizeibeamte einen Beweis der Schuld für die Zulässigkeit der Maßnahme benötigt. Andererseits darf auch nicht die Willkür bzw. die subjektive Überzeugung eines Polizeibeamten ausreichen, dass ein hinreichender Verdacht (probable cause) vorliegt. Wie auch im Buch [ARC] nachzulesen ist, bin ich der gleichen Meinung, dass dieser Standard sehr weich ausformuliert ist. Dies bedeutet, dass die Rechtssprechung Einschätzungsfehler zulässt und somit trotzdem die nicht rechtmäßige Überwachungsmaßnahme mit dieser Begründung rechtfertigt.

Weiters ist von Interesse, dass im vierten Verfassungszusatz nicht dezidiert niedergeschrieben ist, dass Maßnahmen im Sinne von „search“ und „seizure“ eine richterliche Anordnung (warrant) benötigen. Trotzdem hat der Supreme Court in seiner Rechtssprechung speziell in den letzten 100 Jahren stets hervorgehoben, dass die Maßnahmen im Sinne von „search“ und „seizure“ durch einen richterlichen Beschluss verifiziert werden sollen. *„Der Richtervorbehalt soll dazu dienen, dass eine neutrale Instanz, die nicht wie die Polizei auf die Strafverfolgung fokussiert und in die oft schnellen Entscheidungen der Polizei eingebunden ist, das Vorliegen der verfassungsrechtlichen Voraussetzungen eines Eingriffs vor dessen Ausführen überprüft“* [ARC]. Jedoch sind Ausnahmen definiert, wann ein Richtervorbehalt nicht notwendig ist. Ein Beispiel hierfür wäre, dass eine besondere Dringlichkeit vorherrscht, wobei der hinreichende Verdacht (probable cause) für die unmittelbare bevorstehende Begehung einer Straftat auch vorliegt. Weitere Gründe können auch sein, dass der Verdacht besteht, dass Beweismaterial vernichtet wird und somit eine Durchsuchung einer Wohnung oder eine Festnahme einer Person ohne richterlichen Beschluss durchgeführt werden kann. Weiters sieht man in der neueren Rechtssprechung, dass keine richterliche Anordnung für die Durchsuchung von Automobilen notwendig ist. *„Die weitgehende Abkehr von einem generellen Richtervorbehalt ist in der Literatur auf heftige Kritik gestossen, ... Aus der Vielfalt der Ausnahmen wird der Schluss gezogen, dass Überwachungsmaßnahmen ohne richterlichen Beschluss (Übersetzung von warrantless searches) eher die Regel als eine Ausnahme darstellen“* [ARC]. Jedoch muss auch vermerkt werden, dass der Supreme Court es abgelehnt

hat, aufgrund von bestimmten Straftaten, eine generelle Ausnahme zu definieren. Andererseits wurden aber auch Verbesserungsvorschläge, den Richter mittels Telekommunikation die Zulässigkeit einer Maßnahme überprüfen zu können, noch nicht umgesetzt. Somit könnte dem Richtervorbehalt wieder eine gewichtigere Rolle gegeben werden.

Ein weiterer wichtiger Punkt beim vierten Verfassungszusatz wird dem berechtigten Vertrauen auf Schutz der Privatsphäre (Reasonable Expectation of privacy) gegeben. Dieser Begriff ist von bestimmten Situationen abhängig, ob ein Eingriff in die Privatsphäre geschützt ist oder nicht. Wie schon erwähnt, sind Personen, Häuser, Schriftstücke und Privateigentum grundsätzlich geschützt. Neben diesen geschützten Bereichen gab es eine bahnbrechende Entscheidung im Fall Katz vs. United States, indem ein Telefonat aus einer öffentlichen Telefonzelle abgehört wurde. Dies geschah durch die Anbringung einer Einrichtung an der Außenseite der Telefonzelle. Wenn man sich die 4 genannten Schutzbereiche jetzt näher ansieht, kommt man zu dem Schluss, dass dieser Fall nicht unter den Schutz des vierten Verfassungszusatzes fallen würde. Der Supreme Court stellt aber in seiner Entscheidung fest, dass nicht nur Orte oder Vermögensgegenstände geschützt werden, sondern auch der Mensch und seine Privatsphäre. Neben diesen Punkten muss weiters auch die örtliche Gegebenheiten herangezogen werden. Hierbei wurden 2 Passus für die Sicherheitsbehörden geschaffen, indem sie ohne richterlichen Beschluss Durchsuchungen bzw. Überwachungsmaßnahmen durchführen dürfen. Dies ist einerseits die Plain bzw. Open View Doktrin. Diese besagt, dass beobachtbare Gegenstände ohne richterlichen Beschluss beschlagnahmt werden können und weiters nicht als Durchsuchung gelten. Beispiel hierfür wäre, wenn ein Polizeibeamter von der Strasse aus ein Auto in einer Einfahrt eines Privatgrundstückes sieht und innerhalb dieses Autos ein belastbares Material sehen würde. Diese beobachtbaren Gegenstände stehen nicht mehr im Schutz der Privatsphäre, da sie von der Öffentlichkeit einsehbar sind, und können ohne richterlichen Beschluss beschlagnahmt werden. Andererseits gibt es noch die Open Field und Curtilage Doktrin. Diese besagt, dass offene Felder nicht dem Schutzbereich der Privatsphäre unterstehen aber der nähere Besitztum um das Wohnhaus herum schon.

Abschließend möchte ich den genauen Wortlaut des vierten Verfassungszusatzes zitieren und die wichtigsten Punkte fett kennzeichnen:

*“The right of the people to be secure in their **persons, houses, papers, and effects**, against **unreasonable** searches and seizures, shall not be violated, and **no Warrants** shall issue, but upon **probable cause**, supported by Oath or affirmation, and particularly describing the place to be **searched**, and the persons or things to be **seized**.” [FGV]*

7.1.3 Ausforschung von menschlicher Kommunikation

7.1.3.1 *Abhören von Telefongesprächen*

Zu den Routine Tätigkeiten der amerikanischen Sicherheitsbehörde gehört natürlich auch das Abhören von Telefonen (wiretapping) und das Aufzeichnen des in der Öffentlichkeit bzw. in geschlossenen Räumen gesprochenen Wortes (eavesdropping). Wie auch in Österreich ist die Anzahl dieser Überwachungsmaßnahmen speziell in den letzten Jahren stark angestiegen. In den häufigsten Fällen werden Telefone sowie Mobiltelefon abgehört. Um diese Art der Überwachungsmaßnahme abzusegnen, wurde in den siebziger Jahren ein spezieller Gerichtshof eingeführt: der Foreign Intelligence Surveillance Court (FISC). Diese Kontrollinstanz wurde 2007 durch ein Überwachungsgesetz seitens der amerikanischen Regierung (unter Führung von Präsident George W. Bush) abgeschafft, und somit war es möglich, ohne richterlichen Beschluss Gespräche im Inland durch die Sicherheitsbehörden abzuhören. Dies galt nicht nur für Telefongespräche, sondern auch für das Belauschen des E-Mail Verkehrs. Somit wurde der Verdacht, dass schon davor Telefone bzw. E-Mail Verkehr durch Sicherheitsbehörden überwacht werden, legitimiert. Schon 2005 wurde aufgedeckt, dass Präsident Bush die NSA nach den Anschlägen vom 11. September 2001 die Genehmigung erteilt hat, Telefongespräche sowie E-Mail Verkehr überwachen zu dürfen. Sommer 2007 wurde dieses neue Gesetz erlassen, das die rechtliche Grundlage für diese Überwachungen liefert. Es wurde jedoch beschlossen, dass alle 6 Monate das Gesetz bestätigt werden muss.

7.1.3.2 *Pen Register und Trap and Trace*

Bevor ich näher auf die Geräte Pen Register und Trap and Trace eingehen werden, muss natürlich erwähnt werden, dass diese Art der Überwachung nicht soviel Möglichkeiten an Daten bietet, wie der Einsatz von IMSI-Catchern. Es kann auch in den USA davon ausgegangen werden, dass IMSI-Catcher von den Sicherheitsbehörden verwendet werden.

Unter Pen Register ist ein Gerät zu verstehen, dass von einem bestimmten Telefon bzw. ein anderen Kommunikationseinrichtung die angewählten Rufnummern, die Dauer des Gesprächs und die Uhrzeit aufgezeichnet sowie das Gespräch decodieren kann. Weiters werden bei ankommenden Gesprächen nur das „Klingeln“ protokolliert, aber nicht die Rufnummer des Anrufers. Wie im United States Code Annotated Title 18. Crimes and Criminal Procedure Part II–Criminal Procedure Chapter 206–Pen Registers and Trap and Trace Device §3127(3) [USJ] nachzulesen ist, darf keine Information über den Inhalt der Gespräche durch den Pen Register aufgezeichnet werden. In den USA wird heftig darüber diskutiert, ob diese Regelung auch die Erfassung des E-Mail Verkehrs fällt. Dieses Gerät, wie in der nächsten Abbildung ersichtlich, wird fast immer bei den Telefonnetzbetreibern installiert.



Abbildung 12: Pen Register [DUH]

Als zweite Überwachungsmaßnahme möchte ich hier noch Trap and Trace vorstellen. Bei dieser Maßnahme werden die Rufnummern und weitere Informationen bei einem bestimmten Anschluss eingehende Anrufe protokolliert. Wie auch beim Pen Register soll der Inhalt des Gesprächs nicht erfasst werden. Hierfür gelten die gleichen rechtlichen Grundlagen wie für den Pen Register (siehe oben Pen Registers and Trap and Trace Device §3127(3)).

7.1.3.3 Lokalisierung von Mobiltelefonnutzern

In den letzten Jahren ist natürlich die Überwachung von Festnetz-Telefonaten zurückgegangen, und die Lokalisierung von Mobiltelefonnutzern stark angestiegen. Somit zählt diese Art der Überwachungsmaßnahme zu den wichtigsten Ermittlungstätigkeiten für die Sicherheitsbehörden. Dies inkludiert auch einerseits die Ermittlung des Aufenthaltsortes eines Mobilfunkteilnehmers und auch andererseits die Erstellung von Bewegungsprofilen einer verdächtigen Person. Die Feststellung des Aufenthaltsortes eines Verdächtigen war schon vor dem Überwachungsgesetzes vom Sommer 2007 möglich. „*Nach verbindlichen Regelung der Federal Communications Commission (FCC Anmerkung: eine unabhängige Behörde der US Regierung, die direkt dem US Congress untersteht) ist es zulässig, auf Ersuchen der Polizei festzustellen, im Wirkungsbereich welcher Antenne(n) eines Mobilfunknetzes ein Gespräch via Mobiltelefon begonnen und beendet wurde (antenna tower location information), wobei eine genaue Lokalisierung des Nutzers nicht möglich sein soll. Nach einer Regelung der FCC sind die Betreiber von Mobilfunknetzen verpflichtet, dafür Sorge zu tragen, dass der Ort, von dem aus ein Notruf (911) getätigt wird, bis auf einem Radius von 125 m genau bestimmt werden kann [ARC].* In Bezug auf den vierten Verfassungszusatz ist festzuhalten, dass Mobiltelefone meistens außerhalb von der Wohnung genutzt werden und somit der Nutzer im öffentlich zugänglichen respektive einsehbaren Raum aufhält. Deswegen fallen meistens Lokalisierungen von Mobilfunkteilnehmern nicht unter dem Schutz des vierten Verfassungszusatzes, da ja die Anwesenheit von Dritten wahrgenommen bzw. beobachtet werden können. Der Schutz des vierten Verfassungszusatzes dürfte gelten, wenn der Nutzer eines Mobiltelefons in einer Wohnung telefoniert, da hier der Nutzer nicht von Dritten bei der Nutzung gesehen werden kann. Wie aber schon in einem vorherigen Kapitel 7.1.3.1 Abhören von Telefongesprächen beschrieben, wurde diese Regelungen außer Kraft gesetzt und den Sicherheitsbehörden wurden

umfangreiche Befugnisse gewährt, dass nicht nur Lokalisierungen von Mobiltelefonen sondern auch das Abhören der Gesprächsinhalte gewährt wird.

7.1.4 Neue Formen der Überwachung

Durch den USA Patriot Act sowie dem neuen Überwachungsgesetz wurden den Sicherheitsbehörden noch mehr Befugnisse zum Zwecke der Terrorabwehr gewährt. Hierbei ist aber die Trennung zwischen krimineller Strafverfolgung und Abwehr von terroristischer Handlung nicht mehr so klar. Im speziellen bei Abhörmaßnahmen wurden durch den USA Patriot Act die Eingriffsvoraussetzungen mit Blick auf die Privatsphäre einer Person herabgesetzt. Eine Erweiterung war z.B. das illegale Eindringen in ein fremdes Computersystem als zulässige Überwachungsmaßnahme gebilligt wird. Im Jahre 2007 wurde bekannt, dass das FBI eine Spyware namens CIPAV (Computer and Internet Protocol Address Verifier) zum Zweck einer heimlichen Online-Durchsuchung einsetzt. Dieses Programm wird vom FBI über E-Mail oder Instant Messenger an den gewünschten Ziel-Computer geschickt. Wenn dieses Programm einmal installiert ist, dann werden die Namen aller laufenden Programme, die Browser-Informationen, den Typ des Betriebssystems samt Seriennummer und alle Benutzerinformationen aus der Registry protokolliert. Weiters werden die zuletzt besuchten Web-Seiten (inkl. IP-Adressen) übermittelt. Als diese Information durch einen FBI-Agenten an die Öffentlichkeit gelang, gab dieser zu Protokoll, dass Inhaltsdaten nicht betroffen waren. Ob dies mit dem heutigen Stand des Programms auch möglich ist, konnte ich nicht verifizieren. Für den Einsatz des Programms lag ein richterlicher Beschluss vor. Die Übermittlungsmaßnahme wurde deswegen beantragt, da ein ehemaliger Schüler Bombendrohungen an seine Schule gesendet hat. Weiters wurde durch die Aussage des FBI-Agenten bekannt, dass schon davor Key-Logger bei Verdächtigen installiert wurden. Ebenso wurde es als zulässig gewertet, dass gespeicherte Voicemail-Nachrichten (seizure of voice-mail messages) abgehört werden dürfen. Davor wurden diese Nachrichten genauso geschützt wie Telefongespräche (real-time Telefone) oder die Internet-Kommunikation zwischen zwei Personen. *„Dies wird in der Literatur für verfassungsrechtlich problematisch angesehen, weil die vorübergehende Speicherung einer solchen Nachricht (bis diese vom Empfänger abgehört wird), die so vermittelte Kommunikation nicht weniger schützenswert mache als die „unmittelbare“ telefonische Kommunikation. Zukünftig existiert hier ein vereinfachtes Verfahren zur Erlangung eines richterlichen Beschlusses [ARC].*

Eine weitere wichtige Überwachungsmaßnahme wurde in den letzten Jahren stark ausgeweitet: die Videoüberwachung auf öffentlichen Plätzen sowie biometrische Erkennungssysteme. Im Vergleich zu Österreich ist hier anzumerken, dass Videoüberwachung an öffentlichen Orten auch schon Standard ist, aber biometrische Erkennungssystem fast bis gar nicht angewendet werden. In den USA werden diese Geräte nicht nur z.B. an Flughäfen verwendet sondern auch für allgemeine polizeiliche Zwecke verwendet. So ein Beispiel hierfür war schon 2001 bei einem großen Sportereignis. Hier wurden alle Eintrittsgäste per Gesichtserkennung überprüft,

ob sie als gesuchte Kriminelle bzw. Terroristen in einer Datenbank der Sicherheitsbehörde erfasst waren. Es ist davon auszugehen, dass im Laufe der Zeit die Kombination beider Technologien (Videoüberwachung und biometrische Erkennungssysteme) vermehrt in den USA genutzt werden. Die Frage, die diese Kombination aufwirft ist, ob hier ein verfassungsrechtlicher Schutz den Betroffenen gewährt wird oder ob dieser starke Eingriff in die Privatsphäre rechtlich legitimiert ist.

7.2 Deutschland

In diesem Kapitel möchte ich überblicksartig die Überwachungsmethoden bzw. die rechtlichen Grundlagen in unserem Nachbarsland Deutschland beleuchten.

7.2.1 Rechtliche Grundlagen

Grundsätzlich wird das Fernmeldegeheimnis in Deutschland auch so wie in Österreich geschützt. Im Grundgesetz Art. 10 Abs. 1 werden vier Aspekte der Telekommunikation erfasst, die unverletzlich geschützt werden. Diese Aspekte sind: Kommunikationsinhalt, Umstände der Kommunikation, Bedingungen einer freien Telekommunikation und die Verwendung der durch Art. 10 Grundgesetz geschützten Daten. Als weitere wichtige Gesetze bezüglich Überwachungsmaßnahmen im Bereich der Telekommunikation in Deutschland kann die Strafprozessordnung (StPO) bzw. das Telekommunikationsgesetz gesehen werden. In der StPO ist die Überwachung der Telekommunikation geregelt. Diese inkludiert jede Form der Datenübermittlung, insbesondere die elektronische und optische Übertragung. Hierbei ist jede Art der Nachrichtenübermittlung, also Telefongespräche über Festnetz- oder Mobilfunknetz, gemeint. Bezüglich dieses Gesetzes möchte ich noch näher auf die Erhebung von Verkehrsdaten, Standortdaten bzw. den Einsatz von IMSI-Catchern eingehen.

Im § 100g StPO ist die Erhebung von Verkehrsdaten geregelt. Diese besagt folgendes:

„(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer

1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder

2. eine Straftat mittels Telekommunikation begangen hat,

so dürfen auch ohne Wissen des Betroffenen Verkehrsdaten (§ 96 Abs. 1, § 113a des Telekommunikationsgesetzes) erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Im Falle des Satzes 1 Nr. 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der

Sache steht. Die Erhebung von Standortdaten in Echtzeit ist nur im Falle des Satzes 1 Nr. 1 zulässig... [DJI1]

Hierbei wurde durch den Bezug auf den §96 Abs. 1 Telekommunikationsgesetz festgehalten, dass nicht nur Verbindungsdaten zugegriffen werden kann, sondern auf alle Verkehrsdaten.

Bezüglich der Erhebung von Standortdaten ist zu sagen, dass hier die Einschränkung gemacht wurde, dass dies nur bei schwerwiegenden Straftaten durchgeführt werden darf. Hierzu zählen z.B. Straftaten gegen die Landesverteidigung bzw. gegen die öffentlich Ordnung, Mord und Totschlag, Raub und Erpressung bzw. Betrug oder Computerbetrug (dies ist nur ein Auszug aus dem §100a StPO). „Hinsichtlich der Art und Weise der Standortermittlungen lassen sich im Wesentlichen vier Methoden unterscheiden:

- Einsatz eines IMSI-Catcher
- Standorterfassung anhand echter Verbindungsdaten (kommunikationsabhängig)
- Kommunikationsunabhängiger Standorterfassung („Stand-by-Betrieb“)
- Versendung sog. „stiller SMS“ (aktives „pingen“). [KEC]“

Bezüglich dem Einsatz eines IMSI-Catcher wurde ein eigener Paragraph in die StPO aufgenommen: §100i StPO (IMSI-Catcher):

„(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat, so dürfen durch technische Mittel

- 1. die Gerätenummer eines Mobilfunkendgerätes und die Kartenummer der darin verwendeten Karte sowie*
- 2. der Standort eines Mobilfunkendgerätes*

ermittelt werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist.

(2) Personenbezogene Daten Dritter dürfen anlässlich solcher Maßnahmen nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung des Zwecks nach Absatz 1 unvermeidbar ist. Über den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartenummer hinaus dürfen sie nicht verwendet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen.

(3) § 100a Abs. 3 und § 100b Abs. 1 Satz 1 bis 3, Abs. 2 Satz 1 und Abs. 4 Satz 1 gelten entsprechend. Die Anordnung ist auf höchstens sechs Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als sechs weitere Monate ist zulässig, soweit die in Absatz 1 bezeichneten Voraussetzungen fortbestehen.“ [DJI2]

Dieser Passus in der StPO war stark umstritten und im Jahre 2006 wurde eine Klage beim Bundesverfassungsgerichtshofes eingebracht, dass der §100i StPO in Bezug auf das Fernmeldegeheimnis verfassungswidrig ist. Die Klage wurde aufgrund von 3 Begründungen abgewiesen und als verfassungsmäßig bestätigt. Die Begründungen waren:

- 1. Die Bestimmung des § 100i Abs. 1 StPO verstößt nicht gegen das Grundrecht aus Art. 10 Abs. 1 GG da die erhobenen Daten keinen Kommunikationsinhalt im Sinne des Art. 10 Abs. 1 GG darstellen
- 2. § 100i StPO ist auf einer wirksam zu Stande gekommenen gesetzlichen Grundlage entstanden und ist nicht unverhältnismäßig.
- 3. Falls bei Behörden IMSI-Catchern verwendet werden, die das Abhören von Gesprächen unterstützen, dann wäre diese Maßnahme nicht durch den § 100i StPO gedeckt.

Das zweite wichtige Gesetz im Zusammenhang mit Überwachungsmaßnahmen in Deutschland ist das Telekommunikationsgesetz (TKG). Das TKG wurde am 09.11.2007 novelliert. Hier wurde die Richtlinie 2006/24/EG (Vorratsdatenspeicherung) der EU umgesetzt. Das Gesetz inkludiert weiters Identifizierungsmaßnahmen (Daten für Auskunftversuchen der Sicherheitsbehörden), Verwendung von gespeicherten Daten sowie Einzelverbindungsnachweise der Teilnehmer. Da wie schon beschrieben in Österreich noch nicht die Richtlinie 2006/24/EG (Vorratsdatenspeicherung) umgesetzt wurde, möchte ich hier näher darauf eingehen.

Durch die Novellierung des TKG wurde festgesetzt, dass seit dem 01.01.2008 für sechs Monate bestimmte Verkehrsdaten gespeichert werden. Welches Verkehrsdaten davon betroffen sind, werden im §113 TKG definiert.

Im Abs. 1 von §113a TKG wurde die Speicherdauer festgelegt. Hier wurde die unterste Grenze gewählt – 6 Monate. Im Abs. 2 von §113a TKG sind jene Daten aufgelistet, die auf Vorrat gespeichert werden. Diese sind an den Daten von der EU angelehnt (siehe Tabelle 1: Kategorien der Vorratsspeicherung). Im Abs. 3 von §113a TKG regelt die Speicherungspflichten für Anbieter öffentlich zugänglicher E-Mail-Dienste. Das Gegenstück stellt der Abs. 4 von §113 TKG dar, wo die Speicherungspflichten für Anbieter von Internetzugängen geregelt ist. Ein weiterer wichtiger Punkt ist der Absatz 7. Hier wird normiert, dass der Mobilfunkanbieter Auskunft über die geografische Lage einer Funkzelle. Der genaue Gesetzestext ist im Anhang C: Telekommunikationsgesetz §113a (Deutschland): Speicherungspflichtige Daten ersichtlich.

Jedoch muss noch erwähnt werden, dass auch diese Umsetzung sehr umstritten ist und noch verschiedene Autoren die Meinung vertreten, dass die Vorratsspeicherung unverhältnismäßig ist und somit verfassungswidrig ist. Dies untermauert auch die Behauptung von Peter Schaar, Datenschutzbeauftragter in Deutschland, der davor warnte, dass detaillierte Kommunikationsprofile bzw. Bewegungsprofile erstellt werden könnten. Der Bundesdatenschutzbeauftragte

nannte in diesem Zusammenhang, dass sogar die Demokratie in Gefahr damit wäre. In einem kürzlich (Mitte 2009) veröffentlichten Interview im Spiegel gab sich Herr Schaar optimistisch, dass das Gesetz wieder gekippt werden kann [SPO].

7.2.2 Ausblick „Online-Durchsuchung“

Wie in den vorangegangenen Kapiteln beschrieben, ist in Deutschland sowohl der Einsatz von IMSI Catchern (aber nicht zum Abhören von Gesprächen), Stillen SMS Praxis bei den Sicherheitsbehörden. Weiters wurde schon die Richtlinie 2006/24/EG (Vorratsdatenspeicherung) im TKG umgesetzt. Nun stellt sich die Frage, wie die rechtliche Lage bezüglich der Überwachungsmaßnahme „Online-Durchsuchung“ aussieht.

Am 21.02.2006 wurde ein Beschluss von einem Ermittlungsrichter III beim Bundesgerichtshof gefasst, der besagt, dass eine Online-Durchsuchung gestattet wird. Die Begründung hierfür war, dass die Durchsuchung eines PC ohne sein Wissen durch den §102 StPO gedeckt sei. Andererseits beschloss der Ermittlungsrichter I des Bundesgerichtshofs, dass die Ausforschung eines Computers durch einen heimlichen Zugriff gesetzlich nicht gedeckt sei. *„Begründet wurde dies u.a. damit, dass die Durchsuchung gemäß § 102 StPO – ein körperlicher, nicht ein elektronischer Vorgang – eine im Grundsatz auf Offenheit angelegt Maßnahme sei. So darf der „Inhaber“ des Gegenstands der Durchsuchung beiwohnen – also auch in Kenntnis des Umstands, dass eine Ermittlungsmaßnahme gegen ihn vollzogen wird (...). Ist er abwesend, so sind Zeugen hinzuzuziehen. All diese Schutzmechanismen fehlen bei einem heimlichen Datenangriff“ durch Ermittlungsbehörden. [KEC] “*

Mit einem weiteren Beschluss des Bundesgerichtshofs im Januar 2007 wurde abermals untermauert, dass es keine gesetzliche Grundlage für eine Online-Durchsuchung gibt. Mit 01.01.2009 trat dann aber ein neues BKA-Gesetz in Kraft indem es dem Bundeskriminalamt möglich ist, Online Durchsuchungen zu beantragen und durchzuführen. Bezüglich der Ausweitungen auf die Strafverfolgungen gab es Meinungsverschiedenheiten bei den Koalitionspartnern CDU und FDP. Die CDU wollte eine die Erweiterung, wobei die FDP sich strikt dagegen deklariert hat.

7.3 Zusammenfassung

In der nächsten Tabelle möchte ich einen Überblick geben, in welchem Land welche Überwachungsmaßnahmen mit heutigem Stand durchgeführt werden.

	IMSI-Catcher	Vorratsdaten-speicherung	Online-Durchsuchung
Österreich	X		
Deutschland	X	X	(X) ¹
USA	X	(X) ²	X

Tabelle 5: Gegenüberstellung der Überwachungsmaßnahmen in den verschiedenen Ländern

Zu (X)¹ ist zu sagen, dass nur für das BKA eine Erlaubnis der Online-Durchsuchung in Deutschland herrscht, nicht jedoch im Bezug zur Strafverfolgung. In den USA gibt es eigentlich keine Richtlinie zur Vorratsdatenspeicherung. Da aber die NSA immer wieder in den Schlagzeilen kommt, weil Gespräche oder elektronische Kommunikation abgehört oder aufgenommen wird, habe ich mich zu dieser Darstellung entschieden.

Ein weiterer wichtiger Aspekt ist mir bei der Gegenüberstellung zwischen Österreich und Deutschland im Bezug auf die Auskunftsverlangung gegenüber den Sicherheitsbehörden aufgefallen. In Deutschland ist im TKG genau geregelt, dass es sowohl ein automatisiertes als auch ein manuelles Auskunftsverfahren (§112 bzw. §113). In Österreich hingegen gibt es noch kein automatisiertes Verfahren. Die Erfüllung wird weitestgehend manuell durchgeführt.

8 Resümee

Durch den rasanten Aufstieg der Informations- und Kommunikationstechnologie in den letzten Jahren, wurde es ermöglicht, dass Daten effizient, schnell und ohne Rücksicht auf räumliche Distanz ausgetauscht werden können. Personen vertrauen immer mehr persönliche Daten Computersysteme an. Durch den Einsatz von mobilen Endgeräten können dann diese Daten jederzeit und unabhängig von ihrem Standort abgefragt und genutzt werden. Die Technologie ist sogar schon so weit fortgeschritten, dass von einem mobilen Endgerät E-Mails versendet, telefoniert, Termine verwaltet, Bestellungen über das Internet getätigt oder einem Freund eine Nachricht auf seinem Message Board hinterlassen werden kann. Kaum jemand, speziell aus der jungen Generation, kann sich vorstellen, ohne diese Technologien im Privat bzw. Berufsleben auskommen zu können.

Somit kann natürlich auch festgehalten werden, dass diese Entwicklung auch ein wachsendes Interesse bei den Strafverfolgungs- und Sicherheitsbehörden in Bezug auf der Ausnutzung der gleichen Technologien für Überwachungsmaßnahmen geweckt hat. Der rasante Anstieg der Informations- und Kommunikationstechnologien birgt einerseits für die Sicherheitsbehörden enorme Vorteile aber auch erhebliche Nachteile. Einerseits bietet die zunehmende Digitalisierung, Möglichkeiten der Überwachung, an die früher nicht einmal gedacht werden konnte. Andererseits müssen die Sicherheitsbehörden immer am neuesten Stand der Technologie sein, um Verbrechern bzw. Terroristen keinen Vorteil bzw. Vorsprung zu liefern.

Die jeweilige Bundesregierung muss die gesetzlichen Rahmenbedingungen schaffen, dass die Sicherheitsbehörden effizient und erfolgreich arbeiten können, ohne dass der Datenschutz jedes einzelnen Bürgers verletzt wird. Die drei wichtigen Gesetze in dieser Wechselbeziehung sind das Sicherheitspolizeigesetz 2008 (SPG 2008), Telekommunikationsgesetz 2003 (TKG 2003) und das Datenschutzgesetz 2000 (DSG 2000). Durch die Novellierung des SPG im Jahre 2008 wurde meiner Meinung das Gleichgewicht verrückt. Der Grund für diese Behauptung ist, dass durch das SPG, Standortabfragen von mobilen Endgeräten und Abfragen bezüglich IP-Adressen ohne richterlichen Beschluss gewährt werden. Eine große Säule der Demokratie, die Gewaltenteilung, ist für diesen Bereich ausgehebelt worden. Die einzige Kontrollinstanz bildet nun der Rechtsschutzbeauftragte des Innenministeriums. Somit sind sowohl der Großteil der Sicherheitsbehörden und das Kontrollorgan im gleichen Ministerium angesiedelt. Aber nicht nur dieser Punkt bei dieser Novelle ist kritikwürdig. Wie schon im Kapitel 4.3.5 Eingriff in das Fernmeldegeheimnis? angemerkt, wurde eine Verfassungsklage wegen Verletzung des Fernmeldegeheimnisses von Fr. Ringler (Landtagsabgeordnete der Wiener Grünen) und diversen Telekommunikationsbetreibern wegen dem §53 Abs. 3a eingebracht. Die Klage wurde dann zwar im Sommer 2009 wegen formalen Gründen abgelehnt, aber es wurde festgehalten, dass die Novelle keine Erweiterung der Datenspeicherpflicht für die

Telekommunikationsbetreiber darstellt. Weiters wurde vom VfGH klargestellt, dass der Einsatz von IMSI-Catcher nur zur Standortbestimmung eingesetzt werden darf, aber keine Gespräche abgehört werden dürfen. Eine sehr fragwürdige Behauptung wurde in diesem Zusammenhang von dem zuständigen Bundesministerium für Inneres getätigt. Der VfGH hat die Anfrage an das Bundesministerium für Inneres gestellt, ob IMSI-Catcher nicht auch Gespräche abhören können. Hierzu gab das Bundesministerium für Inneres bekannt, dass mit den eingesetzten Geräten das Ermitteln der Gesprächsinhalten nicht möglich ist. Diese Behauptung ist unerklärlich, da einige Geräte sowie im speziellen der neu gekaufte IMSI-Catcher sehr wohl in der Lage sind, Gespräche abzuhören.

Neben diesen angeführten Problematiken möchte ich hier nochmals eine Zusammenfassung der kritikwürdigen Punkte des SPG auflisten:

- Unklare Begriffsbestimmungen im Punkto „IP-Adresse“, „Nachricht“ bzw. „bestimmte Nachricht“
- Eingriff in das Fernmeldegeheimnis
- Eingriff in das Grundrecht auf Achtung der Privatsphäre
- Eingriff in den Gleichheitssatz (Kostenersatz)

In Bezug auf die Richtlinie 2006/24/EG (Vorratsdatenspeicherung) ist meine Meinung eher gespalten. Einerseits erhoffe ich mir durch die Umsetzung der Vorratsdatenspeicherung eine genaue Definition und Handhabung wie und welche Daten von Telekommunikationsbetreibern gespeichert werden müssen. Somit könnte die Umsetzung dieser Richtlinie eine Bereinigung der Unschärfen des SPG darstellen. Andererseits ist es natürlich ein weiterer tiefer Einschnitt in die Privatsphäre. Die Bedenken, dass auch hier die Missbrauchsgefahr ausgenutzt wird, bleibt bestehen.

Zur Überwachungsmaßnahme „Online-Durchsuchung“ ist von meiner Seite zu sagen, dass hier eine exakte Definition der Maßnahme bestehen muss sowie die Kontrollfunktion eines richterlichen Beschlusses. Ein Schnellschuss wie beim SPG würde katastrophale Auswirkungen für jeden einzelnen Staatsbürger nach sich ziehen. Weiters müsste der Betroffene als auch Dritte über diese Überwachungsmaßnahme informiert werden. Dies ist ja bei Überwachungsmaßnahmen durch das SPG auch nicht der Fall. Hier wird die Zukunft weisen, ob diese beiden noch nicht rechtskräftigen Überwachungsmaßnahmen tatsächlich zur objektiven Erhöhung der allgemeinen Sicherheit beitragen.

Abschließend möchte ich anmerken, dass obwohl die staatlichen Überwachungsmaßnahmen speziell in den letzten Jahren zugenommen haben, persönliche Daten immer öfters von Personen preisgegeben werden. Durch den kompetenten Erfolg von Community-Portalen, wie Facebook, StudiVZ oder Twitter tragen immer mehr Privatpersonen ihr Privatleben in die Öffentlichkeit. Diese interessante Entwicklung nahm aber trotz dem Anstieg an staatlichen Überwachungsmaßnahmen nicht ab, sondern sogar zu. Somit möchte ich diese Diplomarbeit mit einem, meiner Meinung nach, sehr gutem Zitat beenden:

„Privatsphäre ist wie Sauerstoff – man schätzt sie erst, wenn sie fehlt“ [EMJ]

Literaturverzeichnis

- [3GP1] Vgl. 3GPP TS 22.016: International Mobile Equipment Identities (IMEI)
<http://www.3gpp.org/ftp/Specs/html-info/22016.htm>
abgerufen am 20.05.2009
- [3GP2] Vgl. 3GPP TS 23.003 Numbering, addressing and identification
<http://www.3gpp.org/ftp/Specs/html-info/23003.htm>
abgerufen am 20.05.2009
- [APA] Überwachung von Telefon und Handy 2003 – 2006 (2007)
Austrian Presse Agentur (APA)
http://apa.cms.apa.at/cms/ebc/attachments/7/1/5/CH0277/CMS1198070227092/02vorratsdatenspeicherung_hires.jpg
abgerufen am 29.11.2009
- [ARC] Clemens Arzt
Polizeiliche Überwachungsmaßnahmen in den USA –
Grundrechtsbeschränkungen durch moderne Überwachungstechniken
und im War on Terrorism (2004)
Verlag für Polizeiwissenschaft
- [BBN] Definitionen des Begriffs "Datenschutz":
<http://beat.doebe.li/bibliothek/w00714.html>
abgerufen am 27.01.2009
- [BEK] Vgl. Walter Berka
Die Grundrechte (Grundfreiheiten und Menschenrechte in Österreich)
(1999), Rz 256,
http://books.google.at/books?id=aBPG6XEI8GEC&dq=berka+grundrechte&printsec=frontcover&source=bl&ots=FgTa3fzM4Z&sig=UXmX7FjR8gtdn1mswcVestnVWLOY&hl=de&ei=f4-6Stb_B42LsAaGicGRBA&sa=X&oi=book_result&ct=result&resnum=1#v=onepage&q=&f=false
abgerufen am 18.08.2009
- [BKA] Bundeskanzleramt: Gesetze im Zusammenhang mit Datenschutz
<http://www.bka.gv.at>
abgerufen am 01.02.2009
- [BJI] BMJ/BMI: Schlussbericht interministerielle Arbeitsgruppe „Online-Durchsuchung“, 2008:
http://209.85.229.132/search?q=cache:QpzZr-mInBQJ:www.justiz.gv.at/cms_upload/docs/AG_OnlineDurchsuchung_Endbericht.pdf+erweiterung+des+ermittlungsinstrumentariums&cd=1&hl=de&ct=clnk&gl=at
abgerufen am 19.12.2009

- [BMI] Bundesministerium für Inneres, Rechtsschutzbeauftragter:
<http://www.bmi.gv.at/rechtsschutzbeauftragter/>
abgerufen am 13.10.2009
- [BWA] Vgl. Bernhard Walke
Mobilfunknetze und ihre Protokolle, Grundlagen GSM, UMTS und
andere zellulare Mobilfunknetze,
http://books.google.at/books?id=wD3GpFuvZ58C&pg=PA390&lpg=PA390&dq=umts+architektur+ue+dom%C3%A4ne&source=bl&ots=NyXSIQN&sig=440iasm2Rk6D6Gv30DiFTOSAuuA&hl=de&ei=UglOSpbGlpgd_Abi-qm5DQ&sa=X&oi=book_result&ct=result&resnum=1#v=onepage&q=&f=false
abgerufen am 05.06.2009
- [COP] Vgl. Copland vs the United Kingdom, Rz41, 43, 44
EGMR 3.4.2007,
<http://www.bailii.org/eu/cases/ECHR/2007/253.html>
abgerufen am 19.10.2009
- [DHO] Vgl. Dragana Damjanovic / Michael Holoubek
Handbuch des Telekommunikationsrechts (2006)
- [DJI1] Deutscher Juristischer Informationsdienst,
Strafprozessordnung (StPO) §100g
<http://dejure.org/gesetze/StPO/100g.html>
abgerufen am 11.12.2009
- [DJI2] Deutscher Juristischer Informationsdienst,
Strafprozessordnung (StPO) §100i
<http://dejure.org/gesetze/StPO/100i.html>
abgerufen am 11.12.2009
- [DJI3] Deutscher Juristischer Informationsdienst,
Telekommunikationsgesetz (TKG) §113a
<http://dejure.org/gesetze/TKG/113a.html>
abgerufen am 11.12.2009
- [DWP] Walter Dohr, Ernst Weiss, Hans-Jürgen Pollirer
Datenschutzrecht (2002) §4 Anm. 2.
- [DSK] Datenschutzkommission: Geschichte und Aufgabe
<http://www.dsk.gv.at/site/6288/default.aspx>
abgerufen am 03.03.2009
- [DUH] Duhaime Portal - Law · Legal Information · Justice (2009)
Foto Pen Register

http://www.duhaime.org/Portals/duhaime/images/pen_register.jpg
abgerufen am 27.12.2009

- [EMJ] Uni Kassel, Hendrik Preuß,
Zitat: John Emontspool
Anonymisierungsdienste: ANONYMITY IS NOT A CRIME (2009),
[http://www.db.informatik.uni-kassel.de/Lehre/WS0910/Seminar/10-Anonymisierungsdienste_\(Hendrik_Preuss\).ppt](http://www.db.informatik.uni-kassel.de/Lehre/WS0910/Seminar/10-Anonymisierungsdienste_(Hendrik_Preuss).ppt)
abgerufen am 31.12.2009
- [EUC] Vgl. EU: Charta der Grundrechte der Europäischen Union
http://www.europarl.europa.eu/charter/pdf/text_de.pdf
abgerufen am 26.02.2009
- [EUJ] Vgl. EU: Freiheit, Sicherheit und Recht: Datenschutz:
http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm
abgerufen am 26.02.2009
- [FGV] US Federal Government Printing Office: Fourth Amendment
<http://www.gpoaccess.gov/constitution/html/amdt4.html>
abgerufen am 26.12.2009
- [FJS] FJ Software, Freeware Produkt MyPhoneExplorer Vers. 1.7.4
<http://www.fjsoft.at/de/>
abgerufen am 15.10.2009
- [FLM] UMTS - mehr als nur zum Telefonieren gut, TU Chemnitz (2001)
Marco Flohrer, Fakultät für Informatik
<http://archiv.tu-chemnitz.de/pub/2001/0070/data/umts.html>
abgerufen am 23.04.2009
- [FMK] Forum Mobilkommunikation, Datenschutz: Nichts ist vollkommen.
http://www.fmk.at/archiv/mobikom/dl/FMK_5-8.pdf
abgerufen am 16.04.2009
- [FOX] Dirk Fox
Datenschutz und Datensicherheit 26 (2002) 4: „Der IMSI-Catcher“:
<http://www.datenschutz-und-datensicherheit.de/jhrg26/imsicatcher-fox-2002.pdf>
abgerufen am 08.09.2009
- [FTZ] Statistik Überwachungsmaßnahmen SPG (2008)
ORF Futurezone,
<http://futurezone.orf.at/stories/256417/>
abgerufen am 30.09.2009
- [FTZ2] Statistik Überwachungsmaßnahmen SPG (2008)
ORF Futurezone,

- <http://futurezone.orf.at/stories/288198/>
abgerufen am 30.09.2009
- [FTZ3] Fekter gegen Entwurf für Data-Retention (2009),
ORF Futurezone,
<http://futurezone.orf.at/stories/1631202/>
abgerufen am 30.09.2009
- [FXS] Flexispy, Produkt Flexispy
<http://www.flexispy.com/de/index.html>
abgerufen am 01.11.2009
- [GÖD] Dieter Görrisch
Moderne Lausch- und Störverfahren (2005),
Verlag Franzis,
- [GRS] Vgl. Social Engineering Fundamentals, Part I: Hacker Tactics (2006)
Sarah Granger,
<http://www.securityfocus.com/infocus/1527>
abgerufen am 05.11.2009
- [GSI] GSM Interceptor buatan Israel
<http://pirantiku.blogspot.com/2009/04/mengintip-mata-mata-jaringan-seluler.html>
abgerufen am 14.11.2009
- [HKE] Sicherheitspolizeigesetz – Polizeiausgabe (2008) §53 Anm. 6.,
Andreas Hauer / Rudolf Keplinger
abgerufen am 30.08.2009
- [HUS] Freeware Produkt HushSMS
<http://www.silentservices.de/HushSMS.html>
abgerufen am 02.11.2009
- [I4J1] Internet4Jurists: Datenschutz im Internet:
<http://www.internet4jurists.at/intern27a.htm>
abgerufen am 15.03.2009
- [I4J2] Internet4Jurists: EBRV zu TKG2003:
http://www.internet4jurists.at/gesetze/bg_tkg01.htm#%C2%A7_92.
abgerufen am 05.08.2009
- [I4J3] Internet4Jurists: Staatsgrundgesetz
<http://www.internet4jurists.at/gesetze/stgg.htm>
abgerufen am 11.08.2009
- [I4J4] Internet4Jurists: Sicherheitspolizeigesetz (2007)
http://internet4jurists.at/gesetze/bg_spg2008.htm
abgerufen am 01.08.2009

- [I4J5] Internet4Jurists: Strafgesetzbuch
http://www.internet4jurists.at/gesetze/bg_stgb01.htm#%C2%A7115.
abgerufen am 21.08.2009
- [KEC] Christop Keller
Telekommunikationsüberwachung und andere versteckte Ermittlungsmaßnahmen, Richard Boorberg Verlag
- [KLA] Vgl. Klass and others vs Germany, Rz41
EGMR 6.9.1978,
http://www.hrcr.org/safrica/limitations/klass_germany.html
abgerufen am 19.10.2009
- [KOH] Vgl. Vortrag Gerd Kramarz von Krohout beim Kongress des Computer Chaos Club (CCC): IMSI-Catcher: GSM Unsicherheit in der Praxis, (2001)
http://tunesdaily.com/930600/Gerd_Kramarz_von_Kohout-IMSI-Catcher_GSM_Unsicherheit_in_der_Praxis.mp3
abgerufen am 25.04.2009
- [KRY] Verschlüsselungsalgorithmen im GSM Standard:
http://gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/gsm_security_algorithms.htm#nav-6
abgerufen am 14.04.2009
- [KUC] Christian Kurz
IT/RAK: Rechnerarchitekturen und Kommunikationsnetze (2003),
Uni Wien, Institut für Informatik und Wirtschaftsinformatik,
- [KUN] Gerhard Kunnert, Dietmar Jahnel (Hrsg.)
Der Sicherheitspolitische Griff nach Telekommunikationsdaten.
Möglichkeiten – Grenzen – Kritik, in Jahnel, Datenschutzrecht und E-Government: Jahresbuch 2008,
abgerufen am 11.09.2009
- [MAL] Vgl. Malone vs the United Kingdom, RZ84
EGMR 2.8.1984,
http://sixthformlaw.info/06_misc/cases/malone_v_uk.htm
abgerufen am 19.10.2009
- [MIC] Spear Phishing: gezielte Phishingangriffe (2006)
Microsoft,
<http://www.microsoft.com/germany/protect/yourself/phishing/spear.msp>
abgerufen am 05.11.2009
- [MNC] Network Security Assessment, Second Edition (2007),
Chris McNab, O`reilly
<http://books.google.at/books?id=zKhCEYRGFuYC&dq=mcnab+netwo>

[rk+security&printsec=frontcover&source=bn&hl=de&ei=yU8RS763Fd eNjAf26uDQAw&sa=X&oi=book_result&ct=result&resnum=4&ved=OC BkQ6AEwAw#v=onepage&q=&f=false](http://www.google.com/search?hl=de&ei=yU8RS763Fd eNjAf26uDQAw&sa=X&oi=book_result&ct=result&resnum=4&ved=OC BkQ6AEwAw#v=onepage&q=&f=false)
abgerufen am 06.11.2009

- [ORF] Statistik Überwachungsmaßnahmen SPG (2008)
ORF,
<http://help.orf.at/?story=7497>
abgerufen am 30.09.2009
- [PAR1] Stellungnahmen zum Ministerialentwurf, 2007,
http://www.parlinkom.gv.at/PG/DE/XXIII/ME/ME_00118/pmh.shtml
abgerufen am 13.09.2009
- [PAR2] Abänderungsantrag SPG, 2007,
http://www.parlament.gv.at/PG/DE/XXIII/AA/AA_00089/pmh.shtml
abgerufen am 15.09.2009
- [PAR3] EBRV zu SPG (2007): Finanzielle Auswirkungen
http://www.parlament.gv.at/PG/DE/XXIII/ME/ME_00118/imfname_086207.pdf
abgerufen am 22.09.2009
- [PAR4] Fragekatalog von Peter Pilz zum SPG (2008)
http://www.parlament.gv.at/PG/DE/XXIV/J/J_00260/imfname_144640.pdf
abgerufen am 01.12.2009
- [PAR5] Anfragebeantwortung des Fragekatalog von Peter Pilz (2009)
http://www.parlament.gv.at/PG/DE/XXIV/AB/AB_00300/pmh.shtml
abgerufen am 01.12.2009
- [PHC] Phonecrypt - Verschlüsselungssoftware für Mobil und Festnetzverbindung (2009)
Fa. Securstar,
http://www.securstar.com/products_phonecrypt.php
abgerufen am 02.11.2009
- [POW] Vgl. Martin Parschalk, Gerald Otto, Jan Weber, Alexander Zuser
Telekommunikationsrecht (2006)
- [REP] Vgl. Paul Reichel
Verfassungsrechtliche Probleme nach Inkrafttreten des SPG 2008
(2008)

- [RFC1] RFC 2821, Section 3.8.2 Received Lines in Gatewaying
<http://www.ietf.org/rfc/rfc2821.txt>
 abgerufen am 13.09.2009

- [RFC2] RFC 791, Section 3.1, Internet Header Format
<http://www.ietf.org/rfc/rfc791.txt>
 abgerufen am 13.09.2009

- [RFC3] RFC 2822, Section 3.6.1. The origination date field
<http://www.ietf.org/rfc/rfc2822.txt>
 abgerufen am 13.09.2009

- [RSC] Rohde & Schwarz: Initiative „Top-Sec“
http://www.rohde-schwarz.com/it-sicherheit/topsec_gsm_de.html
 abgerufen am 30.10.2009

- [SCS] Benjamin Schorn, Philipp Schneider
 Überwachungsstaat Deutschland 2.0? Der „Bundestrojaner“,
 GRIN Verlag für akademische Texte

- [SPG] Parlament, Gesetzestext zur Novelle zum Sicherheitspolizeigesetz
http://www.parlinkom.gv.at/PG/DE/XXIII/I/I_00158/pmh.shtml
 abgerufen am 29.08.2009

- [SPO] Spiegel Online, Interview mit Peter Schaar (2009),
 "Ein Terrorist kann die Speicherung umgehen",
<http://www.spiegel.de/politik/deutschland/0,1518,666911,00.html>
 abgerufen am 11.12.2009

- [SPY] Spy World, Produkt „GSM Interceptor“,
http://www.spyworld.com/Cellular_Interceptor.htm
 abgerufen am 14.11.2009

- [StG] Regierungsvorlage 1166 BlgNr XXI. GP26
http://www.sbg.ac.at/ssk/bgbl/2002_i_134_rv1166.pdf
 abgerufen am 23.10.2009

- [STM] Markus Steinberg
 Erstellung eines Frameworks für eine positionsabhängige
 Auftragsverwaltung in mobilen Netzwerken, Masterarbeit:
http://www.uwe-kern.de/winwiki/index.php?title=Spezial:PdfPrint&page=Optimierung_der_Aussendiensteeinsatzverteilung_durch_LBS-Technologien
 abgerufen am 16.05.2009

- [TV0] Vgl. Sicherheitspolizeigesetz (2008)
 Theodor Thanner, Mathias Vogl

- [ÜVO] Vgl. Verordnung des Bundesministerium für Justiz über den Ersatz der Kosten der Betreiber für die Mitwirkung an der Überwachung einer Telekommunikation (Überwachungskostenverordnung – ÜKVO), BGBl II 322/2004
<http://www.bmvit.gv.at/telekommunikation/recht/aut/verordnungen/downloads/b3222004.pdf>
abgerufen am 21.08.2009
- [USJ] United States Department of Justice,
Pen Register and Trap and Trace (2003,
http://www.justice.gov/criminal/cybercrime/pentrap3121_3127.htm
abgerufen am 27.12.2009
- [USS] Was ist ein IMSI-Catcher? – Überwachungsstaat.at
<http://www.ueberwachungsstaat.at/index.php?id=56276>
abgerufen am 03.09.2009
- [VOG] Mathias Vogl
Rechtsschutz und Vollziehung, in BMI (Hrsg), Der Rechtsschutzbeauftragte (2004)
- [VGH] Vgl. Erkenntnis zum Kostenersatz für die Verpflichtung zur Bereitstellung von Überwachungseinrichtungen, VfGH vom 27.02.2003
http://www.ris.bka.gv.at/Dokumente/Vfgh/JFR_09969773_02G00037_01/JFR_09969773_02G00037_01.html
abgerufen am 07.10.2009
- [WAL] Michael Walker
On the security of 3GPP networks, (2000)
http://www.esat.kuleuven.be/cosic/eurocrypt2000/mike_walker.pdf
abgerufen am 05.11.2009
- [WKH] Vgl. Ewald Wiederin in Karl Korinek (Hrsg), Michael Holoubek
Österreichische Busverfassungsrecht, Band III; Grundrechte Art 10
StGG Rz17
- [WKO] Sicherheitspolizeigesetz Erlass:
http://portal.wko.at/wk/format_detail.wk?AnglID=1&StlID=386310&DstID=5000
abgerufen am 14.09.2009
- [WK02] Auskunftsverlangen gem. §53 Abs. 3a und 3b SPG Formular,
Portal WKO
http://portal.wko.at/wk/dok_detail_file.wk?AnglID=1&DocID=827439&StlID=389446
abgerufen am 12.10.2009

- [WKL] Hardware Keylogger, Firma WirelessKeyLogger
http://www.wirelesskeylogger.com/index.php/controller/product/product_id/2
abgerufen am 29.11.2009
- [WZI] IMSI-Catcher - Wanzen für Mobiltelefons:
<http://hp.kairaven.de/miniwahr/imsi.html>
abgerufen am 12.09.2009
- [XON] Testbericht Flexispy von der Firma Xonio, Veröffentlicht Chip.de
http://www.chip.de/artikel/Flexispy-Spionage-Tool-fuers-Handy_28323138.html
abgerufen am 02.11.2009
- [ZAN] Wolfgang Zankl, Lukas Feiler, Maximillian Raschhofer, Manuel Boka, Christian Simon, Ana Stahov
Auf dem Weg zum Überwachungsstaat? (2009)
- [ZSC] Vgl. Georg Zanger, Susanne Schöll
Telekommunikationsgesetz (2004)

Abbildungsverzeichnis

Abbildung 1: Überwachung von Telefon und Handy 2003 – 2006 [APA]	59
Abbildung 2: Architektur eines GSM-Netz	65
Abbildung 3: UMTS Zellen [FLM]	70
Abbildung 4: Architektur eines UMTS-Netz	71
Abbildung 5: IMSI-Catcher Anlage [WZI]	72
Abbildung 6: IMSI-Catcher Abhören von Gesprächen [WZI]	74
Abbildung 7: 3 alternative IMSI-Catcher Modelle	75
Abbildung 8: Test Stille SMS	80
Abbildung 9: Flexispy Protokollierung Anrufrdaten [XON]	82
Abbildung 10: Flexispy Protokollierung Cell-ID [XON]	82
Abbildung 11: Hardware Key-Logger [WKL]	93
Abbildung 12: Pen Register [DUH]	99
Abbildung 13: Finanziellen Auswirkungen Novelle SPG 2008 [PAR3]	120
Abbildung 14: Auskunftsverlangen gem. §53 Abs. 3a und 3b SPG Formular [WK02]	122

Tabellenverzeichnis

Tabelle 1: Kategorien der Vorratsspeicherung	20
Tabelle 2: Überblick Arten von Überwachung	30
Tabelle 3: Mobilfunk-Generationen	61
Tabelle 4: Aufbau einer IMSI	66
Tabelle 5: Gegenüberstellung der Überwachungsmaßnahmen in den verschiedenen Ländern	104

Abkürzungsverzeichnis

3GPP	3rd Generation Partnership Project
ABI	Amtsblatt
Abs	Absatz
AbwA	Abwehramt
Art	Artikel
AUC	Authentication Center
BGBI	Bundesgesetzblatt
BMI	Bundesministerium für Inneres
BMJ	Bundesministerium für Justiz
BVT	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
bzw.	beziehungsweise
DSG 2000	Datenschutzgesetz 2000
DSK	Datenschutzkommission
DSR	Datenschutzrat
EBRV	Erläuternde Bemerkungen zur Regierungsvorlage
EBT	Einsatzgruppe zur Bekämpfung des Terrorismus
ECG	E-Commerce Gesetz
EDOK	Einsatzgruppe zur Bekämpfung der organisierten Kriminalität
EDGE	Enhanced Data Rates for GSM Evolution
EDPS	European Data Protection Supervisor
E-GovG	E-Government Gesetz
EIR	Equipment Identify Register
EGMR	Europäische Gerichtshof für Menschenrechte
EKMR	Europäische Kommission für Menschenrecht
EMRK	Europäische Menschenrechtskonvention
EMS	Enhanced Message Service
ETSI	European Telecommunications Standards Institute
EuGH	Europäischer Gerichtshof
FCC	Federal Communications Commission
GGSN	Gateway GPRS Support Node
GMSC	Gateway Mobile Switching Center
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
HNaA	Heeresnachrichtenamt
HLR	Home Location Register
HTTP	Hypertext Transfer Protocol
IKT	Informations- und Kommunikationstechnik
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
IMT2000	International Mobile Telecommunication 2000
IP	Internet Protocol
ITU	International Telecommunication Union
MCC	Mobile Country Code
MMS	Multimedia Message Service;
MNC	Mobile Network Code
MSC	Mobile Switching Center
MSIN	Mobile Station Identification Number
MSISDN	Mobile Subscriber Integrated Services Digital Network
PLMN	Public Land Mobile Network

RFID	Radio Frequency Identification
RL	Richtlinie
RNC	Radio Network Controller
RNS	Radio Network Subsystem
SGSN	Serving GPRS Support Node
SMS	Short Message Service
SMTP	Simple Mail Transfer Protokoll
SPG 2008	Sicherheitspolizeigesetz 2008
StGB	Strafgesetzbuch
StGG	Staatsgrundgesetz
StPO	Strafprozessordnung
TKG 2003	Telekommunikationsgesetz 2003
TSG GERAN	Technical Specification Group GSM EDGE Access Network UMTS
UMTS	Universale Mobile Telecommunications System
USIM	UMTS Subscriber Identity Module
VLK	Visitor Location Register
VfGH	Verfassungsgerichtshof
WAP	Wireless Application Protocol
WLAN	Local Area Network

Anhang A: Auszug aus der EBRV zum SPG 2008

Hier ein Auszug aus der EBRV zum SPG 2008 bezüglich den finanziellen Auswirkungen der Novelle:

3. Finanzielle Auswirkungen:

3.1. laufende Ausgaben:

VICLAS-Datenbank:

Lizenzgebühr pro Jahr: ca. € 15.000,-- .

zusätzlicher Personalbedarf (für Dateneingabe, -pflege und -analyse):

Anzahl	Wertigkeit	Jahreswert	Summe
1	A1/3	€ 61.619,00	€ 61.619,--
1	E2a/7	€ 50.116,00	€ 50.116,--
3	E2a/5	€ 50.116,00	€ 150.348,--
1	A3	€ 33.906,00	€ 33.906,--
6		€ 195.757,00	€ 295.989,--

Personalausgaben:	€ 295.989,--
-------------------	--------------

zzgl. 20% Verwaltungsgemeinkosten	€ 59.198,--
zzgl. 12% Sachkosten	€ 35.519,--
zzgl. Raum-/Bürokosten	€ 12.196,--
	€ 106.912,--

Sachausgaben:	€ 106.912,--
---------------	--------------

Gesamtausgaben:	€ 402.901,--
-----------------	--------------

3.2. einmalige Ausgaben:

Neuankauf eines IMSI-Catchers: ca. € 600.000,--.

Kosten für EPS-web:

Die erforderliche Software steht aufgrund der Kooperation mit dem Bayerischen Staatsministerium des Innern kostenlos zu Verfügung. Im BMI ist eine entsprechende Web-Farm zu errichten, dazu werden voraussichtlich zwei bis drei Web-Server zusätzlich angeschafft werden müssen. Die Kosten für einen Server belaufen sich auf ca. 10.000,-- €. Die Schulungen sollen mit Multiplikatoren noch vor der EM 2008 durchgeführt werden, dazu fallen ev. Gebühren nach der RGV an.

Abbildung 13: Finanziellen Auswirkungen Novelle SPG 2008 [PAR3]

Anhang B: Auskunftsverlangen gem. §53 Abs. 3a und 3b SPG Formular

- Briefkopf der Dienststelle -

Betreff: Auskunftsverlangen gemäß § 53 Abs. 3a u. 3b SPG bzw. § 98 TKG
GZ:

per FAX – Nr.:

- Anfrage betreffend:
- ☐ Daten gemäß § 53 Abs. 3a Z 1 SPG (Auskunft erfolgt kostenlos)
 - ☐ Daten gemäß § 53 Abs. 3a Z 2 SPG (Auskunft erfolgt kostenlos)
 - ☐ Daten gemäß § 53 Abs. 3a Z 3 SPG (Auskunft erfolgt kostenlos)
 - ☐ Daten gemäß § 53 Abs. 3a 2. Satz SPG (Auskunft erfolgt kostenlos)
 - ☐ Daten gemäß § 53 Abs. 3b SPG (Auskunft ist kostenpflichtig)
 - ☐ Daten gemäß § 98 TKG (Auskunft erfolgt kostenlos)

Die oben angeführte Behörde/Dienststelle ersucht um unverzügliche Übermittlung der unter Anfrage angeführten Daten.

Die anfragende Behörde/Dienststelle bestätigt ausdrücklich, dass sie im Sinne des § 7 Abs. 2 Z. 2 DSG 2000 zur Durchführung der zugrunde liegenden Amtshandlung gesetzlich zuständig ist, wobei die Sicherheitsbehörde die Verantwortung für die rechtliche Zulässigkeit des obigen Auskunftsbegehrens trifft.

Die Verwendung der Daten durch die anfragende Behörde/Dienststelle ist wesentliche Voraussetzung für die Wahrnehmung der sicherheitspolizeilichen Aufgabe nach der jeweiligen unter Anfrage angeführten Bestimmung.

Es wird ersucht, die Auskunft wie folgt zu erteilen:

- ☐ per Fax unter
- ☐ per E-Mail unter
- ☐ fernmündlich unter

Beilage: Liste

Bei der Sicherheitsexekutive bekannte Anfragekriterien	
Name	
Anschrift	
Teilnehmernummer	
Zeitraum und passive Teilnehmernummer eines geführten Telefongesprächs	
Bekannte Informationen zu einer bestimmten Nachricht im Internet	
IP-Adresse und bestimmter Zeitpunkt (inklusive Zeitzone) ihrer Übermittlung	
Dokumentation bei Auskunftsverlangen gem. § 53 Abs. 3b SPG und § 98 TKG: Anführung der SPG-Aufgabe (z. B. erste allgem. Hilfeleistungspflicht)	

Umfang des Auskunftsbegehrens und Auskunft des Betreibers/Diensteanbieters		
Sicherheitsexekutive kreuzt in der mittleren Spalte die begehrte Auskunft an Betreiber/Diensteanbieter beauskunftet die begehrten Daten in der rechten Spalte		
Name		
Anschrift		
Teilnehmernummer		
IP-Adresse zur bei der Sicherheitsexekutive vorliegenden Nachricht und Zeitpunkt (inklusive Zeitzone) der Übermittlung		
Standortdaten		
Internationale Mobilteilnehmerkennung (IMSI)		

Abbildung 14: Auskunftsverlangen gem. §53 Abs. 3a und 3b SPG Formular [WK02]

Anhang C: Telekommunikationsgesetz §113a (Deutschland): Speicherungspflichtige Daten

„(1) Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten nach Maßgabe der Absätze 2 bis 5 sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern. Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ohne selbst Verkehrsdaten zu erzeugen oder zu verarbeiten, hat sicherzustellen, dass die Daten gemäß Satz 1 gespeichert werden, und der Bundesnetzagentur auf deren Verlangen mitzuteilen, wer diese Daten speichert.

(2) Die Anbieter von öffentlich zugänglichen Telefondiensten speichern:

1.	die Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,
2.	den Beginn und das Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone,
3.	in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, Angaben zu dem genutzten Dienst,
4.	im Fall mobiler Telefondienste ferner:
a)	die internationale Kennung für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss,
b)	die internationale Kennung des anrufenden und des angerufenen Endgerätes,
c)	die Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzten Funkzellen,
d)	im Fall im Voraus bezahlter anonymer Dienste auch die erste Aktivierung des Dienstes nach Datum, Uhrzeit und Bezeichnung der Funkzelle,
5.	im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adresse des anrufenden und des angerufenen Anschlusses.

Satz 1 gilt entsprechend bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei sind anstelle der Angaben nach Satz 1 Nr. 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht zu speichern.

(3) Die Anbieter von Diensten der elektronischen Post speichern:

1.	bei Versendung einer Nachricht die Kennung des elektronischen Postfachs und die Internetprotokoll-Adresse des Absenders sowie die Kennung des
----	---

		<i>elektronischen Postfachs jedes Empfängers der Nachricht,</i>
	2.	<i>bei Eingang einer Nachricht in einem elektronischen Postfach die Kennung des elektronischen Postfachs des Absenders und des Empfängers der Nachricht sowie die Internetprotokoll-Adresse der absendenden Telekommunikationsanlage,</i>
	3.	<i>bei Zugriff auf das elektronische Postfach dessen Kennung und die Internetprotokoll-Adresse des Abrufenden,</i>
	4.	<i>die Zeitpunkte der in den Nummern 1 bis 3 genannten Nutzungen des Dienstes nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.</i>

(4) Die Anbieter von Internetzugangsdiensten speichern:

	1.	<i>die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,</i>
	2.	<i>eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt,</i>
	3.	<i>den Beginn und das Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.</i>

(5) Soweit Anbieter von Telefondiensten die in dieser Vorschrift genannten Verkehrsdaten für die in § 96 Abs. 2 genannten Zwecke auch dann speichern oder protokollieren, wenn der Anruf unbeantwortet bleibt oder wegen eines Eingriffs des Netzwerkmanagements erfolglos ist, sind die Verkehrsdaten auch nach Maßgabe dieser Vorschrift zu speichern.

(6) Wer Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert, ist zur Speicherung der ursprünglichen und der neuen Angabe sowie des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone verpflichtet.

(7) Wer ein Mobilfunknetz für die Öffentlichkeit betreibt, ist verpflichtet, zu den nach Maßgabe dieser Vorschrift gespeicherten Bezeichnungen der Funkzellen auch Daten vorzuhalten, aus denen sich die geografischen Lagen der die jeweilige Funkzelle versorgenden Funkantennen sowie deren Hauptstrahlrichtungen ergeben.

(8) Der Inhalt der Kommunikation und Daten über aufgerufene Internetseiten dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

(9) Die Speicherung der Daten nach den Absätzen 1 bis 7 hat so zu erfolgen, dass Auskunftersuchen der berechtigten Stellen unverzüglich beantwortet werden können.

{10} Der nach dieser Vorschrift Verpflichtete hat betreffend die Qualität und den Schutz der gespeicherten Verkehrsdaten die im Bereich der Telekommunikation erforderliche Sorgfalt zu beachten. Im Rahmen dessen hat er durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich hierzu von ihm besonders ermächtigten Personen möglich ist.

{11} Der nach dieser Vorschrift Verpflichtete hat die allein auf Grund dieser Vorschrift gespeicherten Daten innerhalb eines Monats nach Ablauf der in Absatz 1 genannten Frist zu löschen oder die Löschung sicherzustellen.“ [DJI3]