



Institut suisse de droit comparé
Schweizerisches Institut für Rechtsvergleichung
Istituto svizzero di diritto comparato
Swiss Institute of Comparative Law

**GUTACHTEN ÜBER
STRAFPROZESSUALE GRUNDLAGEN UND KOSTEN DER
ÜBERWACHUNG VON FERNMELDEVERKEHR
IN DÄNEMARK, DEUTSCHLAND, FRANKREICH,
ITALIEN, DEN NIEDERLANDEN,
ÖSTERREICH UND DEM VEREINIGTEN KÖNIGREICH**

Avis 12-051

Lausanne, 24.05.2013

INHALTSVERZEICHNIS

ZUSAMMENFASSUNG	6
1. Strafprozessrechtliche Grundlagen	6
2. Prozess- und Organisationsstrukturen.....	7
3. Kostenersatz.....	8
I. SACHVERHALT	10
II. FRAGESTELLUNG.....	11
III. ÜBERSICHT	12
1. Rechtliche Grundlagen der Fernmeldeüberwachung	12
2. Organisationstrukturen für Überwachung im Rahmen der Strafverfolgung.....	13
3. Kosten/Finanzierungsmodelle	14
3.1. Grundsätze.....	15
3.2. Vergleich der Kosten bei einer aktiven Telefonüberwachung	15
3.3. Vergleich der Kosten bei einer rückwirkenden Telefonüberwachung.....	17
3.4. Vergleich der Kosten für Technisch Administrative Auskünfte resp. Bestandsdaten	19
3.5. Vergleich der Kosten für Auskünfte über IP-Adressen (statisch, dynamisch).....	20
IV. LÄNDERBERICHTE	21
A. DÄNEMARK	21
1. Übersicht über die strafprozessualen Grundlagen	21
2. Übersicht über Prozess- und Organisationsstrukturen	23
2.1. Die Unterstützungspflicht der Telekommunikationsanbieter	23
2.2. Organisation	24
3. Kosten und Finanzflüsse	24
B. DEUTSCHLAND	26
1. Übersicht über die strafprozessualen Grundlagen	26
1.1. Inhaltsdaten.....	26
1.2. Verkehrsdaten	30
1.3. Bestandsdaten	31
1.4. Sonstige Ermächtigungsgrundlagen ausserhalb der dStPO.....	31
2. Übersicht über Prozess- und Organisationsstrukturen	32
2.1. Durchführung strafprozessualer Massnahmen.....	32
2.2. Technische Umsetzung.....	33
3. Kosten und Finanzflüsse	35
3.1. Rechtsgrundlage für Finanzierung	35

3.2.	Entscheidstrukturen über Kostentragung einer Überwachung im Einzelfall	39
3.3.	Kostenverteilung.....	39
3.4.	Finanzierungsmechanismen ausserhalb der einzelnen Verfahren	39
4.	Tarifvergleich Schweiz – Deutschland.....	40
C.	FRANKREICH.....	48
1.	Übersicht über die strafprozessualen Grundlagen der Fernmeldeüberwachung	49
1.1.	Definition.....	49
1.2.	Richterliche Aufhebung des Korrespondenzgeheimnisses.....	49
1.3.	Administrative Aufhebung des Korrespondenzgeheimnisses	51
2.	Übersicht über Prozess- und Organisationsstrukturen	52
2.1.	Strafprozessuale Massnahmen	52
2.2.	Administrative Massnahmen	53
3.	Kosten und Finanzflüsse	54
3.1.	Rechtsgrundlage für Finanzierung	54
3.2.	Entscheidstrukturen über Kostentragung einer Überwachung im Einzelfall	55
3.3.	Kostenverteilung.....	55
3.4.	Finanzierungsmechanismen ausserhalb der einzelnen Verfahren	61
4.	Tarifvergleich Schweiz – Frankreich	62
D.	ITALIEN.....	70
1.	Übersicht über die strafprozessualen Grundlagen der Fernmeldeüberwachung	70
1.1.	Der Begriff der Fernmeldeüberwachung	70
1.2.	Zulässigkeitsvoraussetzungen	71
1.3.	Weitere Fernmeldeüberwachungsmassnahmen: Rufdatenrückfassung.....	72
2.	Übersicht über die Prozess- und Organisationsstrukturen.....	74
2.1.	Fernmeldeüberwachung in Verfahren wegen gewöhnlicher Kriminalität.....	74
2.2.	Verbrechen der organisierten Kriminalität und des Terrorismus.....	78
2.3.	Vorsorgliche Telefonüberwachung.....	79
2.4.	Rufdatenrückfassung	80
3.	Kosten und Finanzflüsse	82
3.1.	Rechtsgrundlage für die Finanzierung	82
3.2.	Entscheidstrukturen für die Kostentragung einer Überwachung im Einzelfall	83
3.3.	Kostenverteilung.....	84
3.4.	Finanzierungsmechanismen ausserhalb der einzelnen Verfahren	84
E.	NIEDERLANDE	86
1.	Übersicht über die strafprozessualen Grundlagen der Fernmeldeüberwachung	86
1.1.	Strafprozessordnung.....	86

1.2.	Allgemeiner Nachrichten- und Sicherheitsdienst der Niederlande	88
2.	Übersicht über Prozess- und Organisationsstrukturen	88
2.1.	Mitwirkungspflicht der Anbieter	88
2.2.	Zentralstelle für Telekommunikationsermittlungen (CIOT)	89
2.3.	Verfahren nach Strafprozessordnung.....	89
2.4.	Verfahren nach dem Gesetz über den Nachrichten- und Sicherheitsdienst	90
3.	Kosten und Finanzflüsse	91
3.1.	Rechtsgrundlage für Finanzierung	91
3.2.	Entscheidstrukturen über Kostentragung einer Überwachung im Einzelfall	91
3.3.	Kostenverteilung.....	93
3.4.	Finanzierungsmechanismen ausserhalb der einzelnen Verfahren	93
4.	Tarifvergleich Schweiz – Niederlande	94
F.	ÖSTERREICH	101
1.	Übersicht über die strafprozessualen Grundlagen der Fernmeldeüberwachung	101
1.1.	Fernmelde- und Kommunikationsgeheimnis.....	101
1.2.	Datenauskunft	102
1.3.	Nachrichtenüberwachung	103
1.4.	Auskunft und Verarbeitung von Stammdaten	104
2.	Übersicht über Prozess- und Organisationsstrukturen	105
2.1.	Prozess- und Organisationsstrukturen	105
2.2.	Mitwirkungspflicht auf Seiten der Anbieter	105
3.	Kosten und Finanzflüsse	107
3.1.	Rechtsgrundlage für Finanzierung	107
3.2.	Entscheidstrukturen über Kostentragung einer Überwachung im Einzelfall	109
3.3.	Kostenverteilung.....	109
3.4.	Finanzierungsmechanismen ausserhalb der einzelnen Verfahren	109
4.	Tarifvergleich Schweiz – Österreich	110
G.	VEREINIGTES KÖNIGREICH (ENGLAND)	118
1.	Übersicht über die strafprozessualen Grundlagen	118
1.1.	Abhörmassnahmen	118
1.2.	Das Erlangen und Übermitteln von Kommunikationsdaten	120
2.	Übersicht über Prozess- und Organisationsstrukturen	121
2.1.	Abhörungsverfahren	121
2.2.	Verfahren zum Erlangen und Mitteilen von Kommunikationsdaten.....	123
3.	Kosten und Finanzflüsse	125
3.1.	Rechtsgrundlage für Finanzierung	125

3.2.	Entscheidstrukturen über Kostentragung einer Überwachung im Einzelfall	126
3.3.	Kostenverteilung.....	127
3.4.	Finanzierungsmechanismen ausserhalb der einzelnen Verfahren	128
V.	SCHLUSSFOLGERUNG	129

ZUSAMMENFASSUNG

Das vorliegende Gutachten stellt für eine anstehende Totalrevision des Schweizer Rechts im Bereich der Post- und Fernmeldeüberwachung die Rechtslage zur Fernmeldeüberwachung anhand eines vorgegebenen Fragenkatalogs in sieben verschiedenen Rechtsordnungen (Dänemark, Deutschland, Frankreich, Italien, Niederlande, Österreich, Vereinigtes Königreich) dar. Die Länderberichte behandeln zunächst die strafprozessualen Grundlagen, stellen in einem zweiten Teil die Prozess- und Organisationsstrukturen und in einem dritten Teil die allfälligen Regelungen für einen Kostenersatz dar. Soweit angesichts der verfügbaren Informationen möglich, schliessen die Länderberichte mit einem direkten Tarifvergleich zwischen der Schweiz und dem jeweils untersuchten Land. Entsprechend dieser Struktur beginnt die folgende Zusammenfassung mit den strafprozessualen Grundlagen, welche insbesondere auf die materiell-rechtlichen Ermächtigungsgrundlagen und die damit verbundenen Voraussetzungen fokussiert (1.). Danach werden die Prozess- und Organisationsstrukturen (2.) und die Regelungen für einen eventuellen Kostenersatz für die Telekommunikationsbetreiber (3.) verglichen, was insbesondere hinsichtlich der Kosten ein Fazit im Vergleich mit der Schweiz (4.) ermöglicht.

1. Strafprozessrechtliche Grundlagen

In allen Rechtsordnungen ist ein Eingriff in das verfassungsrechtlich verankerte **Telekommunikationsgeheimnis** (auch Fernmelde- oder Kommunikationsgeheimnis) nur mit **gesetzlicher Grundlage** zulässig. Hinsichtlich dieser materiell-rechtlichen Ermächtigungsgrundlage kann zwischen (1) Massnahmen im Rahmen des Ermittlungsverfahrens und (2) sonstigen Massnahmen unterschieden werden.

(1) Die Voraussetzungen für Eingriffe im Rahmen des Ermittlungsverfahrens sind jeweils in den nationalen Strafprozessordnungen geregelt. Ein Vergleich der untersuchten Rechtsordnungen zeigt, dass diese für die Zulässigkeit in der Regel u.a. an einen bestimmten **Strafraahmen** anknüpfen, wobei der Schweregrad der aufzuklärenden Straftat divergiert. Während in Frankreich und Österreich die Anordnung einer Überwachungsmassnahme bereits bei Verdacht auf eine mit mind. einem (Österreich) oder zwei Jahren (Frankreich) Freiheitsstrafe bedrohte Straftat zulässig ist, liegt das Mindestmass in den anderen Rechtsordnungen bei drei (Vereinigtes Königreich, wo vom erwarteten Strafmass ausgegangen wird), vier (Niederlande), fünf (Deutschland, Italien) oder sechs (Dänemark) Jahren. Darüber hinaus kommen Überwachungsmassnahmen auch für bestimmte ausdrücklich genannte Delikte in Betracht. Die Unterschiede im Strafraahmen werden dabei teilweise durch eine grosse Zahl von Delikten, welche für Überwachungsmassnahmen berechtigen, ausgeglichen. Im Weiteren wird in der Regel die Verhältnismässigkeit der Massnahme oder gar deren Notwendigkeit (in Frankreich, Vereinigtes Königreich und Italien) sowie deren Relevanz für die Untersuchung vorausgesetzt. Die Durchführung einer **Überwachungsmassnahme** erfordert ausser im Vereinigten Königreich eine schriftliche **Genehmigung** durch das Gericht (**Richtervorbehalt**), wovon in Einzelfällen (Gefahr in Verzug) abgewichen werden kann. In Frankreich ist in der Regel der Untersuchungsrichter zuständig, der als Leiter der Untersuchung keine unabhängige richterliche Funktion innehat. Im Vereinigten Königreich wird die Genehmigung durch eine Verwaltungsbehörde erteilt – bei Gesuchen zur Kenntnisnahme des Inhalts von Kommunikationen der Vorsteher des *Home Office* (*Secretary of State*), bei Gesuchen um Zugang zu Verkehrs-, Bestandes- und Stammdaten eine dafür vorgesehene Person innerhalb der Verwaltungsbehörde. Allerdings – und wohl als Konsequenz dieser Regelung – können nur Verkehrsdaten im Strafprozess als Beweismittel verwendet werden. Überall hat die genehmigende Behörde die Überwachungsmassnahme nach den gesetzlichen Vorgaben zu prüfen, so z.B. auf die **Erfolgsaussichten** und die **Verhältnismässigkeit**.

(2) Die Anordnung von Überwachungsmassnahmen wird in den Rechtsordnungen auch **abseits des strafprozessrechtlichen Ermittlungsverfahrens** geregelt, etwa zur Abwehr von Gefahren, die die nationale Sicherheit betreffen. Die Voraussetzungen für diese meist präventive Nutzung der Telekommunikationsüberwachung werden in den Länderberichten lediglich in groben Zügen skizziert (Dänemark, Deutschland, Frankreich, Österreich, Vereinigtes Königreich), zumal der Fokus auf den strafprozessrechtlichen Rahmen gelegt wurde.

2. Prozess- und Organisationsstrukturen

Am Verfahren zur Durchführung von Überwachungsmassnahmen sind folgende Akteure beteiligt: (1) die Strafverfolgungsbehörden, (2) die Gerichte bzw. im Vereinigten Königreich die genehmigende Behörde / Person und (3) die Telekommunikationsbetreiber (mitunter in Zusammenarbeit mit bestimmten zentralen staatlichen Stellen).

(1) Abhängig von der Ausgestaltung des Strafrechtssystems in den jeweiligen Staaten hat die genannte gerichtliche Genehmigung aufgrund eines **Antrags** durch den **Staatsanwalt** zu erfolgen, der die polizeilichen Ermittlungen anordnet und leitet (Deutschland, Niederlande, Italien, Österreich). In Dänemark sind Staatsanwaltschaft und Polizeiorganisation sehr eng verknüpft. Einzig in Frankreich wird das Ermittlungsverfahren von einem Untersuchungsrichter geführt, der auch über die Überwachungsmassnahme entscheidet. Im Vereinigten Königreich können Massnahmen direkt durch die jeweilige Untersuchungsbehörde (wie z.B. Polizei, *Serious Organised Crime Agency*) beantragt werden – die Ermittlungs- und Anklagephase scheinen stärker getrennt als in anderen Rechtsordnungen.

(2) Wie bereits erwähnt, ist in allen Rechtsordnungen mit Ausnahme des Vereinigten Königreichs die genehmigende Behörde eine richterliche Behörde. Unterschiede bestehen jedoch hinsichtlich der **Gültigkeitsdauer der Genehmigung**: In Deutschland und im Vereinigten Königreich (für das Abhören) ist die Genehmigung für drei Monate gültig, in Frankreich für vier Monate. Im Gegensatz dazu sehen die Niederlande (ein Monat), Dänemark (maximal 4 Wochen) und Italien (15 Tage) eine kürzere Dauer vor. In Österreich wird dem Gericht hinsichtlich der **Dauer** der Anordnung – unter Anwendung des Verhältnismässigkeitsgrundsatzes – keine gesetzliche Vorgabe gemacht. Die Bewilligung ist in allen Rechtsordnungen verlängerbar.

(3) Zur Beteiligung der Telekommunikationsbetreiber ist zu bemerken, dass diese in allen Rechtsordnungen zur Mitwirkung an den Überwachungsmassnahmen verpflichtet sind, jedoch in unterschiedlicher Konkretisierung. Die einheitliche Regelung in diesem Bereich geht auch auf die europarechtlichen Vorgaben in Form der Richtlinien 2002/58/EG sowie 2006/24/EG zurück. Der **allgemeinen Mitwirkungspflicht** ist zu entnehmen, dass die Betreiber dazu angehalten sind, die technischen Einrichtungen bereitzuhalten um den Überwachungsanordnungen unverzüglich Folge zu leisten. Es fällt auf, dass Österreich und Deutschland vergleichsweise **detaillierte Regelungen** für die Auskunftspflicht je nach Art der Daten treffen. In diesen beiden Rechtsordnungen sind die Betreiber etwa unter bestimmten Voraussetzungen zur unverzüglichen und kostenfreien Ausgabe von Stamm- oder Bestandsdaten verpflichtet.

In organisatorischer Hinsicht bestehen einerseits Vorgaben an die Telekommunikationsbetreiber. So muss in Dänemark und Deutschland jeder Telekommunikationsbetreiber eine Kontaktstelle für die Strafverfolgungsbehörden bezeichnen. Andererseits wurden in einer Reihe von Rechtsordnungen **zentrale staatliche Stellen** eingerichtet, die entweder die Erarbeitung einheitlicher technischer Vorgaben (Deutschland) und die sichere Datenübermittlung gewährleisten sollen (Österreich), direkt zur Datenausgabe herangezogen werden (Niederlande), als Informationsstelle zur vereinfachten Kontaktaufnahme mit den Telekommunikationsbetreibern fungieren (Deutschland), oder eine überwa-

chende Funktion haben (so der *Interception of Communications Commissioner* im Vereinigten Königreich).

3. Kostenersatz

Betrachtet man den Umfang des Kostenersatzes in den verschiedenen Rechtsordnungen, lässt sich feststellen, dass zwischen folgenden Kosten differenziert werden kann: (1) Investitionen, die von den Telekommunikationsbetreibern getätigt wurden, um die technischen Voraussetzungen für die Durchführung der Überwachungsmaßnahmen zu erfüllen (hier **Vorhaltekosten**), (2) den Wartungs- und **Instandhaltungskosten** sowie (3) den für die einzelnen Überwachungsmaßnahmen anfallenden Kosten (hier **Überwachungskosten** im engeren Sinn).

(1) Nur nach österreichischem, französischem, englischem sowie möglicherweise nach italienischem Recht ergibt sich ein **teilweiser Ersatz für die Vorhaltekosten**, die jeweils Gegenstand eines staatlichen Prüfungsverfahrens sind.

(2) Das Prüfungsverfahren umfasst in Frankreich, im Vereinigten Königreich und anscheinend auch in Italien die **Instandhaltungskosten**, wobei im Vereinigten Königreich der Ersatz dieser Kosten zwischen den Anbietern und der Verwaltung vereinbart wird. In Dänemark, Deutschland und den Niederlanden sind sowohl die Vorhalte – als auch die Instandhaltungskosten von den Telekommunikationsbetreibern selbst zu tragen (siehe für die Niederlande aber unten (3)).

(3) Für tatsächlich durchgeführte Überwachungsmaßnahmen gebührt den Betreibern nach allen diesem Gutachten zu Grunde liegenden Rechtsordnungen Kostenersatz. Dieser errechnet sich in Deutschland, Frankreich und Österreich sowie in den Niederlanden nach **pauschalierten gesetzlich festgelegten Tarifen** nach Rechnungslegung durch die Telekommunikationsbetreiber (siehe dazu die Vergleichstabellen in den Länderberichten). Im Vereinigten Königreich wird grundsätzlich anders vorgegangen, indem die Vergütungen mit den grösseren Anbietern jährlich neu verhandelt werden. Eine ähnliche Besonderheit ergibt sich für die Niederlande, wo neben der gesetzlichen Pauschalvergütung eine befristete **Vergleichsvereinbarung** (*settlement agreement*) mit den fünf grössten Telekommunikationsunternehmen geschlossen wurde, um die Inanspruchnahme der Dienste pauschal zu vergüten. Auch in Dänemark werden nach unseren Abklärungen die Tarife von der Polizei **mit jedem Anbieter separat verhandelt**. Die verhandelten Tarife werden dabei vertraulich behandelt; in Dänemark gelten die Angaben als Geschäftsgeheimnis, im Vereinigten Königreich werden Gründe des Wettbewerbs zwischen den Anbietern und der Wunsch nach bestmöglicher Kooperation mit den Behörden für die Vertraulichkeit angeführt, in den Niederlanden sind es Sicherheitsgründe. In Dänemark und für gewisse Massnahmen im Vereinigten Königreich würde eine Rechtsgrundlage für eine Verordnung bestehen, doch wurde diese Kompetenz nicht ausgeschöpft.

In **Italien** lässt sich keine exakte Aussage über den Kostenersatz treffen. Laut Auskunft des Ministeriums umfasst dieser nach pauschalierten Tarifen alle den Telekommunikationsunternehmen anfallenden Kosten (Vorhaltekosten, Instandhaltungskosten sowie Überwachungskosten im engeren Sinne). Die Tarife sind allerdings nicht einsehbar.

4. Vergleich des Kostenersatzes mit der Schweiz

Die grundsätzlich unterschiedliche Handhabung des Kostenersatzes im Strafverfahren im Allgemeinen und gegenüber den Telekommunikationsanbietern im Besonderen, strukturelle Unterschiede und insbesondere die fehlende Verfügbarkeit von Informationen in verschiedenen Rechtsordnungen

verunmöglichen eine abschliessende Beurteilung der Kostenersatzregelung der Schweiz im internationalen Vergleich. Trotz dieser Schwierigkeiten drängen sich einige grundsätzliche Bemerkungen auf.

Zunächst fällt auf, dass nur in der Schweiz eine **Vergütung der von staatlichen Stellen geleisteten Dienstleistungen** im Zusammenhang mit der Überwachung gesetzlich vorgesehen und in Verordnungen reguliert ist. In den anderen Rechtsordnungen finden sich keine ausdrücklichen Regelungen über die Vergütung von staatlichen Dienstleistungen; lediglich die Vergütungen an die Telekommunikationsunternehmen sind teilweise gesetzlich festgelegt.

Bei der Kostentragung entspricht die schweizerische Regelung derjenigen in verschiedenen Staaten (Deutschland, Österreich, Italien, in der Regel in den Niederlanden), welche eine **nachträgliche individualisierte Rückerstattung durch die anordnende Behörde** für jede einzelne Massnahme vorsieht. In Frankreich erfolgt ebenfalls eine individualisierte Rückerstattung für jede Massnahme, wobei hier das Justizministerium die Kosten trägt. Im Vereinigten Königreich werden die Kosten aufgrund einer auf Erfahrungswerten basierenden Schätzung vom Innenministerium getragen, diese verrechnen die Beträge jedoch den anordnenden Behörden weiter. Die Grundsätze und Grundlagen dieser Rechnungsstellung sind allerdings nicht ersichtlich. Auch in Dänemark finden sich keine eindeutigen Angaben zur Rechnungsstellung, doch deuten verschiedene Elemente auf eine pauschalisierte Abrechnung hin.

Schliesslich ist zu den für die einzelnen Massnahmen anfallenden Kosten zu bemerken, dass die in der Schweiz vorgesehenen Kosten (und damit auch der Ersatz) betragsmässig im Vergleich jeweils **eher hoch** scheinen. Die Unterschiede sind bei Bestandsdaten und Auskünften über dynamische IP Adressen besonders ausgeprägt. Das Kostenniveau lässt sich immerhin mit demjenigen in Österreich vergleichen. Ein Grund für das relativ hohe Niveau könnte darin liegen, dass das Schweizer Recht für Vorhalte – und Instandhaltungskosten keinen spezifischen Ersatz vorsieht (Art. 16 Abs. 1 BÜPF), während diese Kosten in anderen Rechtsordnungen (wenn auch nicht in Deutschland) zusätzlich vergütet werden. Wie eingangs erwähnt wurde, ist gerade diesbezüglich jedoch angesichts der unterschiedlichen Tarifstrukturen und der Vertraulichkeit der Information in drei der untersuchten Rechtsordnungen keine abschliessende Beurteilung möglich.

I. SACHVERHALT

Der Dienst Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) ist eine Bundesbehörde und zuständig für die Durchführung von Überwachungsmassnahmen im Post- und Fernmeldebereich, die von Strafverfolgungsbehörden des Bundes und der Kantone im Rahmen von Strafuntersuchungen, Rechtshilfeverfahren oder der Suche und Rettung vermisster Personen angeordnet werden. Die Tätigkeiten des Dienstes ÜPF sind primär in folgenden Rechtsgrundlagen geregelt:

- im Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF; SR 780.1);
- in der Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF; SR 780.11);
- in der Verordnung vom 7. April 2004 über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (GebV-ÜPF; SR 780.115.1).

Für die Anordnung und Genehmigung von Überwachungsmassnahmen ist zudem die Schweizerische Strafprozessordnung vom 5. Oktober 2007 (StPO; SR 312.0) massgebend (siehe Art. 269 bis 279).

Die VÜPF und die GebV-ÜPF wurden einer Teilrevision unterzogen und die entsprechenden Änderungen sind am 1. Januar 2012 in Kraft getreten. Bei der Teilrevision der VÜPF ging es darum, bisher nicht ausdrücklich geregelte Überwachungstypen, die aber in der Rechtsprechung anerkannt und in der Praxis seit längerem unter dem Titel „Spezialmassnahmen“ durchgeführt wurden, aufzunehmen. Folglich musste auch die GebV-ÜPF mit entsprechenden Gebühren- und Entschädigungsposten nachgeführt werden, wobei man sich an der bisherigen Kostenstruktur orientierte. Für das BÜPF läuft derzeit ein Gesetzgebungsverfahren für dessen Totalrevision. In diesem Zusammenhang werden erneut Änderungen der VÜPF und der GebV-ÜPF erforderlich sein.

Aufgrund der laufenden bzw. anstehenden Rechtsetzungsarbeiten wurde der Dienst ÜPF vom Generalsekretariat EJPD beauftragt, durch Dritte eine Analyse der effektiven Kosten der Post- und Fernmeldeüberwachung sowie einen internationalen Rechtsvergleich im Bereich der Fernmeldeüberwachung (FMÜ) durchführen zu lassen. Beim Rechtsvergleich soll es vor allem um die Kosten der Fernmeldeüberwachung gehen und um die Frage, wie diese auf die Akteure verteilt werden.

II. FRAGESTELLUNG

Mit Blick auf den vorgehend dargelegten Sachverhalt bittet das Informatik Service Center ISC-EJPD um die Erstellung eines rechtsvergleichenden Gutachtens zu den Rechtsordnungen Dänemarks, Deutschlands, Frankreichs, Italiens, der Niederlande, Österreichs und dem Vereinigten Königreich zu folgenden Fragen:

1. Übersicht über die strafprozessualen Grundlagen der Fernmeldeüberwachung in den Ländern
2. Übersicht über deren Prozess- und Organisationsstrukturen im Bereich der Fernmeldeüberwachung
3. Rechtsgrundlage für Finanzierung
 - 3.1. Entscheidungsstrukturen über Kostentragung einer Überwachung im Einzelfall
 - 3.2. Kostenverteilung
 - 3.3. Finanzierungsmechanismen ausserhalb der einzelnen Verfahren
4. Tarifvergleich Schweiz – untersuchtes Land

III. ÜBERSICHT

1. Rechtliche Grundlagen der Fernmeldeüberwachung

Land	Rechtsquelle
Dänemark	Retsplejeloven 1008/2012 (Prozessgesetz), Lov 169/2011 om elektroniske kommunikationsnet og -tjenester (Gesetz 169/2011 über elektronische Kommunikationsnetze und -dienste)
Deutschland	Strafprozessordnung (dStPO), Telekommunikationsgesetz (TKG), Telekommunikations-Überwachungsverordnung (TKÜV), teilweise auch Polizeigesetze der Länder
Frankreich	Code de procédure pénale (CPP), Code des postes et des communications électroniques (CPCE), Décret 2006-358
Italien	Codice di procedura penale; D.L. 13.5.1991, n. 152, conv. in L. 12.3.1991, n. 203; D.Lgs. 1.8.2003, n. 259, Codice delle comunicazioni elettroniche, D.L. 18.10.2001, n. 374, conv. in L. 15.12.2001, n. 438; D.M. 26 aprile 2001 (<i>Listino prestazioni organismi di telecomunicazioni</i>); D.P.R. 30.5.2002, n. 115
Niederlande	Criminal Procedure Act, Telecommunications Act, Intelligence and Security Services Act
Österreich	Strafprozessordnung (öStPO), Telekommunikationsgesetz (öTKG), Sicherheitspolizeigesetz (SPG)
Vereinigtes Königreich	Police Act 1997, Intelligence Services Act 1994, Regulation of Investigatory Powers Act 2000 (RIPA)

2. Organisationstrukturen für Überwachung im Rahmen der Strafverfolgung

<i>Land</i>	<i>Genehmigende Behörde</i>	<i>Durchführende Behörde(n)</i>	<i>Aufsichtsorgan</i>	<i>Andere Bemerkungen</i>
Dänemark	Gerichte	Polizei, Technische Unterstützungseinheit des PET (<i>Danish Security and Intelligence Service</i>)	Keine spezifische Aufsicht	Telekom-Unternehmen müssen Kontaktstelle einrichten
Deutschland	Gerichte	Staatsanwaltschaft; Polizei für präventive Überwachungsmaßnahmen im Rahmen der Gefahrenabwehr	--	Bundesnetzagentur, Kontaktstelle Telekom-Unternehmen
Frankreich	<i>Juge d'instruction</i> (Untersuchungsrichter)	<i>Police judiciaire</i>	Keine Rechtsmittel	Pflicht der Beamten des für Telekommunikation zuständigen Ministeriums sowie der Telekom-Unternehmen zur Zusammenarbeit
Italien	Gerichte	<i>Procura della Repubblica</i> (Staatsanwaltschaft)	Gerichte	
Niederlande	Untersuchungsrichter, Staatsanwaltschaft	Staatsanwaltschaft Zentralstelle für Telekommunikationsermittlungen (CIOT)	Justizministerium	Zentrale Auskunftsstelle (CIOT) und Datenbank
Österreich	Gerichte	Kriminalpolizei	Staatsanwaltschaft	Pflicht der Telekom-Unternehmen zur Zusammenarbeit
Vereinigtes Königreich	Inhaltsdaten: <i>Secretary of State</i> Verkehrs-, Bestandes- und Stammdaten: Person innerhalb der Behörde	Polizei	<i>Interception of Communications Commissioner</i>	Inhaltsdaten können grundsätzlich nicht als Beweismittel im Strafprozess verwendet werden.

3. Kosten/Finanzierungsmodelle

Einleitende Vorbemerkung des Dienstes ÜPF zur Vergleichbarkeit der Gebühren- und Kostenstruktur

Aufgrund der stark divergierenden Kosten- und Gebührenstruktur im direkten Vergleich der Schweiz mit dem europäischen Ausland, rechtfertigt sich ein Blick auf die **unterschiedliche organisatorische Ausgestaltung und die Aufgaben** im Bereich der Überwachungsdienstleistungserbringung, die der Dienst Überwachung Post- und Fernmeldeverkehr ÜPF schweizweit erbringen muss.

Die Zentralisierung dieser Dienstleistungen in einer Verwaltungseinheit des Bundes bietet für die Strafverfolgungsbehörden der Schweiz folgende **Vorteile** gegenüber dezentral erbrachten Dienstleistungen:

- Know-How im Bereich Lawful-Interception (technischer, prozessgestützter und rechtlicher Art) steht zentral allen Strafverfolgungsbehörden im gleichen Masse zur Verfügung;
- Die Kantone müssen keine eigenen Systeme zur Fernmeldeüberwachung evaluieren, finanzieren und deren weitgehend unterbruchsfreien Betrieb garantieren;
- Die Kantone müssen keine Speichersysteme betreiben und deren weitgehend unterbruchsfreien Betrieb garantieren;
- Überwachungsdienstleistungen werden von erfahrenem, geschultem und qualifiziertem Personal in konstanter Qualität unter Berücksichtigung eines modernen Controllings erbracht.

Die Strafverfolgungsbehörden auch bevölkerungsärmerer Kantone werden durch die zentrale Dienstleistungserbringung des Bundes kostengünstig in die Lage versetzt, rasch und effizient auch im Bereich des Internets zur Aufklärung und Bekämpfung von Kapitalverbrechen Überwachungsmassnahmen durchzuführen.

Die Post- und Fernmeldedienstleister, als Erfüllungsgehilfen für diese Art staatlicher geheimer Zwangsmassnahmen, profitieren im gleichen Masse durch die zentrale Dienstleistungserbringung. Ihnen steht ein einziger Partner zur Verfügung mit einem eingespielten Team von Spezialistinnen und Spezialisten und eine einheitliche Infrastruktur. Die Zentralisierung bietet weiter den Vorteil klarer und einheitlicher Prozessabläufe mit überschaubaren technischen und administrativen Vorgaben zur Erfüllung der gesetzlich verankerten Pflichten von Seiten der Post- und Fernmeldedienstleister.

Die Zentralisierung der Überwachungsdienstleistungen führt weiter dazu, dass die Kosten im Bereich der gerichtspolizeilichen Post- und Fernmeldeüberwachung klar und transparent darstellbar und einsehbar sind. Der Anteil versteckter Kosten im Bereich der Post- und Fernmeldeüberwachung dürfte daher in der Schweiz niedriger sein, als im europäischen Ausland.

3.1. Grundsätze

<i>Rechtsordnung</i>	<i>Kosten für das Schaffen der technischen Voraussetzungen</i>	<i>Instandhaltungskosten</i>	<i>Überwachungskosten</i>
Dänemark	Telekom-Unternehmen	Telekom-Unternehmen	Kostenersatz (gemäss mit jedem Unternehmen verhandelten Tarifen); allg. Tarif vorgesehen, aber (noch) nicht verabschiedet
Deutschland	Telekom-Unternehmen	Telekom-Unternehmen	Kostenersatz gemäss Tarif
Frankreich	Teilweise Staat (gemäss Vereinbarung)	Teilweise Staat (gemäss Vereinbarung)	Kostenersatz in der Regel gemäss Tarif
Italien	Teilweise Staat	unklar	Kostenersatz in der Regel gemäss Tarif
Niederlande	Telekom-Unternehmen	Telekom-Unternehmen	Kostenersatz (besondere Vereinbarung)
Österreich	Teilweise Staat	Telekom-Unternehmen	Kostenersatz 80%
Vereinigtes Königreich	Teilweise Staat (gemäss Vereinbarung)	Staat (mindestens teilweise, gemäss Vereinbarung)	Kostenersatz gemäss mit jedem Unternehmen verhandelten Tarifen

3.2. Vergleich der Kosten bei einer aktiven Telefonüberwachung

Da in der Schweiz eine Überwachungsmassnahme im Schnitt 77 Tage dauert, wurde der internationale Kostenvergleich auf dieser Basis durchgeführt.

Aufgrund der auf unterschiedlichen Voraussetzungen erbrachten Dienstleistungen (siehe dazu die detaillierten Tabellen über die erbrachte Dienstleistung pro Gebührentarif bei den jeweiligen Länderberichten) ist der internationale Kostenvergleich bei einer aktiven Telefonüberwachung **nur bedingt aussagekräftig**.

	CH	A	D	NL ¹	F ²
Telefon-anschluss	Sfr. 2410,00 ³	EUR 2053: EUR 128,00 (Einrichtung der Überwachung) EUR 1925,00 (Auswertung der Daten für 77 Tage)	EUR 325,00	EUR 41,55	Übertragung (tech. Installation): EUR 256,50 (120,00 + 45,50 pro Monat) ⁴ Dazu wohl EUR 350 (Weiterleitungssonde) ⁵ Verbindungsübersicht EUR 24 ⁶
ISDN-Anschluss	Sfr. 2410,00		EUR 475,00	EUR 41,55	EUR 354,00 (217,50 + 45,50 pro Monat) ⁷ zusätzlich wohl EUR 350
Primär-multiplex	Pro Nummer Sfr. 2410,00		EUR 4675,00	EUR 41,55	Keine separate Kategorie
CH-Provider-VoIP	Sfr. 2410,00		EUR 700,00	EUR 41,55	EUR 24 (Überwachung IP Telefonie) ⁸ ; keine Angaben zur Internetzugangüberwachung

¹ An Wochenenden beträgt die Gebühr 50% mehr, an nationalen Feiertagen 100% mehr. Der Nachweis höherer Personalkosten ist jeweils vorbehalten.

² Kosten für die technischen Voraussetzungen und Instandhaltung werden gemäss einer Vereinbarung mit dem jeweiligen Unternehmen ebenfalls vom Staat getragen.

³ Diese Gebühr umfasst die Entschädigung an die Fernmeldedienstanbieterinnen in Höhe von Sfr. 1330,00 und die Entschädigung an den Dienst ÜPF in Höhe von Sfr. 1080,00 gemäss Art. 2 (A. Leitungsvermittelte Fernmeldedienste) der Verordnung vom 7. April 2004 über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (GebV-ÜPF, SR 780.115.1) für die erbrachten zentralen Überwachungsdienstleistungen (Betrieb zentrales Überwachungssystem, Beratung der Strafverfolgungsbehörden, Datenausleitung und Support) für die Strafverfolgungsbehörden in der Schweiz.

⁴ Art. A43-9 Code de procédure pénale (CPP): FI10; diese Gebühr (ohne Steuern) umfasst die Einrichtung einer temporären (analogen) Abhörleitung (ligne de renvoi) sowie die monatliche Abonnementsgebühr. 77 Tage wurden auf drei Monate umgerechnet.

⁵ Art. A43-9 CPP: FI17 für die Installation und Aufhebung der Abhörvorrichtung (*sonde de renvoi*).

⁶ Art. A43-9 CPP: FI 20, 21, 22; der Tarif umfasst das Erteilen der detaillierten Information über die Kommunikationen (*d'un détail de communications*) am Ende der Überwachungsperiode. Es stehen keine Informationen zur Verfügung, ob die Leistung und der Tarif notwendig und kumulativ mit den übrigen Überwachungsmassnahmen kombiniert werden.

⁷ Art. A43-9 CPP: FI11 ; diese Gebühr umfasst die Einrichtung einer temporären (digitalen) Abhörleitung sowie die monatliche Abonnementsgebühr.

⁸ Art. A43-9 CPP: FI23; diese Gebühr für die „Interception des communications de téléphonie de voix sur IP“ umfasst das Erteilen der detaillierten Informationen (*détail de trafic*) während der Überwachungsperiode.

3.3. Vergleich der Kosten bei einer rückwirkenden Telefonüberwachung

Da in der Schweiz eine Überwachungsmassnahme im Schnitt 77 Tage dauert, wurde der internationale Kostenvergleich auf dieser Basis durchgeführt.

Aufgrund der auf unterschiedlichen Voraussetzungen erbrachten Dienstleistungen (siehe dazu die detaillierten Tabellen über die erbrachte Dienstleistung pro Gebührentarif in den Länderberichten) ist der internationale Kostenvergleich bei einer rückwirkenden Telefonüberwachung **nur bedingt aussagekräftig**.

	CH	A	D	NL ⁹	F ¹⁰
Historische Verkehrsdaten	Sfr. 700,00 ¹¹	EUR 64,00 (Einrichtung) + EUR 500,50 (Auswertung pro Tag) (§ 8 ÜKVO)	Auskünfte über gespeicherte Verkehrsdaten für jede Kennung, die der Auskunftserteilung zugrunde liegt: EUR 30,00 ¹²	EUR 7,52	EUR 50,40 (je 15,30 für die unteilbare Dauer von 31 Tagen + 1,50 EUR pro Monat) ^{13, 14}

⁹ An Wochenenden beträgt die Gebühr 50% mehr, an nationalen Feiertagen 100% mehr. Der Nachweis höherer Personalkosten ist jeweils vorbehalten.

¹⁰ Kosten für die technischen Voraussetzungen und Instandhaltung werden gemäss einer Vereinbarung mit dem jeweiligen Unternehmen ebenfalls vom Staat getragen.

¹¹ Diese Gebühr umfasst die Entschädigung an die Fernmeldedienstanbieterinnen in Höhe von Sfr. 540.00 und die Entschädigung an den Dienst ÜPF in Höhe von Sfr. 160.00 gemäss Art. 2 GebV-ÜPF (A. Leitungsvermittelte Fernmeldedienste) für die erbrachten zentralen Überwachungsdienstleistungen (Betrieb zentrales Überwachungssystem, Beratung der Strafverfolgungsbehörden, Datenausleitung und Support) für die Strafverfolgungsbehörden in der Schweiz.

¹² Für ausführliche Angaben siehe Kostenvergleich im Länderbericht Deutschland.

¹³ Art. A43-9 CPP: MT20, MT21, MT22, MT24 bzw. FT 10. Diese Gebühr für die Leistung der Telekom-Anbieter umfasst die Angaben über eingehende und ausgehende Verbindungen in einem Zeitraum von 31 Tagen, ohne Identifikation der Nummern, aber bei der Mobiltelefonie inkl. Lokalisierung der Zellen (4,59 EUR pro Identifikation; MA 02, MA 04, MA 06, MA 08).

¹⁴ Für eine Verbindungsübersicht (ohne Lokalisierung) bei der Mobiltelefonie lediglich 33.57 EUR (je 9.69 für die unteilbare Dauer von 31 Tagen) +1.50 EUR pro Monat: Art. A43-9 CPP: MT10, MT11, MT12, MT13, MT14 Identifikation des Kunden in der Kosten nicht enthalten (4,59 EUR pro Identifikation; MA 02, MA 04, MA 06, MA 08).

	CH	A	D	NL	F
Antennensuchlauf (Zellanalyse)	Sfr. 600,00 ¹⁵	EUR 64,00 (Einrichtung) + EUR 500,50 (Auswertung) (§ 7 ÜKVO)	Standortabfrage: 1 Standort: EUR 60; Fläche: abhängig von der Distanz: EUR 190 (bis 10 km) / EUR 930 (25 – 44 km) / EUR 110 pro 10 km Zellanalyse: EUR 30 plus EUR 4 für jede weitere Zelle	EUR 30,12 (Zellanalyse)	Netzanalyse nicht vorgesehen; EUR 12,75 für Standortdaten (Zellanalyse) während 4 Stunden innerhalb der letzten 12 Monate ¹⁶ (maximale Rate nicht ersichtlich)

Die Pauschalentschädigungen sind nur bedingt vergleichbar. Es ergeben sich beispielsweise bei der Zellanalyse Differenzen aus der Tatsache, dass der deutsche Erlass die Entschädigung auch von der Flächenabdeckung und der Anzahl der überwachten Zellen abhängig macht. Die Schweizerische Gebührenverordnung legt die Entschädigung von Sfr. 600.00 pro analysierter Zelle fest, unabhängig von der möglichen Flächenabdeckung der zu analysierenden Zellen.

¹⁵ Die Gebühr für den vorgängigen Antennensuchlauf selbst, umfasst die Entschädigung an die Fernmeldedienstanbieterinnen in Höhe von Sfr. 2000.00 und die Entschädigung an den Dienst ÜPF in Höhe von Sfr. 200.00 gemäss Art. 2 GebV-ÜPF (A. Leitungsvermittelte Fernmeldedienste) für die erbrachten zentralen Überwachungsdienstleistungen (Betrieb zentrales Überwachungssystem, Beratung der Strafverfolgungsbehörden, Datenausleitung und Support) für die Strafverfolgungsbehörden in der Schweiz.

¹⁶ Art. A43-9 CPP: MT 40, Identifikation der Nummern + 0.980 EUR pro identifiziertem Abonnent.

3.4. Vergleich der Kosten für Technisch Administrative Auskünfte und Bestandsdaten

Aufgrund der auf unterschiedlichen Voraussetzungen erbrachten Dienstleistungen (siehe dazu auch die detaillierten Tabellen über die erbrachte Dienstleistung pro Gebührentarif in den Länderberichten) ist der internationale Kostenvergleich für technisch administrative Auskünfte und Bestandsdaten **nur bedingt aussagekräftig**.

	CH	A	D	NL ¹⁷	F ¹⁸
Allgemein	Sfr. 360,00 ¹⁹ / Auskunft (Technisch Administrative Auskünfte A1-A4)	EUR 40 für Stamm- und Zugangsdaten nach § 92 Abs. 3 Ziff. 3 und 4a	EUR 18,00 ²⁰ (Bestandsdaten nach §3 Nr. 3 TKG je angefragter Kundensatz)	EUR 7,52 pro Anfrage ²¹	EUR 3,81 pro Anfrage + EUR 0,08 pro Seite ²²
Sonderkategorien		EUR 32 Bekanntgabe Puk-Code	EUR 35,00 (Bestandsdaten nach §3 Nr. 3 TKG bis 10 Kundensätze)		EUR 4,59 PUK Code falls das Handy blockiert ist ²³ . Für die verschiedenen anderen Sonderkategorien, s. Länderbericht

¹⁷ An Wochenenden beträgt die Gebühr 50% mehr, an nationalen Feiertagen 100% mehr. Der Nachweis höherer Personalkosten ist jeweils vorbehalten.

¹⁸ Kosten für die technischen Voraussetzungen und Instandhaltung werden gemäss einer Vereinbarung mit dem jeweiligen Unternehmen ebenfalls vom Staat getragen.

¹⁹ Diese Gebühr umfasst die Entschädigung an die Fernmeldedienstanbieterinnen in Höhe von Sfr. 250,00 und die Entschädigung an den Dienst ÜPF in Höhe von Sfr. 110,00 gemäss Art. 2 GebV-ÜPF (A. Leitungsvermittelte Fernmeldedienste) für die erbrachten zentralen Überwachungsdienstleistungen (Betrieb zentrales Überwachungssystem, Beratung der Strafverfolgungsbehörden, Datenausleitung und Support) für die Strafverfolgungsbehörden in der Schweiz.

²⁰ Falls die Auskunft nicht über ein automatisiertes Auskunftsverfahren erteilt werden kann und die Unmöglichkeit der Auskunftserteilung nicht vom Unternehmen zu vertreten ist oder für die Erteilung der Auskunft nicht auf die Verkehrsdaten zurückgegriffen werden muss.

²¹ Diese Gebühr umfasst die gesamte Bearbeitung (Entgegennahme der Anfrage, Vorprüfung, Erteilen der Information, Fakturierung).

²² Gebühr nach Art. R213 CPP. Nach Art. A43-9 CPP – MD10, MD11, MD12, FD10, FD11, FD12, umfasst die Gebühr all die folgende Dokumente als Kopien: den Vertrag, die Fakturierung, die Anhänge des Vertrags.

²³ Art. A43-9 CPP: MA70, MA71.

3.5 Vergleich der Kosten für Auskünfte über IP-Adressen (statisch, dynamisch)

Aufgrund der auf unterschiedlichen Voraussetzungen erbrachten Dienstleistungen (siehe dazu die detaillierten Tabellen über die erbrachte Dienstleistung pro Gebührentarif in den Länderberichten) ist der internationale Kostenvergleich für Auskünfte über IP-Adressen (statisch, dynamisch) nur **bedingt aussagekräftig**.

	CH	A	D	NL	F ²⁴
Statische IP-Adresse	Sfr. 10,00 ²⁵ (A 0.1)		EUR 35,00 ²⁶ Bestandsdaten nach § 3 Nr. 3 TKG bis 10 IP-Adressen	EUR 7,52	EUR 6,12 ²⁷ (Identifizierung eines ADSL- Abonnenten)
Dynamische IP-Adresse	Sfr. 250,00 ²⁸ (A 0.2)		EUR 35,00	EUR 7,52	Keine Sonderkategorie

²⁴ Kosten für die technischen Voraussetzungen und Instandhaltung werden gemäss einer Vereinbarung mit dem jeweiligen Unternehmen ebenfalls vom Staat getragen.

²⁵ Diese Gebühr umfasst die Entschädigung an die Fernmeldedienstanbieterinnen in Höhe von Sfr. 10,00. Es erfolgt keine Entschädigung an den Dienst ÜPF gemäss Art. 2 GebV-ÜPF (B. Paketvermittelte Fernmeldedienste) für die erbrachten zentralen Überwachungsdienstleistungen (Betrieb zentrales Überwachungssystem, Beratung der Strafverfolgungsbehörden, Datenausleitung und Support) für die Strafverfolgungsbehörden in der Schweiz.

²⁶ Für die Erteilung der Auskunft muss auf die Verkehrsdaten zurückgegriffen werden. Gemäss Anlage 3 zu § 23 Abs. 1 JVEG umfasst der Begriff "Kennung" auch eine IP-Adresse.

²⁷ Art. A43-9 CPP: FA51 unterscheidet nicht zwischen „statischen“ und „dynamischen“ IP-Adressen.

²⁸ Diese Gebühr umfasst die Entschädigung an die Fernmeldedienstanbieterinnen in Höhe von Sfr. 250.00. Es erfolgt keine Entschädigung an den Dienst ÜPF gemäss Art. 2 GebV-ÜPF (B. Paketvermittelte Fernmeldedienste) für die erbrachten zentralen Überwachungsdienstleistungen (Betrieb zentrales Überwachungssystem, Beratung der Strafverfolgungsbehörden, Datenausleitung und Support) für die Strafverfolgungsbehörden in der Schweiz.

IV. LÄNDERBERICHTE

A. DÄNEMARK

1. Übersicht über die strafprozessualen Grundlagen

Die wichtigste **Rechtsquelle** für die Fernmeldeüberwachung ist das Gerichtsorganisations- und Prozessgesetz (*Retsplejeloven*; Administration of Justice Act; im Folgenden RPL)²⁹, welches innerhalb von Buch 4 (Strafprozess) unter dem zweiten Abschnitt (Zwangsmassnahmen) mit dem Kapitel 71 die Arten von und die Voraussetzungen für Eingriffe in das Kommunikationsgeheimnis (*meddelelseshemmeligheden*) regelt. Post- und Telekommunikationsgeheimnis sind auf Verfassungsebene zusammen mit dem Eigentum durch Art. 72 der dänischen Verfassung³⁰ geschützt, Einschränkungen sind nur mit gesetzlicher Grundlage und / oder mit gerichtlicher Ermächtigung möglich. Daneben sind das Gesetz zur Kameraüberwachung (durch private Organisationen)³¹, das Datenschutzgesetz³² und das Strafgesetz³³ von Bedeutung. Insbesondere ist zu erwähnen, dass Eingriffe in „geschlossene“ Kommunikationen³⁴ sowie das Abhören³⁵ und Verschaffen von Zugang zu digitalen Daten³⁶ strafrechtlich verboten sind.

Die Fernmeldeüberwachung wurde insbesondere im Rahmen der sogenannten Anti-Terrorismus-Gesetzgebung in den Jahren 2002, 2004 und 2007³⁷ erheblich erweitert. § 780 RPL zählt die verschiedenen gesetzlich vorgesehenen **Arten von Eingriffen und Überwachungsmassnahmen** auf. Die Aufzählung nennt das Abhören von Telefongesprächen (und von anderer entsprechender Telekommunikation), das Abhören von anderen Gesprächen und Äusserungen mit einer technischen Vorrichtung, die einfache und die erweiterte Überwachung von Telefonen und anderen entsprechenden

²⁹ Gesetzbekanntmachung Nr. 1008 vom 24. Oktober 2012, verfügbar unter <https://www.retsinformation.dk/forms/R0710.aspx?id=143192> (15.04.2012).

³⁰ Dänische Verfassung, Gesetz Nr. 169 vom 5. Juni 1953, verfügbar unter <http://www.grundloven.dk/>

³¹ Das Gesetz über CCTV Überwachung (Gesetz Nr. 1190 vom 11. Oktober 2007); *This act is however addressed for non-government use and the police are not governed by the law and therefore the law is not legally relevant for this opinion. It should however be noted that a provision was inserted in the Act in 2006 according to which the police may request that public authorities or private companies establish CCTV surveillance in accordance with current legislation. A request to set up CCTV surveillance is expected to be made in particular where it is found that this type of surveillance may be of importance to preventing or investigating possible terrorist attacks. A provision has furthermore been inserted in the Act on CCTV Surveillance which allows the police to make demands on public authorities or private companies regarding quality standards for the recordings of images on videotapes, film or the like as well as for the storage of such recordings (Sec. 4b, inserted 10/6 by Act No. 542 of 8/6 2006).*

³² Gesetz Nr. 429 vom 31. Mai 2000, verfügbar unter <https://www.retsinformation.dk/Forms/R0710.aspx?id=828>

³³ Gesetz Nr. 1062 vom 17. November 2011, verfügbar unter <https://www.retsinformation.dk/Forms/R0710.aspx?id=138671>

³⁴ Art 263.1: *The definition of closed communication: to break or evade any letter, telegram or other closed message or record, or acquaint oneself with the content. To gain access to other peoples private storages. To use a device to secretly intercept or record statements made in private, telephone calls or other conversation between others or negotiation in closed meetings where one has improperly obtained access.*

³⁵ Strafgesetzbuch, Kapitel 27, Art. 263.1.

³⁶ Strafgesetzbuch, Kapitel 27, Art. 263.2.

³⁷ Gesetz Nr 378 vom 6. Juni 2002 (terror-package I), verfügbar unter <https://www.retsinformation.dk/Forms/R0710.aspx?id=1344>
Gesetz Nr. 542 vom 8. Juni 2006 (terror-package II), verfügbar unter <https://www.retsinformation.dk/Forms/R0710.aspx?id=2364>

Kommunikationsapparaten (das Einholen von Daten in Bezug auf ein Telefon oder in Bezug auf einen näher bestimmten Kreis von Telefonapparaten, d.h. mit welchen Telefonen oder anderen Kommunikationsapparaten eine Verbindung aufgenommen wird) sowie das Zurückhalten und Öffnen von Briefen, Telegrammen und anderen Sendungen. In einer Sonderbestimmung sind die Beobachtung mit technischen Mitteln (Fotografie, Video), das Lesen von Daten in nicht-öffentlichen Informationssystemen und die Störung oder der Abbruch von Radio- und Telekommunikation geregelt (§ 791a bis 791c RPL). Für alle in § 780 RPL aufgezählten Massnahmen bestehen allgemeine Voraussetzungen und ein grundsätzlich einheitliches Verfahren (§ 781 – 789 RPL). Sonderbestimmungen bestehen für die letzten drei Massnahmen, d.h. für die Überwachung von privaten Orten, das Lesen von Daten (inkl. E-mails) und die Störung von Radio- und Telekommunikation. Diese werden hier nicht weiter behandelt, da sie nicht im Zentrum der vorliegenden Untersuchung stehen.

Gemäss § 781 RPL ff. kann eine in § 780 vorgesehene Massnahme durchgeführt werden, wenn:

1. Grund zur **Annahme** besteht, dass durch das betroffene Kommunikationsmittel von oder an die verdächtige Person eine **Mitteilung** erfolgt (§ 781 Abs. 1 (1) RPL);
2. der Eingriff von **entscheidender Bedeutung für die Strafuntersuchung** ist (§ 781 Abs. 1 (2) RPL);
3. die Strafuntersuchung eine **hinreichend schwere Straftat** betrifft (s. unten, nächster Absatz);
4. der Eingriff **verhältnismässig** ist (§ 782 RPL), und
5. der Eingriff **gerichtlich** beschlossen wurde (§ 783 RPL).

Während die ersten beiden Voraussetzungen im Gesetz nicht weiter erläutert werden, ist die Voraussetzung einer **hinreichend schweren Straftat** sehr konkret formuliert, so dass hier kein Ermessensspielraum besteht. § 781 Abs. 1 (3) RPL sieht vier Varianten vor:

1. Die Straftat ist mit einer **Freiheitsstrafe von mindestens 6 Jahren** bedroht;
2. Es handelt sich um eine **Straftat gegen** die Selbständigkeit und Sicherheit des **Staates** (Kapitel 12 Strafgesetz) oder gegen die Staatsverfassung und die oberste Staatsgewalt, insbesondere um Terrorismus (Kapitel 13 Strafgesetz);
3. Es handelt sich um einen der **ausdrücklich aufgezählten Tatbestände**: Befreiung einer gefangenen oder verwahrten Person (§ 124 (2) Strafgesetz); Hinderung der Strafverfolgung (§ 125 Strafgesetz); Wehrdienstverweigerung (§ 127), Verleiten zur Prostitution oder Betreiben von Bordellen (§ 228), Pornographie (§ 235), qualifiziertes Androhen einer strafbaren Handlung (§ 266) sowie Erpressung (§ 281);
4. gewisse Verstösse gegen das **Ausländergesetz** (Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt; § 59 (7) (1 bis 5) Ausländergesetz).

Die Voraussetzung einer hinreichend schweren Straftat ist gemäss § 781 Abs. 1 ff. RPL für **gewisse Überwachungsmassnahmen auch bei anderen Verdachtsmomenten** erfüllt. So kann Telefonabhören und -überwachen auch bei einem Verdacht auf unberechtigtes Zugangsverschaffen zu Aufnahmen und Datensystem eines anderen (§ 263 Abs. 2 Strafgesetz) durchgeführt werden (§ 781 Abs. 2 RPL); die Telefonüberwachung (aber nicht das -abhören) kann auch bei einem dem „Stalking“ vergleichbaren Tatbestand (§ 263 Strafgesetz) erfolgen sowie bei Verdacht auf Datenbetrug gemäss § 279a Strafgesetz oder auf Gebrauch einer fremden Sache (§ 293 Abs. 1 Strafgesetz) unter Anwendung eines Telekommunikationsdienstes, oder auch bei Verdacht auf gewisse Widerhandlungen gegen das Wertpapiergesetz (§ 781 Abs. 3 RPL). Das Briefgeheimnis kann zudem zu Konfiskationszwecken oder zur Restitution verletzt werden (§ 781 Abs. 4 RPL). Schliesslich ist gemäss § 781 Abs. 5 RPL das Abhören und die Überwachung auch zulässig bei Verdacht auf eine Straftat, welche Menschenleben oder bedeutende Gesellschaftswerte (*samfundsvaerdier*) gefährdet. Die Überwachung bzw. das Erfassen von Stammdaten ist auch möglich, wenn die erste Bedingung, d.h. das erwartete Versenden von Mitteilungen, nicht erfüllt ist.

Ein Eingriff erfordert wie erwähnt einen gerichtlichen Beschluss, wobei der richterliche Beschluss auch den Zeitraum, innert dessen die Massnahme durchzuführen ist, angeben muss (§ 783 Abs. 1 und 3 RPL). Eine Massnahme darf nicht für länger als 4 Wochen genehmigt werden (§ 783 Abs. 3 RPL). Sofern der Zweck des Eingriffs eine **richterliche Ermächtigung** nicht möglich macht, kann dieser auch ohne gerichtlichen Beschluss durchgeführt werden, die Polizei muss den Sachverhalt aber innert höchstens 24 Stunden einem Gericht vorlegen (§ 783 Abs. 4 RPL).

Im Gerichtsverfahren vertritt ein **Anwalt** die Interessen der betroffenen Person; er muss angehört werden (§ 784 Abs. 1 RPL). Der Anwalt darf sich zwar mit dem Material vertraut machen, er darf aber weder die verdächtige Person noch Dritte kontaktieren (§ 785 Abs. 1 RPL). In einer Verordnung des Justizministeriums³⁸ wird die Auswahl von und die Anforderungen (insbesondere Sicherheitsüberprüfung) an die zuständigen Anwälte geregelt (§ 784 Abs. 2 RPL).

Nach erfolgter Massnahme wird die betroffene Person in der Regel (d.h. sofern daraus für die Nachforschungen keine Nachteile entstehen) **informiert**, auch über die betroffene Straftat (§ 788 RPL).

Auch im strafprozessualen Rahmen wird die **Beistands- und Aufnahmepflicht** der Telekommunikationsdienstleister gegenüber der Polizei und das Verfahren zur Einsichtnahme vorgeschrieben (s. unten, 2.; § 786 ff. RPL).

2. Übersicht über Prozess- und Organisationsstrukturen

Die Prozess- und Organisationsstrukturen im Bereich der Fernmeldeüberwachung sind soweit ersichtlich nur teilweise ausdrücklich geregelt. Ausdrückliche Vorschriften finden sich in Bezug auf die Pflichten der Telekommunikationsanbieter im Zusammenhang mit der Telekommunikationsüberwachung (2.1.). Weniger ausführlich sind die Regeln zur Organisation (2.2.).

2.1. Die Unterstützungspflicht der Telekommunikationsanbieter

§ 786 RPL enthält eine Pflicht von Post- und Telekommunikationsanbietern zur **Mithilfe** gegenüber der Polizei beim Durchführen der oben beschriebenen Eingriffs- und Überwachungsmassnahmen. Neben der allgemeinen Pflicht zur Unterstützung bei der Durchführung einzelner Überwachungsmassnahmen (2.1.1.) besteht auch eine allgemeine Erfassungspflicht (2.1.2.).

2.1.1. Die allgemeine Unterstützungspflicht

Gemäss § 786 Abs. 1 RPL müssen Post- und Telekommunikationsanbieter die Polizei beim Durchführen der Eingriffs- und Überwachungsmassnahmen unterstützen. Nach § 10 Abs. 1 Telekommunikationsgesetz³⁹ müssen die Telekommunikationsanbieter (auf eigene Kosten, s. unten, 3.) sicherstellen, dass die **technischen Systeme** einen Zugang der Polizei zur Durchführung der gesetzlich vorgesehenen Eingriffe in das Telekommunikationsgeheimnis erlauben. Die Anbieter müssen die Polizei auch beim **Durchführen der Eingriffe** unterstützen und sicherstellen, dass die Anordnungen der Polizei schnell behandelt werden (§ 10 Abs. 3 und 4 Telekommunikationsgesetz).

³⁸ Bekendtgørelse 1630 af 21.12.2010 om advokater, der kan beskikkes i visse sager om indgreb i meddelelseshemmeligheden mv., verfügbar unter <https://www.retsinformation.dk/Forms/R0710.aspx?id=134760> (10.06.2012).

³⁹ Lov 169 af 03.03.2011 om elektroniske kommunikationsnet og -tjenester, verfügbar unter <https://www.retsinformation.dk/Forms/R0710.aspx?id=136073> (10.06.2012).

2.1.2. Die Pflicht zur Erfassung und Aufbewahrung von Telekommunikationsdaten

Im Jahr 2002 wurde im Rahmen der ersten Anti-Terror-Gesetzgebung mit einer Änderung des Verfassungsgesetzes eine allgemeine Pflicht, Verkehrsdaten **während eines Jahres** aufzubewahren, eingeführt (§ 786 Abs. 4 RPL). Zur Konkretisierung erliess das Justizministerium 2006 eine Verordnung über die Registrierung und Aufbewahrung von Angaben über Televerkehr durch die Anbieter von elektronischen Kommunikationsnetzen und -dienstleistungen⁴⁰, welche auch die europäische Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/85/EG umsetzt.

2.2. Organisation

Ganz allgemein obliegt das Durchführen der Überwachungsmassnahmen gemäss Gesetzestext der **Polizei**. In einer grossen Anzahl von Fällen wird die Überwachung wohl vom Nachrichtendienst der Polizei (*Politiets Efterretningstjeneste*: PET)⁴¹ durchgeführt. Das Hauptquartier der Polizei (*Rigspolitiet*) hat zudem ein „Telecenter“, welches (mindestens bei der Anmeldung von Dienstleistern) Kontaktstelle für die Telekomanbieter ist.⁴²

Die Telekommunikationsanbieter sind umgekehrt gemäss einer eigens dafür erlassenen Verordnung⁴³ verpflichtet, eine **Verbindungsstelle** für die Polizei oder mindestens eine zuständige Person mit einem Vertretungsplan einzurichten.

3. Kosten und Finanzflüsse

§ 786 Abs. 8 RPL sieht vor, dass das Justizministerium in einer Verordnung festsetzt, wie die Kosten der Telekommunikationsanbieter im Zusammenhang mit der Unterstützung der Polizei beim Durchführen von Überwachungsmassnahmen erstattet werden. Unseres Wissens wurde allerdings diese **Verordnungskompetenz bis anhin nicht wahrgenommen**.⁴⁴ Als allgemeiner Grundsatz zur Kostentragung wird davon auszugehen sein, dass nur die konkreten, durch die jeweilige Massnahme verursachten Kosten zu tragen wären.⁴⁵ Das Einrichten und Betreiben der Verbindungsstelle (s. oben) geht ohne Entschädigung zu Lasten der Anbieter.

Gemäss telefonischen Auskünften werden die Tarife **mit jedem Anbieter separat vereinbart** und sind **vertraulich**. Die Tarife unterscheiden jeweils zwischen einer einmaligen Einrichtungsentschädigung und einer täglichen Gebühr für die Dauer der Massnahme. Dabei wird zwischen einer Vielfalt ver-

⁴⁰ Bekendtgørelse 988 af 28.09.2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen), verfügbar unter <https://www.retsinformation.dk/Forms/R0710.aspx?id=2445> (10.06.2012); in Kraft getreten am 15.09.2007.

⁴¹ www.pet.dk.

⁴² S. dazu das online zugängliche Formular für die Anmeldung von Fernmeldedienstleistern bei der Polizei: <http://www.politi.dk/da/hjaelp/politiet/teleindb/> (23.06.2012).

⁴³ Bekendtgørelse 1145 af 20.11.2006 om telenet- og telenetudbyderes praktiske bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden (døgnbetjent kontaktpunkt), verfügbar unter <https://www.retsinformation.dk/Forms/R0710.aspx?id=2491> (10.06.2012).

⁴⁴ Bestätigt durch eine telefonische Auskunft des dänischen Justizministeriums vom 10. September 2012.

⁴⁵ So gemäss den Materialien 1998/1 LSF 41 zum Lov nr 229 af 21 april 1999, Lov om ændring af retsplejeloven, Kommentare zu § 786 Abs. 8.

schiedener Massnahmen unterschieden (Echtzeitüberwachung (12 verschiedene Tarife), historische Daten).⁴⁶

Gemäss § 10 Abs. 1 des Telekommunikationsgesetzes müssen die Telekommunikationsanbieter ohne Kosten für den Staat sicherstellen, dass die Systeme das **technische Durchführen von Überwachungsmassnahmen** erlauben. Über die Kostentragung der Unterstützung im Einzelfall (§ 10 Abs. 3 und § 13 Telekommunikationsgesetz) enthält das Gesetz keine Regelung. Hier ist wohl ebenfalls § 786 Abs. 8 RPL anwendbar. Auch ohne Bestehen einer Verordnung scheinen im Einzelfall Kosten erstattet zu werden, wobei auch hier wohl die vertraulichen, mit den Anbietern verhandelten Tarife zur Anwendung kommen.⁴⁷

⁴⁶ Alle Informationen basieren auf telefonischen und elektronischen Auskünften von einer Person bei der nationalen Polizeibehörde im IT- und Telekom-Department (13. September 2012).

⁴⁷ S. Bericht der Kommission an den Rat und das Europäische Parlament, Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24/EG), KOM(2011)225 endgültig, S. 33; verfügbar unter <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:DE:PDF> (22.06.2012).

B. DEUTSCHLAND

In Deutschland sind die Vorgaben, die Betreibern von Telekommunikationsanlagen und Kommunikationsdienstleistern gesetzlich auferlegt sind, um die technische Umsetzung von Überwachungsmaßnahmen sowie die Erteilung von Auskünften zu gewähren, im **Telekommunikationsgesetz**⁴⁸ (TKG) geregelt. Die materiell-rechtlichen Ermächtigungen für die Anordnung von Überwachungsmaßnahmen ergeben sich aus bundes- und landesrechtlichen Vorschriften, insbesondere aus der Strafprozessordnung.⁴⁹ Diese greifen in das in Art. 10 Abs. 1 Grundgesetz⁵⁰ (GG) verankerte Fernmeldegeheimnis ein, dessen Beschränkung nach Art. 10 Abs. 2 S. 1 GG nur auf Grund eines Gesetzes angeordnet werden kann.

Die Regelungen der Strafprozessordnung sowie die anderen Ermächtigungsgrundlagen enthalten selbst – im Gegensatz zu den Vorschriften des TKG – keine Regelungen darüber, an welcher technischen Einrichtung eine Überwachungsmaßnahme geschaltet wird. Sie regeln nur, unter welchen Voraussetzungen Telekommunikation überhaupt aufgezeichnet werden darf. Die genaueren **technischen und organisatorischen Anforderungen** an die Umsetzung von Überwachungsmaßnahmen werden durch die **Telekommunikations-Überwachungsverordnung**⁵¹ (TKÜV) geregelt, deren Ermächtigungsgrundlage in § 110 Abs. 2 TKG enthalten ist. Die TKÜV enthält wie § 110 TKG keine Rechtsgrundlage für die Anordnung von Überwachungsmaßnahmen. Sie verpflichtet die von der Vorschrift in die Pflicht genommenen Betreiber von Telekommunikationsnetzen, sich auf die Durchführung von Überwachungsanordnungen vorzubereiten.⁵²

1. Übersicht über die strafprozessualen Grundlagen

Telekommunikationsüberwachung ist die im Strafverfahrensrecht und Polizeirecht in Deutschland übliche Bezeichnung für die Überwachung von Telekommunikationsvorgängen und -inhalten. Die rechtlichen Voraussetzungen für den Zugriff auf Telekommunikationsdaten richten sich nach der **Art der Daten**. Dabei wird zwischen Inhaltsdaten (s.u. 1.1), Verkehrsdaten (s.u. 1.2) und Bestandsdaten (s.u. 1.3) unterschieden.

1.1 Inhaltsdaten

Der mit Wirkung zum 1. Januar 2008 neugefasste **§ 100a der Strafprozessordnung**⁵³ (dStPO) regelt allein und abschliessend den Zugriff auf Inhaltsdaten von Telekommunikationsvorgängen im Rahmen

⁴⁸ Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Beschl. des BVerfG – 1 BvR 1299/05 – vom 24. 1. 2012 (BGBl. I S. 460).

⁴⁹ Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, ber. S. 1319), zuletzt geändert durch Art. 2 Abs. 30 G zur Änd. von Vorschriften über Verkündung und Bekanntmachungen sowie der ZPO, des EGZPO und der AO vom 22. 12. 2011 (BGBl. I S. 3044).

⁵⁰ Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949 (BGBl. S. 1), zuletzt geändert durch Art. 1 ÄndG (Art. 91e) vom 21. 7. 2010 (BGBl. I S. 944).

⁵¹ Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung – TKÜV), vom 3. November 2005, (BGBl. I S. 3136), zuletzt geändert durch Art. 4 Terrorismusabwehr-G vom 25. 12. 2008 (BGBl. I S. 3083).

⁵² Bundestagsdrucksache 15/5199, S.1., verfügbar unter:
<http://dipbt.bundestag.de/doc/btd/15/051/1505199.pdf> (24.05.12).

⁵³ § 100a StPO [Überwachung der Telekommunikation]
(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

straftprozessualer Massnahmen und erlaubt damit einen Eingriff in das Grundrecht des Fernmeldegeheimnisses.⁵⁴ Inhaltsdaten betreffen den durch das Fernmeldegeheimnis geschützten **Inhalt einer Telekommunikation**.⁵⁵ Durch die Änderung der Vorschrift im Rahmen des Telekommunikationsbegleitgesetzes vom 17. Dezember 1997 wurde der Begriff des Fernmeldeverkehrs durch den Begriff der Telekommunikation ersetzt.⁵⁶

Die nach § 100a dStPO zu erlassende Anordnung ist auf die **Überwachung** und **Aufzeichnung** der Telekommunikation gerichtet. Der Begriff der **Telekommunikation** ist in § 3 Nr. 22 TKG i.V.m. § 3 Nr. 23 TKG legal definiert und stellt einen technischen Vorgang des Aussendens, Übermittels und Empfangens von Nachrichten jeglicher Art in Form von Zeichen, Sprache, Bildern oder Tönen mittels technischer Einrichtungen oder Systemen, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können. Es werden demnach alle Vorgänge erfasst, die mit dem Versenden und Empfangen von Nachrichten mittels Telekommunikationsanlagen in Zusammenhang stehen.⁵⁷ Im Hinblick auf die Entwicklung neuartiger Übertragungstechniken ist der Begriff der Telekommunikation als **entwicklungsoffen** anzusehen.⁵⁸ Der **Umfang** der Telekommunikation betrifft nur den **eigentlichen technischen Vorgang**. Darunter ist der Vorgang vom Absenden der Signale bis zu deren Empfang beim Adressaten zu verstehen.⁵⁹

Zu den von § 100a dStPO erfassten **Arten der Telekommunikation** gehören insbesondere Gespräche mittels Telefon, Nachrichten in Form von Kurzmitteilungen (SMS), Multimediadaten (MMS), Fax, Satellitenübertragung, Bildtelefon, Telex, Teletex, Telebox, Fernschreiben, die Kommunikation mit Online-Diensten und Videodienste. Auch die Kommunikation im Internet fällt darunter. Hier kann aber wegen des Inhalts der übertragenen Daten der Grundrechtsschutz enger gefasst werden, etwa bei Datenbankabfragen.⁶⁰

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,

2. die Tat auch im Einzelfall schwer wiegt und

3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

(2) [Anm.: Abs. 2 enthält eine umfangreiche Liste von Straftaten, die aufgrund ihres Umfangs hier nicht wiedergegeben wird]

(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt.

(4) 1. Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. 2. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 erlangt wurden, dürfen nicht verwertet werden. 3. Aufzeichnungen hierüber sind unverzüglich zu löschen. 4. Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen.

⁵⁴ J. GRAF in Beck'scher Online-Kommentar StPO, Stand: 01.02.2010, §100a Rn. 5.

⁵⁵ J. GRAF in Beck'scher Online-Kommentar StPO, op.cit., §100a Rn. 22.

⁵⁶ BGBl. I 1997, S. 3113.

⁵⁷ Bundesgerichtshof, Urteil vom 14.03.2003, Az.: 2 StR 341/02, Neue Zeitschrift für Strafrecht 2003, S. 668.

⁵⁸ Bundesverfassungsgericht, Urteil vom 02.03.2006, Az.: 2 BvR 2099/04, Neue Juristische Wochenschrift 2006, S. 978.

⁵⁹ J. GRAF in Beck'scher Online-Kommentar StPO, op.cit., §100a Rn. 8.

⁶⁰ A. NACK in Karlsruher Kommentar zur Strafprozessordnung 6. Auflage, München 2008, § 100a Rn. 14.

Die Ausnutzung technischer Schwachstellen oder Aussendungen eines Gerätes, insbesondere eines Computers, für Abhörmassnahmen sowie Nachrichten, Signale oder Daten, die noch nicht oder nicht mehr gesendet, übermittelt oder empfangen werden, und abgespeicherte Daten, vom Anrufbeantworter aufgezeichnete Gespräche, eingegangene SMS-Nachrichten oder die vom Empfangsgerät automatisch aufgezeichneten Rufnummern eingegangener Anrufe werden **nicht von § 100a dStPO erfasst**.⁶¹

1.1.1 Anordnungsvoraussetzungen

Die Anordnung einer Überwachung nach § 100a dStPO kann nur erfolgen, wenn bestimmte Tatsachen den **Verdacht** begründen, dass jemand eine **schwere Straftat**, die im Straftatenkatalog des § 100a Abs. 2 dStPO enthalten ist, begangen hat und wenn diese auch im **Einzelfall schwer wiegt**.

Der **Anlasstaten**katalog zählt auf, welche Straftaten schwere Straftaten i.S.d. § 100a Abs. 1 Nr. 1 dStPO sind. Es handelt sich um Delikte, für die eine Höchststrafe von fünf Jahren oder mehr festgelegt ist.⁶² Dabei ist die Teilnahme (Beihilfe oder Anstiftung) der Täterschaft gleichgestellt, ebenso der strafbare Versuch und die strafbare Vorbereitung einer Katalogtat.

Weiterhin müssen bestimmte Tatsachen den für die Anordnung erforderlichen **Tatverdacht** begründen, der jedoch weder dringend, noch hinreichend sein muss. Es muss jedoch auf Grund der Lebenserfahrung oder der kriminalistischen Erfahrung fallbezogen aus Zeugenaussagen, Observationen oder anderen sachlichen Beweisanzeichen auf das Vorliegen einer Katalogtat geschlossen werden können.⁶³ Zudem müssen konkrete und in gewissem Umfang verdichtete Umstände als Tatsachenbasis für den Verdacht vorhanden sein, die bereits ein gewisses Mass an Konkretisierung erreicht haben.⁶⁴ Dem für die Entscheidung zuständigen Richter oder Staatsanwalt wird durch das Gesetz aber ein **Beurteilungsspielraum** eingeräumt.⁶⁵ Aus der richterlichen Entscheidung müssen die wesentlichen Entscheidungsgrundlagen hervorgehen, und die notwendige Einzelfallprüfung muss zumindest in groben Zügen erkennbar sein.⁶⁶

Nach 100a Abs. 1 Nr. 2 dStPO muss die zugrunde liegende Anlasstat nicht nur abstrakt, sondern auch **im Einzelfall schwer wiegen**. Anhaltspunkte sind dafür beispielsweise die Folgen der Tat, die Schutzwürdigkeit des verletzten Rechtsguts und das Hinzutreten besonderer Umstände, wie etwa das Zusammenwirken des Beschuldigten mit anderen Straftätern oder die besondere kriminelle Intensität.⁶⁷

Nach § 100a Abs. 1 Nr. 3 dStPO darf eine Massnahme nur angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten ansonsten **wesentlich**

⁶¹ Bundesverfassungsgericht, Urteil vom 27. 2. 2008, Az.: 1 BvR 370/07, 1 BvR 595/07, Neue Juristische Wochenschrift 2008, S.825; A. NACK, Karlsruher Kommentar zur Strafprozessordnung, op.cit., § 100a Rn. 5.

⁶² Bundestagsdrucksache 16/5846 S. 40, verfügbar unter: <http://dip21.bundestag.de/dip21/btd/16/069/1606979.pdf>, (24.05.2012).

⁶³ Bundesverfassungsgericht, Beschluss vom 30. 4. 2007, Az.: 2 BvR 2151/06, Neue Juristische Wochenschrift 2007, S. 2753.

⁶⁴ Bundesverfassungsgericht, Urteil vom 12. 3. 2003, Az.: 1 BvR 330/96 u. 1 BvR 348/99, Neue Juristische Wochenschrift, S. 1791.

⁶⁵ Bundesgerichtshof, Urteil vom 16.02.1995, Az.: 4 StR 729/94, Neue Juristische Wochenschrift 1995, S. 1975.

⁶⁶ J. GRAF in Beck'scher Online-Kommentar StPO, zit., §100a Rn. 37.

⁶⁷ MEYER-GÖßNER, Kommentar zur Strafprozessordnung, 53. Auflage, München 2011, § 100a Rn. 11.

erschwert⁶⁸ oder **aussichtslos**⁶⁹ wäre (Subsidiarität). Grösserer Arbeitsaufwand rechtfertigt die Massnahme nur, wenn er so umfangreich wäre, dass die Strafverfolgungsinteressen überwiegen. Auch insoweit kommt dem Anordnenden ein **Beurteilungsspielraum** zu.⁷⁰ Der Kostenaufwand darf grundsätzlich allerdings keine Rolle spielen.⁷¹ Darüber hinaus ist die **Verhältnismässigkeit** der Anordnung sowohl bei ihrem Erlass als auch fortlaufend während ihres Andauerns zu prüfen. Eingeleitete Massnahmen sind deshalb auch sofort abubrechen, wenn sich ihre Unverhältnismässigkeit ergibt.⁷²

1.1.2 Betroffene

Nach § 100a Abs. 3 dStPO kann sich die Massnahme gegen den **Beschuldigten** oder auch gegen **Nichtverdächtige** richten. Beschuldigter ist der Tatverdächtige, gegen den bereits ein Ermittlungsverfahren eingeleitet oder gegen den es mit der Anordnung nach § 100a dStPO eingeleitet wird, wobei seine Identität noch nicht bekannt sein muss.⁷³

Bei Personen, die nicht zu den Beschuldigten gehören, muss auf Grund bestimmter Tatsachen anzunehmen sein, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben (**Nachrichtensmittler**) oder dass der Beschuldigte ihren Anschluss benutzt. Für die Annahme, dass der von der Anordnung Betroffene für den Beschuldigten Mitteilungen entgegennimmt oder weiterleitet, muss eine **hinreichend sichere Tatsachenbasis** vorliegen.⁷⁴

Die Überwachung von nicht auf den Beschuldigten angemeldeten Telekommunikationsanschlüssen ist zulässig, sofern der Beschuldigte diese benutzt, auch wenn die Inhaber hiervon **keine Kenntnis** haben. Dabei kann es sich um Nachbarn, Freunde, Unternehmen oder um den Arbeitsplatz handeln.⁷⁵ Auch die Überwachung einer **öffentlichen Fernsprechkabine** ist möglich. Unvermeidbar ist, dass durch die Massnahme auch unbeteiligte Dritte mitbetroffen sind.⁷⁶ Das Abhören des Telefonanschlusses eines Verteidigers, dessen Mandant einer Katalogtat nach § 100a dStPO beschuldigt ist, ist nicht erlaubt, da die Abhörmassnahme in einem unlösbaren Widerspruch zur Rechtsgarantie des unüberwachten mündlichen Verkehrs zwischen Verteidiger und Beschuldigtem nach § 148 dStPO stünde.⁷⁷

1.1.3 Kernbereichsschutz

Nach § 100a Abs. 4 dStPO ist eine Überwachungsmassnahme unzulässig, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch die Massnahme allein Erkenntnisse aus dem **Kernbereich privater Lebensgestaltung** erlangt werden. Diese Erkenntnisse dürfen in einem folgenden Strafprozess nicht verwertet werden; Aufzeichnungen hierüber sind unverzüglich zu löschen. Mit dieser Regelung wurde der Forderung des Bundesverfassungsgerichts Rechnung getragen, dass bei

⁶⁸ Andere Ermittlungsmethoden wären zeitlich erheblich aufwändiger und würden daher zu einer wesentlichen Verfahrensverzögerung führen; A. NACK, Karlsruher Kommentar zur Strafprozessordnung, op.cit., § 100a Rn. 35.

⁶⁹ Andere Ermittlungsmöglichkeiten stehen nicht zur Verfügung oder haben keine Aussicht auf Erfolg; J. GRAF in Beck'scher Online-Kommentar StPO, op.cit., § 100a Rn. 40.

⁷⁰ MEYER-GÖßNER, Kommentar zur Strafprozessordnung, op.cit., § 100a Rn. 13.

⁷¹ A. NACK in Karlsruher Kommentar zur Strafprozessordnung, op.cit., § 100a Rn. 35.

⁷² A. NACK in Karlsruher Kommentar zur Strafprozessordnung, op.cit., § 100a Rn. 35.

⁷³ J. GRAF in Beck'scher Online-Kommentar StPO, op.cit., § 100a Rn. 43.

⁷⁴ Bundesverfassungsgericht, Urteil vom 12. 3. 2003, Az.: 1 BvR 330/96 u. 1 BvR 348/99, Neue Juristische Wochenschrift 2003, S. 1787.

⁷⁵ J. GRAF in Beck'scher Online-Kommentar StPO, op.cit., § 100a Rn. 49.

⁷⁶ MEYER-GÖßNER, Kommentar zur Strafprozessordnung, op.cit., § 100a Rn. 13.

⁷⁷ Bundesverfassungsgericht, Beschluss vom 18. 4. 2007, Az.: 2 BvR 2094/05, Neue Juristische Wochenschrift 2007, S. 2749.

der Überwachung von Telekommunikation gesetzlich Vorkehrungen zum Schutz individueller Entfaltung im Kernbereich privater Lebensgestaltung zu treffen sind.⁷⁸

1.2 Verkehrsdaten

Verkehrsdaten können durch die Strafverfolgungsbehörden mittels einer Anordnung nach der hierfür zentralen Ermächtigungsnorm des § 100g dStPO⁷⁹ erhoben werden. Nach § 3 Nr. 30 TKG sind Verkehrsdaten diejenigen Daten, die **bei der Erbringung** eines Telekommunikationsdienstes **erhoben, verarbeitet oder genutzt** werden. Die Verkehrsdaten umfassen die **Rufnummer** oder sonstige Kennung des anrufenden und des **angerufenen Anschlusses** oder der jeweiligen Endeinrichtung, personenbezogene Berechtigungskennungen, bei Kundenkarten die Kartenummer und bei mobilen Anschlüssen die Standortkennung des Absenders bzw. des Empfängers. Ausserdem fallen unter die Verkehrsdaten Leitwege, Zeitpunkt und Dauer der Verbindung sowie die übermittelten Datenmengen, das verwendete Protokoll, Format der Nachricht, das Netz, von dem die Nachricht ausgeht bzw. an das gesendet wird, die in Anspruch genommene Telekommunikationsdienstleistung, die Endpunkte von festgeschalteten Verbindungen sowie deren Zeitpunkt und Dauer und sonstige zum Aufbau und zur Aufrechterhaltung sowie zur Entgeltabrechnung erforderlichen Verbindungsdaten.⁸⁰ Ihr Zweck ist die **Erforschung des Sachverhalts** oder die **Ermittlung des Aufenthaltsortes** des Beschuldigten.

⁷⁸ Bundesverfassungsgericht, Urteil vom 27. 7. 2005, Az.: 1 BvR 668/04, Neue Juristische Wochenschrift 2005, S. 2612.

⁷⁹ **§ 100g StPO [Erhebung von Verkehrsdaten]**

(1) 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. 2 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. 3 Die Erhebung von Standortdaten in Echtzeit ist nur im Falle des Satzes 1 Nr. 1 zulässig.

(2) 1 § 100a Abs. 3 und § 100b Abs. 1 bis 4 Satz 1 gelten entsprechend. 2 Abweichend von § 100b Abs. 2 Satz 2 Nr. 2 genügt im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(3) Erfolgt die Erhebung von Verkehrsdaten nicht beim Telekommunikationsdiensteanbieter, bestimmt sie sich nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften.

(4) Über Maßnahmen nach Absatz 1 ist entsprechend § 100b Abs. 5 jährlich eine Übersicht zu erstellen, in der anzugeben sind:

1. die Anzahl der Verfahren, in denen Maßnahmen nach Absatz 1 durchgeführt worden sind;

2. die Anzahl der Anordnungen von Maßnahmen nach Absatz 1, unterschieden nach Erst- und Verlängerungsanordnungen;

3. die jeweils zugrunde liegende Anlassstrafat, unterschieden nach Absatz 1 Satz 1 Nr. 1 und 2;

4. die Anzahl der zurückliegenden Monate, für die Verkehrsdaten nach Absatz 1 abgefragt wurden, bemessen ab dem Zeitpunkt der Anordnung;

5. die Anzahl der Maßnahmen, die ergebnislos geblieben sind, weil die abgefragten Daten ganz oder teilweise nicht verfügbar waren.

⁸⁰ B. HOLZNAGEL/T. RICKE in Spindler/Schuster, Recht der elektronischen Medien, 2. Auflage, 2011.

Die Verkehrsdatenerhebung ist zum einen bei Tätern oder Teilnehmern einer **Straftat von auch im Einzelfall erheblicher Bedeutung** gestattet (Abs. 1 S. 1 Nr. 1). Solche Straftaten sind insbesondere die Katalogtaten des § 100a Abs. 2 dStPO (s. oben, 1.1.2.). Darüber hinaus ist die Verkehrsdatenerhebung auch bei Straftaten gestattet, die **mittels Telekommunikation begangen** wurden (Abs. 1 S. 1 Nr. 2), und zwar auch, wenn diese Straftaten nicht von erheblicher Bedeutung sind. Nach Abs. 2 S. 1 i.V.m. § 100a Abs. 3 dStPO darf sich die Massnahme nur gegen Beschuldigte und Nachrichtensmittler richten, **nicht** hingegen **gegen Zeugen**.

1.3 Bestandsdaten

Rechtsgrundlage für die Auskunftserteilung an die Justiz- und Strafverfolgungsbehörden über die Bestandsdaten sind §§ 161 Abs. 1 S. 1⁸¹, 163 dStPO^{82, 83}. Nach § 3 Abs. 1 Nr. 3 TKG sind **Bestandsdaten** die Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines **Vertragsverhältnisses** über Telekommunikationsdienste erhoben werden. Dazu gehören insbesondere der Name und die Anschrift des Kunden ebenso wie die IP-Adresse bei der Internetkommunikation, gleichgültig ob sie statisch oder dynamisch ist.⁸⁴

1.4 Sonstige Ermächtigungsgrundlagen ausserhalb der StPO

Die **Verfassungsschutzbehörden** des Bundes und der Länder, der **militärische Abschirmdienst** und der **Bundesnachrichtendienst** haben aufgrund des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses⁸⁵ (G 10-Gesetz) die Ermächtigung, zur Abwehr drohender Gefahren für die demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes Überwachungen vorzunehmen.

⁸¹ § 161 StPO [Ermittlungen; Verwendung von Daten aus verdeckten Ermittlungen]

(1) 1 Zu dem in § 160 Abs. 1 bis 3 bezeichneten Zweck ist die Staatsanwaltschaft befugt, von allen Behörden Auskunft zu verlangen und Ermittlungen jeder Art entweder selbst vorzunehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen zu lassen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln.

⁸² § 163 StPO [Aufgaben der Polizei]

(1) 1. Die Behörden und Beamten des Polizeidienstes haben Straftaten zu erforschen und alle keinen Aufschub gestattenden Anordnungen zu treffen, um die Verdunkelung der Sache zu verhüten. 2. Zu diesem Zweck sind sie befugt, alle Behörden um Auskunft zu ersuchen, bei Gefahr im Verzug auch, die Auskunft zu verlangen sowie Ermittlungen jeder Art vorzunehmen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln.

(2) 1. Die Behörden und Beamten des Polizeidienstes übersenden ihre Verhandlungen ohne Verzug der Staatsanwaltschaft. 2. Erscheint die schleunige Vornahme richterlicher Untersuchungshandlungen erforderlich, so kann die Übersendung unmittelbar an das Amtsgericht erfolgen.

(3) 1. Bei der Vernehmung eines Zeugen durch Beamte des Polizeidienstes sind § 52 Absatz 3, § 55 Absatz 2, § 57 Satz 1 und die §§ 58, 58a, 68 bis 69 entsprechend anzuwenden. 2. Über eine Gestattung nach § 68 Absatz 3 Satz 1 und über die Beordnung eines Zeugenbeistands entscheidet die Staatsanwaltschaft; im Übrigen trifft die erforderlichen Entscheidungen die die Vernehmung leitende Person. 3. Bei Entscheidungen durch Beamte des Polizeidienstes nach § 68b Absatz 1 Satz 3 gilt § 161a Absatz 3 Satz 2 bis 4 entsprechend. 4. Für die Belehrung des Sachverständigen durch Beamte des Polizeidienstes gelten § 52 Absatz 3 und § 55 Absatz 2 entsprechend. 5. In den Fällen des § 81c Absatz 3 Satz 1 und 2 gilt § 52 Absatz 3 auch bei Untersuchungen durch Beamte des Polizeidienstes sinngemäß.

⁸³ J. GRAF in Beck'scher Online-Kommentar StPO, op.cit., § 100a Rn. 13.

⁸⁴ Bundestagsdrucksache 16/5846 S. 86, verfügbar unter:
<http://dip21.bundestag.de/dip21/btd/16/058/1605846.pdf> (24.05.2012).

⁸⁵ Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10) vom 26. Juni 2001 (BGBl. I S. 1254, ber. S. 2298), zuletzt geändert durch Art. 5 G zur Änderung des BundesverfassungsschutzG vom 7. 12. 2011 (BGBl. I S. 2576).

Mittlerweile finden sich darüber hinaus in den verschiedenen Polizeigesetzen der Bundesländer Ermächtigungsgrundlagen, um im Rahmen der **Gefahrenabwehr präventive Überwachungsmaßnahmen** durchzuführen. So ist z.B. nach Art. 34a des Bayrischen Polizeiaufgabengesetzes⁸⁶ (Bay PAG) eine Telekommunikationsüberwachung zulässig zur Abwehr von einer anderen Person drohenden Gefahr für Leben, Leib oder Freiheit, soweit dies im Einzelfall verhältnismässig ist.

2. Übersicht über Prozess- und Organisationsstrukturen

2.1 Durchführung strafprozessualer Massnahmen

§ 100b dStPO regelt das **Verfahren** im Zusammenhang mit den Massnahmen einer Telekommunikationsüberwachung nach § 100a dStPO und § 100g dStPO. Auskünfte über Bestandsdaten aufgrund eines Auskunftersuchens nach §§ 161 Abs. 1 S. 1, 163 dStPO sind den Strafverfolgungsbehörden zu erteilen, ohne dass es weiterer Anordnungsvoraussetzungen bedarf.⁸⁷

Eine Überwachungsanordnung darf auf Antrag der Staatsanwaltschaft grundsätzlich nur durch das Gericht (**Richtervorbehalt**) erfolgen. **Ausschliesslich bei Gefahr im Verzug** kann die Staatsanwaltschaft die Massnahme selbst anordnen. Ermittlungspersonen der Staatsanwaltschaft haben allerdings insoweit keinerlei Befugnisse und keine Eilkompetenz. Gefahr im Verzug besteht, wenn die richterliche Anordnung nicht eingeholt werden kann, ohne dass der Zweck der Massnahme gefährdet wird.⁸⁸ Die Eilanordnung der Staatsanwaltschaft tritt nach § 100b Abs. 1 S. 3 dStPO ausser Kraft, wenn sie nicht innerhalb von **drei Werktagen vom Gericht bestätigt** wird.

Die Anordnung nach § 100b Abs. 2 dStPO hat **schriftlich** als Beschluss zu ergehen und den Namen und die Anschrift des Betroffenen sowie seine Rufnummer oder eine Kennung seines Telekommunikationsanschlusses zu enthalten. Ausserdem müssen in den Beschluss **Art, Dauer und Umfang** der Überwachungsanordnung aufgenommen werden, die **nur jeweils für drei Monate** geschaltet werden darf. Die Anforderungen gelten auch, wenn sich die Massnahme gegen einen anderen als den Beschuldigten richtet.

Der auf Antrag der Staatsanwaltschaft erlassene richterliche oder als staatsanwaltschaftliche Eilanordnung ergangene Überwachungsbeschluss nach §§ 100a, 100b dStPO wird den Telekommunikationsdienstleistern durch die Staatsanwaltschaft oder in deren Auftrag durch Ermittlungspersonen per Telefax oder auf gesichertem elektronischen Weg vorab **übermittelt** oder sogleich unmittelbar als schriftliches Dokument **übergeben**.⁸⁹ In Eilfällen genügt ein mündliches Ersuchen an die betroffene Niederlassung des Telekommunikationsdienstleisters, wobei die schriftlichen Unterlagen dann nachträglich zugeleitet werden können.⁹⁰ Der Dienstleister ist weder berechtigt noch verpflichtet nachzuprüfen, ob die rechtlichen Voraussetzungen für die angeordnete Massnahme vorliegen.⁹¹

⁸⁶ Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (Polizeiaufgabengesetz - PAG) in der Fassung der Bekanntmachung vom 14. September 1990 (GVBl S. 397), zuletzt geändert durch § 14 G zur Anpassung an das Neue Dienstrecht vom 20. 12. 2011 (GVBl S. 689).

⁸⁷ J. GRAF in Beck'scher Online-Kommentar StPO, op.cit., § 100a Rn. 13.

⁸⁸ Bundesverfassungsgericht, Urteil vom 20. 2. 2001, Az.: 2 BvR 1444/00, Neue Juristische Wochenschrift, S. 1121.

⁸⁹ Vgl. hierzu § 12 Abs. 2 TKÜV.

⁹⁰ MEYER-GOßNER, Kommentar zur Strafprozessordnung, op.cit., § 100b Rn. 7.

⁹¹ Bundestagsdrucksache 16/5846 S. 72, verfügbar unter: <http://dip21.bundestag.de/dip21/btd/16/058/1605846.pdf> (24.05.2012).

Nach § 100b Abs. 3 dStPO hat jeder, der Telekommunikationsdienstleistungen erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen die Massnahmen nach § 100a dStPO zu **ermöglichen** und die erforderlichen Auskünfte **unverzüglich zu erteilen**. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, richtet sich nach § 110 TKG und der Telekommunikations-Überwachungsverordnung (TKÜV, s. dazu unten, 2.2.). Dabei ist die **Bundesnetzagentur** für die Erarbeitung der technischen Vorgaben und die Kontrolle der entsprechenden Einrichtungen und organisatorischen Massnahmen zuständig.⁹² Kommen Dienstleister ihrer Verpflichtung nicht nach, können nach § 100b Abs. 3 S. 3 dStPO i.V.m. § 95 Abs. 2 dStPO **Ordnungs- und Zwangsmittel** gegen sie festgesetzt werden.

2.2 Technische Umsetzung

2.2.1 Technische Umsetzung nach TKG

Die Vorschrift des § 110 TKG betrifft im Wesentlichen die Vorgaben zur technischen Umsetzung von Überwachungsmassnahmen, die auf Grund der Strafprozessordnung angeordnet werden und setzt deren Zulässigkeit bereits voraus.

Verpflichtet zur Vorhaltung technischer Einrichtungen zur Umsetzung von Massnahmen zur Überwachung der Telekommunikation sind Unternehmen, die eine Telekommunikationsanlage **betreiben**, mit der Telekommunikationsdienste für die Öffentlichkeit erbracht werden.⁹³ Die Begrenzung auf ein Angebot an die Öffentlichkeit dient dem Ausschluss von geschlossenen Benutzergruppen und so genannten Corporate Networks.⁹⁴ Die **Kosten** für die Vorhaltung der Einrichtungen haben die **Unternehmen selbst** zu tragen. Dass die erforderlichen Vorkehrungen getroffen wurden, müssen die Unternehmen unverzüglich nach Inbetriebnahme gegenüber der Bundesnetzagentur erklären. Für die praktische Umsetzung müssen sie ausserdem eine **Stelle in Deutschland** benennen, die die Anordnungen entgegennimmt. Mit der Meldung an die Bundesnetzagentur wird dies die zentrale Stelle, bei der die Ermittlungsbehörden erfahren können, wohin eine Überwachungsanordnung zu übermitteln ist.⁹⁵

Derjenige, der nur Telekommunikationsdienste für die Öffentlichkeit erbringt, **ohne zugleich** eine Telekommunikationsanlage zu betreiben, wird dadurch nicht völlig von diesen Verpflichtungen freigestellt. Er ist verpflichtet, sich bei der Auswahl des Betreibers der genutzten Telekommunikationsanlage zu **vergewissern**, dass dieser in der Lage ist, die Anordnung zur Überwachung von Telekommunikationsdiensten umzusetzen.⁹⁶

2.2.2 Telekommunikations-Überwachungsanordnung

Zur Regelung der näheren Einzelheiten für die technische und organisatorische Umsetzung von Überwachungsmassnahmen und der Erteilung von Auskünften hat die Bundesregierung mit Zustimmung des Bundesrates auf der Grundlage der Ermächtigung in § 110 Abs. 2 Nr. 1 a TKG die TKÜV

⁹² Siehe hierzu Bundesnetzagentur, Technische Umsetzung nach § 110 TKG, verfügbar unter http://www.bundesnetzagentur.de/cln_1911/DE/Sachgebiete/Telekommunikation/TechRegTelekommunikation/TechnischeUmsetzung110TKG/TechUmsetzung110TKG_node.html (20.05.2010).

⁹³ J. GRAF in Beck'scher Online-Kommentar StPO, op.cit., § 110 TKG Rn. 3.

⁹⁴ M. BOCK in Beck'scher TKG-Kommentar, 3. Auflage, München 2006, § 110 Rn. 9.

⁹⁵ G. LÖWENAU in Scheurle/Mayen, Kommentar zum Telekommunikationsgesetz, 2. Auflage, München 2008, § 110 Rn. 11.

⁹⁶ J. GRAF in Beck'scher Online-Kommentar StPO, op.cit., § 110 TKG Rn. 3.

erlassen. Deren Teil 2 regelt die Umsetzung der Massnahmen nach der Strafprozessordnung, des Artikel 10-Gesetzes⁹⁷ und nach Landesrecht.

Zum Kreis der nach der TKÜV **Verpflichteten** gehören nach § 3 Abs. 1 TKÜV diejenigen Betreiber, mit deren Telekommunikationsanlagen **Telekommunikationsdienste für die Öffentlichkeit** erbracht werden. § 3 Abs. 2 TKÜV enthält für bestimmte Gruppen Ausnahmen von der Vorhaltepflcht, unter anderem für Betreiber von Telekommunikationsanlagen, an die nicht mehr als 10'000 Teilnehmer oder sonstige Nutzungsberechtigte angeschlossen sind.

Im 2. Abschnitt der TKÜV sind die **technischen Anforderungen** festgelegt. Der Verpflichtete hat seine Überwachungseinrichtungen so zu gestalten, dass er eine Anordnung **sofort umsetzen** kann (§ 6 Abs. 1 TKÜV). Ausserdem hat er sicherzustellen, dass die Verfügbarkeit seiner Überwachungseinrichtungen der Verfügbarkeit seiner Telekommunikationsanlage entspricht, soweit dies mit vertretbarem Aufwand realisierbar ist (§ 6 Abs. 2 TKÜV).

Die vom Verpflichteten nach § 7 TKÜV **bereitzustellenden Daten** umfassen in Fällen, in denen die Telekommunikation von der zu überwachenden Kennung ausgeht, unter anderem die gewählte Rufnummer und die Telekommunikationsdaten im Rahmen von Anwahlversuchen und unvollständigen Verbindungen. In Mobilfunknetzen gehören dazu auch die Angaben zum Standort des Mobilfunkgerätes mit der grösstmöglichen Genauigkeit, die in dem das Mobilfunkgerät versorgenden Netz für diesen Standort üblicherweise zur Verfügung steht. Diese Daten hat der Verpflichtete der berechtigten Stelle als Überwachungskopie bereitzustellen.

Anforderungen an die **Organisation** und **Schutzanforderungen** werden in Abschnitt 3 der TKÜV aufgestellt. Nach § 12 Abs. 1 TKÜV haben die nach der TKÜV verpflichteten Unternehmen sicherzustellen, dass sie **jederzeit** über das Vorliegen einer Anordnung und die Dringlichkeit ihrer Umsetzung **benachrichtigt werden können**. Innerhalb der üblichen Geschäftszeiten ist die jederzeitige Möglichkeit der Entgegennahme der Anordnung erforderlich. Ausserhalb der üblichen Geschäftszeiten muss eine unverzügliche Entgegennahme sichergestellt werden, spätestens jedoch innerhalb von sechs Stunden nach der Benachrichtigung. Nach § 12 Abs. 2 S. 2 TKÜV hat der Verpflichtete bei einer auf Grundlage einer Telefaxsendung eingerichteten Telekommunikationsüberwachungsmassnahme diese abzuschalten, wenn ihm das Original oder eine beglaubigte Abschrift der Anordnung nicht binnen einer Woche nach Übermittlung der Kopie vorgelegt wird.

Nach § 15 TKÜV darf der Verpflichtete Informationen über **Art und Weise**, wie Überwachungsmassnahmen in seiner Telekommunikationsanlage umgesetzt werden, Unbefugten nicht zugänglich machen. Der Verpflichtete hat zudem nach § 16 Abs. 1 TKÜV sicherzustellen, dass jede Anwendung seiner Überwachungseinrichtungen, die als integraler Bestandteil der Telekommunikationsanlage gestaltet sind, bei der Eingabe der für die technische Umsetzung erforderlichen Taten **automatisch und lückenlos protokolliert** wird. § 16 Abs. 2 TKÜV regelt die spezifischen Anforderungen an die **technische Gestaltung des Zugriffs und Löschfunktionen**, die durch die Verpflichteten sicherzustellen sind.⁹⁸

⁹⁷ Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10) vom 26. Juni 2001 (BGBl. I S. 1254, ber. S. 2298), zuletzt geändert durch Art. 5 G zur Änderung des BundesverfassungsschutzG vom 7. 12. 2011 (BGBl. I S. 2576).

⁹⁸ So ist beispielsweise eine Funktionstrennung dergestalt vorgesehen, dass Personal, welches die Überwachungsmassnahme eingerichtet hat, keine Löschrechte hat.

2.2.3 Technische Richtlinie

§ 110 Abs. 3 TKG stellt des Weiteren die Rechtsgrundlage für den **Erlass einer technischen Richtlinie** durch die Bundesnetzagentur dar, in der technische Einzelheiten, die zur Sicherstellung einer vollständigen Erfassung der zur überwachenden Telekommunikation und zur Auskunftserteilung sowie zur Gestaltung des Übergabezeitpunkts zu den berechtigten Stellen erforderlich sind, festgelegt sind. Ausführungen zum **Regelungsrahmen** der Technischen Richtlinie finden sich derzeit in § 11 TKÜV. Dieser enthält eine Aufzählung verschiedener Paragraphen, zu denen technische Einzelheiten von der Bundesnetzagentur unter Beteiligung der Verbände der Verpflichteten, der berechtigten Stelle sowie der Hersteller der Überwachungseinrichtungen und der Aufzeichnungs- und Auswertungseinrichtungen in einer technischen Richtlinie festgelegt werden sollen. Gleichzeitig soll die Technische Richtlinie an den **Stand der Technik** angepasst werden. Ergänzungen oder Anpassungen an neue Anforderungen erarbeitet die Bundesnetzagentur im Benehmen⁹⁹ mit den berechtigten Stellen und unter Beteiligung der Verbände und der Hersteller. Dabei werden grundsätzlich vorhandene Standards sowie der Stand der Technik berücksichtigt. Aus Transparenzgründen ist die Technische Richtlinie neben der Bekanntgabe im Amtsblatt auf der Internetseite¹⁰⁰ der Bundesnetzagentur **veröffentlicht**.¹⁰¹

3. Kosten und Finanzflüsse

3.1. Rechtsgrundlage für Finanzierung

Während die verpflichteten Telekommunikationsunternehmen nach § 110 Abs. 1 Nr. 1 TKG die technischen Einrichtungen zur Umsetzung gesetzlich vorgesehener Massnahmen zur Überwachung der Telekommunikation auf **eigene Kosten** vorhalten müssen, sieht § 23 Abs. 1 i.V.m. Anlage 3 JVEG¹⁰² die Entschädigung von Telekommunikationsunternehmen vor, soweit von ihnen **Anordnungen** zur Überwachung der Telekommunikation **umgesetzt** oder **Auskünfte erteilt** werden, für die in der Anlage 3 besondere Entschädigungen bestimmt sind.

Im Hinblick auf die Entschädigung wird zwischen der Überwachung der Telekommunikation, der Übermittlung von Bestandsdaten, der Übermittlung von Verkehrsdaten und sonstigen Auskünften unterschieden. Die Entschädigung erfolgt dabei auf der Grundlage eines **Pauschalentschädigungssystems**, das auf dem für die einzelnen Massnahmen üblicherweise erforderlichen **Zeitaufwand** aufbaut.¹⁰³ In den Pauschalen sind bereits sämtliche Nebenkosten enthalten. Eine zusätzliche Entschädi-

⁹⁹ Benehmen bedeutet, dass der anderen Stelle Gelegenheit zur Stellungnahme ohne Bindungswirkung gegeben werden muss.

¹⁰⁰ Verfügbar unter:
http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/TechnischeRegulierung/TechnischeUmsetzungUeberwachung/Downloads/02_ENTWURFTRTKUEV6.2Notifizierung.pdf?__blob=publicationFile (24.05.2012).

¹⁰¹ Bundestagsdrucksache, 16/2581, S. 28, verfügbar unter:
<http://dip21.bundestag.de/dip21/btd/16/025/1602581.pdf> (24.05.2012).

¹⁰² Gesetz über die Vergütung von Sachverständigen, Dolmetscherinnen, Dolmetschern, Übersetzerinnen und Übersetzern sowie die Entschädigung von ehrenamtlichen Richterinnen, ehrenamtlichen Richtern, Zeuginnen, Zeugen und Dritten (Justizvergütungs- und Justizentschädigungsgesetz - JVEG) vom 5. Mai 2004 (BGBl. I S. 718, 776), zuletzt geändert durch Art. 7 Abs. 3 G zur Modernisierung von Verfahren im anwaltl. und notariellen Berufsrecht, zur Errichtung einer Schlichtungsstelle der Rechtsanwaltschaft sowie zur Änd. sonstiger Vorschr. vom 30. 7. 2009, (BGBl. I S. 2449).

¹⁰³ Bundestagsdrucksache 16/7103, S. 6, verfügbar unter:
<http://dip21.bundestag.de/dip21/btd/16/120/1612016.pdf> (24.05.2012.)

gung von Auslagen erfolgt nicht, insbesondere auch keine Umsatzsteuererstattung, auch wenn sie vom herangezogenen Unternehmen an Dritte zu zahlen ist.¹⁰⁴

Anlage 3 (zu § 23 Abs. 1 JVEG)^{105, 106}

Abschnitt 1: Überwachung der Telekommunikation

Nr.	Tätigkeit	Höhe
Die Vorschriften dieses Abschnitts gelten für die Heranziehung im Zusammenhang mit Funktionsprüfungen der Aufzeichnungs- und Auswertungseinrichtungen der berechtigten Stellen entsprechend.		
100	Umsetzung einer Anordnung zur Überwachung der Telekommunikation, unabhängig von der Zahl der dem Anschluss zugeordneten Kennungen: je Anschluss Mit der Entschädigung ist auch der Aufwand für die Abschaltung der Maßnahme entgolten.	100,00 EUR
101	Verlängerung einer Maßnahme zur Überwachung der Telekommunikation oder Umschaltung einer solchen Maßnahme auf Veranlassung der Strafverfolgungsbehörde auf einen anderen Anschluss dieser Stelle Leitungskosten für die Übermittlung der zu überwachenden Telekommunikation: für jeden überwachten Anschluss,	35,00 EUR
102	- wenn die Überwachungsmaßnahme nicht länger als eine Woche dauert	24,00 EUR
103	- wenn die Überwachungsmaßnahme länger als eine Woche, jedoch nicht länger als zwei Wochen dauert	42,00 EUR
104	- wenn die Überwachungsmaßnahme länger als zwei Wochen dauert: je angefangenen Monat (1) Die Nummern 102 bis 104 sind auch bei der Überwachung eines Voice-over-IP-Anschlusses anzuwenden. (2) Leitungskosten werden nur erstattet, wenn die betreffende Leitung innerhalb des Überwachungszeitraums mindestens einmal zur Übermittlung überwachter Telekommunikation an die Strafverfolgungsbehörde genutzt worden ist. Der überwachte Anschluss ist ein ISDN-Basisanschluss:	75,00 EUR
105	- Die Entschädigung nach Nummer 102 beträgt	40,00 EUR
106	- Die Entschädigung nach Nummer 103 beträgt	70,00 EUR
107	- Die Entschädigung nach Nummer 104 beträgt	125,00 EUR
Der überwachte Anschluss ist ein ISDN-Primärmultiplexanschluss:		
108	- Die Entschädigung nach Nummer 102 beträgt	490,00 EUR
109	- Die Entschädigung nach Nummer 103 beträgt	855,00 EUR
110	- Die Entschädigung nach Nummer 104 beträgt	1 525,00 EUR
Der überwachte Anschluss ist ein digitaler Teilnehmeranschluss mit hoher Übertragungsgeschwindigkeit (DSL):		
111	- Die Entschädigung nach Nummer 102 beträgt	65,00 EUR
112	- Die Entschädigung nach Nummer 103 beträgt	110,00 EUR
113	- Die Entschädigung nach Nummer 104 beträgt	200,00 EUR

¹⁰⁴ Binz/Dörndorfer/Petzold/Zimmermann, Kommentar zum Gerichtskostengesetz, 2. Auflage, München 2009, Anlage 3 zu § 23 Abs. 1 JVEG, Rn. 4.

¹⁰⁵ Online verfügbar unter: <http://www.gesetze-im-internet.de/bundesrecht/jveg/gesamt.pdf> (24.05.2012).

¹⁰⁶ **Vorbemerkung zur Anlage 3 JVEG:**

(1) Die Entschädigung nach dieser Anlage schließt alle mit der Erledigung des Ersuchens der Strafverfolgungsbehörde verbundenen Tätigkeiten des Telekommunikationsunternehmens sowie etwa anfallende sonstige Aufwendungen (§ 7 JVEG) ein.

(2) Für Leistungen, die die Strafverfolgungsbehörden über eine zentrale Kontaktstelle des Generalbundesanwalts, des Bundeskriminalamtes, der Bundespolizei oder des Zollkriminalamtes oder über entsprechende für ein Bundesland oder für mehrere Bundesländer zuständige Kontaktstellen anfordern und abrechnen, ermäßigen sich die Entschädigungsbeträge nach den Nummern 100, 101, 300 bis 310, 400 und 401 um 20 Prozent.

Abschnitt 2: Auskünfte über Bestandsdaten

200	Auskunft über Bestandsdaten nach § 3 Nr. 3 TKG, sofern 1. die Auskunft nicht über das automatisierte Auskunftsverfahren nach § 112 TKG erteilt werden kann und die Unmöglichkeit der Auskunftserteilung auf diesem Wege nicht vom Unternehmen zu vertreten ist und 2. für die Erteilung der Auskunft nicht auf Verkehrsdaten zurückgegriffen werden muss: je angefragten Kundendatensatz	18,00 EUR
201	Auskunft über Bestandsdaten, zu deren Erteilung auf Verkehrsdaten zurückgegriffen werden muss: für bis zu 10 in demselben Verfahren gleichzeitig angefragte Kennungen, die der Auskunftserteilung zugrunde liegen Bei mehr als 10 angefragten Kennungen wird die Pauschale für jeweils bis zu 10 weitere Kennungen erneut gewährt. Kennung ist auch eine IP-Adresse.	35,00 EUR

Abschnitt 3: Auskünfte über Verkehrsdaten

300	Auskunft über gespeicherte Verkehrsdaten: für jede Kennung, die der Auskunftserteilung zugrunde liegt Die Mitteilung der die Kennung betreffenden Standortdaten ist mit abgegolten.	30,00 EUR
301	Auskunft über gespeicherte Verkehrsdaten zu Verbindungen, die zu einer bestimmten Zieladresse hergestellt wurden, durch Suche in allen Datensätzen der abgehenden Verbindungen eines Betreibers (Zielwahlsuche): je Zieladresse Die Mitteilung der Standortdaten der Zieladresse ist mit abgegolten.	90,00 EUR
302	Auskunft über gespeicherte Verkehrsdaten für eine von der Strafverfolgungsbehörde benannte Funkzelle (Funkzellenabfrage)	30,00 EUR
303	Auskunft über gespeicherte Verkehrsdaten für mehr als eine von der Strafverfolgungsbehörde benannte Funkzelle: Die Pauschale 302 erhöht sich für jede weitere Funkzelle um	4,00 EUR
304	Auskunft über gespeicherte Verkehrsdaten in Fällen, in denen lediglich Ort und Zeitraum bekannt sind: Die Abfrage erfolgt für einen bestimmten, durch eine Adresse bezeichneten Standort Die Auskunft erfolgt für eine Fläche: – Die Entfernung der am weitesten voneinander entfernten Punkte beträgt nicht mehr als 10 Kilometer: Die Entschädigung nach Nummer 304 beträgt	60,00 EUR
305	– Die Entfernung der am weitesten voneinander entfernten Punkte beträgt mehr als 10 und nicht mehr als 25 Kilometer: Die Entschädigung nach Nummer 304 beträgt	190,00 EUR
306	– Die Entfernung der am weitesten voneinander entfernten Punkte beträgt mehr als 25, aber nicht mehr als 45 Kilometer: Die Entschädigung nach Nummer 304 beträgt	490,00 EUR
307	Liegen die am weitesten voneinander entfernten Punkte mehr als 45 Kilometer auseinander, ist für den darüber hinausgehenden Abstand die Entschädigung nach den Nummern 305 bis 307 gesondert zu berechnen.	930,00 EUR
308	Die Auskunft erfolgt für eine bestimmte Wegstrecke: Die Entschädigung nach Nummer 304 beträgt für jeweils angefangene 10 Kilometer Länge	110,00 EUR
309	Umsetzung einer Anordnung zur Übermittlung künftig anfallender Verkehrsdaten in Echtzeit: je Anschluss Mit der Entschädigung ist auch der Aufwand für die Abschaltung der Übermittlung und die Mitteilung der den Anschluss betreffenden Standortdaten entgolten.	100,00 EUR
310	Verlängerung der Maßnahme im Fall der Nummer 309 Leitungskosten für die Übermittlung der Verkehrsdaten in den Fällen der Nummern 309 und 310:	35,00 EUR
311	– wenn die Dauer der angeordneten Übermittlung nicht länger als eine Woche dauert	8,00 EUR
312	– wenn die Dauer der angeordneten Übermittlung länger als eine Woche, jedoch nicht länger als zwei Wochen dauert	14,00 EUR
313	– wenn die Dauer der angeordneten Übermittlung länger als zwei Wochen dauert: je angefangenen Monat	25,00 EUR
314	Übermittlung der Verkehrsdaten auf einem Datenträger	10,00 EUR

Abschnitt 4: Sonstige Auskünfte

400	Auskunft über den letzten dem Netz bekannten Standort eines Mobiltelefons (Standortabfrage)	90,00 EUR
401	Auskunft über die Struktur von Funkzellen: je Funkzelle	35,00 EUR.

3.2. Entscheidungsstrukturen über Kostentragung einer Überwachung im Einzelfall

Nach § 4 Abs. 1 JVEG erfolgt die **Festsetzung der Entschädigung** der Telekommunikationsunternehmen durch **gerichtlichen Beschluss**, wenn der Berechtigte oder die Staatskasse die gerichtliche Festsetzung beantragt oder das Gericht sie für angemessen hält. Nach § 4 Abs. 6 JVEG können Anträge schriftlich oder zu Protokoll der Geschäftsstelle abgegeben werden.

3.3. Kostenverteilung

Die dem verpflichteten Unternehmen nach § 23 Abs. 1 i.V.m. Anlage 3 JVEG von der Justiz zu erstattende Entschädigung wird von dem **verurteilten Angeklagten** nach Nr. 9005 des Kostenverzeichnisses zum Gerichtskostengesetz¹⁰⁷ (KVGKG) erhoben.¹⁰⁸ In Fällen, in denen es nicht zur Verurteilung kommt, sowie bei Präventivmassnahmen fallen die Kosten der Staatskasse zur Last.

3.4. Finanzierungsmechanismen ausserhalb der einzelnen Verfahren

Nach § 4 Abs. 1 S. 2 JVEG ist eine Vergütung oder Entschädigung von Telekommunikationsunternehmen ausserhalb des § 23 Abs. 1 i.V.m. Anlage 3 JVEG **ausgeschlossen**. Darüber hinaus existieren nach unserer Recherche **keine weiteren Finanzierungsmechanismen**.

¹⁰⁷ Gerichtskostengesetz (GKG) vom 5. Mai 2004 (BGBl. I S. 718), zuletzt geändert durch Art. 10 G über den Rechtsschutz bei überlangen Gerichtsverfahren und strafrechtl. Ermittlungsverfahren vom 24.11.2011 (BGBl. I S. 2302).

¹⁰⁸ MEYER-GÖßNER, Kommentar zur Strafprozessordnung, op.cit., § 100b Rn. 13.

4. Tarifvergleich Schweiz – Deutschland

Schweiz				Deutschland				
Massnahme	Gebühren		Entschädigungen		Massnahme	Gebühren		Entschädigungen
	CHF	Anm.	CHF	Anm.		€	Anm.	Informationsgewinn
TELEFONÜBERWACHUNG AKTIV (Überwachung leitungsvermittelte Fernmeldedienste)	2410	CS 1-3: Nutzinformationen und Verkehrsdaten	1330	Art. 16 lit. a, b und c VÜPF: 1. die verfügbaren Adressierungselemente (Rufnummern der abgehenden und ankommenden Kommunikationsvorgänge), 2. die tatsächliche bekannte Zielrufnummer und die eingeschalteten verfügbaren Rufnummern, falls der Anruf um- oder weitergeleitet wurde, 3. die erzeugten Signale, einschliesslich der Zeichengabe für den Bereitschaftszustand, die Parameter der Fernmeldeanlagen (z.B. IMSI-Nummer, IMEI-Nummer) und die erzeugten Signale für die Aktivierung der Konferenzschaltung oder der Anrufumleitung, 4. bei Mobiltelefonie: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist, 5. das Datum und die Uhrzeit	Überwachung der Telekommunikation (Inhaltsdaten): Def. Telekommunikation nach § 3 Nr. 22 TKG (i.V.m. Nr. 23) technischer Vorgang des Aussendens, Übermittels und Empfangens von Signalen mittels Telekommunikationsanlagen (technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können); Begriff ist entwicklungs offen Bsp: Gespräche mittels Telefon, SMS, MMS, Fax, Bildtelefon, Online-Dienste, Kommunikation im Internet		Gebühren werden im Gesetz nicht gesondert angeführt	100 Anlage 3, Abschnitt 1, Nr. 100: Pauschale für jede Überwachungsanordnung - Gemäss Vorbemerkung zur Anlage 3 JVEG reduziert sich diese um 20 % für Leistungen, die die Strafverfolgungsbehörden über eine zentrale Kontaktstelle des Generalbundesanwalts, Bundeskriminalamts, der Bundespolizei oder des Zollkriminalamts oder eine für ein Bundesland zuständige Kontaktstelle anfordern und abrechnen.

									Nr 102-104: Leistungskosten für die Übermittlung der zu überwachenden Telekommunikation für jeden überwachten Anschluss 24 42 < 1 Woche 75 1-2 Wochen > 2 Wo pro angefangenem Monat Nr. 105-107: der überwachte Anschluss ist ein ISDN-Basisanschluss 40 70 < 1 Woche 125 1-2 Wochen > 2 Wo pro angefangenem Monat Nr. 108-110: der überwachte Anschluss ist ein ISDN-Primärmultiplexanschluss : 490 855 < 1 Woche 1525 1-2 Wochen > 2 Wo pro angefangenem Monat Nr 111-113: der überwachte Anschluss ist ein DSL Anschluss 65 110 < 1 Woche 200 1-2 Wochen > 2 Wo pro angefangenem Monat Nr. 309: 100 in Echtzeit je Anschluss
									Verkehrsdaten Definition Verkehrsdaten nach § 3 Nr. 30 TKG: Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden Bsp.: Rufnr., Zeitpunkt und Dauer der Verbindung, übermittelte Datenmenge, Format der Nachricht

TELEFONÜBERWACHUNG RÜCKWIRKEND	700	CS 4: Historische Verkehrsdaten	540	Art. 16 lit. d VÜPF: 1. die verfügbaren Adressierungselemente (Rufnummern der abgehenden und eingehenden Kommunikationsvorgänge, sofern diese der Fernmeldediensteanbieterin bekannt sind), 2. die Kommunikationsparameter des Endgerätes der Mobiltelefonie und die Parameter zur Teilnehmeridentifikation (wie die IMSI-Nummer und die IMEI-Nummer), 3. bei Mobiltelefonie: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist, 4. das Datum, die Zeit und die Dauer der Verbindung	Auskunft über Vorratsdaten: unzulässig wegen Verfassungswidrigkeit				
	2200	CS 5: Antennensuchlauf (Geografische Koordinaten)	2000	Art. 16 lit. e VÜPF: der Antennensuchlauf: rückwirkende Eruiierung aller an einem bestimmten Standort angefallenen mobilen Kommunikationsvorgänge während eines bestimmten Zeitraumes, sofern es zum Aufbau einer Kommunikation gekommen ist.					
	600	CS 6: Antennensuchlauf (Cell ID)	600	Definition nach Art. 16 lit. e VÜPF (siehe oben)					
INTERNETÜBERWACHUNG (Überwachung paketvermittelte Fernmeldedienste)	4160	PS 1: Nutzinformationen und Verkehrsdaten gem. Art. 24a lit. a und b VÜPF	1330	Art. 24a lit. a und b VÜPF: a. die Übermittlung sämtlicher Daten, die über den überwachten Zugang gesendet oder empfangen werden; b. die Bereitstellung und die simultane oder periodische Übermittlung der folgenden Angaben über den Internetzugang: 1. das Datum und die Uhrzeit,	nicht gesondert angeführt: wie Überwachung der Telekommunikation				

	800	PS 2: Verkehrsdaten gem. Art. 24a lit. b VÜPF	640	zu der die Datenverbindung hergestellt und getrennt wird, 2. die Art der Datenverbindung oder des Anschlusses, 3. die verwendeten Anmeldungsdaten (Log-in), 4. die verfügbaren Adressierungselemente, insbesondere des Ursprungs der Kommunikation, 5. die Kommunikationsparameter der Endgeräte und die Parameter zur Teilnehmeridentifikation (z.B. MAC-Adresse, IMEI-Nummer, IMSI-Nummer), 6. bei Zugang über ein Mobilfunknetz: die Bestimmung und die periodische Übertragung des Zell-Identifikators (Cell ID), des Standortes und der Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person momentan verbunden ist Art. 24a lit. b VÜPF: b. die Bereitstellung und die simultane oder periodische Übermittlung der folgenden Angaben über den Internetzugang: 1. das Datum und die Uhrzeit, zu der die Datenverbindung hergestellt und getrennt wird, 2. die Art der Datenverbindung oder des Anschlusses, 3. die verwendeten Anmeldungsdaten (Log-in), 4. die verfügbaren Adressierungselemente, insbesondere des Ursprungs der Kommunikation, 5. die Kommunikationsparameter der Endgeräte und die Parameter zur Teilnehmeridentifikation (z.B. MAC-Adresse, IMEI-Nummer, IMSI-Nummer),					
--	-----	---	-----	--	--	--	--	--	--

				6. bei Zugang über ein Mobilfunknetz: die Bestimmung und die periodische Übertragung des Zell-Identifikators (Cell ID), des Standortes und der Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person momentan verbunden ist,					
	2410	PS 3: Nutzerinformationen und Verkehrsdaten gem. Art. 24a lit. c VÜPF	1330	7. die technischen Änderungen, die während der Verbindung stattfinden, und, falls bekannt, ihre Ursachen; Art. 24a lit. c VÜPF: die Übermittlung der Nutzinformationen, die über die überwachte Anwendung gesendet oder empfangen werden;					
	800	PS 4: Verkehrsdaten einer Anwendung gem. Art. 24a lit. d VÜPF	640	Art. 24a lit. d VÜPF: die Bereitstellung und die simultane oder periodische Übermittlung folgender Angaben über die überwachte Anwendung: 1. das Datum und die Uhrzeit der Kommunikation (Beginn und Ende), 2. die verfügbaren Adressierungselemente, insbesondere diejenigen des Ursprungs und des Ziels der Kommunikation, 3. die verwendeten Anmeldungsdaten (Log-in), 4. bei der Überwachung von E-Mail-Verkehr: die Umschlaginformationen gemäss dem benutzten Protokoll, 5. die anderen verfügbaren Kommunikationsparameter, 6. die technischen Änderungen während der Kommunikation und ihre Ursachen, falls bekannt.					

	700 250	PS 5: Verkehrsdaten nach Art. 24b lit. a VÜPF - Angaben nach Ziffern 1-6 - Angaben nach Ziffern 2,3,4 und 5 (jede Kombination möglich)	540 250	Art. 24b lit. a VÜPF: a. die Übermittlung der folgenden Angaben über den überwachten Zugang: 1. das Datum und die Uhrzeit, zu der die Datenverbindung hergestellt und getrennt wurde, 2. die Art der Datenverbindung oder des Anschlusses, 3. die verwendeten Anmeldungsdaten (Log-in), 4. die verfügbaren Adressierungselemente, insbesondere des Ursprungs der Kommunikation, 5. die Kommunikationsparameter der Endgeräte und die Parameter zur Teilnehmeridentifikation (z.B. MAC-Adresse, IMEI-Nummer, IMSI-Nummer), 6. bei Zugang über ein Mobilfunknetz: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist.					
	700	PS 6: Benutzeridentifikation des asynchronen Postdienstes nach Art. 24b lit. b VÜPF	540	Art. 24b lit. b VÜPF: b. die Übermittlung der folgenden Angaben bei Versand oder Empfang von Meldungen durch einen asynchronen elektronischen Postdienst: 1. das Datum und die Uhrzeit des Versands oder des Empfangs von Mitteilungen bei der Internetzugangsanbieterin, 2. bei der Überwachung von E-Mail-Verkehr: die Umschlaginformationen gemäss benutztem Protokoll, 3. die IP-Adressen der sendenden und empfangenden Fernmeldeanlagen der asynchronen					

				elektronischen Postdienste, 4. die anderen verfügbaren Adressierungselemente.				
EINFACHE AUSKÜNFTE: Telefon	4	A 0: Basisinformationen wie Rufnr., Teil- nehmeradresse, SIM-Nr.	4		Auskünfte über Bestandsdaten Def. Bestandsdaten gemäss § 3 Nr. 3 TKG: Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsver- hältnisses über Telekommuni- kationsdienste erhoben werden Bsp: Name und Anschrift des Kunden, IP Adresse bei Inter- netkommunikation (statisch + dynamisch)	Gebühren werden im Gesetz nicht gesondert angeführt	18	Nr. 200: sofern nicht auf Verkehrsdaten zurückgegrif- fen werden muss pro Kun- densatz
	360	A1-A4: versch. Angaben zu Fernmeldean- schlüssen	250	Art. 14 Abs. 1 lit. a-c BÜPF: a. Name, Adresse und, sofern vorhanden, Beruf der Teilneh- merin oder des Teilnehmers; b. Adressierungselemente nach Artikel 3 Buchstabe f des Fernmeldegesetzes vom 30. April 1997; c. Art der Anschlüsse Art. 27 Abs. 1 VÜPF: a. bei IP-Adressen: die Art des Anschlusses, das Datum und die Uhrzeit der Zuteilung oder das Datum und die Uhrzeit des Anfangs und gegebenenfalls des Endes des Zuteilungszeit- raumes, den Namen, die Adres- se, die Anmeldungsdaten (Log- in) und, soweit bekannt, den Beruf der Teilnehmerin oder des Teilnehmers, sowie weitere IP-Adressen, die die Internet- zugangsanbieterin dieser oder diesem zugeteilt hat; b. bei EDV-Systemen: sofern verfügbar, zusätzlich die Do- mainnamen und weitere Adressierungselemente unter denen diese der Internetzu- gangsanbieterin bekannt sind.	nicht gesondert angeführt: wie Auskünfte über Bestandsdaten		35	Nr. 201: bis zu 10 angefragte Kennungen; bei mehr als 10 angefragten Kennungen wird die Pauschale für jeweils bis zu 10 weiteren Kennungen erneut gewährt
Internet	10	A 0.1: Basisinformationen Internet	10					

	250	A 0.2 Basisinformation Internet (z.B. Dynamische IP Adresse)	250	c. bei elektronischen Postdiensten, sofern sie von den Internetzugangsanbieterin zur Nutzung durch Kunden eingerichtet sind: soweit bekannt, den Namen, die Adresse und den Beruf der Teilnehmerin oder des Teilnehmers. Art. 14 Abs. 4 BÜPF: Wird eine Straftat über das Internet begangen, so ist die Internet-Anbieterin verpflichtet, der zuständigen Behörde alle Angaben zu machen, die eine Identifikation des Urhebers oder der Urheberin ermöglichen				
ZUSÄTZLICHE KOSTEN: Zusätzliche Pauschalen für Dienstleistungen ausserhalb der Normalarbeitszeit	250	Art. 3 GebV-ÜPF: Für Dienstleistungen, die ausserhalb der Zeit von Montag bis Freitag zw. 8 u 17 Uhr erbracht werden. Die Fallpauschale wird hälftig dem Dienst und den Post- und Fernmelde-dienstanbieterinnen sowie den Internetzugangsanbieterinnen gutgeschrieben.						
Zusätzliche Auslieferung von Datenträgern	125	Art. 3a GebV-ÜPF: Für die Lieferung von zusätzlichen Datenträgern mit bereits ausgelieferten Daten pro Datenträger						
Gebühren für nicht angeführte Dienstleistungen	160	Art. 4 GebV-ÜPF: - Gebühren für nicht angeführte Dienstleistungen werden im Einzelfall nach Zeit- und Sachaufwand nach einem Stundensatz festgelegt. - Kosten für die Bereitstellung von Geräten und Material werden durch den Dienst zusätzlich in Rechnung gestellt.	160	Art. 4a GebV-ÜPF: - Entschädigungen für nicht angeführte Dienstleistungen werden im Einzelfall nach Zeit- und Sachaufwand nach Stundensatz festgesetzt; Entschädigungen werden als Teil der Gebühr nach Art. 4 [GebV-ÜPF] in Rechnung gestellt - Einreichung einer detaillierten Abrechnung ihres Aufwands - Entschädigungen decken 80 % des gesamten Zeit- und Sachaufwands				

C. FRANKREICH

Das Telekommunikationsgeheimnis (*secret des correspondances émises par la voie des communications électroniques*) stellt einerseits ein Verfassungsrecht dar und ist andererseits eine Folge des Rechts auf Privatsphäre. Es wurde von der *Cour de Cassation*¹⁰⁹ und vom *Conseil d'Etat*¹¹⁰ als Grundrecht qualifiziert. Die Menschenrechts- und Bürgerrechtserklärung von 1789 verweist bezüglich dieser Freiheit auf den Artikel 11 der Erklärung, welcher Folgendes festhält: „Die freie Kommunikation von Gedanken und von Meinungen ist eines der wertvollsten Rechte der Menschheit, jeder Bürger darf also sprechen, schreiben und sich frei ausdrücken, ausser es handelt sich um einen im Gesetz beschriebenen Missbrauchsfall dieser Freiheit.“ Ausserdem hat der *Conseil constitutionnel* in einer Entscheidung vom 23. Juli 1999¹¹¹ festgehalten, dass „die Freiheit von Artikel 2 der Menschen- und Bürgerrechtserklärung, wonach das Ziel jeder politischen Vereinigung die Erhaltung der natürlichen und unverjährbaren Rechte des Menschen, also der Freiheit, des Eigentums, der Sicherheit, des Widerstands gegen die Unterdrückung sei, den Respekt der Privatsphäre impliziert“.

Es handelt sich beim Telekommunikationsgeheimnis jedoch nicht um ein absolutes Recht, sondern um ein relatives, welches mit anderen Rechten und/oder Bedürfnissen kombiniert werden muss. Bis zum Inkrafttreten des *loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques* stützte sich die französische Rechtsprechung auf Artikel 81 der Strafprozessordnung (CPP), welcher ganz allgemein festhält, dass der Untersuchungsrichter alle Handlungen vornehmen kann, welche er zur Ermittlung der Wahrheit als notwendig erachtet. Auf der Grundlage dieses Artikels konnten die Untersuchungsrichter lange Zeit Kenntnis von privater Korrespondenz in jeder Form nehmen und diese beschlagnahmen. Zwei Urteile¹¹² des Europäischen Gerichtshofs für Menschenrechte haben Frankreich aufgrund von Art. 8 EMRK gerügt mit der Begründung, dass nur ein öffentlich zugängliches und voraussehbares Gesetz die Privatsphäre (*le secret de la vie privée*) einschränken darf. Der Gesetzgeber hat durch das Verabschieden des *loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques* reagiert. Dieses Gesetz wird durch das *loi n° 2004-669 relative aux communications électroniques et aux services de communication audiovisuelle* abgeändert und durch die *Ordonnance n° 2012-351 du 12 mars 2012* teilweise aufgehoben.¹¹³

Das französische Recht regelt somit heute die Erfassung und die Beschaffung von Daten der elektronischen Kommunikation sowie das Abfangen solcher Kommunikation als eine Ausnahme des Korrespondenzgeheimnisses, welches durch das Gesetz¹¹⁴, die Verfassung¹¹⁵, die EMRK¹¹⁶ sowie durch die universelle Menschenrechtserklärung¹¹⁷ geschützt ist.

¹⁰⁹ Chambre sociale 2. Oktober 2001 - Bull. 2001, V, n° 291, S. 233 (Fall Nikon).

¹¹⁰ *Conseil d'Etat*- 10. und 9. *Sous-sections* vereinigt – 9. April 2004 – Gemeinde von Drancy - n° 263759 – Recueil Lebon.

¹¹¹ Entscheid n° 99-416 DC (Loi portant création d'une couverture maladie universelle).

¹¹² EGMR 24. April 1990, D. 1990, p. 353, note Pradel, RTDH 1990, S.185 obs. G. Cohen-Jonathan.

¹¹³ Siehe Art. 19 (V) der Verordnung.

¹¹⁴ Art. 9 des Code civil, art. 226-15 und 432-9 des Code pénal.

¹¹⁵ Die Universelle Erklärung von 1948 zitiert neben den Rechten des Individuums, diejenigen Rechte auf Privatsphäre. Der *Conseil constitutionnel* bestätigte, dass das Recht auf Privatsphäre von der Freiheit, welche in Art. 2 der Menschen- und Bürgerrechtserklärung von 1789 festgehalten ist, abgeleitet werden kann. Die Rechtsprechung präziserte den Begriff im Laufe der Zeit indem sie auch den Schutz der Korrespondenz darunter fasste. Es ist festzuhalten, dass das Recht auf Privatsphäre explizit durch Art. 9 des Code civil geschützt ist.

¹¹⁶ Art. 8 EMRK.

¹¹⁷ Art. 12.

1. Übersicht über die strafprozessualen Grundlagen der Fernmeldeüberwachung

Die Ausnahmen vom Korrespondenzgeheimnis sind im Rahmen des Gesetzes Nr. 91-646 vom 10. Juli 1991 geregelt sowie in den Bestimmungen des Strafgesetzbuches (*Code pénal*: CP), der Strafprozessordnung (*Code de procédure pénale*: CPP) und im *Code des postes et des communications électroniques* (CPCE). Spezifische Massnahmen finden sich auch im Gesetz über die Innere Sicherheit (*Code de la sécurité intérieure*: CSI), dem Gesetz Nr. 2004-204 vom 9. März 2004 über die neuen Formen der Kriminalität (*Loi n° 2004-204 relative aux nouvelles formes de criminalité*) und dem Gesetz Nr. 2006-64 vom 23. Januar 2006 über die Terrorismusbekämpfung (*Loi n° 2006-64 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*), das durch das Gesetz Nr. 2008-1245 vom 1. Dezember 2008 teilweise verlängert wurde. Verschiedene Dekrete, Verordnungen und Urteile präzisieren die Bestimmungen der oben erwähnten Gesetze.

Die erlaubten Einschränkungen des Korrespondenzgeheimnisses erfüllen zwei Zwecke: die einen dienen dem Funktionieren des Justizsystems, hauptsächlich im Rahmen von **Strafuntersuchungen**, andere betreffen die „**Aufrechterhaltung**“ der **Öffentlichen Ordnung** und der Sicherheit angesichts besonderer Risiken. Die Gesetzgebung beinhaltet demzufolge zwei Arten von Einschränkungen: die einen zu Gunsten der **Justizbehörden**; die andere zu Gunsten der **administrativen Behörde**.

Nach einer Beschreibung der gesetzlichen Definition von „elektronischer Kommunikation“ (1.1), wird die gerichtliche (1.2.) und anschliessend die administrative Aufhebung (1.2.) des Telekommunikationsgeheimnisses behandelt.

1.1 Definition

Artikel L32 CPCE gibt folgende Definition der elektronischen Kommunikation: „Unter elektronischer Kommunikation versteht man das Übermitteln, die Übertragung und den Empfang von Zeichen, Signalen, Schriften, Bildern oder Tönen über den elektromagnetischen Weg“¹¹⁸; diese Aufzählung beinhaltet alle momentan bekannten Fernmeldeleistungen, wie z.B. die Kommunikation via Telefon, oder diejenige via Telekopie, via Fax und via Satellitennetzwerk; das globale Internet und alle damit verbundenen Dienstleistungen, wie z.B. diejenige des elektronischen Nachrichtenaustausches, gelangen also in den Anwendungsbereich der Gesetzgebung zur elektronischen Kommunikation. Die Definition deckt eine grosse Bandbreite von Korrespondenz, welche über moderne Technologien übermittelt wird, und betrifft alle Arten des Abfangens.

1.2 Richterliche Aufhebung des Korrespondenzgeheimnisses

Das Aufheben des Korrespondenzgeheimnisses durch die Justizbehörde ist entweder für die Beschaffung und die Konsultation von Daten (1.2.1) oder für das Abfangen von Daten erlaubt (1.2.2). Das Beschaffen und die Konsultation von Daten sowie das Abfangen stellen im Rahmen der Justizbehörde ein Ermittlungsmittel dar und haben einen repressiven Charakter.

1.2.1. Beschaffen von Daten

Artikel L34-1 CPCE, der die Richtlinie 2006/24/EG umsetzt, erwähnt im Punkt II den Grundsatz des Korrespondenzgeheimnisses indem betont wird, dass die Anbieter von elektronischer Kommunikation die Verpflichtung haben, jegliche Verkehrsdaten zu löschen oder zu anonymisieren. Allerdings

¹¹⁸ „On entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique“.

kann die Anonymisierung für die Dauer eines Jahres aufgeschoben werden (Art. L34-1 III CPCE), sofern dies „für Zwecke der Nachforschung, der Feststellung und der Verfolgung strafrechtlicher Delikte“ notwendig ist und ausschliesslich dem Zweck dient, die Daten der gerichtlichen Behörde zur Verfügung zu stellen. Die Arten von Daten und die Länge der Konversationen sind in Art. R10-12 CPCE geregelt.

1.2.2. Abfangen von Kommunikation

Die allgemeinen Voraussetzungen für das Abfangen von elektronisch übermittelter Korrespondenz durch die richterlichen Behörden sowie die für bestimmte Berufe spezifischen Modalitäten sind hauptsächlich in den Artikeln 100 bis 100-7 CPP geregelt; gewisse Untersuchungsverfahren fallen jedoch unter andere Bestimmungen.

1.2.2.1 Grundsatz

Der Ausdruck « Abfangen von Kommunikation » (*interception de communications*) zielt auf einen **laufenden Kommunikationsaustausch** ab: diese Spontanität ist eine wichtige Voraussetzung der rechtlichen Regelung. Deshalb muss oft ein Kunstgriff angewendet werden um die Auskunft zu bekommen.¹¹⁹ Es handelt sich dabei um eine Ermittlungsmassnahme mit aussergewöhnlichem Charakter (s. auch unten, 2.1.2.1.).

Gemäss Art. 100 CPP sind die Abhörungen denkbar im Bereich des Strafrechts, unter der Voraussetzung, dass die voraussichtliche **Strafe mindestens zwei Jahre Gefängnis beträgt**. Die Massnahme kann nur angeordnet werden, wenn „**die Notwendigkeit der Auskunft dies erfordert**“.

Artikel 100 Abs. 1 CPP bestätigt das Monopol des **Untersuchungsrichters**: nur er ist im Stande, „das Abfangen, die Registrierung und die Transkription von Korrespondenz, welche durch die Telekommunikation übermittelt wird, anzuordnen, sofern dies notwendig ist“. Das Abfangen geschieht unter seiner Anordnung und Kontrolle.

Das Gesetz präzisiert nicht, welche Personen **Gegenstand von solchen Massnahmen** sein können. Daraus folgt – wie das Zirkulationsschreiben vom 26. September 1991 erwähnt –, dass es sich dabei um einen Beschuldigten oder um Dritte handeln kann, welche bei den fraglichen Handlungen beteiligt zu sein scheinen oder welche Informationen über diese Handlungen haben können.

1.2.2.2 Besondere Fälle

Das Gesetz Nr. 2002-1038 vom 9. September 2002 hat, neben den generellen Voraussetzungen von Art. 100 CPP, Artikel 80-4 CPP erlassen. Der Untersuchungsrichter, welcher in diesem Rahmen für das Ermitteln von Todesursachen oder Ermittlungen im Zusammenhang mit verdächtigem Verschwinden (von Minderjährigen oder gewissen Volljährigen) im Sinne von Art. 74 und 74-1 CPP zuständig ist, kann entscheiden, ob das Abfangen von Korrespondenz vorgenommen wird.

Das Gesetz Nr. 2004-204 vom 9. März 2004¹²⁰ bezüglich neuer Formen der Kriminalität enthält eine Ausnahme vom Grundsatz, wonach das Abfangen von Korrespondenz nur im Rahmen der Ermittlungsphase (d.h. nach der Eröffnung des Strafverfahrens) erlaubt ist. Um den Kampf gegen die organisierte Kriminalität zu verbessern kann gemäss Art. 706-95 CPP der Haftrichter (*juge des libertés et de la détention*) einer *Cour de grande instance* auf Antrag des Staatsanwalts das Abfangen, die Re-

¹¹⁹ Crim. 14.04.1999, n°98-97.224, Bull. crim. N°82, D. 1999, somm. 324, obs. J. Pradel, Procédures 1999, comm. n°238, obs. J. Buisson, Dr. Pénal 1999, comm. n°124, obs. A. Maron.

¹²⁰ Modifiée par la loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure

gistrierung oder die Transkription von elektronisch übermittelter Korrespondenz für einen maximalen Zeitraum von 15 Tagen mit der Möglichkeit einer einmaligen Verlängerung erlauben, falls die Notwendigkeit von Ermittlungen *in flagranti* oder von Voruntersuchungen über ein Delikt im Anwendungsbereich von Art. 706-73 CPP (**organisierte Kriminalität**) dies verlangen. Dabei sind die Modalitäten von Art. 100 Abs. 2, 100-1 und 100-3 bis 100-7 CPP anwendbar.

Art. 74-2 CPP, welcher durch das Gesetz vom 9. März 2004 „*portant adaptation de la justice aux évolutions de la criminalité*“ geändert wurde, erlaubt auf Antrag und Information des Staatsanwalts, dass der **Haftrichter** das Abfangen der via Telekommunikation übermittelten Korrespondenz erlaubt. Diese Massnahmen werden unter seiner Anordnung und Kontrolle im Rahmen der Suche nach einer sich auf **der Flucht befindenden Person** angeordnet, und dies für „eine maximale Zeit von zwei Monaten, welche erneut unter den gleichen Form- und Zeitvoraussetzungen, jedoch in diesem Bereich für höchstens sechs Monate, angeordnet werden können“. Das Gesetz definiert drei Arten der sich auf der Flucht befindende Person (Haftbefehl im Untersuchungs- oder im Urteilsverfahren, rechtskräftige Verurteilung zu einer Freiheitsstrafe ohne Bewährung von mindestens einem Jahr).

Schliesslich sieht das Gesetz spezifische Bestimmungen vor, um Personen, deren **Beruf** einem Berufsgeheimnis unterstellt ist, einen bestimmten verstärkten Schutz des Korrespondenzgeheimnisses zu gewähren. Art. 100-7 CPP schreibt vor, welche Bedingungen zu respektieren sind, sofern es sich um einen **Parlamentarier, einen Anwalt oder einen Richter** handelt. In diesen Fällen ist das übergeordnete Organ des betreffenden Berufes zu informieren (z.B. „*le bâtonnier pour les avocats*“ oder der zuständige Präsident der Parlamentarier¹²¹).

1.3 Administrative Aufhebung des Korrespondenzgeheimnisses

Es erscheint angebracht, auf die Spezialgesetzgebung hinzuweisen, welche die Aufhebung des Korrespondenzgeheimnisses **durch Verwaltungsbehörden** aus Gründen der Sicherheit erlaubt: die Beschaffung von Daten (1.3.1) und das Abfangen von elektronischer Kommunikation (1.3.2) sind ein Präventionsmittel, da sie erst vor dem Begehen einer Straftat stattfinden und nur den höchsten Staatsbehörden anvertraut sind.

1.3.1 Beschaffung von Daten

Gemäss Art. L222-2 du CSI, können die entsprechend berechtigten Beamten des Polizeidienstes sowie der nationalen Polizei Einsicht in die von den Telekommunikationsunternehmen aufbewahrten Daten nehmen, mit dem Ziel **Terrorismusanschläge** zu verhindern. Die Einzelheiten sind in Artikel L34-1-1 CPCE geregelt.

1.3.2 Abfangen

Bis zum 1. Mai 2012 waren der II. Titel sowie ein Teil des III. Titels des Gesetzes von 1991 dem Abfangen von Informationen aus Sicherheitsgründen gewidmet. Seit diesem Datum sind die Bestimmungen bezüglich Sicherheitsabfangungen im Gesetz über nationale Sicherheit enthalten (Buch II, Titel IV).

Gemäss Art. L241-2 CSI handelt es sich dabei um ausserordentliche Bewilligungen für Massnahmen, welche Informationen von Belang für die nationale Sicherheit und für die Bewahrung des wirtschaftlichen und wissenschaftlichen Potentials des Landes sowie für die Prävention des Terrorismus und

¹²¹ Modification de la loi n°95-125 du 08.02.1995 ; les parlementaires européens ne bénéficient pas de cette protection : Cass. Crim. 16.03.2005, n°05-80.092, BICC 2005, n°1169, AJ pén. 2005.

der organisierten Kriminalität ermitteln sollen.¹²² Die Einzelheiten sind in den Artikeln R10-15 bis R10-22 CPCE und in Art. L242-1 CSI geregelt.

2. Übersicht über Prozess- und Organisationsstrukturen

2.1 Strafprozessuale Massnahmen

2.1.1 Beschaffung von Daten

Wie bereits erwähnt werden nach Art. L34-1 III CPCE gewisse Daten nicht unmittelbar anonymisiert. Dabei handelt es sich gemäss Art. R10-13 CPCE um Informationen, welche den Nutzer oder den Empfänger von Kommunikation zu identifizieren erlauben sowie um technische Charakteristika, Daten über die Endgeräte und über zusätzliche Dienstleistungen. Die aufbewahrten Daten „können in keinem Fall in irgend einer Form im Rahmen der Kommunikation den Inhalt der ausgetauschten Kommunikation oder konsultierte Informationen wiedergeben“.

Nach Art. 60-2 Abs. 2 CPP kann ein Beamter der *police judiciaire* auf **Geheiss der Staatsanwaltschaft** und nach vorgängiger **Genehmigung des Haftrichters** die Massnahmen anordnen, um für maximal ein Jahr den Inhalt der Informationen zu sichern, welche von Nutzern konsultiert worden waren. Die Anbieter stellen die benötigten Informationen über den Weg der Telematik oder die Informatik fristgerecht zur Verfügung.

Nach Art. 99-3 CPP kann der **Untersuchungsrichter** oder der von ihm angewiesene Beamte der *police judiciaire* auch die Beschaffung von Daten verlangen, welche für die Ermittlungen relevant sein könnten.

2.1.2 Abfangen von elektronischer Kommunikation

2.1.2.1 Bewilligung

Der Untersuchungsrichter ist zuständig um über die Abhörung zu entscheiden. Die Abhörung wird wie bereits erwähnt gemäss Art. 100 CPP unter seiner Kontrolle ausgeführt. Art. 100-2 CPP präzisiert, dass die Dauer dabei nicht **vier Monate** überschreiten darf; diese Massnahme ist jedoch soweit notwendig unter denselben formellen und zeitlichen Voraussetzungen verlängerbar. Diese Voraussetzungen präzisieren den Rahmen solcher Abfangungen. Insbesondere können sie nur anlässlich einer eigentlichen, formell eröffneten Strafuntersuchung (*information judiciaire*) und nicht im Rahmen einer Voruntersuchung oder einer „in flagranti“ Untersuchung stattfinden.

Die Entscheidung des Untersuchungsrichters muss **schriftlich** ergehen, sie muss jedoch nicht begründet sein. Gegen diese Entscheidung kann kein Rechtsmittel ergriffen werden, da sie keinen „richterlichen Charakter“ (*nature juridictionnelle*) hat. Gemäss Art. 100-1 CPP beinhaltet die Entscheidung „alle Identifikationselemente des Abfangverhältnisses, das Vergehen, welches die Massnahme begründet sowie die jeweilige Dauer.“ Die Rechtsnatur der Anordnung einer Abhörungsmassnahme durch den Untersuchungsrichter ist nicht definiert. Es handelt sich entweder um eine Anordnung (*ordonnance*) oder um eine *commission rogatoire*.

¹²²

S. für den Begriff der nationalen Sicherheit: J. PRADEL, Ein Beispiel für die Restauration der kriminellen Legalität: Das Abfangungsregim von Korrespondenz, welche über den Weg der Telekommunikation übermittelt wird, D. 1992, chron. 49, n°12, p. 52 ; für den Begriff *sauvegarde des éléments essentiels du potentiel scientifique et économique de la France* : P. BONFILS & E. GALLARDO, Secret des correspondances, Rép. pén., Dalloz, 2009, S. 29.

Im oben erwähnten Sonderfall von Fall von Art. 80-4 CPP ist auch der Untersuchungsrichter zuständig, die Dauer ist aber auf **zwei Monate** (mit möglicher Verlängerung) beschränkt.

2.1.2.2 Ausführung

Nach Art. 100-3 CPP kann der Untersuchungsrichter (oder ein von ihm beauftragter Beamter der *police judiciaire* sowie gewisse Zollbeamte¹²³) von jedem entsprechend qualifizierten Vertreter einer Abteilung oder eines Organismus unter der Aufsicht oder Verwaltung des für Telekommunikation zuständigen Ministeriums oder von jedem qualifizierten Vertreter eines zugelassenen Netzwerkbetreibers oder Telekom-Dienstleistungsanbieters verlangen, eine Abhöreinrichtung zu installieren.¹²⁴ Nach Art. L32 CPCE kann das entsprechende Eingreifen von „jeder natürlichen oder juristischen Person welche ein öffentliches elektronisches Kommunikationsnetz betreibt oder der Öffentlichkeit eine elektronische Kommunikation anbietet, sowie von den Personen, welche als berufliche Haupt- oder Nebenbeschäftigung der Öffentlichkeit eine *On-Line*-Verbindung durch einen Zugang zum Netz anbieten (insbesondere die ‚cyber-café‘)“ verlangt werden.

Jedes Abfangen und Aufzeichnen von Kommunikation muss in einem **Protokoll** aufgezeichnet werden, das den Beginn und das Ende der Operation mit Datum und Zeit angibt (Art. 100-3 CPP). Die Protokolle werden unter Siegel aufbewahrt.

2.1.2.3 Bearbeitung

Nach Art. 100-5 CPP kann der Untersuchungsrichter oder der von ihm beauftragte Beamte der *police judiciaire* das Gespräch bzw. die Nachricht (*la correspondance*) transkribieren, soweit es für die Ermittlung der Wahrheit nützlich ist. Dabei muss ein Protokoll erstellt werden. Ein Protokoll wird erstellt, und die Transkription wird zu den Verfahrensakten hinzugefügt.

Die Aufzeichnungen werden auf Betreiben der Staatsanwaltschaft nach Verjährung der Strafverfolgung vernichtet. Dabei muss auch für die Zerstörung ein Protokoll erstellt werden.

2.2 Administrative Massnahmen

Der Gesetzgeber ist bestrebt, die Möglichkeit eines Zugangs der öffentlichen Verwaltungsbehörden zu Daten aus elektronischer Kommunikation zu begrenzen: Es bestehen strenge Voraussetzungen sowie eine eigens dafür geschaffene unabhängige Überwachungsbehörde: die ***Commission nationale de contrôle des interceptions de sécurité***.

Da das vorliegende Gutachten auf die strafprozessualen Überwachungsmaßnahmen fokussiert ist, wird das Verfahren nicht im Detail behandelt. Es ist in Art. R10-15 bis R10-22 CPCE geregelt. Nach Art. L242-1 CSI erteilt der **Premierminister** oder eine speziell von ihm dafür delegierte Person die Genehmigung für das Durchführen einer Massnahme. Die Entscheidungen und Genehmigungen unterstehen der Kontrolle der unabhängigen Überwachungsbehörde, deren Zusammensetzung und Funktionsweise in Art. L243-1 bis L243-12 CSI (Kapitel III) geregelt sind.

¹²³ Gemäss Art. 28-1 CPP können gewisse Zollbeamte zum Führen von strafrechtlichen Untersuchungen ermächtigt und berechtigt werden und haben dieselben Berechtigungen wie die *police judiciaire* (Abs. VI).

¹²⁴ Nach Art. 100 CPP und der Rechtsprechung muss der zuständige Vertreter nicht vereidigt werden, s. Crim., 23.05.2006, n°06-81.705, Bull. Crim. N°141, AJ pénal 2006. 413, obs. Roussel.

3. Kosten und Finanzflüsse

3.1. Rechtsgrundlage für Finanzierung

3.1.1 Strafprozessuale Massnahmen

Die Entschädigung der Fernmeldeunternehmen ist im *Code de la poste et des communications électroniques* (CPCE) sowie in der Strafprozessordnung (CPP) geregelt. Nach Art. D98-7 IV CPCE garantiert der Staat dem Unternehmen eine „gerechte Entschädigung“ (*juste rémunération*) für die Vorkehrungen der Betreiber im Zusammenhang mit der Anwendung des *Loi 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques*.

Die „gerechte Entschädigung“ besteht gemäss derselben Bestimmung in der Deckung der folgenden Kosten:

- „a) die Kosten für die Studien, das Ingenieurwesen, die Konzeption und die Installation der Systeme;
- b) die Kosten für den Unterhalt und gegebenenfalls für die Miete der Mittel, welche das Funktionieren der Systeme gewährleisten;
- c) die Kosten für die Bearbeitung der Anfragen.

Die in Anwendung der drei zitierten Buchstaben vom Betreiber getroffene Wahl (der jeweiligen Massnahmen) muss vom für Telekommunikation zuständigen Minister genehmigt werden.

Die Entschädigung gemäss lit. a und b erfolgt im Rahmen einer **Vereinbarung mit dem Staat**. Die Entschädigung gemäss lit. c wird durch **Verordnung (arrêté)** des für Telekommunikation und des für das Budget zuständigen Ministers bestimmt.“

Auch nach Art. L34-1 III CPCE wird der Grundsatz einer Entschädigung der Betreiber vorgesehen, mindestens soweit es um identifizierbare und spezifische Mehrkosten im Zusammenhang mit den für den Staat erbrachten Leistungen in Anwendung dieses Grundsatzes geht. Die Ansätze sowie die weiteren Modalitäten sollen gemäss der zitierten Bestimmung durch den Conseil d'Etat in einem Dekret festgelegt werden.

Die Strafprozessordnung (CPP) enthält verschiedene Bestimmungen über die Tarife. Nach Art. R92 Ziff. 23 CPP werden die Kosten (*frais*) für die Mitteilung der in Anwendung von Art. L34-1 II CPCE aufbewahrten Daten und in Ziffer 24 die mit der Behandlung von Anfragen zum Abfangen der elektronischen Kommunikation verbundenen Kosten (*coûts*) als Kosten der Straf- und Polizeijustiz (*frais de justice*) definiert. In Art. R213-1 und R213-2 CPP wird festgehalten, dass die zwei Arten von Gebühren in Verordnungen (*arrêts*) bestimmt werden.¹²⁵

Es ist Art. A43-9 CPP (geändert u.a. durch den *arrêté du 21 mars 2012 pris en application des articles R. 213-1 et R. 213-2 du code de procédure pénale fixant la tarification applicable aux réquisitions des*

¹²⁵

Art. R213-1 CPP: « Les tarifs relatifs aux frais mentionnés au 23° de l'article R. 92 correspondant à la fourniture des données conservées en application du II de l'article L. 34-1 du code des postes et des communications électroniques sont fixés par un arrêté du ministre de l'économie, des finances et de l'industrie et du garde des sceaux. »

Art. R10-13 titre IV. CPCE: « Les surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture des données relevant des catégories mentionnées au présent article sont compensés selon les modalités prévues à l'article R. 213-1 du code de procédure pénale. »

L'art. R213-2 CPP prévoit la compétence du ministre de la justice et du ministre chargé du budget pour fixer les tarifs pour un remboursement des frais correspondant au traitement des demandes d'interceptions.

opérateurs de communications électroniques en matière de téléphonie, der die Tarife für beide Arten von Massnahmen vorsieht (s. dazu unten, 3.3.1.).

3.1.2 Verwaltungsrechtliche Massnahmen

Für die sicherheitsbedingten Massnahmen sieht Art. R10.21 CPCE in ähnlicher Weise wie Art. R10-13 CPCE (s. oben) vor, dass die identifizierbaren und spezifischen Mehrkosten der Betreiber durch den Staat erstattet werden; die entsprechende Verordnung (*arrêté*) soll gemeinsam durch das Innenministerium und der für das Budget und die elektronischen Kommunikationen zuständigen Ministerien erlassen werden.

3.2. Entscheidstrukturen über Kostentragung einer Überwachung im Einzelfall

3.2.1 Strafprozessuale Massnahmen

Im *Code de procédure pénale* wird bei den Bestimmungen zu den verschiedenen Überwachungs-massnahmen auch angegeben, welche Behörde die Tarife dafür festsetzt. Nach Art. R213-1 CPP ist das **Ministerium für Wirtschaft, Finanzen und Industrie sowie das Justizministerium** zuständig für das Festsetzen der Tarife für die Datenübermittlung. Nach derselben Bestimmung soll der entsprechende Tarif gemäss der Art von Daten und der angeforderten Leistung unterscheiden und den identifizierbaren und spezifischen Mehrkosten der von den richterlichen Behörden für Datenlieferung angefragten Betreiber Rechnung tragen.

Entsprechend wird in Art. R213-2 CPP bestimmt, dass die Tarife für die Überwachungsmassnahmen durch den **Justizminister** und den **für das Budget zuständigen Minister** zu tragen sind.

Ganz grundsätzlich ist zu erwähnen, dass die strafprozessualen Kosten (*frais de justice criminelle, correctionnelle et de police*) grundsätzlich **zu Lasten des Staates** gehen (Art. 800-1 CPP), ausser, bei der verurteilten Person handelt es sich um eine juristische Person. Die Einzelheiten sind in Art. R91 ff. CPP geregelt. So müssen die Kosten von den Parteien (also auch den Untersuchungsbehörden) aufgelistet werden und der „Gerichtsschreiberei“ (*greffe*) des zuständigen Gerichts unterbreitet werden (Art. R222 f. CPP). Diese werden dann der Staatsanwaltschaft (*parquet*) übermittelt, der sie mit seinem Antrag dem zuständigen Magistraten (dem Präsidenten der Gerichtsbarkeit oder einem von ihm delegierter Magistrat) weiterleitet. Dieser setzt die Kosten fest (Art. R226 f. CPP). Gegen die Entscheidung kann ein Rechtsmittel ergriffen werden.

3.2.2 Verwaltungsrechtliche Massnahmen

Für die verwaltungsrechtliche Sicherheitsüberwachung wird auf die obigen Ausführungen (3.1.2.) verwiesen.

3.3. Kostenverteilung

3.3.1. Tarife für Massnahmen im Rahmen einer Strafuntersuchung

Wie bereits erwähnt, enthält Art. A43-9 CPP die Tarife für Kostenerstattung der Anbieter von elektronischer Kommunikation (auf Rechnung und Beleg).¹²⁶ Fehlt ein Tarif, ist der Betrag nach **Kostenvoranschlag** zu bestimmen.

¹²⁶

Art. L32 (15) CPCE: « On entend par opérateur toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques. »

3.3.1.1 Lieferung von Angaben

I. Tarife für Dienstleistungen von Mobiltelefonbetreibern

Art der Angaben	Code	Leistungen	Tarif (in Euro)
Informationen, welche die Identifizierung des Benutzers ermöglichen.	MA 01 MA 03 MA 05 MA 07	Identifizierung nach Anzahl Teilnehmer (<i>Identification en nombre d'abonnés</i>) mit technischen Spezifikationen der Linie, auf der Grundlage ihrer Rufnummer oder SIM-Karte (mit oder ohne Bankdaten), elektronischer, kopierbarer Antrag. Preis pro Rufnummer mit einem Minimum von 20 Nummern.	0,80
	MA 02 MA 04 MA 06 MA 08	Identifizierung eines Teilnehmers (<i>abonné</i>) auf der Grundlage seiner Rufnummer mit den technischen Eigenschaften der Linie oder der Nummer der SIM-Karte (mit oder ohne Bankdaten). Anfrage auf Papier, Fax oder in elektronischer Form (nicht kopierbar).	4,59
	MA 21 MA 22 MA 23	Historische Daten zur Zuteilung einer Rufnummer, einer SIM ¹²⁷ -Karten-Nummer oder der Identifizierungsnummer eines Teilnehmers (IMSI Nummer ¹²⁸).	4,59
	MA 30 MA 31	Identifizierung eines Teilnehmers auf der Grundlage seines Namens oder seiner Firma.	9,69
	MA 40	Identifizierung der Rufnummern und der damit verbundenen Teilnehmer auf der Grundlage der benutzten Zahlungsmittel. Der Tarif beinhaltet die Identifizierung des Teilnehmers.	12,75
	MA 41 MA 42	Identifizierung eines Teilnehmers und der von ihm verwendeten Zahlungsmittel auf der Grundlage einer Rufnummer oder einer SIM-Karten-Nummer. Der Tarif beinhaltet die Identifizierung des Teilnehmers.	12,75
	MA 50	Nachforschung nach der Rufnummer und Identifizierung eines Teilnehmers auf der Grundlage einer IMEI ¹²⁹ -Nummer. Der Tarif beinhaltet die Identifizierung des Teilnehmers.	7,65
	MA 51 MA 52	Nachforschung nach den Identifikatoren des Mobiltelefons (<i>identifiants de téléphone mobile</i>) und Identifizierung des Teilnehmers auf der Grundlage seiner Rufnummer oder einer SIM-Karten-Nummer. Der Tarif beinhaltet die Identifizierung des Teilnehmers.	7,65

¹²⁷ Subscriber Identity Module.

¹²⁸ International Mobile Subscriber Identity.

¹²⁹ International Mobile Equipment Identity.

	MD 10	Kopie des Abonnementvertrags (Lieferung innerhalb eines Monats).	Tarif gemäss Art. R213 CPP ¹³⁰
	MD 11	Kopie der einem Vertrag beiliegenden Dokumente (Lieferung innerhalb eines Monats).	Tarif gemäss Art. R213 CPP
	MD 12	Kopie der Rechnungen (Lieferung innerhalb eines Monats).	Tarif gemäss Art. R213 CPP
Angaben zu den verwendeten Endgeräten ¹³¹	MA 70 MA 71	Angabe des Entsperrungscodes (PUK Code) einer SIM-Karte, welche nach drei erfolglosen Versuchen blockiert ist.	4,59
Technische Angaben und Datum, Zeit und Dauer jeder Kommunikation	MT 10 MT 11 MT 12 MT 14	Verkehrsdaten (<i>détails de trafic</i>) eines Teilnehmers oder eines Endgeräts während eines unteilbaren Zeitraums von 31 Tagen. Die Identifikation des Teilnehmers ist nicht inbegriffen.	9,69 + 1,50 pro Monat
	MT 13	Verkehrsdaten auf der Grundlage einer ausländischen Rufnummer oder auf eine ausländische Nummer, welche sich auf dem Netz des Betreibers in Roaming befindet, während eines unteilbaren Zeitraums von 31 Tagen. Die Identifikation des Teilnehmers ist nicht inbegriffen.	9,69 + 1,50 pro Monat
	MT 20 MT 21 MT 22 MT 24	Verkehrsdaten und Ortung der Endgeräte eines Teilnehmers oder des Endgeräts, verbunden mit der Adresse des Relais (Zelle) über welches die Verbindungen begonnen haben, im unteilbaren Zeitraum von 31 Tagen. Der Preis beinhaltet die Identifizierung aller Zellen, aber nicht die Identifizierung der Teilnehmer.	15,30 + 1,50 pro Monat
	MT 23	Verkehrsdaten mit Ortung der Endgeräte eines Teilnehmers eines ausländischen Anbieters, verbunden mit der Adresse des Relais (Zelle), über welche die Verbindungen begonnen haben, während eines unteilbaren Zeitraums von 31 Tagen. Der Preis beinhaltet die Identifizierung aller Zellen, aber nicht die Identifizierung der Teilnehmer.	15,30 + 1,50 pro Monat
	MT 30	Angaben über die Verbindungen zu einem ausländischen Teilnehmer im unteilbaren Zeitraum von 31 Tagen. Die Identifizierung des Teilnehmers ist nicht inbegriffen.	9,69 + 1,50 pro Monat
	MT 40	Detaillierte Angaben zu den Verbindungen über ein bestimmtes Relais (Zelle) in einem	12,75

130

Art. R213 CPP: « Il est alloué à chaque propriétaire ou dépositaire de documents imprimés, conservés sur support de quelque nature que ce soit, une indemnité de 3,81 euros par réquisition pour l'ensemble des recherches d'archives nécessaires auxquelles il procède et une indemnité de 0,08 euro par page pour les reproductions délivrées de ces documents. »

131

Art. L32 (10) CPCE: « On entend par équipement terminal tout équipement destiné à être connecté directement ou indirectement à un point de terminaison d'un réseau en vue de la transmission, du traitement ou de la réception d'informations. Ne sont pas visés les équipements permettant exclusivement d'accéder à des services de radio et de télévision. »

		Zeitraum von 4 Stunden innerhalb der letzten 12 Monaten. Die Identifizierung der Teilnehmer ist nicht inbegriffen.	
	MT 41	Detaillierte Angaben zu den Verbindungen über ein bestimmtes Relais (Zelle) mit Identifizierung der Teilnehmer in einem Zeitraum von 4 Stunden innerhalb der letzten 12 Monaten.	12,75 + 0,80 pro identifiziertem Teilnehmer
Angaben zu den verlangten oder verwendeten Zusatzdienstleistungen	MA 72	Identifizierung eines Dienstleistungserbringers auf der Grundlage einer Kurznummer.	4,59
	ME 50	Nachforschungen zur Adresse eines Telefonrelais (Zelle) auf der Grundlage seiner Identifikationsnummer.	4,59
	ME 51	Karte mit der optimalen Abdeckung einer Zelle.	9,69
	ME 52	Karte mit der sekundären Abdeckung einer Zelle.	9,69
	ME 53	Nachforschung nach einer Zelle auf der Grundlage einer Ortsangabe (theoretische optimale Abdeckung).	9,69
Angaben, welche die Identifikation der Empfangsperson der Kommunikation erlauben.	MA 60 MA 61 MA 62 MA 63	Nachforschung nach einer Verkaufsstelle auf der Grundlage einer Rufnummer, einer SIM-Karten-Nummer, einer Abonnementnummer (IMSI) oder einer Telefonidentifikationsnummer (IMEI).	6,12

II. Tarife (ohne Steuern) für von **Fixtelefonbetreibern** angeforderte Dienstleistungen

Art der Angaben	Code	Leistungen	Tarif (in Euro)
Information, welche die Identifizierung des Benutzers erlaubt.	FA 01 FA 03	Identifizierung nach Anzahl Teilnehmer (<i>identification en nombre d'abonnés</i>) auf der Grundlage ihrer Rufnummer (mit oder ohne Bankdaten), elektronischer und kopierbarer Antrag. Preis pro Rufnummer mit einem Minimum von 20 Nummern.	0,80
	FA 02 FA 04	Identifizierung eines Teilnehmers (<i>abonné</i>) auf der Grundlage seiner Rufnummer (mit oder ohne Bankdaten) mit den technischen Eigenschaften der Linie. Anfrage auf Papier, Fax oder in elektronischer Form (nicht kopierbar).	6,12
	FE 10	Detaillierte Angaben zu den technischen Eigenschaften der Linie im Hinblick auf eine Überwachung, kopierbare Anfrage in elektronischer Form.	6,12
	FA 05	Nachforschung und Identifizierung eines Teilnehmers, der über eine Vermittlungsstelle (<i>tête de ligne</i>) oder einen Server anruft.	15,30
	FA 06	Historische Daten zur Zuteilung einer Nummer.	6,12

	FA 07		
	FA 10 FA 11	Identifizierung eines Teilnehmers auf der Grundlage des Namens oder der Firma und Filter nach anderen Kriterien.	15,30
	FA 20	Identifizierung eines Teilnehmers auf der Grundlage der Adresse der Telefoninstallation.	15,30
	FA 30	Identifizierung einer Verkaufsstelle (<i>point de vente</i>) auf der Grundlage einer Prepaid-Karte.	15,30
	FA 31	Identifizierung einer Prepaid-Karte und einer angerufenen Nummer.	13,44 pro Nummer
	FA 40	Nachforschung nach der Rufnummer und Identifizierung eines Teilnehmers auf der Grundlage der Zahlungsart (<i>moyen de paiement</i>). Die Kosten für die Identifizierung des Teilnehmers sind inbegriffen.	15,30
	FA 41	Identifizierung des Teilnehmers und seiner Zahlungsart auf der Grundlage einer Rufnummer. Die Kosten für die Identifizierung des Teilnehmers sind inbegriffen.	15,30
	FA 51	Identifizierung eines Teilnehmers sowie dessen Internetzugangsanbieters.	6,12
	FD 10	Kopie des Abonnementvertrags (Lieferung innerhalb eines Monats).	Tarif gemäss Art R213 CPP
	FD 11	Kopie der einem Vertrag beiliegenden Dokumente (Lieferung innerhalb eines Monats).	Tarif gemäss Art. R213 CPP
	FD 12	Kopie der Rechnungen (Lieferung innerhalb eines Monats).	Tarif gemäss Art. R213 CPP
Angaben zu den verwendeten Endgeräten	FA 21	Identifizierung der öffentlichen Sprechstellen (Telefonzellen) innerhalb einer gegebenen geographischen Zone.	15,30
	FA 50	Nachforschung nach einem Drittanbieter auf der Grundlage seiner Bündelnummer (<i>numéro de faisceau</i>).	9,69
Technische Eigenschaften sowie Datum, Zeit und Dauer der Kommunikation	FT 10	Details über eingehende und ausgehende Verbindung eines Teilnehmers innerhalb eines unteilbaren Zeitraums von 31 Tagen. Die Identifizierung des Teilnehmers ist zusätzlich.	15,30 + 1,50 pro Monat
	FT 20	Details über die Verbindungen in Bezug auf einen Teilnehmer eines ausländischen Anbieters in einem unteilbaren Zeitraum von 31 Tage.	15,30 + 1,50 pro Monat
	FT 21	Detaillierte Angaben zu den Verbindungen eines Teilnehmers mit einem Server.	16,00
	FT 40	Detaillierte Angaben in Bezug auf die Verbindung einer Prepaid-Karte.	15,30 + 1,50 pro Monat

3.3.1.2 Überwachungsmassnahmen (Interception)

Art der Angaben	Code	Leistungen	Tarif (in Euro)
Abfangen der Kommunikation auf fixen Linien	FI 20 FI 21 FI 22	Der Tarif beinhaltet das Liefern einer Übersicht über die Kommunikationen am Ende der Massnahme.	24,00
Vorläufige Weiterleitungslinie	FI 10	Einrichten und Installieren einer vorübergehenden analogen Weiterleitungslinie sowie die monatliche Abonnementsgebühr.	120,00 + 45,50 pro Monat
	FI 11	Einrichten und Installieren einer vorübergehenden digitalen (Grundzugang ISDN) Weiterleitungslinie sowie die monatliche Abonnementsgebühr.	217,50 + 45,50 pro Monat
Weiterleitungssonde (sonde de renvoi)	FI 17	Installation und Entfernen der Sonde ausserhalb der Weiterleitungslinie.	350,00
Gemietete Weiterleitungslinien ¹³²	FI 12 FI 13	Zusätzlich zu den fixen Zugangskosten, für die Verbindungen von höchstens 10 km, Abonnement pro unteilbarem Zeitraum von 31 Tagen: $1,1 \times (37,77 \text{ €} + 0,79 \text{ € pro km})$.	497,00 für die fixen Zusatzkosten (abgesehen von bereits eingerichteten Standorten)
		Zusätzlich zu den fixen Zugangskosten, für die Verbindungen von mehr als 10 km, Abonnement pro unteilbarem Zeitraum von 31 Tagen: $1,1 \times (60,10 \text{ €} + 0,08 \text{ € pro km})$.	
Abfangen von Voice-mail Kommunikation auf IP ¹³³	FI 23	Der Tarif beinhaltet das Liefern einer Übersicht über die Kommunikationen am Ende der Massnahme.	24,00
Abfangen von Kommunikation auf internationaler Ebene	FI 27	Der Tarif beinhaltet das Liefern einer Übersicht über die Kommunikationen am Ende der Massnahme.	24,00
Abfangen von mobiler Telefonkommunikation	MI 20	Der Tarif beinhaltet das Liefern einer Übersicht über die Kommunikationen am Ende der Massnahme.	24,00
Verfolgen der Verbindungen.	MS 14	Echtzeitübermittlung der getätigten und erhaltenen Anrufe mit dem Code der von einem überwachten Mobiltelefon aktivierten Zelle. Die Leistung enthält die Ortung, die Installation und einen chronologischen Überblick.	17,50 pro Nummer + 17,50 pro Monat

¹³² Article R*9 Abs. 1 CPCE : «On entend par 'liaison louée' la mise à disposition par un opérateur d'une capacité de transmission entre des points de terminaison déterminés d'un réseau ouvert au public, au profit d'un utilisateur, à l'exclusion de toute commutation contrôlée par cet utilisateur.»

¹³³ Internet Protocol.

3.3.2. Tarif für Sicherheitsmassnahmen

Wie bei den strafprozessualen Massnahmen ist auch bei der verwaltungsrechtlichen Sicherheitsüberwachung die Entschädigung für die Instandhaltungs- und Einrichtungskosten gemäss einer besonderen Vereinbarung vorgesehen (Art. D98-7 CPCE). Abgesehen davon wurden die Tarife durch zwei Verordnungen (*arrêté*) vom 26. März 2012 festgesetzt, die eine in Anwendung von Art. R10-21 CPCE, anwendbar auf die Lieferung von Daten gemäss Art. L23-1-1- CPCE, die andere in Anwendung von Art. D98-7 CPCE, anwendbar auf die Sicherheitsabhörungen. Die beiden Tarife sind ähnlich aufgebaut wie diejenigen der strafprozessualen Massnahmen, sehen aber leicht andere Sätze vor. Ein Ersatz gemäss den Tarifen erfolgt jeweils gegen Rechnung und gegen Vorlage von Belegen.

Da das vorliegende Gutachten in erster Linie auf strafprozessuale Massnahmen und deren Kosten begrenzt ist, wird auf eine detaillierte Auflistung der Tarife verzichtet.

3.4. Finanzierungsmechanismen ausserhalb der einzelnen Verfahren

Ausserhalb der beschriebenen Tarife bestehen noch zwei weitere Finanzierungsmechanismen. So werden wie bereits erwähnt die Kosten für die Dienstleistungen der Betreiber gemäss Art. D98-7 IV lit. a und b CPCE¹³⁴ (**Installations- und Instandhaltungskosten**) gemäss Vereinbarungen mit den Betreibern erstattet. Andere Kosten, welche nicht auf den Tarif Tabellen aufgeführt sind, werden gemäss Kostenvoranschlag erstattet.

¹³⁴

« IV. - L'Etat garantit à l'opérateur une juste rémunération des dispositions prises par ce dernier au titre du III du présent article. La juste rémunération de l'opérateur correspond à la couverture :

- a) Des coûts exposés pour les études, l'ingénierie, la conception et le déploiement des systèmes demandés au titre du III du présent article ;
- b) Des coûts liés à la maintenance et, le cas échéant, à la location des moyens permettant le fonctionnement des systèmes demandés au titre du III du présent article ;

(...) La rémunération de l'opérateur au titre du a et du b est assurée dans le cadre d'une convention signée avec l'Etat.

4. Tarifvergleich Schweiz - Frankreich

Schweiz					Frankreich				
Massnahme	Gebühren		Entschädigungen		Massnahme	Gebühren		Entschädigungen	
	CHF	Anm.	CHF	Anm.		€	Anm.	€	Informationsgewinn
TELEFONÜBERWACHUNG AKTIV (Überwachung leitungsvermittelte Fern- meldedienste)	2410	CS 1-3: Nutzinformationen und Ver- kehrsdaten	1330	Art. 16 lit. a, b und c VÜPF: 1. die verfügbaren Adressierungs- elemente (Rufnummern der abge- henden und ankommenden Kommu- nikationsvorgänge), 2. die tatsächliche bekannte Zielruf- nummer und die eingeschalteten verfügbaren Rufnummern, falls der Anruf um- oder weitergeleitet wurde, 3. die erzeugten Signale, einschliess- lich der Zeichengabe für den Bereit- schaftszustand, die Parameter der Fernmeldeanlagen (z.B. IMSI- Nummer, IMEI-Nummer) und die erzeugten Signale für die Aktivierung der Konferenzschaltung oder der Anrufumleitung, 4. bei Mobiltelefonie: den Zell- Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist, 5. das Datum und die Uhrzeit	Telefonüberwachung (inter- ception de téléphonie): Arret 43-9 CPP regelt die Entschädigungen in Tarifsta- bellen; die Auskünfte über Daten nach Anlage III (Tarifs appli- cables aux interceptions de téléphonie) beziehen sich auf aktive und zukünftige Überwachungen		Gebühren werden im Gesetz nicht gesondert angeführt	24	FI 20, 21, 22 Inhaltsdaten einer Überwa- chung eines Festnetzanschlusses (<i>fourniture d'un détail de communication</i>)
									FI 10, 11: Einrichtung einer " ligne tempo- raire de renvoi ": - 120 + 45,50/Monat - 217,50 + 45,50/Monat 350 497 FI 17" Sonde de Renvoi ": Einrichtung und Entfernen der Sonde FI 12, 13: Miete für die technische Ausrüs- tung eines Telekommunikationsbetreibers inkl Zugang zu den Verbindungen - innerhalb 10 km - über 10 km

TELEFONÜBERWACHUNG RÜCKWIRKEND	700	CS 4: Historische Verkehrsdaten	540	Art. 16 lit. d VÜPF: 1. die verfügbaren Adressierungselemente (Rufnummern der abgehenden und eingehenden Kommunikationsvorgänge, sofern diese der Fernmeldediensteanbieterin bekannt sind), 2. die Kommunikationsparameter des Endgerätes der Mobiltelefonie und die Parameter zur Teilnehmeridentifikation (wie die IMSI-Nummer und die IMEI-Nummer), 3. bei Mobiltelefonie: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist, 4. das Datum, die Zeit und die Dauer der Verbindung	Auskunft über Verkehrsdaten (détail de trafic)			24 - 9,69 + 1,50/Monat - 15,30 + 1,50/Monat	MI 20 Inhalts- und Bestandsdaten für die Überwachung eines Mobiltelefons - MT 10, 11, 12, 14: Verkehrsdaten für 31 Tage - MT 20, 21, 22, 24: Verkehrsdaten, benutzte Kommunikationsmittel und lokalisierte Adressen (<i>localisation des équipements terminaux, accompagné de l'adresse du relais téléphonique</i>)
	2200	CS 5: Antennensuchlauf (Geografische Koordinaten)	2000	Art 16 lit. e VÜPF: der Antennensuchlauf: rückwirkende Eruiierung aller an einem bestimmten Standort angefallenen mobilen Kommunikationsvorgänge während eines bestimmten Zeitraumes, sofern es zum Aufbau einer Kommunikation gekommen ist.	Auskunft über historische Verkehrsdaten			12,75 (+ 0,80)	MT 40: historische Verkehrsdaten für 4 Stunden in den letzten 12 Monaten (+ Identifikation des Teilnehmers)
	600	CS 6: Antennensuchlauf (Cell ID)	600	Definition nach Art 16 lit. e VÜPF (siehe oben)					
INTERNETÜBERWACHUNG (Überwachung paketvermittelte Fernmeldedienste)	4160	PS 1: Nutzinformationen und Verkehrsdaten gem. Art. 24a lit. a und b VÜPF	1330	Art. 24a lit. a und b: a. die Übermittlung sämtlicher Daten, die über den überwachten Zugang gesendet oder empfangen werden; b. die Bereitstellung und die simul-	nicht gesondert angeführt: nach unseren Recherchen beziehen sich die Auskünfte in Anlage I-III auch auf Daten zur Internetüberwachung				

	800	PS 2: Verkehrsdaten gem. Art. 24a lit. b VÜPF	640	tane oder periodische Übermittlung der folgenden Angaben über den Internetzugang: 1. das Datum und die Uhrzeit, zu der die Datenverbindung hergestellt und getrennt wird, 2. die Art der Datenverbindung oder des Anschlusses, 3. die verwendeten Anmeldungsdaten (Log-in), 4. die verfügbaren Adressierungselemente, insbesondere des Ursprungs der Kommunikation, 5. die Kommunikationsparameter der Endgeräte und die Parameter zur Teilnehmeridentifikation (z.B. MAC-Adresse, IMEI-Nummer, IMSI-Nummer), 6. bei Zugang über ein Mobilfunknetz: die Bestimmung und die periodische Übertragung des Zell-Identifikators (Cell ID), des Standortes und der Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person momentan verbunden ist Art. 24a lit b: b. die Bereitstellung und die simultane oder periodische Übermittlung der folgenden Angaben über den Internetzugang: 1. das Datum und die Uhrzeit, zu der die Datenverbindung hergestellt und getrennt wird, 2. die Art der Datenverbindung oder des Anschlusses, 3. die verwendeten Anmeldungsdaten (Log-in), 4. die verfügbaren Adressierungselemente, insbesondere des Ursprungs der Kommunikation, 5. die Kommunikationsparameter der Endgeräte und die Parameter zur Teilnehmeridentifikation (z.B. MAC-Adresse, IMEI-Nummer, IMSI-Nummer),					auf Kostenvoranschlag
--	-----	---	-----	---	--	--	--	--	-----------------------

				6. bei Zugang über ein Mobilfunknetz: die Bestimmung und die periodische Übertragung des Zell-Identifikators (Cell ID), des Standortes und der Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person momentan verbunden ist, 7. die technischen Änderungen, die während der Verbindung stattfinden, und, falls bekannt, ihre Ursachen; Art. 24a lit. c VÜPF: die Übermittlung der Nutzinformationen, die über die überwachte Anwendung gesendet oder empfangen werden; Art. 24a lit. d VÜPF: die Bereitstellung und die simultane oder periodische Übermittlung folgender Angaben über die überwachte Anwendung: 1. das Datum und die Uhrzeit der Kommunikation (Beginn und Ende), 2. die verfügbaren Adressierungselemente, insbesondere diejenigen des Ursprungs und des Ziels der Kommunikation, 3. die verwendeten Anmeldungsdaten (Log-in), 4. bei der Überwachung von E-Mail-Verkehr: die Umschlaginformationen gemäss dem benutzten Protokoll, 5. die anderen verfügbaren Kommunikationsparameter, 6. die technischen Änderungen während der Kommunikation und ihre Ursachen, falls bekannt.					
	2410	PS 3: Nutzerinformationen und Verkehrsdaten gem. Art. 24a lit. c VÜPF	1330						
	800	PS 4: Verkehrsdaten einer Anwendung gem. Art. 24a lit. d VÜPF	640						

	700 250	PS 5: Verkehrsdaten nach Art. 24b lit. a VÜPF - Angaben nach Ziffern 1-6 - Angaben nach Ziffern 2,3,4 und 5 (jede Kombination möglich)	540 250	Art. 24b lit. a VÜPF: a. die Übermittlung der folgenden Angaben über den überwachten Zugang: 1. das Datum und die Uhrzeit, zu der die Datenverbindung hergestellt und getrennt wurde, 2. die Art der Datenverbindung oder des Anschlusses, 3. die verwendeten Anmeldungsdaten (Log-in), 4. die verfügbaren Adressierungselemente, insbesondere des Ursprungs der Kommunikation, 5. die Kommunikationsparameter der Endgeräte und die Parameter zur Teilnehmeridentifikation (z.B. MAC-Adresse, IMEI-Nummer, IMSI-Nummer), 6. bei Zugang über ein Mobilfunknetz: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist.					
	700	PS 6: Benutzeridentifikation des asynchronen Postdienstes nach Art. 24b lit. b VÜPF	540	Art. 24b lit. b VÜPF: b. die Übermittlung der folgenden Angaben bei Versand oder Empfang von Meldungen durch einen asynchronen elektronischen Postdienst: 1. das Datum und die Uhrzeit des Versands oder des Empfangs von Mitteilungen bei der Internetzugangsanbieterin, 2. bei der Überwachung von E-Mail-Verkehr: die Umschlaginformationen gemäss benutztem Protokoll, 3. die IP-Adressen der sendenden und empfangenden Fernmeldeanlagen der asynchronen elektronischen Postdienste, 4. die anderen verfügbaren Adressierungselemente.					

EINFACHE AUSKÜNFTE: Telefon	4	A 0: Basisinformationen wie Rufnr., Teilnehmeradresse, SIM-Nr.	4		Auskünfte über Identifikationsdaten ("information permettant d'identifier l'utilisateur"): der Erlass (arrêté) differenziert hierbei - nach Art der Ausgangsinformation (ausgehend von einer Telefonnr, Rechnungsinformation etc.) - sowie Art der Leitung (téléphonie mobile Code Mx /téléphonie fixe: Code Fx) Bsp: Name, Vorname, Adresse, Beruf (Art R10-3 CPCE) Die Daten werden sehr genau differenziert, und hier auszugsweise wiedergegeben. Für eine detaillierte Differenzierung sei auf den Länderbericht verwiesen. - Auskünfte über Internet sind nicht gesondert angeführt, die Liste bezieht sich daher auf die genannten Kategorien			0,80 (x 20)	MA 01, 03, 05, 07 + FA 01, FA 03: Identifikationsdaten inkl. technische Details der Leitung ausgehend von Telefonnummer oder Nummer der SIM Karte für mind 20 Teilnehmer der selben SIM (die einer jurist. Person zugeordnet ist) - MA 02, 04, 06, 08: für einen Teilnehmer einer <i>ligne mobile</i> - FA 02, 04: für einen Teilnehmer einer <i>ligne fixe</i>
	360	A1-A4: versch. Angaben zu Fernmeldeanschlüssen	250	Art. 14 Abs. 1 lit. a-c BÜPF: a. Name, Adresse und, sofern vorhanden, Beruf der Teilnehmerin oder des Teilnehmers; b. Adressierungselemente nach Artikel 3 Buchstabe f des Fernmeldegesetzes vom 30. April 1997; c. Art der Anschlüsse				4,59 6,12	
								9,69 15,30 12,75 15,30	MA 30, 31: Identifikation ausgehend vom Namen der Person oder Gesellschaft - FA 10, 11: für Teilnehmer einer <i>ligne fixe</i> MA 40: Teilnehmersauskunft und angerufene Nummern ausgehend von benutztem Zahlungsmittel - FA 40: für <i>ligne fixe</i>

Internet	10	A 0.1: Basisinformationen Internet	10	Art. 27 Abs. 1 VÜPF: a. bei IP-Adressen: die Art des Anschlusses, das Datum und die Uhrzeit der Zuteilung oder das Datum und die Uhrzeit des Anfangs und gegebenenfalls des Endes des Zuteilungszeitraumes, den Namen, die Adresse, die Anmeldungsdaten (Log-in) und, soweit bekannt, den Beruf der Teilnehmerin oder des Teilnehmers, sowie weitere IP-Adressen, die die Internetzugangsanbieterin dieser oder diesem zugeteilt hat; b. bei EDV-Systemen: sofern verfügbar, zusätzlich die Domain-namen und weitere Adressierungselemente unter denen diese der Internetzugangsanbieterin bekannt sind c. bei elektronischen Postdiensten, sofern sie von den Internetzugangsanbieterin zur Nutzung durch Kunden eingerichtet sind: soweit bekannt, den Namen, die Adresse und den Beruf der Teilnehmerin oder des Teilnehmers.				7,65	MA 50: Teilnehmersauskunft und angerufene Nummern ausgehend von der IMEI Nummer
	250	A 0.2 Basisinformation Internet (z.B. Dynamische IP Adresse)	250	Art. 14 Abs. 4 BÜPF: Wird eine Straftat über das Internet begangen, so ist die Internet Anbieterin verpflichtet, der zuständigen Behörde alle Angaben zu machen, die eine Identifikation des Urhebers oder der Urheberin ermöglichen				jeweils 3,81 + 0,08 pro Seite	jeweils für ein Monat: MD 10/FD10: Vertragskopie MD 11/FD 11: Kopie über die Anlagen zum Vertrag MD 12/FD 12: Rechnungskopien
								4,59 6,12 15,30 13,44 / Nummer 15,30 6,12	MA 70, 71: Auskunft über PUK Code FE 10 Auskunft über technische Informationen der zu überwachenden Leitung FA 20: Teilnehmersauskunft ausgehend von der Adresse der Telefonanlage FA 31: Identifikation einer Wertkarte und einer angerufenen Nummer FA 41: Teilnehmeridentifikation und Auskunft über Zahlungsmethode ausgehend von einer Telefonnummer FA 51: Identifikation eines ADSL Teilnehmers

ZUSÄTZLICHE KOSTEN: Zusätzliche Pauschalen für Dienstleistungen ausserhalb der Normalarbeitszeit	250	Art. 3 GebV-ÜPF: Für Dienstleistungen, die ausserhalb der Zeit von Montag bis Freitag zwischen 8 und 17 Uhr erbracht werden Fallpauschale wird hälftig dem Dienst und den Post- und Fernmeldedienstanbieterinnen sowie den Internetzugangsanbieterinnen gutgeschrieben.							
Zusätzliche Auslieferung von Datenträgern	125	Art. 3a GebV-ÜPF Für die Lieferung von zusätzlichen Datenträgern mit bereits ausgelieferten Daten pro Datenträger						-	Die Tariftabellen und die im Gutachten erwähnten gesetzlichen Grundlagen der Telekommunikationsüberwachung enthalten keine diesbezüglichen Informationen
Gebühren für nicht aufgeführte Dienstleistungen	160	Art. 4a GebV-ÜPF: - Gebühren für nicht angeführte Dienstleistungen werden im Einzelfall nach Zeit- und Sachaufwand nach einem Stundensatz festgelegt - Kosten für die Bereitstellung von Geräten und Material werden durch den Dienst zusätzlich in Rechnung gestellt	160	Art. 4a GebV-ÜPF: - Entschädigungen für nicht angeführte Dienstleistungen werden im Einzelfall nach Zeit- und Sachaufwand nach Stundensatz festgesetzt; Entschädigungen werden als Teil der Gebühr nach Art. 4 [GebV-ÜPF] in Rechnung gestellt - Einreichung einer detaillierten Abrechnung ihres Aufwands - Entschädigungen decken 80 % des gesamten Zeit- und Sachaufwands	Gebühren für nicht aufgeführte Dienstleistungen			- eventuell auf Kostenvoranschlag	- Die französischen Tariftabellen sind sehr detailliert und enthalten keine Pauschalkategorie für nicht angeführte Leistungen.

D. ITALIEN

1. Übersicht über die strafprozessualen Grundlagen der Fernmeldeüberwachung

Die italienische Rechtsordnung versteht die Fernmeldeüberwachung als **richterlich anzuordnende** Massnahme. Artikel 15 der Verfassung der Republik Italien (ItVerf.) hält einen entsprechenden Gesetzes- und Gerichtsvorbehalt fest:

«Die Freiheit und das Geheimnis des Schriftverkehrs und jeder anderen Form der Mitteilung sind unverletzlich.

Ihre Einschränkung darf nur auf Grund einer begründeten Verfügung der Gerichtsbehörde unter gesetzlich bestimmten Garantien erfolgen.»

Anders als in anderen Ländern¹³⁵ darf die Kriminalpolizei keinerlei Fernmeldeüberwachungen durchführen.¹³⁶ Für den Schutz der Vertraulichkeit und der Privatsphäre¹³⁷ sind ausschliesslich die **Gerichte** zuständig; diesen ist der Schutz der Grundrechte verfassungs- und definitionsgemäss anvertraut, wobei sie einzig dem Gesetz verpflichtet sind.¹³⁸

Die Fernmeldeüberwachung ist zur Hauptsache in der **italienischen Strafprozessordnung** (itStPO)¹³⁹ geregelt. Ausnahmen sind vorgesehen, um den Einsatz der Fernmeldeüberwachung in Fällen von organisiertem Verbrechen und Terrorismus zu vereinfachen.¹⁴⁰ Nebst der Überwachung zur Fortführung der Ermittlungen gibt es auch **präventive Überwachungsmassnahmen**,¹⁴¹ deren Anordnung keiner gerichtlichen Kontrolle bedarf. Diese Massnahmen dienen ausschliesslich Fahndungszwecken und die so gewonnen Informationen dürfen nicht in einem Strafverfahren berücksichtigt werden.

1.1. Der Begriff der Fernmeldeüberwachung

Das Abhören von Gesprächen und Mitteilungen¹⁴² ist ein **Mittel zur Beweisführung**, d.h. die Gerichtsbehörden **ermitteln und sichern** dadurch Beweise zur Belegung von Handlungen, die sich auf Zurechnung, Strafbarkeit und Strafzumessung beziehen.¹⁴³ Der Gesetzgeber regelt die Telefon-,¹⁴⁴

¹³⁵ Vgl. neben den Länderberichten auch die Ausführungen des Senats, wonach die (unterschiedlichen Formen) der Fernmeldeüberwachung vorwiegend in die Zuständigkeit von Verwaltungs- oder Polizeibehörden fallen, wenn nicht gar allein den Nachrichtendiensten vorbehalten sind. Senat der Republik, S. 15. Legislaturperiode, Parlamentsunterlagen, Dokument XVII Nr. 2, gutgeheissen von der Justizkommission in der Sitzung vom 29.11.2006 im Anschluss an die zur Telefonüberwachung, S. 22 f., verfügbar unter

<http://www.senato.it/service/PDF/PDFServer?tipo=BGT&id=230367>.

¹³⁶ SIRACUSANO et al., Diritto processuale penale, Bd I, Mailand 2006, S. 407.

¹³⁷ Diese Rechte sind auch durch Art. 8 EMRK umfassend geschützt, vgl. dazu DI MASI, Le intercettazioni tra frizioni interne e giurisprudenza della Corte di Strasburgo, in Diritto penale e processo, 9/2011, 1159 ff.

¹³⁸ Art. 101 Abs. 2 ItVerf.

¹³⁹ Art. 266-271 itStPO.

¹⁴⁰ APRILE & SPIEZIA, Le intercettazioni telefoniche ed ambientali, Mailand 2004, S. 1, 2, 87.

¹⁴¹ Art. 226 der Durchführungsbestimmungen ItStPO; Art. 5 Gesetzesdekret Nr. 374 vom 18.10.2001, umgewandelt in Gesetz Nr. 438 vom 15.12.2001; vgl. dazu VIRGILIO, Il nuovo regime delle intercettazioni preventive, in La Giustizia penale 2002, III, 545.

¹⁴² Abschnitt IV 3. Titel (Mittel zur Beweisführung) 3. Buch (Beweise) der italienischen Strafprozessordnung (itStPO).

¹⁴³ SIRACUSANO et al., Diritto processuale penale, Bd I, Mailand 2006, 400.

¹⁴⁴ Art. 266 Abs. 1 itStPO.

Gesprächs-,¹⁴⁵ Informatik- und Fernübertragungsüberwachung,¹⁴⁶ die sich als **heimliche Kenntnissnahme des Inhalts vertraulicher Gespräche oder Mitteilungen durch eine aussenstehende Person** umschreiben lässt. Wesentlich ist dabei, dass die Kommunikation nicht schriftlich erfolgt (der Postverkehr geniesst zwar ebenfalls Verfassungsschutz,¹⁴⁷ ist aber prozessrechtlich in Art. 254 und 353 itStPO geregelt).¹⁴⁸ Technische Vorgänge, die nicht unter diesen Begriff fallen (z.B. Gespräche mittels Sprechfunkgeräten, Aufzeichnung von Gesprächen durch einen der Gesprächsteilnehmer, Fahndungen mittels GPS-Satellitensystem, Rufdatenrück Erfassung und Datenaufbewahrung, aber auch die Aufzeichnung von Bildmaterial in der Öffentlichkeit) unterliegen weder den Ermächtigungsverfahren noch den Ausführungsregeln für Überwachungsmaßnahmen.¹⁴⁹

1.2. Zulässigkeitsvoraussetzungen

In Umsetzung des Vorbehalts in Artikel 15 ItVerf. bezeichnet das Gesetz – ausgehend vom verfahrensauslösenden Straftatbestand und vom Strafraum – abschliessend die Fälle, in denen die Telefon-, Gesprächs-, Informatik- und Fernübertragungsüberwachung zulässig ist.

Die Überwachung von telefonischen Gesprächen oder Mitteilungen und anderen Formen der Übermittlung im Fernmeldewesen sowie von Mitteilungen unter anwesenden Personen (sog. Gesprächsüberwachung) ist in Verfahren **wegen folgender strafbarer Handlungen** erlaubt:¹⁵⁰

- a) nicht fahrlässig begangene Verbrechen, für die eine lebenslange Gefängnisstrafe oder eine Gefängnisstrafe vorgesehen ist, deren **Höchstmass** bei Bemessung gemäss Artikel 4 itStPO über **fünf Jahren** liegt;
- b) Verbrechen gegen die öffentliche Verwaltung, für die eine Gefängnisstrafe vorgesehen ist, deren Höchstmass bei Bemessung gemäss Artikel 4 itStPO nicht unter fünf Jahren liegt;
- c) Verbrechen, die **Betäubungsmittel** oder psychotrope Mittel betreffen;
- d) Verbrechen, die Waffen und Sprengstoffe betreffen;
- e) Verbrechen, die den Schmuggel betreffen;
- f) strafbare Handlungen der Beleidigung, der Drohung, des Geldwuchers, der missbräuchlichen Finanztätigkeit, des Missbrauchs von Insiderinformationen, der Marktmanipulation, der Belästigung oder Störung von Personen durch das Telefon;
- fbis) Verbrechen nach Artikel 600ter Absatz 3¹⁵¹ des italienischen Strafgesetzbuches (StGB), auch wenn sie sich auf pornographisches Material gemäss Artikel 600quater StGB beziehen.

Die Möglichkeit zur Überwachung von **Verkehrsdaten**, d.h. des Informationsflusses zwischen mehreren Systemen,¹⁵² beschränkt sich nicht auf die erwähnten strafbaren Handlungen, sondern erstreckt

¹⁴⁵ Art. 266 Abs. 2 itStPO.

¹⁴⁶ Art. 266bis itStPO.

¹⁴⁷ Art. 14 ItVerf.: „1. Die Wohnung ist unverletzlich. 2. Überwachungen, Durchsuchungen oder Beschlagnahmen dürfen darin nicht vorgenommen werden, ausser in den gesetzlich vorgesehenen Fällen und Formen gemäss den zum Schutz der persönlichen Freiheit vorgesehenen Bestimmungen. 3. Die Erhebungen und Untersuchungen aus Gründen der öffentlichen Gesundheit und der öffentlichen Sicherheit oder für wirtschaftliche und steuerliche Zwecke werden durch Sondergesetze geregelt.“

¹⁴⁸ Vgl. dazu FANUELE, *Sequestro di corrispondenza proveniente da persona detenuta: una forma d'intercettazione «mascherata»*, in *Diritto penale e processo* 4/2010, 465 ff.

¹⁴⁹ Vgl. APRILE & SPIEZIA, *Le intercettazioni telefoniche*, zit., 125 ff. Zur Aufzeichnung von Bildmaterial in der Öffentlichkeit, d.h. an öffentlich zugänglichen oder einsehbaren Orten (vgl. KassGH, II. Strafsenat, 24.4.2007, Nr. 35300; KassGH Vereinigte Senate, 28.3.2006, Nr. 26795 in *Dir. Internet*, 2/2007, 177 ff., mit Anmerkung von PORTELLI, *Videoriprese in luoghi pubblici e in ambienti domiciliari*); die Videoaufzeichnung von Kommunikationshandlungen – nicht aber blosser Handlungen – an privaten Aufenthaltsorten mag unter Umständen als Überwachung gelten (VerfGH 24.4.2002, Nr. 135).

¹⁵⁰ Art. 266 itStPO.

¹⁵¹ Verbreitung und Veröffentlichung von Kinderpornographie durch Fernübertragung.

sich auf jede Art von Straftat, sofern zu deren **Begehung Informatik- und Fernübertragungstechniken** eingesetzt wurden.¹⁵³

Die Überwachung¹⁵⁴ setzt das Vorliegen **schwerwiegender Indizien für eine strafbare Handlung**¹⁵⁵ und die **absolute Notwendigkeit der Massnahme zur Fortführung der Ermittlungen**¹⁵⁶ voraus. Für Gesprächsüberwachungen an **privaten Aufenthaltsorten**¹⁵⁷ muss ferner **berechtigter Grund zur Annahme bestehen, dass dort die verbrecherische Tätigkeit ausgeübt wird.**¹⁵⁸

Bei Vorliegen der erwähnten Zulässigkeitsvoraussetzungen unterliegt die Durchführung von Telefonüberwachungsmassnahmen in der Regel keiner subjektiven Einschränkung. Allerdings bestehen Ausnahmen (z.B. Verteidiger und Parlamentarier),¹⁵⁹ bedingt durch die spezielle Position oder Funktion der Person, deren Gespräche abgehört werden sollen.

1.3. Weitere Fernmeldeüberwachungsmassnahmen: Rufdatenrückfassung

Rufdaten sind Ermittlungsinstrumente von grundlegender Bedeutung. Darunter sind Informationen zu verstehen, die sich **nicht auf den Gesprächsinhalt** beziehen. Die Telefondienstbetreiber sind in der Lage, für jede Verbindung die Identifizierungsdaten des Ursprungs- bzw. Empfängeranschlusses, Zeitpunkt und Dauer des Anrufs sowie den genauen Standort des Mobiltelefons zurückzuverfolgen.

Die Rechtsprechung hat – nach anfänglicher Unsicherheit¹⁶⁰ – klargestellt, dass die Rufdatenrückfassung nicht unter die Bestimmungen zur Fernmeldeüberwachung fällt.¹⁶¹

¹⁵² Z.B. die Überwachung des E-Mail-Verkehrs und des Faxverkehrs zwischen verschiedenen PCs; vgl. PARODI, La disciplina delle intercettazioni telematiche, in *Diritto penale e processo*, Nr. 7/2003, S. 891.

¹⁵³ Art. 266*bis* itStPO, eingefügt durch Art. 11 Gesetz Nr. 547 vom 23.12.1993. Für eine weit gefasste Auslegung der Vorschrift vgl. PARODI, La disciplina delle intercettazioni telematiche, zit., S. 889 f. Eine andere Lehrmeinung vertritt die strikte Auslegung, wonach die Fernübertragungsüberwachung nur für Straftaten zulässig ist, die streng genommen unter Art. 266 ItStPO fallen; vgl. FILIPPI, L'intercettazione di comunicazioni, Mailand 1997, S. 82 f.

¹⁵⁴ Art. 267 Abs. 1 itStPO.

¹⁵⁵ Womit das Vorliegen der Straftat und nicht die Schuld des Angeklagten gemeint ist; KassGH IV. Strafsenat, 16.11.2005, Nr. 1848.

¹⁵⁶ Dies lässt den Schluss zu, dass das Überwachungsersuchen auf den Verfahrensabschnitt der Voruntersuchung zu beschränken ist; APRILE & SPIEZIA, Le intercettazioni telefoniche, zit., S. 9.

¹⁵⁷ Vgl. dazu FANUELE, Il concetto di «privata dimora» ai fini delle intercettazioni ambientali, in KassGH 2001, 2748.

¹⁵⁸ Art. 266 Abs. 2 itStPO. Die restriktivere Haltung erklärt sich dadurch, dass diese Form der Überwachung die Installation von Abhör- und Aufnahmegeräten durch heimliches Eindringen in Wohnungen und andere private Aufenthaltsräume erfordert. Diese Strenge wird aufgeweicht bei Verbrechen der organisierten Kriminalität und des Terrorismus; vgl. Kap. 2.2 weiter unten.

¹⁵⁹ Art. 103 Abs. 5 itStPO verbietet das Abhören von Gesprächen oder Mitteilungen der Verteidiger, der verfahrensbeauftragten ermächtigten Privatdetektive, der Parteisachverständigen und ihrer Gehilfen sowie solcher zwischen den genannten Personen und ihren Klienten. Art. 68 ItVerf. besagt, dass die Einschränkung der persönlichen Freiheiten eines Mitglieds des Parlaments der Ermächtigung der Kammer bedarf, der dieses angehört (vgl. Gesetz Nr. 140 vom 20.6.2003); in Umsetzung dieser Bestimmung untersagt Art. 343 Abs. 2 und 3 itStPO das Abhören von Personen, gegen die ein Ersuchen um Ermächtigung zur Strafverfolgung vorliegt. Weitere Einschränkungen sind vorgesehen für den Präsidenten des Ministerrates (Art. 96 ItVerf.; Art. 10 Abs. 1 Verfassungsgesetz Nr. 1 vom 16.1.1989 i.V.m. Art. 1 Abs. 4 Gesetz Nr. 219 vom 5.6.1989), den Präsidenten der Republik (Art. 7 Abs. 3 Gesetz Nr. 219 vom 5.6.1989) und die Richter des Verfassungsgerichtshofes (Art. 3 Abs. 1 Verfassungsgesetz Nr. 1 vom 9.2.1948).

¹⁶⁰ Mit Urteil vom 11.3.1993, Nr. 81 (Giurisprudenza italiana, 1995, I, S. 108), hat der VerfGH die Verfassungswidrigkeit von Art. 266 itStPO wegen Widerspruchs mit Art. 15 ItVerf. insofern ausgeschlossen,

Das einschlägige Regelwerk ist **Legislativdekret Nr. 196 vom 30.6.2003** (sog. *Datenschutzkodex*), das in Artikel 123-132 die Verarbeitung von Verkehrsdaten regelt, wobei präzise zeitliche Vorgaben formuliert und spezielle Erfassungsmodalitäten vorgeschrieben werden.¹⁶²

Artikel 132 (in der Fassung gemäss Legislativdekret Nr. 109 vom 30.5.2008 zur Übernahme der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG)¹⁶³ sieht insbesondere vor, dass der Anbieter die Daten über den Telefon- und den Fernübertragungsverkehr (nicht aber den Inhalt der Mitteilungen) ab dem Tag der Mitteilung **zum Zwecke der Ermittlung und der Bekämpfung von Straftaten** vierundzwanzig bzw. zwölf Monate lang aufbewahrt.¹⁶⁴ Die über unbeantwortete Anrufe, die von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder eines öffentlichen Kommunikationsnetzes vorübergehend verarbeitet werden, müssen dreissig Tage lang aufbewahrt werden.¹⁶⁵ Die Missachtung der Aufbewahrungsvorschriften wird mit einer Geldbusse geahndet.¹⁶⁶

als dieser die Regelung der Zulässigkeitsgrenzen der Fernmeldeüberwachung nicht auf die Rufdatenrückfassung ausweitet. Die Daten zur Identifizierung der Gesprächsteilnehmer und solche über Zeit und Ort der stattgefundenen Mitteilung seien zwar durch Art. 15 ItVerf. verfassungsrechtlich geschützt, aber nicht Gegenstand einer Fernmeldeüberwachung im eigentlichen Sinn. Desgleichen hat der VerfGH mit Urteil vom 17.7.1998, Nr. 281 (*Cass. pen.* 1999, 27), die Frage der Verfassungsmässigkeit von Art. 267 Abs. 1 itStPO wegen angeblichen Widerspruchs mit Art. 3 Abs. 1 ItVerf. insofern abgewiesen, als dieser das Erfordernis der gerichtlichen Verfügung nicht auf die Erfassungsmodalitäten für nichtinhaltliche Gesprächsdaten ausweitet. *Kontra*: KassGH Vereinigte Senate, 13.7.1998, Nr. 21 (in *Foro italiano*, 1999, II, 87): Da das Ausdrucken nichtinhaltlicher Gesprächsdaten diese bereits in nachvollziehbarer Form dokumentiere, würden für deren Erfassung dieselben Garantien in Bezug auf Geheimnis und Freiheit der Mitteilungen mittels Informatiksystemen nach Art. 266bis itStPO gelten. Daraus ergab sich eine uneinheitliche Praxis, in der die Rufdatenrückfassung teils durch begründete Verfügungen der Staatsanwaltschaft, teils im Ermächtungsverfahren durch den Untersuchungsrichter angeordnet wurde. Zur Doktrin vgl. ZACCHÉ, *Acquisizione di dati esterni ai colloqui telefonici*, in *Diritto Penale e Processo* 3/1999, S. 334 ff.

¹⁶¹ Vgl. KassGH Vereinigte Senate, 21.6.2000, Nr. 16 (in KassGH 2000, 3259), und KassGH Vereinigte Senate, 23.2.2000, Nr. 6 (in KassGH 2000, 2545): Für die Herausgabe der Identifizierungsdaten des Telefonverkehrs aus den Informatikarchiven der Betreiber genüge grundsätzlich die **begründete Verfügung der Gerichtsbehörde**, da es aufgrund des sich daraus ergebenden unterschiedlich schweren Eingriffs in die Privatsphäre nicht zwingend sei, die Vorschriften zum Abhören von Gesprächen oder Mitteilungen gemäss Art. 266 f. itStPO einzuhalten. Zur Doktrin vgl. FILIPPI, *Il revirement delle Sezioni Unite sul tabulato telefonico: un'occasione mancata per riconoscere una prova incostituzionale*, in KassGH 2000, 3245; MELILLO, *Intercettazioni ed acquisizione di tabulati telefonici: un opportuno intervento correttivo delle Sezioni Unite*, in KassGH 2000, 2545.

¹⁶² Vgl. Kap. 2.4 weiter unten.

¹⁶³ Vgl. auch die Verordnung der Datenschutzbehörde vom 17.1.2008 zur Datensicherheit im Telefon- und Fernübertragungsverkehr, verfügbar unter <http://www.garanteprivacy.it/garante/doc.jsp?ID=1482111>.

¹⁶⁴ Art. 132 Abs. 1 Legislativdekret Nr. 196 von 2003.

¹⁶⁵ Art. 132 Abs. 1bis Legislativdekret Nr. 196 von 2003.

¹⁶⁶ Art. 162bis Legislativdekret Nr. 196 von 2003.

2. Übersicht über die Prozess- und Organisationsstrukturen

2.1. Fernmeldeüberwachung in Verfahren wegen gewöhnlicher Kriminalität

2.1.1. Das Ermächtigungsverfahren

Die Fernmeldeüberwachung wird auf **Antrag der Staatsanwaltschaft** durch **begründete Verfügung** des **Untersuchungsrichters** angeordnet; dieser hat zu prüfen, ob die Zulässigkeitsvoraussetzungen für die Anordnung der Massnahme bestehen.¹⁶⁷ In **Dringlichkeitsfällen** und wenn ein berechtigter Grund zur Annahme besteht, dass durch eine Verzögerung die Untersuchungen schwer beeinträchtigt werden können, kann die Staatsanwaltschaft von sich aus tätig werden und eine begründete Verfügung erlassen, die unverzüglich und jedenfalls binnen höchstens vierundzwanzig Stunden dem Untersuchungsrichter zur allfälligen Bestätigung zu melden ist. Erfolgt die Bestätigung nicht innerhalb von achtundvierzig Stunden, darf die Überwachung nicht fortgesetzt und dürfen deren Ergebnisse nicht verwertet werden.¹⁶⁸

Die anordnende Verfügung der Staatsanwaltschaft legt die Überwachungsmodalität und -dauer fest.¹⁶⁹ Diese scheinbar ausschliesslich in Dringlichkeitsfällen geltende Vorschrift ist laut einer weit verbreiteten Ansicht auch anwendbar, wenn die Überwachung vom Untersuchungsrichter bewilligt wird;¹⁷⁰ nach erfolgter Bewilligung **kann die Staatsanwaltschaft die Überwachungsmodalitäten auswählen**, die sie zum Zwecke der Beweisaufnahme für angezeigt erachtet.

Die **Dauer** der Überwachung darf **fünfzehn Tage** nicht überschreiten, **kann** aber vom Gericht für weitere Zeiträume von jeweils fünfzehn Tagen **verlängert werden**, sofern die Zulässigkeitsvoraussetzungen noch bestehen.¹⁷¹ Der Fristenlauf beginnt mit dem tatsächlichen Beginn der Überwachungstätigkeiten.¹⁷²

2.1.2. Die Durchführung der Telefonüberwachung

Die Staatsanwaltschaft nimmt die Telefonüberwachung selbst vor oder bedient sich dazu eines höheren Amtsträgers der Kriminalpolizei.¹⁷³ Die Überwachung darf **ausschliesslich mit den bei der Staatsanwaltschaft eingerichteten Anlagen** erfolgen.¹⁷⁴ Die Errichtung von Anlagen in den Räumlichkeiten der Staatsanwaltschaft soll **Gewähr gegen allfälligen Missbrauch** durch die Polizei bieten und sicherstellen, dass die Gerichtsbehörde die erforderliche Kontrolle ausüben kann, damit nur bewilligte Überwachungen durchgeführt werden und diese nicht über das bewilligte Mass hinausgehen.¹⁷⁵

¹⁶⁷ Art. 267 Abs. 1 itStPO.

¹⁶⁸ Art. 267 Abs. 2 itStPO.

¹⁶⁹ Art. 267 Abs. 3 itStPO.

¹⁷⁰ Auch wenn das Gericht die Fernmeldeüberwachung bewilligt, muss die Staatsanwaltschaft eine zweite nicht begründete Verfügung erlassen, mit der die Massnahme unter Angabe der Modalitäten und der Dauer angeordnet wird. Vgl. FUMU, unter Art. 267 in Comm. Chiavario, II, Torino 1990, 787.

¹⁷¹ Art. 267 Abs. 3 itStPO. Diese Frist gilt sowohl für Überwachungsmassnahmen, die vom Untersuchungsrichter bewilligt wurden, als auch für solche, die von der Staatsanwaltschaft im Dringlichkeitsverfahren angeordnet und vom Untersuchungsrichter bestätigt wurden: vgl. KassGH VI. Strafsenat 10.3.1995, Nr. 5415.

¹⁷² KassGH Vereinigte Senate, 23.2.2000, Nr. 6.

¹⁷³ Art. 267 Abs. 4 itStPO. Der Gesetzgeber hat ausgeschlossen, dass die Gespräche von einfachen Beamten abgehört werden. Sollte dies vorkommen, dürfte der Gesetzesverstoss aufgrund der Verbindung von Art. 267 mit Art. 271 itStPO die Unverwertbarkeit der Ergebnisse nach sich ziehen: vgl. APRILE & SPIEZIA, Le intercettazioni telefoniche, zit., S. 24 f.

¹⁷⁴ Art. 268 Abs. 3 itStPO.

¹⁷⁵ Vgl. VerfGH 6.4.1973, Nr. 34.

Dennoch ist die Verwendung der Roaming-Technologie (**Fernabhören**) zulässig. Dabei erfolgt die Überwachung technisch bei der Staatsanwaltschaft, das Signal wird aber mit einer zeitlichen Verzögerung von wenigen Sekunden in die Räumlichkeiten der Kriminalpolizei weitergeleitet, wo die zuständige Person das Gespräch mittels eines Abhörgeräts mitverfolgt. Auf diese Weise wird die Telefonüberwachung von der Staatsanwaltschaft bestätigt und das Signal wird lediglich der organisatorischen Einfachheit halber weitergeleitet.¹⁷⁶

Wenn sich allerdings diese Anlagen als **ungenügend oder ungeeignet** erweisen und **aussergewöhnliche Dringlichkeitsgründe** vorliegen, kann die Staatsanwaltschaft mit begründeter Verfügung anordnen,¹⁷⁷ dass die Telefonüberwachung mit **Anlagen des öffentlichen Dienstes oder mit solchen, die zur Ausstattung der Kriminalpolizei gehören**, zu erfolgen hat.¹⁷⁸ Zu diesem Zweck **müssen die Festnetz- und Mobilfunkbetreiber** die von den Gerichtsbehörden verlangten **Leistungen erbringen**, um die Durchführung der Telefonüberwachung zu ermöglichen.¹⁷⁹ Die Vorschrift, dass zwingend polizeiliche Vorrichtungen zu verwenden sind, zielt keinesfalls auf das Rechtsgeschäft (Kauf, Leihe, Miete usw.), durch das die Kriminalpolizei sich die Geräte verschafft – diese können auch Privateigentum verbleiben. Vielmehr wird damit Dritten der Zugang zu den Anlagen untersagt, solange diese zu Überwachungszwecken im Einsatz sind. Als Ausstattung der Kriminalpolizei gilt dementsprechend jegliches Gerät, das ihr in ihren Räumlichkeiten zur Verfügung steht – einschliesslich des technischen Materials, das Privaten gehört und von diesen durch Verleih oder einen beliebigen anderen Vertrag befristet abgetreten wird.¹⁸⁰

Lediglich im Falle der **Informatik- und Fernübertragungsüberwachung** kann die Staatsanwaltschaft, sofern natürlich die übrigen Voraussetzungen gegeben sind,¹⁸¹ auch die Durchführung mittels **Anlagen, die sich in privatem Besitz befinden**, anordnen.¹⁸² In der Praxis werden häufig staatsanwaltsexterne Anlagen beigezogen, insbesondere im Falle von Ausstattungsengpässen bei der Staatsanwaltschaft infolge zeitgleicher Durchführung mehrerer Untersuchungen, welche die vorhandenen Vorrichtungen beanspruchen.¹⁸³

Eine Untersuchung der Justizkommission des Senats der Republik zum Phänomen der Telefonüberwachung hat ergeben, dass die Staatsanwaltschaft der Kriminalpolizei nach Erhalt der Ermächtigung zwei Dokumente abgibt: die **Untersuchungsvollmacht** zur konkreten Durchführung der Telefonüberwachung und das **Raster** (sog. *griglia*) mit einer Übersicht der technischen Angaben, die dem Telefondienstbetreiber zu übermitteln sind, damit er die Überwachung konkret durchführen kann. Der

¹⁷⁶ Vgl. KassGH IV. Strafsenat, 24.11.2010, Nr. 3571. Vgl. dazu APRILE, SPIEZIA, Le intercettazioni telefoniche, zit., 46 f.

¹⁷⁷ Vgl. dazu CAMPILONGO, Intercettazioni ambientali, impianti esterni alla procura ed obbligo di motivazione: un ulteriore intervento delle Sezioni unite, KassGH 2004, 4133; SANTALUCIA, Sulla motivazione del decreto per l'uso degli impianti esterni di intercettazione: un altro intervento, si spera risolutivo, delle Sezioni Unite, KassGH 2008, 81.

¹⁷⁸ Art. 268 Abs. 3 itStPO.

¹⁷⁹ Art. 96 Legislativdekret Nr. 259 vom 1.8.2003, «Kodex über die elektronische Kommunikation».

¹⁸⁰ KassGH I. Strafsenat, 7.10.2005, Nr. 45103; KassGH II. Strafsenat, 18.11.2004, Nr. 48461; KassGH VI. Strafsenat, 16.6.2005, Nr. 28514.

¹⁸¹ Kommentar zur italienische Strafprozessordnung, unter Art. 268 Kap. 2, verfügbar unter <http://pluris-cedam.utetgiuridica.it>. Kontra PARODI, La disciplina delle intercettazioni telematiche, zit., S. 895, wonach die Einfügung eines neuen, nicht an Abs. 3 von Art. 268 itStPO gebundenen Absatzes den Schluss zulässt, dass die dort vorgesehenen Befugnisse eigenständig sind und losgelöst von den Kriterien bestehen, die für die allgemeine Verwendung von Anlagen des öffentlichen Dienstes bzw. der Kriminalpolizei gelten.

¹⁸² Art. 268 Abs. 3bis itStPO.

¹⁸³ APRILE & SPIEZIA, Le intercettazioni telefoniche, zit., S. 29 f.

Betreiber stellt der Kriminalpolizei eine spezielle Telefonleitung für die Abwicklung der Telefonüberwachung zur Verfügung; mieten kann die Staatsanwaltschaft diese Leitung beim Betreiber selbst oder bei privaten Firmen oder Konsortien, die auch über alle weiteren technischen Geräte für die Abwicklung der Telefonüberwachung verfügen.¹⁸⁴ Die Privatfirma, welche die Geräte liefert, wird von der Staatsanwaltschaft bestimmt.¹⁸⁵

Das Verfahren zur **Aufnahme** der abgehörten Gespräche in **die Akten** unterteilt sich in die Schritte Aufzeichnung, Abhören und Protokollierung.¹⁸⁶ Diese Handlungen sind nach detaillierten Vorgaben des Gesetzgebers vorzunehmen. Die abgehörten Mitteilungen werden aufgezeichnet, und über die Telefonüberwachung wird ein Protokoll verfasst,¹⁸⁷ in das der Inhalt der abgehörten Mitteilungen, auch in zusammenfassender Form, übertragen wird.¹⁸⁸ Die Protokolle und die Aufzeichnungen sind unverzüglich der Staatsanwaltschaft zu übermitteln, die innerhalb von fünf Tagen nach Abschluss der Telefonüberwachung deren Hinterlegung zusammen mit den entsprechenden Anordnungs-, Genehmigungs-, Bestätigungs- oder Verlängerungsverfügungen in ihrem Sekretariat zuhanden der Verteidigung anordnet.¹⁸⁹ Die Verteidiger der Parteien werden unverzüglich benachrichtigt, dass sie Einsicht in die Akten nehmen und sich die Aufzeichnungen anhören, d.h. Kenntnis des Informatik- bzw. Fernübertragungsverkehrs¹⁹⁰ erhalten können; entsprechend können sie sowohl das allfällige Vorliegen von Nichtverwertungsgründen beurteilen, als auch die abgehörten Inhalte im Hinblick auf die anschließende Aufnahme in die Akten einsehen.

Nachdem die Parteien Einblick in die Überwachungsergebnisse erhalten haben, sind sie verpflichtet, in nichtöffentlicher Sitzung dem Gericht die Gespräche und Daten anzugeben, die zu den Akten zu nehmen sind. Das **Gericht beseitigt** von Amtes wegen jene **Aufzeichnungen und Protokolle**, deren Verwertung verboten ist. Die Parteien haben das Recht, an der Beseitigung teilzunehmen und sind davon mindestens vierundzwanzig Stunden vorher zu benachrichtigen. Nach Auswahl der als relevant eingestuften Aufzeichnungen ordnet der Richter deren vollständige Übertragung oder das Aus-

¹⁸⁴ Senat der Republik, 15. Legislaturperiode, Justizkommission, *Indagine conoscitiva sul fenomeno delle intercettazioni telefoniche*, 16. Sitzung (Vormittag), 4. stenographisches Protokoll, Donnerstag, 20. Juli 2006, verfügbar unter:

<http://www.senato.it/documenti/repository/commissioni/stenografici/15/comm02/02a-20060720a-IC-0053.pdf>. Das Verfahren zur Fernübertragungsüberwachung ist ähnlich aufgebaut.

¹⁸⁵ Die Vollmachten beauftragen gewissermassen irgendein Unternehmenskonsortium oder enthalten eine Liste von Firmen; andernfalls übermittelt die Kriminalpolizei der Staatsanwaltschaft die Vorschläge verschiedener Firmen zur Kosteneinschätzung: vgl. Senat der Republik, Justizkommission, *Indagine conoscitiva sul fenomeno delle intercettazioni telefoniche*, zit., S. 2, 21.

¹⁸⁶ APRILE & SPIEZIA, *Le intercettazioni telefoniche*, zit., S. 26.

¹⁸⁷ Laut Art. 89 Durchführungsbestimmungen muss das Abhörprotokoll folgende Angaben enthalten: Kerndaten der Überwachungsverfügung, Umschreibung der Aufzeichnungsmodalitäten, Angabe von Tag und Uhrzeit des Überwachungsbeginns und -endes sowie die Namen der Personen, die an der Überwachung teilgenommen haben.

¹⁸⁸ Art. 268 Abs. 1 und 2 itStPO. Beim Erkennen und Beurteilen des Beweisergebnisses der Telefonüberwachung darf lediglich auf die Tonbandaufzeichnung Bezug genommen werden; die Zeugenaussage der Person, die die Überwachung vorgenommen hat, ist ausgeschlossen.

¹⁸⁹ Art. 268 Abs. 4 itStPO. Wird ein schwerwiegender Nachteil für die Erhebungen befürchtet, so ermächtigt der Richter die Staatsanwaltschaft, die Hinterlegung längstens bis zum Abschluss der Voruntersuchungen hinauszuzögern: Art. 268 Abs. 5 itStPO.

¹⁹⁰ Art. 268 Abs. 6 itStPO. Die Nichtbeachtung der Vorschrift bewirkt keine Unverwertbarkeit im Sinne von Art. 271 itStPO; diese setzt voraus, dass entweder die Mitteilungen nicht aufgezeichnet wurden oder kein Überwachungsprotokoll erstellt wurde bzw. dass die zwingend vorgeschriebenen Abhöranlagen nicht zum Einsatz kamen. Ein Teil der Lehre vertritt die Meinung, eine Nichtbenachrichtigung verletze das Recht auf Verteidigung und habe entsprechend die Nichtigkeit nach Art. 178 Abs. 1 lit. c und 180 itStPO zur Folge (vgl. FILIPPI, *L'intercettazione di comunicazioni*, zit., S. 137).

drucken der im Informatik- oder Fernübertragungsverkehr enthaltenen Informationen in nachvollziehbarer Form an, unter Beachtung der **für die Erstellung von Amtsgutachten vorgesehenen Formen, Vorgangsweisen und Garantien**; danach werden Überträge und Ausdrucke in die Akte für die Hauptverhandlung aufgenommen.¹⁹¹

Die nicht in die Akte der Staatsanwaltschaft aufgenommenen Protokolle und Aufzeichnungen müssen vollständig bei der **Staatsanwaltschaft aufbewahrt** werden. Die Aufbewahrungspflicht erlischt erst, wenn ein unwiderrufliches Urteil ergeht; zum Schutz ihrer Privatsphäre können die Betroffenen jedoch beim Richter die Vernichtung der nicht verfahrensrelevanten Unterlagen verlangen.¹⁹²

2.1.3. Verwertungsverbot

Die Ergebnisse der Telefonüberwachung dürfen nur in Verfahren, für die sie angeordnet wurde, verwertet werden.¹⁹³ Dieses Verbot gilt nicht, wenn die Überwachungsergebnisse «für die Feststellung von Verbrechen, für die die Anhaltung auf frischer Tat zwingend vorgeschrieben ist, unerlässlich erscheinen»; damit wird die **Verwertung in anderen Verfahren** zulässig.¹⁹⁴ Die Übermittlung der Überwachungsakten kann in jeder Lage und Instanz der beiden Verfahren erfolgen; entsprechend hängt die Aktenaufnahme jeweils von der Regelung ab, die für die gerade aktuelle Verfahrenslage und -instanz gilt.¹⁹⁵

Das **Verwertungsverbot** der Überwachungsergebnisse gelangt in drei Fällen zur Anwendung:¹⁹⁶

- a) **Überwachungen, die ausserhalb der vom Gesetz zugelassenen Fälle vorgenommen wurden** (nach Art. 266 und 266bis ItStPO);¹⁹⁷
- b) **Überwachungen, die in Verletzung der Vorschriften zum Ermächtigungsverfahren und der Durchführungsregeln vorgenommen wurden** (Nichtbeachtung der Bestimmungen von Art. 267 und 268 Abs. 1 und 3);¹⁹⁸
- c) **Überwachung von Gesprächen oder Mitteilungen von Berufsgeheimnisträgern, wenn sie Tatsachen zum Gegenstand haben, von denen diese auf Grund ihres Auftrages, Amtes oder Berufes Kenntnis erlangt haben.** Die Vorschrift knüpft an das Verbot von Artikel 103 Abs. 5 ItStPO an, wonach das Abhören von Gesprächen oder Mitteilungen der Verteidiger, der verfahrensbeauftragten ermächtigten Privatdetektive, der Parteisachverständigen und ihrer Gehilfen sowie solcher zwischen den genannten Personen und ihren Klienten nicht erlaubt ist.

¹⁹¹ Art. 268 Abs. 6 und 7 ItStPO.

¹⁹² Art. 269 ItStPO. Die Bestimmung scheint den Fall der Informatik- oder Fernüberwachungsüberwachung nicht zu regeln.

¹⁹³ Stellt allerdings die Fernmeldeüberwachung selbst ein deliktisches Verhalten dar, so unterliegt deren Aufnahme in die Akten den Regeln zur prozessualen Verwertung des Corpus Delicti: vgl. KassGH VI. Strafsenat, 18.12.2007, Nr. 5141.

¹⁹⁴ Art. 270 ItStPO. Das Aktenaufnahme- und Beseitigungsverfahren soll erneuert werden (mit Verweis auf Art. 268 Abs. 6, 7 und 8 ItStPO).

¹⁹⁵ Kommentar zur Italienische Strafprozessordnung im Hypertextformat, Kap. 10, verfügbar unter <http://pluris-cedam.utetgiuridica.it>.

¹⁹⁶ Art. 271 ItStPO. Ein weiteres Verwertungsverbot betrifft die Mitglieder des Parlaments (vgl. Art. 343 Abs. 2 und 3 ItStPO sowie Art. 4 und 6 Gesetz Nr. 140 vom 20.6.2003) und den Präsidenten der Republik (vgl. Art. 7 Abs. 4 Gesetz Nr. 219 vom 5.6.1989).

¹⁹⁷ Darunter fallen durch Rechtshilfe im Ausland erfolgte Überwachungsmassnahmen, wenn der ausländische Staat gemäss Art. 729 ItStPO Bedingungen für die Verwendbarkeit der ersuchten Verfahrenshandlungen stellt. Die Nichteinhaltung dieser Bedingungen durch die italienische Gerichtsbehörde bewirkt die Unzulässigkeit der Verwertung nach Art. 191 Abs. 2, wie in Art. 729 Abs. 2 ItStPO festgehalten wird.

¹⁹⁸ Zu den Folgen der Nichtbeachtung von Art. 268 Abs. 3bis ItStPO, vgl. oben, 2.1.2.

Widerrechtlich erlangte Erkenntnisse sind unverwertbar und werden behandelt, als hätten sie nie existiert; entsprechend schreibt das Gesetz deren Vernichtung vor, es sei denn, es handle sich um Überführungsstücke.

2.1.4. Die Regelung des Staatsgeheimnisses

Wurden **dienstliche Mitteilungen** von **Mitarbeitern des Amtes für Sicherheitsinformationen («Dipartimento delle informazioni per la sicurezza»)** oder der **Nachrichtendienste**¹⁹⁹ abgehört, so gelangt eine spezielle Regelung zum Schutze des Staatsgeheimnisses zur Anwendung.²⁰⁰ Die Unterlagen, Träger und Akten über diese Mitteilungen sind unverzüglich an einem geschützten Ort unter Verschluss aufzubewahren. Ist die Gerichtsbehörde der Ansicht, besagtes Material sei beizuziehen, so muss sie sich beim Präsidenten des Ministerrates erkundigen, ob die zugrundeliegenden Mitteilungen und Informationen dem Staatsgeheimnis unterliegen. Für das entsprechende Verfahren ist eine Frist von höchstens sechzig Tagen vorgesehen, innert derer sich der Ministerratspräsident nur dann formell zu äussern hat, wenn er das Staatsgeheimnis anrufen will. Läuft diese Frist ohne Berufung auf das Staatsgeheimnis ab, so kann die Gerichtsbehörde das Material formell zu den Akten nehmen. Bei Berufung auf das Staatsgeheimnis wird das Material jedoch unverwertbar, wobei die Gerichtsbehörde aufgrund von Umständen, die unabhängig von den Geheimakten bestehen, befasst werden kann.²⁰¹ Solange die Frist noch läuft, kann die Gerichtsbehörde die eingeholten Informationen verwerten, sofern Verschleierungs- oder Fluchtgefahr besteht oder die Begehung einer Straftat unterbrochen oder verhütet werden muss, für die eine Gefängnisstrafe mit Höchstmass nicht unter vier Jahren vorgesehen ist.

2.2. Verbrechen der organisierten Kriminalität und des Terrorismus

Die Gesetzgebung²⁰² sieht bei Verbrechen der **organisierten Kriminalität**²⁰³ oder der **Drohung durch das Telefon**²⁰⁴ Ausnahmen von den ordentlichen Überwachungsvoraussetzungen und -modalitäten vor; die weniger strenge Ausgestaltung soll die Ermittlungen gegen diese Deliktarten vereinfachen. Dieselben Ausnahmeregelungen gelangen auch in **Terrorismusverfahren** zur Anwendung.²⁰⁵

¹⁹⁹ Vgl. Art. 2 Gesetz 124/2007.

²⁰⁰ Art. 270bis itStPO, eingeführt durch Gesetz Nr. 124 vom 3.8.2007, *Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto*.

²⁰¹ Gegen die Entscheidung besteht das Rechtsmittel der Beschwerde beim Verfassungsgerichtshof, der mit Zuweisungskonflikten befasst werden kann, wobei die Berufung auf das Staatsgeheimnis nicht möglich ist. Verneint der Gerichtshof das Vorliegen des Geheimnisses, ist es nicht mehr möglich, sich in derselben Sache darauf zu berufen. Im umgekehrten Fall darf die Gerichtsbehörde Akten oder Urkunden, für die das Staatsgeheimnis geltend gemacht wurde, weder heranziehen noch direkt oder indirekt verwerten.

²⁰² Art. 13 Gesetzesdekret Nr. 152 vom 13.5.1991, umgewandelt in Gesetz Nr. 203 vom 12.3.1991.

²⁰³ Die Sonderregelung von Art. 13 Gesetzesdekret 152/1991 gilt auch für den Tatbestand der Lösegeldentführung, da diese Straftat als typisches Verbrechen der organisierten Kriminalität gilt. Es genügt der alleinige Hinweis auf den Durchführungsmodus der Lösegeldforderung, die in der Regel telefonisch erfolgt: vgl. KassGH V. Strafsenat, 5.11.2003, Nr. 46963.

²⁰⁴ Art. 13 verweist nicht auf Art. 266bis itStPO, wodurch strittig wird, ob sich die Regelung auch auf die Informatik- und Fernübertragungsüberwachung ausdehnen lässt. Systematische und teleologische Gründe sprechen allerdings für diese Option: PARODI, *La disciplina delle intercettazioni telematiche*, zit., S. 893.

²⁰⁵ Insbesondere bei den Straftaten nach Art. 270ter und 280bis itStGB sowie Art. 407 Abs. 2 Bst. a Ziff. 4 itStPO, in der Regelung von Art. 3 Gesetzesdekret Nr. 374 vom 18.10.2001, umgewandelt in Gesetz Nr. 438 vom 15.12.2001, mit dringlichen Bestimmungen zur Bekämpfung des internationalen Terrorismus.

Die Überwachungsermächtigung wird erteilt, wenn **hinreichende** (und nicht «**schwerwiegende**») **Indizien für eine strafbare Handlung** vorliegen und die Überwachung für die **Vornahme der Untersuchungen** (und nicht die «**Fortführung**» derselben) **notwendig** (anstatt «**unerlässlich**») erscheint. Auch die **Höchstdauer** unterscheidet sich von den ordentlichen Fristen: **vierzig Tage** anstatt fünfzehn, mit der Möglichkeit nachträglicher **Verlängerungen um zwanzig Tage** anstelle der fünfzehn im ordentlichen Verfahren. In Abweichung von der Regelung in Artikel 267 ItStPO können die Staatsanwaltschaft und der höhere Amtsträger der Kriminalpolizei auch die Hilfe **einfacher Amtsträger der Kriminalpolizei** in Anspruch nehmen. In Dringlichkeitsfällen verlängert die Staatsanwaltschaft die Überwachungstätigkeit, wobei jedoch die Pflicht zur Einhaltung des Bestätigungsverfahrens nach Artikel 267 Abs. 2 ItStPO unberührt bleibt.

Was die **Gesprächsüberwachung** anbelangt, so ist das Abhören anwesender Personen im Domizil zulässig, **auch wenn kein «berechtigter Grund zur Annahme besteht, dass dort die verbrecherische Tätigkeit ausgeübt wird»**.

2.3. Vorsorgliche Telefonüberwachung

Präventive Überwachungsmassnahmen²⁰⁶ werden **ohne gerichtliche Kontrolle** angeordnet und dürfen in Verfahren nicht berücksichtigt werden. Dabei handelt es sich um Überwachungstätigkeiten, die der Innenminister bei der Staatsanwaltschaft beantragen kann – direkt oder über bestimmte Amtsträger (Verantwortliche der Kriminalpolizei, der Carabinieri, der Finanzwache, der Staatspolizei) oder über die Polizeidirektoren oder die Provinzialkommandanten der Staatspolizei, der Carabinieri oder der Finanzwache; die Staatsanwaltschaft bewilligt die Massnahme (ohne Ermächtigungs- oder Bestätigungsverfügungen durch den Untersuchungsrichter),²⁰⁷ sofern diese für das Einholen von Nachrichten zur Verhütung von Straftaten nach den Artikeln 407 Absatz 2 Buchstabe a Ziffer 4 und 51 Absatz 3bis ItStPO erforderlich ist (besonders schwerwiegende Straftaten, speziell bei Mafia- oder Terrorismuskriminalität). zur Gewährleistung des Informatikschutzes der mit Dekret des Innenministers bezeichneten kritischen IT-Infrastrukturen von nationalem Interesse und zur Verhütung und Bekämpfung von Terrorakten oder Terrorismusbegünstigung mittels Informatikmitteln können die höheren Amtsträger der Kriminalpolizei, die dem Organ des Innenministeriums für die Sicherheit und die Ordnungsmässigkeit der Fernmeldedienste angehören, die Handlungen gemäss Art. 226 Durchführungs-

²⁰⁶ Geregelt ist das Sachgebiet durch Art. 226 Durchführungsbestimmungen ItStPO und Art. 5 Gesetzesdekret Nr. 374 vom 18.10.2001, sog. «Antiterrorismusedekret», umgewandelt in Gesetz Nr. 438 vom 15.12.2001. Art. 226 Abs. 1 Durchführungsbestimmungen ItStPO liest sich in etwa wie folgt: „Der Innenminister oder, in dessen Auftrag, die Verantwortlichen der Zentralen Dienste gemäss Art. 12 Legislativdekret Nr. 152 vom 13.05.1991, mit Abänderungen umgewandelt aus Gesetz Nr. 203 vom 12.07.1991, sowie der Polizeidirektor oder der Provinzialkommandant der *Carabinieri* und der Finanzwache beantragen bei der Staatsanwaltschaft am Landesgericht im Hauptort des Bezirks, in dem sich die zu überwachende Person aufhält, bzw. – bei Unbestimmbarkeit – des Bezirks, in dem das Präventionsbedürfnis entstanden ist, die Ermächtigung zur Überwachung von Mitteilungen und Gesprächen, auch durch Fernübertragung, sowie zur Überwachung von Mitteilungen oder Gesprächen unter anwesenden Personen, auch wenn sie an den in Art. 614 ItStGB bezeichneten Orten stattfinden, sofern dies zur Einholung von Nachrichten zur Verhütung von Straftaten nach Art. 407 Abs. 2 Bst. a Ziff. 4 und 51 Abs. 3bis ItStGB notwendig ist. Bei Straftaten nach Art. 51 Abs. 3bis ItStGB kann der Innenminister im Übrigen den Direktor der Antimafia-Ermittlungsdirektion beauftragen. Bewilligt werden kann auch die Nachverfolgung der Telefonanrufe und der Fernübertragungsmitteilungen sowie das Einholen der Verkehrsdaten der erfolgten Telefonate und Fernübertragungen wie auch jeder anderen nützlichen Information, über welche die Fernmeldebetreiber verfügen.“

²⁰⁷ APRILE & SPIEZIA, Le intercettazioni telefoniche, zit., S. 110.

bestimmungen auch auf Antrag oder in Zusammenarbeit mit den darin bezeichneten Organen der Kriminalpolizei vornehmen.²⁰⁸

Die Staatsanwaltschaft bewilligt die Überwachung mit **begründeter Verfügung**, falls Ermittlungsumstände vorliegen, die eine präventive Tätigkeit rechtfertigen, und sie es für notwendig erachtet. Die Bewilligung gilt für höchstens vierzig Tage und kann für weitere Zeiträume von zwanzig Tagen verlängert werden, sofern die gesetzlichen Voraussetzungen noch bestehen.²⁰⁹

Die vorsorgliche Telefonüberwachung **erfolgt mittels Anlagen, die bei der Staatsanwaltschaft oder bei anderen geeigneten, durch die bewilligende Staatsanwaltschaft bezeichneten Einrichtungen installiert sind.**²¹⁰ Über die durchgeführten Tätigkeiten und die abgehörten Inhalte ist ein kurzes Protokoll zu verfassen, das zusammen mit den verwendeten Trägern innerhalb von fünf Tagen nach Abschluss der Überwachung bei der bewilligenden Staatsanwaltschaft zu hinterlegen ist. Diese überprüft, dass die vorgenommenen Handlungen mit der Bewilligung übereinstimmen, und ordnet anschliessend **die unverzügliche Vernichtung der Träger und der Protokolle an.**²¹¹

Die mit präventiven Massnahmen in Erfahrung gebrachten Umstände dürfen – Ermittlungszwecke vorbehalten – weder im Strafverfahren verwendet noch in Untersuchungshandlungen erwähnt werden; sie dürfen auch nicht Gegenstand von Zeugenaussagen sein oder in anderer Weise weiterverbreitet werden.²¹²

2.4. Rufdatenrückfassung

Die Daten über den Telefon- und den Fernübertragungsverkehr werden²¹³ – innerhalb der Frist von Artikel 132 Absatz 1 Legislativdekret Nr. 196 von 2003²¹⁴ – mit **begründeter Verfügung des Staatsanwalts**²¹⁵ **auch auf Antrag des Verteidigers des Angeklagten, des Beschuldigten, des Geschädigten oder anderer privater Parteien** beim Anbieter **eingeholt.**²¹⁶ Unter bestimmten Voraussetzungen kann der Verteidiger des Angeklagten oder des Beschuldigten beim Anbieter direkt die Daten über Anschlüsse anfordern, die auf den Namen seines Klienten lauten.²¹⁷

²⁰⁸ Art. 7bis Gesetzesdekret Nr. 144 vom 27.7.2005, umgewandelt aus Gesetz Nr. 155 vom 31.7.2005, mit dringlichen Bestimmungen zur Bekämpfung des internationalen Terrorismus.

²⁰⁹ Art. 226 Abs. 2 Durchführungsbestimmungen itStPO.

²¹⁰ Art. 5 Abs. 3 Gesetzesdekret Nr. 374 vom 18.10.2001, umgewandelt in Gesetz Nr. 438 vom 15.12.2001.

²¹¹ Art. 226 Abs. 3 Durchführungsbestimmungen itStPO.

²¹² Art. 226 Abs. 5 Durchführungsbestimmungen itStPO.

²¹³ Besondere Vorsicht ist bei der Rückfassung der Rufdaten von Parlamentsmitgliedern vorgeschrieben: vgl. Gesetz Nr. 140 vom 20.6.2003, mit Bestimmungen zur Umsetzung von Art. 68 ItVerf.

²¹⁴ Vgl. oben, 1.2.

²¹⁵ Laut KassGH VI. Strafsenat, 4.5.2006, Nr. 33435, richtet sich die Unverwertbarkeit wegen einer Rufdatenrückfassung ohne begründete Verfügung der Gerichtsbehörde nicht gegen den eigentlichen Sachverhalt als Darstellung der darin festgehaltenen Wirklichkeit, sondern gegen die Methoden, mit der dieser in Erfahrung gebracht wurde; entsprechend kann nach Feststellung der Unverwertbarkeit im selben Verfahren eine begründete Verfügung zur Einholung der entsprechenden Daten erlassen werden, damit diese rechtmässig verwertet werden können.

²¹⁶ Gemäss Art. 132 Abs. 2 Legislativdekret Nr. 196 von 2003 mussten nach Ablauf der Frist von Abs. 1 die Daten über den Telefonverkehr, einschliesslich jener über unbeantwortete Anrufe, vom Anbieter weitere 24 Monate lang aufbewahrt werden, die Daten über den Fernübertragungsverkehr hingegen weitere sechs Monate lang, und zwar zum ausschliesslichen Zwecke der Ermittlung und der Bekämpfung der Straftaten nach Art. 407 Abs. 2 Bst. a ItStPO sowie der strafbaren Handlungen zum Schaden von Informatik- oder Fernübertragungssystemen. Die Bestimmung wurde durch Art. 2 Legislativdekret Nr. 109 von 2008 aufgehoben.

²¹⁷ Art. 132 Abs. 3 Legislativdekret Nr. 196 von 2003.

Zum Zwecke der Durchführung **vorbeugender Nachforschungen** gemäss Artikel 226 Durchführungsbestimmungen ItStPO²¹⁸ oder zur **Ermittlung oder Bekämpfung von Straftaten** kann der Innenminister, auch in Zusammenhang mit allfälligen Anträgen ausländischer Ermittlungsbehörden, den Anbietern und Mitarbeitern von Informatik- oder Fernübertragungsdiensten – direkt oder über bestimmte Amtsträger²¹⁹ – anordnen, die Daten über den Fernübertragungsverkehr, nicht aber den Inhalt der Mitteilungen, mit den vorgegebenen Modalitäten und für einen Zeitraum von höchstens neunzig Tagen aufzubewahren und zu schützen. Die Verfügung, die bei begründetem Bedarf für insgesamt höchstens sechs Monate verlängert werden darf, kann vorsehen, dass besondere Modalitäten für die Verwahrung der Daten anzuwenden sind und dass diese Daten den Anbietern und Mitarbeitern von Informatik- oder Fernübertragungsdiensten oder Dritten eventuell nicht zur Verfügung stehen.²²⁰

Die getroffenen Anordnungen sind umgehend, auf jeden Fall aber **innerhalb von achtundvierzig Stunden** ab Zustellung an den Empfänger, **schriftlich** der **Staatsanwaltschaft** des Ausführungsortes **mitzuteilen**, die sie bestätigt, wenn die Voraussetzungen dafür gegeben sind. Wird eine Anordnung nicht bestätigt, verliert sie ihre Wirksamkeit.²²¹

²¹⁸ Vgl. Kap. 2.3.

²¹⁹ Art. 132 Abs. 4ter Legislativdekret Nr. 196 von 2003: „Die Personen, die für die zentralen Fachämter für Informatik oder Fernübertragung der Staatspolizei, der *Carabinieri* und der Finanzwache verantwortlich sind, sowie die anderen Personen, die in Art. 226 Abs. 1 der mit Legislativdekret Nr. 271 vom 28. Juli 1989 erlassenen Durchführungs-, Koordinierungs- und Übergangsbestimmungen zur Strafprozessordnung angegeben sind.“

²²⁰ Art. 132 Abs. 4ter Legislativdekret Nr. 196 von 2003. Dieser Absatz wurde durch Art. 10 Gesetz Nr. 48 vom 18.3.2008 eingefügt, zur Ratifizierung und Umsetzung des Europarat-Übereinkommens über die Cyberkriminalität, abgeschlossen in Budapest am 23. November 2001, mit Vorschriften zur Angleichung der innerstaatlichen Ordnung. „Erhält ein Anbieter oder Mitarbeiter eines Informatik- oder Fernübertragungsdienstes die in Absatz 4ter vorgesehene Anordnung, muss er sie umgehend befolgen und der anordnenden Behörde unverzüglich die Befolgung bestätigen. Er ist ausserdem verpflichtet, die erhaltene Anordnung und die Tätigkeiten, die er daraufhin für den von der Behörde vorgegebenen Zeitraum durchgeführt hat, geheim zu halten. Bei Nichteinhaltung dieser Verpflichtung ist, sofern nicht eine schwerere Straftat vorliegt, Art. 326 StGB anzuwenden.“

²²¹ Art. 132 Abs. 4^{quinqies} Legislativdekret Nr. 196 von 2003.

3. Kosten und Finanzflüsse

Die Betreibung der Dienste für die Telefon-, Fernübertragungs- und Gesprächsüberwachung ist ein Ausgabeposten, der über **40 % der gesamthaften Verfahrenskosten**²²² ausmacht.

Die Überwachungskosten ergeben sich aus drei gesonderten Posten:

- Entschädigung der Betreiber für die Durchführung der Überwachung
- Gerätemiete
- Rufdatenrückfassung²²³

3.1. Rechtsgrundlage für die Finanzierung

Artikel 96 Legislativdekret 259/2003 (Kodex der elektronischen Kommunikation)²²⁴ **verpflichtet die Betreiber** zur Erbringung von Leistungen für gerichtliche Belange aufgrund von Überwachungs- oder

²²² Bericht vom 8.05.2012 des Ministers für die Beziehungen zum Parlament (Giarda), «*Elementi per una revisione della spesa pubblica*», Kap. 4.4., verfügbar unter <http://www.governo.it/backoffice/allegati/66288-7712.pdf>.

Die Aufwendungen für die Überwachungstätigkeiten gehen zulasten des Justizministeriums. Was die vorsorgliche Telefonüberwachung anbelangt, so trägt das Justizministerium laut Stellungnahme des Staatsrates vom 02.04.2003 die dem Betreiber rückzuerstattenden Kosten für die Überwachungsaktivierung, nicht aber die allgemeinen Auslagen für die Bereitstellung der Anlagen in den Polizeistellen bzw. die organisatorischen Auslagen für den Einsatz des abhörenden Polizeipersonals: vgl. Rundschreiben des Justizministeriums, 15.3.2006, «Razionalizzazione e contenimento delle spese di giustizia», verfügbar unter

http://www.giustizia.it/giustizia/it/mg_1_8_1.wp;jsessionid=53BFFCDDF28925BDD9C2C7831D83518B.aipAL01?previousPage=mg_1_8&contentId=SDC50842.

²²³ http://www.camera.it/cartellecomuni/leg15/RapportoAttivitaCommissioni/testi/02/02_cap02_sch01.htm.

²²⁴ Art. 96 Legislativdekret 259/2003:

„1. Die Betreiber sind verpflichtet, aufgrund von Überwachungs- oder Auskunftsbeglehen der zuständigen Gerichtsbehörden Leistungen für gerichtliche Belange zu erbringen; die Zeiten und Modalitäten werden bis zur Genehmigung des Verzeichnisses nach Abs. 2 mit besagten Behörden abgesprochen.

2. Die Leistungen nach Abs. 1 sind in einem speziellen Verzeichnis eingetragen, das die Durchführungsmodalitäten und -zeiten der Leistungen und die spezifischen Pflichten der Betreiber festlegt. Die Entschädigung der Betreiber für die erlittenen Unkosten und die Zahlungsmodalitäten werden durch Dekret des Justizministeriums im Einvernehmen mit dem Wirtschafts- und Finanzminister und dem Minister für Wirtschaftsentwicklung in Form einer Jahresgebühr festgesetzt, die sich unter anderem aus der Menge und der Art der gesamthaft im Vorjahr erbrachten Leistungen bestimmt. Die derart bestimmten Kosten dürfen den Staatshaushalt keinesfalls zusätzlich zu den Kosten belasten, die sich aus der Anwendung der Preisliste von Abs. 4 ergeben. Genehmigt wird das Verzeichnis mit innerhalb von 180 Tagen ab Inkrafttreten des vorliegenden Kodex zu erlassendem Dekret des Ministers für Wirtschaftsentwicklung im Einvernehmen mit dem Justiz- und dem Innenminister.

3. Bei Nichtbeachtung der Pflichten gemäss dem Verzeichnis in Abs. 2 gelangt Art. 32 Abs. 2, 3, 4, 5 und 6 zur Anwendung.

4. Bis zum Erlass des Dekrets nach Abs. 2 zweiter Satz werden Informationen über den Telefonverkehr kostenlos abgegeben. Für Leistungen für gerichtliche Belange, die nicht unter den vorhergehenden Satz fallen, gilt auch weiterhin die Preisliste gemäss Ministerialdekret vom 26.04.2001 des Ministers für Kommunikationswesen, veröffentlicht im Gesetzesanzeiger der Republik Nr. 104 vom 7.05.2001.

5. Zur Erbringung der Leistungen nach Abs. 2 sind die Betreiber verpflichtet, die Verknüpfungsmodalitäten untereinander auszuhandeln, um die Bereitstellung und die Interoperabilität der Leistungen sicherzustellen. Der Minister kann bei Bedarf von Amtes wegen oder, in Ermangelung einer Einigung der Betreiber, auf Antrag eines Betreibers tätig werden.“

Auskunftsbegehren der zuständigen Gerichtsbehörden. Die Telefondienstbetreiber haben Anspruch auf eine finanzielle Gegenleistung für die vorgenommenen Überwachungstätigkeiten. Derzeit richtet sich die Unkostenvergütung nach den Vorschriften des **Ministerialdekrets vom 26. April 2001** (*Listino prestazioni organismi di telecomunicazioni*)²²⁵, das einheitliche Tarife für das gesamte Staatsgebiet festlegt. Das System sieht die Ausstellung von Rechnungen durch die Fernmeldebetreiber vor, bezogen auf **die täglichen Einheitskosten pro überwachte Zielperson**; dies aufgrund der Vorschriften über die Eintreibung der Überwachungskosten, die (zum Zwecke einer allfälligen späteren Eintreibung) in die Akte des Beschuldigten aufzunehmen sind, was deren analytische Quantifizierung voraussetzt²²⁶. Die Abgabe von Informationen über den Telefonverkehr erfolgt **kostenlos** (Art. 96 Abs. 4 Legislativdekret 259/2003).

Diese Regelung gilt **bis zur Genehmigung eines speziellen Verzeichnisses**, das die Durchführungsmodalitäten und -zeiten der Leistungen und die spezifischen Pflichten der Betreiber festlegt.²²⁷ Insbesondere sieht Art. 96 Abs. 2 Legislativdekret 259/2003 den Erlass eines interministeriellen Dekrets vor, das die Entschädigung der Betreiber für die erlittenen Unkosten und die Zahlungsmodalitäten in Form einer Jahresgebühr festsetzt, die sich unter anderem aus der Menge und der Art der gesamthaft im Vorjahr erbrachten Leistungen bestimmt.

3.2. Entscheidungsstrukturen für die Kostentragung einer Überwachung im Einzelfall

Die Kosten für die Telefon-, Fernübertragung- und Gesprächsüberwachung fallen unter die Verfahrenskosten, wie sie im Dekret des Präsidenten der Republik Nr. 115 vom 30.5.2002²²⁸ umschrieben sind. Insbesondere fallen sie, wie das Rundschreiben des Justizministeriums Nr. 6/2002 festhält, in die Kategorie der **ausserordentlichen Auslagen**, d.h. Ausgaben, die im Einheitstext nicht vorgesehen sind und die das befassende Gericht für unerlässlich hält (Art. 70 Dekret 115/2002).

Zur Bestimmung der Kosten hat das Gericht, soweit vereinbar, die Bestimmungen der Artikel 61, 62, 63 und 277²²⁹ des zitierten Dekrets anzuwenden und den Betrag anhand ähnlicher Tarife festzulegen. Dies geschieht anhand des **Zahlungsbefehls**, der in den Artikeln 168, 169, 170 und 171²³⁰ geregelt ist.

²²⁵ Gemäss Art. 6 ist die Preisliste fester Bestandteil des Dekrets und kann beim Ministerium für Kommunikationswesen, Generaldirektion für die Regelung und die Qualität der Dienste, viale America, 201-00144 Rom, sowie bei den Gebietsinspektoraten desselben Ressorts bezogen werden: Die in Art. 1 Abs. 2 bezeichneten Telekommunikationsorganisationen sind gehalten, sich mit der Preisliste zu versehen. Der Zugriff auf die Preisliste ist laut Ministerialbeamten den Telekommunikationsorganisationen vorbehalten.

²²⁶ Als Lösungsansatz unterstrich die technische Kommission für öffentliche Finanzen in ihrem Bericht von 2008 die Notwendigkeit einer Pauschalisierung der täglichen Einheitskosten, die in die Akte des Beschuldigten aufzunehmen sind, Bericht verfügbar unter http://www.camera.it/dati/leg16/lavori/documentiparlamentari/indiceetesti/208/019_RS/00000015.pdf.

²²⁷ Eine Aufforderung zum Erlass der Verfügungen, die der Kodex der elektronischen Kommunikation vorsieht, findet sich in Art. 2 Abs. 82 Gesetz Nr. 244 vom 24.12.2007, wonach „das Justizministerium innert dem 31.01.2008 veranlasst, dass die Verwirklichung eines landesweit einheitlichen, auf Bezirksebene als Oberlandesgericht ausgestalteten Systems für die gerichtlich angeordnete oder bewilligte Telefon-, Gesprächs-, Informatik- oder Fernübertragungsüberwachung in die Wege geleitet wird, allenfalls durch Rationalisierung der derzeit von Rechtspflegeorganen vorgenommenen Tätigkeiten.“, vgl. dazu http://www.camera.it/dati/leg16/lavori/documentiparlamentari/indiceetesti/208/019_RS/00000015.pdf.

²²⁸ Einheitstext der Gesetzes- und Verordnungsbestimmungen über die Verfahrenskosten.

²²⁹ Bestimmungen über den Abbruch widerrechtlich errichteter Bauwerke und die Wiederherstellung des ursprünglichen Zustands im Straf- und Verwaltungsverfahren.

²³⁰ Bestimmungen über den gerichtlich erlassenen Zahlungsbefehl.

Der Zahlungsbefehl ist durch das Gericht auszustellen²³¹; die zur Bezahlung verwendeten Geldmittel werden von einem Beauftragten verwaltet.

Das Verfahren beginnt mit einer Verfügung der Gerichtsbehörde, die eine Überwachung anordnet; die Telefondienstbetreiber bzw. die Anbieter der Apparatmiete stellen die entsprechende Rechnung aus; das Gerichtsamt begleicht die Rechnung, nachdem es die Ordnungsmässigkeit der Leistungen überprüft hat. Die Zahlungsverfügung wird schliesslich ins Register der von der öffentlichen Hand (*Erario*) vorgestreckten Kosten eingetragen und zusammen mit den Belegen an den Beauftragten zur Zahlung weitergeleitet.²³² Die Verfahrenskosten werden über Krediteröffnungen zugunsten der Beauftragten (i.d.R. die Leiter der Oberlandesgerichte und der Generalstaatsanwaltschaften) bewirtschaftet und im Laufe des Jahres mehrmals mittels Verwaltungsdekret der Generaldirektion für Zivilrecht bestimmt.²³³

3.3. Kostenverteilung

Der Staat bevorschusst und trägt die Kosten, die zur Ausübung jeglicher mit einem bestimmten Strafverfahren kausal verbundenen Tätigkeit nötig sind (unabhängig davon, ob diese von Rechtspflegeorganen oder von Dritten in deren Vertretung vorgenommen wird).

Das Rechtsinstitut der **Bevorschussung** bringt mit sich, dass die Kosten des Strafverfahrens von der öffentlichen Hand (*Erario*) vorgestreckt werden, vorbehaltlich der **Möglichkeit**, sie in den vorgesehenen Fällen von den unterliegenden Parteien **zurückzufordern**.²³⁴

Da die Kosten für die Telefonüberwachung als ausserordentliche Auslagen²³⁵ gelten, fallen sie unter die erstattungsfähigen Kosten²³⁶ und können entsprechend zurückgefordert werden, allerdings erst nach erfolgter **Feststellung der strafrechtlichen Verantwortlichkeit** mit anschliessender **Verurteilung zur Tragung der Verfahrenskosten**.²³⁷ Da sich die Zahlungsverpflichtung nicht automatisch aus dem Schuldspruch ergibt, ist sie in der Verfügung eigens festzuhalten.²³⁸

3.4. Finanzierungsmechanismen ausserhalb der einzelnen Verfahren

Die in Kapitel 3.1 beschriebene Regelung nach Massgabe des *Kodex der elektronischen Kommunikation* gilt lediglich für Pflichtleistungen (d.h. Entschädigung der überwachenden Telefondienstbetreiber für die Abhöraktivierung und die Weiterleitung des Signals in den Räumlichkeiten der zuständi-

²³¹ Vgl. KassGH IV. Senat, 22.6.2006, Nr. 21757, wonach bei der Telefonüberwachung die Auszahlung der von den Telefondienstbetreibern für die Rufdatenrückfassung in Rechnung gestellten Kosten dem Gericht obliegt, das zum Zeitpunkt der Einreichung des Auszahlungsantrags befassen ist. Ist der Antrag auf Erlass des Strafbefehls ergangen, fällt der Entscheid über die Verfahrenskosten demnach in die Zuständigkeit des Untersuchungsrichters.

²³² Vgl. Rundschreiben des Justizministeriums 14.12.2010, verfügbar unter http://www.giustizia.palermo.it/CorteAppello/allegati_p_gestione/Circolare_164111.pdf.

²³³ Vgl. Art. 185 Dekret 115/2002. Die Kosten für die Telefon-, Fernübertragung- und Gesprächsüberwachung, einschliesslich jener für die Apparatmiete, sind Kapitel 1363 zu belasten, eingerichtet mit Gesetz zur Genehmigung des Haushaltsvoranschlags für das Finanzjahr 2010: http://www.giustizia.it/giustizia/it/mg_2_9_6_2.wp.

²³⁴ Art. 4 Dekret 115/2002.

²³⁵ Art. 70 Dekret 115/2002; Rundschreiben Nr. 6/2002 vom 8.10.2002 des Justizministeriums, Hauptabteilung für Justizangelegenheiten.

²³⁶ Art. 5 Dekret 115/2002.

²³⁷ Art. 204 Dekret 115/2002.

²³⁸ BOCCHINI / BRUNI / LEONI, Spese nel processo penale, in *Digesto delle Discipline Penalistiche*, Turin 2005, Kap. 2.

gen Staatsanwaltschaft). Die «**Apparatmiete**» (d.h. sämtliche Güter und Dienstleistungen zwecks Aufzeichnung, Aufbewahrung, Auswertung und Verarbeitung der Daten über die Telefon-, Gesprächs-, Fernübertragungs- und Internetüberwachung) erfolgt hingegen **ohne einschlägige gesetzliche Regelung**; die Dienstleistung wird von den einzelnen Staatsanwaltschaften auf dem freien Markt erworben.²³⁹

²³⁹

Diese Art der Leistungsbeschaffung hatte ein Vertragsverletzungsverfahren durch die Europäische Kommission zur Folge. Bemängelt wurde insbesondere das komplette Fehlen eines europäischen Vergabeverfahrens für die Beschaffung und die Miete derartiger Ausrüstungen. Bericht vom 8.05.2012 des Ministers für die Beziehungen zum Parlament (Giarda), Elementi per una revisione della spesa pubblica, Kap. 4.4., verfügbar unter <http://www.governo.it/backoffice/allegati/66288-7712.pdf>. Der Bericht legt die Notwendigkeit dar, die Beschaffung solcher Leistungen zentralisiert und pauschal vorzunehmen sowie die Tarife für Pflichtleistungen im Hinblick auf eine mögliche Pauschalierung dieses Ausgabepostens zu überarbeiten. Da die verarbeiteten Informationen besonders heikel sind, ist ein vertraulicher Vertragsabschluss erforderlich (nach Art. 17 Legislativdekret Nr. 163 vom 12.4.2006, „Kodex der Verträge“).

E. NIEDERLANDE

Die niederländische **Verfassung**²⁴⁰ schützt das Kommunikationsgeheimnis in Artikel 13. Artikel 13 (1) der Verfassung legt fest, dass der Privatsphärenbereich des Telefons und Telegraphs nicht verletzt werden darf, ausser in den gesetzlich vorgesehen Fällen, sofern eine Ermächtigung durch die im Gesetz als zuständig bezeichnete Stelle vorliegt.

In den Niederlanden ist die Telekommunikationsüberwachung in verschiedenen Rechtsvorschriften geregelt. Das **Strafgesetzbuch** (*‘Wetboek van Strafrecht’*)²⁴¹, die **Strafprozessordnung** (*‘Wetboek van Strafvordering’*)²⁴² und das **Gesetz über den Nachrichten- und Sicherheitsdienst**²⁴³ (*‘Wet op de inlichtingen- en veiligheidsdiensten 2002’*)²⁴⁴ enthalten verfahrensrechtliche Regelungen bezüglich der Telekommunikationsüberwachung. Sämtliche Bestimmungen über die Telekommunikationsdienstleistungen und -netzwerke (im Folgenden als *‘der/die Anbieter’* bezeichnet) sind im **Telekommunikationsgesetz** (*‘Telecommunicatiewet’*)²⁴⁵ geregelt. Im Gesetz werden Telekommunikationsnetzwerke und -dienstleistungen als Anbieter definiert.²⁴⁶

Verschiedene, auf der Grundlage des Telekommunikationsgesetzes erlassene Vorschriften, regeln praktische Fragen, welche sich im Zusammenhang mit dem Telekommunikationsgesetz stellen. Für die vorliegende Stellungnahme ist der folgende ministerielle Erlass der Wichtigste (*‘ministeriële regeling’*): **„Erlass der Abhörungskosten und der Datenbeschaffung“**, welche die Kostenentschädigung für die Telekommunikationsüberwachung regelt (*‘Regeling kosten aftappen en gegevensverstrekking’*)²⁴⁷ sowie der königliche Beschluss (*‘Koninklijk Besluit’*) zur **Beschaffung der Telekommunikationsdaten** (*‘Besluit verstrekking gegevens telecommunicatie’*)²⁴⁸, welcher die Beschaffung der Daten von Anbietern der Telekommunikationsüberwachung regelt.

1. Übersicht über die strafprozessualen Grundlagen der Fernmeldeüberwachung

1.1. Strafprozessordnung

Das vorliegende Gutachten legt einen Schwerpunkt auf das Aufzeichnen von Telekommunikation (Telefone) sowie auf die Beschaffung von Internet Datenverkehr (Artikel 126m und 126n nStPO). In den Artikeln 126n ff. der Strafprozessordnung (nStPO) werden verschiedene Straftatbestände umschrieben. Da es sich dabei um sehr detaillierte und technische Tatbestände handelt, ginge eine Darlegung deren Inhaltes über den Umfang des vorliegenden Gutachtens hinaus.

²⁴⁰ Die gesamte niederländische Gesetzgebung ist – auf Niederländisch – verfügbar auf der offiziellen Website der niederländischen Regierung: www.overheid.nl (06.06.2012).

²⁴¹ http://wetten.overheid.nl/BWBR0001854/geldigheidsdatum_06-06-2012 (06.06.2012).

²⁴² http://wetten.overheid.nl/BWBR0001903/geldigheidsdatum_06-06-2012 (06.06.2012).

²⁴³ Eine englische Fassung des Gesetzes über den Nachrichten- und Sicherheitsdienst ist auf der Website des niederländischen Nachrichten- und Sicherheitsdienstes verfügbar:

<https://www.aivd.nl/english/aivd/the-intelligence-and/> (07.06.2012).

²⁴⁴ http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_06-06-2012 (06.06.2012).

²⁴⁵ http://wetten.overheid.nl/BWBR0009950/geldigheidsdatum_06-06-2012 (06.06.2012).

²⁴⁶ Artikel 1.1 (ee und ff) des Telekommunikationsgesetzes definiert ein öffentliches Telekommunikationsnetzwerk als „elektronisches Kommunikationsnetzwerk, das genutzt wird, um öffentliche Telekommunikationsdienste anzubieten, soweit dieses Netzwerk nicht genutzt wird, um Programme zu verbreiten“. Ein öffentliches Telekommunikationsnetzwerk ist ein „für die Öffentlichkeit verfügbarer Dienst, der über ein elektronisches Kommunikationsnetzwerk Signale überträgt, soweit dieser Dienst nicht zur Verbreitung von Programmen genutzt wird“.

²⁴⁷ http://wetten.overheid.nl/BWBR0018150/geldigheidsdatum_06-06-2012 (06.06.2012).

²⁴⁸ http://wetten.overheid.nl/BWBR0011123/geldigheidsdatum_06-06-2012 (06.06.2012).

Artikel 126m nStPO sieht vor, dass Telekommunikationsanbieter durch die Staatsanwaltschaft verpflichtet werden können, einen Datenverkehr offenzulegen, an welchem eine für ein begangenes Delikt tatverdächtige Person mutmasslich teilgenommen haben soll.

Gemäss dieser Bestimmung kann die Staatsanwaltschaft nach Ermächtigung durch den Untersuchungsrichter (s. 2.3.) einen **ermittelnden Beamten** anweisen, mit Hilfe von technischen Hilfsmitteln und in Zusammenarbeit mit einem Anbieter für Telekommunikationsdienstleistungen²⁴⁹ Telekommunikation aufzuzeichnen, sofern verdächtigt wird, dass ein **Delikt** i.S.v. **Artikel 67 (1) nStPO** begangen worden ist, welches aufgrund seiner Natur oder in Verbindung mit anderen, durch den Tatverdächtigen begangene Delikte als schwerwiegende Verletzung der Rechtsordnung angesehen wird. Ausserdem muss die Überwachung für die Untersuchung dringend erforderlich sein.

Bei **Delikten** nach Artikel 67 (1) des Strafgesetzbuches handelt es sich um diejenigen Delikte, für welche **Untersuchungshaft** angeordnet werden kann. Für die meisten dieser Delikte ist eine **maximale Freiheitsstrafe von 4 Jahren oder mehr** vorgesehen. Neben den Delikten, welche eine Freiheitsstrafe von 4 Jahren oder mehr vorsehen, enthält Art. 67 (1b und 1c) nStPO eine abschliessende Liste von Delikten, welche von dieser Bestimmung erfasst sind und eine maximale Freiheitsstrafe von weniger als 4 Jahren vorsehen.²⁵⁰

Artikel 552oa StPO hält fest, dass die in Artikel 126m nStPO vorgesehene Massnahme auch ausgeübt werden kann, wenn hierfür ein gestützt auf einen Vertrag oder ein Abkommen zulässiges Gesuch bei den **Behörden eines anderen Staates** eingegangen ist.

Gemäss Artikel 126n nStPO kann die **Staatsanwaltschaft** im Interesse der Ermittlungen die **Bekanntgabe von Informationen zum gesamten Datenverkehr via Telekommunikationsinfrastruktur** oder via öffentliche Telekommunikationsinstallation, in welchem der Tatverdächtige mutmasslich teilge-

²⁴⁹ Der Begriff „Telekommunikation“ bedeutet im Sinne dieser Bestimmung Kommunikation, die nicht für die Öffentlichkeit bestimmt ist und die über Telekommunikationsinfrastruktur oder über Telekommunikationsinstallationen, welche ihre Dienstleistungen der Öffentlichkeit anbieten, stattfindet.

²⁵⁰ Die abschliessende Liste von Delikten, welche von Artikel 67 (1b) nStPO erfasst sind und eine maximale Freiheitsstrafe von weniger als 4 Jahren vorsehen:

Schwerwiegende Delikte gegen die öffentliche Ordnung (Artikel 132, 138a, 138b, 139c, 139d (1) und 2, 141a, 137c (2), 137d (2), 137e (2), 137g (2) des Strafgesetzbuches); ernsthafte Gefährdung der allgemeinen Sicherheit von Personen und Eigentum (Artikel 161sexies (1 und 2) des Strafgesetzbuches); Schwerwiegende Delikte gegen die Staatsgewalt (Artikel 184a des Strafgesetzbuches); Schwerwiegende Delikte gegen die Sittlichkeit (Artikel 254a, 248d, 248e des Strafgesetzbuches); Schwerwiegende Delikte gegen die persönliche Freiheit (personal liberty) (Artikel 285 (1), 285b des Strafgesetzbuches); körperlicher Missbrauch (Artikel 300 (1) des Strafgesetzbuches); Veruntreuung (Artikel 323a des Strafgesetzbuches); Betrug (Artikel 326c (2) des Strafgesetzbuches); Sachbeschädigung oder Schadensverursachung (Artikel 350a, 351 des Strafgesetzbuches); Schwerwiegende Delikte im Zusammenhang mit der Schiff- und Luftfahrt (Artikel 395 des Strafgesetzbuches); Kooperation nach begangener Tat (Artikel 417bis, 420quater des Strafgesetzbuches).

Die abschliessende Liste von Delikten, welche von Artikel 67 (1) StPO erfasst sind und eine maximale Freiheitsstrafe von weniger als 4 Jahren vorsehen:

Artikel 122 des Tiergesundheitsgesetzes (*Gezondheids- en welzijnswet voor dieren*); Artikel 175 (2b und 3) bezüglich (1b) Strassenverkehrsgesetz 1994 (*Wegenverkeerswet 1994*); Artikel 30 (2) des Gesetzes über aussergewöhnliche Befugnisse ziviler Behörden (*Wet buitengewone bevoegdheden burgerlijk gezag*); Artikel 52, 53 (1) und 54 Militärdienstverweigerungsgesetz (*‘Wet gewetensbezwaren militaire dienst’*); Artikel 31 Gesetz über das Glücksspiel (*Wet op de kansspelen*); Artikel 11 (2) des Opiumgesetzes (*Opiumwet*); Artikel 55 (2) des Waffen- und Munitionsgesetzes (*Wet wapens en munitie*); Artikel 5:56, 5:57 und 5:58 Finanzaufsichtsgesetz (*Wet op het financieel toezicht*); Artikel 11 des Gesetzes über das befristete Hausverbot (*Wet tijdelijk huisverbod*).

nommen hat, anordnen, sofern einer der folgenden Fälle vorliegt: eine Überführung *in flagrante delicto*, der Verdacht auf ein Delikt i.S.v. Artikel 67 (1) nStPO oder der Verdacht auf ein Delikt, auf welches in Artikel 138a des Strafgesetzbuches Bezug genommen wird („eine Person, die absichtlich und widerrechtlich ein von einem Computer gesteuertes Gerät oder System zur Speicherung und Verarbeitung von Daten oder in Teile eines solchen Gerätes oder Systems eindringt“).

1.2. Allgemeiner Nachrichten- und Sicherheitsdienst der Niederlande

Neben den prozessualen Regelungen der Strafprozessordnung stehen dem **Allgemeinen Nachrichten- und Sicherheitsdienst** der Niederlande (im Folgenden AIVD) Befugnisse im Bereich der Telekommunikationsüberwachung zu (siehe 2.3). Artikel 6 des Gesetzes über den Nachrichten- und Sicherheitsdienst regelt, dass der AIVD unter anderem die Aufgabe hat, **im Interesse der nationalen Sicherheit** Ermittlungen zu führen bezüglich Organisationen und Personen, welche aufgrund der Ziele, die sie verfolgen, oder aufgrund ihrer Handlungen, Anlass zu ernsthaftem Verdacht geben, dass sie eine Gefahr für das demokratische Rechtssystem oder für die Sicherheit und die wesentlichen Staatsinteressen darstellen.

2. Übersicht über Prozess- und Organisationsstrukturen

2.1. Mitwirkungspflicht der Anbieter

Gemäss Artikel 13.1 des Telekommunikationsgesetzes dürfen Anbieter ihren Kunden nur solche Netzwerke und Dienstleistungen zur Verfügung stellen, welche abgehört werden können. Die technischen Einzelheiten darüber, wie eine Dienstleistung oder ein Netzwerk für Abhörungen empfänglich gemacht werden können, sind im *‘Besluit aftappen openbare telecommunicatiewerken- en diensten’*²⁵¹ geregelt.

Anbieter sind verpflichtet, **Anträgen auf Abhörung oder Aufzeichnung** von Telekommunikation nachzukommen, wenn die in Frage stehende Telekommunikation über ihr Netzwerk oder über ihre Dienstleistungen stattfindet und wenn der Antrag durch die einschlägigen Bestimmungen der Strafprozessordnung oder des Gesetzes über den Nachrichten- und Sicherheitsdienst 2002 gedeckt ist (Artikel 13.2 Telekommunikationsgesetz). Geht ein Antrag gemäss Artikel 126n StPO oder gemäss Artikel 28 des Gesetzes über den Nachrichten- und Sicherheitsdienst 2002 ein, so sind die **Anbieter ausserdem verpflichtet, Auskunft über Nutzerdaten und Datenverkehrsinformationen zu erteilen** (Artikel 13.2a Telekommunikationsgesetz).

Wie oben dargelegt, sind Telekommunikationsanbieter (Telefon- und Internetanbieter) verpflichtet, der zuständigen Behörde Auskunft über gewisse Informationen zu erteilen. Gemäss Artikel 4 (1) des Dekrets zur Beschaffung von Telekommunikationsdaten muss ein **Telefonanbieter** jederzeit in der Lage sein, folgende Informationen über seine Netzwerk- und Dienstleistungsnutzer bekannt zu geben: Name; Adresse und Nummer; Postleitzahl und Wohnsitz; Information zu den genutzten Dienstleistungen und zu den Nummern, welche dem Nutzer zur Verfügung gestellt wurden sowie Informationen zum Anbieter, welcher dem Nutzer Dienstleistungen erbracht hat.

Die Informationen, über welche **Internetanbieter** verfügen müssen, weichen davon folgendermassen leicht ab: Name; Adresse und Nummer; Postleitzahl und Wohnsitz; Information zu den genutzten Dienstleistungen, einschliesslich zur Verbindung; Nutzernamen; Name zum Einloggen; E-Mail Adresse; ID-Nummern der Geräte; Internet-Protokollnummern, welche dem Nutzer bei der Aktualisierung der Datei zugeteilt wurden sowie der Name des Anbieters.

²⁵¹

http://wetten.overheid.nl/BWBR0009999/geldigheidsdatum_07-06-2012 (07.06.2012).

2.2. Zentralstelle für Telekommunikationsermittlungen (CIOT)

Um zu verhindern, dass jeder einzelne Ermittlungsbeamte mit unterschiedlichen Anbietern in Kontakt treten muss, wurde vom Sicherheits- und Justizministerium **eine Zentralstelle**, genannt CIOT, eingerichtet, bei welcher **Kundendaten** eingeholt werden können. Die Grundlage für das CIOT findet sich in Artikel 2 des Dekrets zur Beschaffung von Telekommunikationsdaten. Telefonunternehmen und Internetanbieter sind verpflichtet, ihre Kundendaten alle 24 Stunden zu aktualisieren (Artikel 4 (3) des Dekrets zur Beschaffung von Telekommunikationsdaten). Für diese Telefon- und Dateninformationen betreibt das CIOT ein automatisches Informationssystem (CIS). Ermittlungsbeamte können ihren Antrag über das CIS-System stellen. Das System leitet diesen Antrag sodann an die Datenbank der Anbieter weiter. Auf die Frage z.B., welche Daten zur Telefonnummer eines Tatverdächtigen gehören, antwortet das System innert Sekunden und liefert Name und Adresse, sodass der Ermittlungsbeamte seine Ermittlung weiterführen kann. Die Arbeitsmethoden des CIOT sind im Dekret selbst sowie in einer darauf basierenden Verordnung festgelegt.

Folgenden Organisationen hat das Sicherheits- und Justizministerium eine **Bewilligung zur Nutzung des Informationssystems des CIOT** erteilt: Ermittlungsbehörden (Polizei, Departement der Staatspolizei für nationale Ermittlungen (*Rijksrecherche*), Militärpolizei (*Koninklijke Marechaussee*), Staatsanwaltschaft (OM, *landelijk parket*) und 112); Besondere Untersuchungsbehörden (FIOD, AID, IOD, *Inspectie SZW* und *Inspectie voor de gezondheidszorg*), Nachrichten- und Sicherheitsdienst (AIVD und Verteidigungs-, Nachrichten- und Sicherheitsdienst). Nur eine bestimmte Anzahl Personen pro Organisation wurde vom Minister dazu ernannt, mit dem CIOT in Kontakt treten zu können.

2.3. Verfahren nach Strafprozessordnung

Ein Beschluss über die **Aufzeichnung von Telekommunikation** nach Artikel 126m nStPO hat schriftlich zu erfolgen und muss folgende Informationen enthalten: a. das Delikt und, soweit bekannt, den Namen oder eine möglichst genaue Beschreibung des Tatverdächtigen; b. die Tatsachen oder Umstände, welche darauf schliessen lassen, dass die Voraussetzungen von Artikel 67 (1) nStPO erfüllt sind; c. die Verbindungsnummer sowie Name und Adresse des Nutzers; d. die Dauer der Gültigkeit des Beschlusses und e. den Namen des technischen Hilfsmittels, welches zur Aufzeichnung beigezogen wird. Der **Beschluss** ergeht **durch den Staatsanwalt**, nachdem dieser vom **Untersuchungsrichter** (*‘Rechter-Commissaris’*) schriftlich dazu beauftragt wurde. Die Gültigkeitsdauer des Beschlusses beträgt **höchstens 4 Wochen** und kann beliebig oft um höchstens 4 Wochen verlängert werden. Änderungen, Verlängerungen oder Ergänzungen können nur auf der Grundlage einer schriftlichen Verfügung vorgenommen werden. Bei Dringlichkeit **kann die Verfügung mündlich erfolgen**. Innerhalb von 3 Tagen muss diese dann schriftlich nachgereicht werden (Artikel 126l (4) ff. nStPO).

Der **Antrag auf Datenherausgabe nach Artikel 126n nStPO** kann bei jedem nach dem Telekommunikationsgesetz festgelegten Telekommunikationsanbieter eingereicht werden. Die Anfrage für einen Antrag ergeht durch den **Staatsanwalt** in der Form einer Erklärung (*‘proces verbaal’*) und enthält folgende Punkte: a. das Delikt und, soweit bekannt, den Namen oder eine möglichst genaue Beschreibung des Tatverdächtigen; b. die Tatsachen oder Umstände, welche darauf schliessen lassen, dass die Voraussetzungen von Artikel 67 (1) nStPO erfüllt sind; c. soweit bekannt, den Namen der Person, über welche Informationen angefordert werden; d. die Bezeichnung der Information, welche angefordert wird sowie die Angabe der Zeitspanne, über welche die Anfrage betrifft. Für jede Änderung in einem oder in mehreren dieser Punkte hat eine neue Erklärung durch den Staatsanwalt zu ergehen. Die Anfrage für einen Antrag betrifft eine Zeitspanne von höchstens 3 Monaten. Eine Verfügung durch den Untersuchungsrichter ist nicht erforderlich.

2.4. Verfahren nach dem Gesetz über den Nachrichten- und Sicherheitsdienst

Das Anordnen von Massnahmen eines Anbieters von Dienstleistungen²⁵² gemäss Gesetz über den Nachrichten- und Sicherheitsdienst, ist nur erlaubt, sofern das Gesetz dies nicht anders bestimmt, sofern eine Bewilligung des **zuständigen Ministers** oder, im Namen des Ministers, des zuständigen Dienstvorstehers vorliegt. Der Dienstvorsteher kann durch schriftlichen Beschluss einen untergeordneten Beamten ernennen, welcher in seinem Namen die Bewilligung erteilt. Dem Minister ist eine Kopie des Beschlusses zuzustellen. Die Bewilligung wird, unter Vorbehalt einer abweichenden gesetzlichen Regelung, für eine **Dauer von höchstens 3 Monaten** erteilt. Auf Anfrage kann sie jedes Mal um drei Monate verlängert werden (Artikel 19 des Gesetzes über den Nachrichten- und Sicherheitsdienst).

Artikel 25 gestattet das gezielte Abhören, Empfangen, Aufnehmen und Überwachen jeder Form von Konversation, Telekommunikation oder Datenübermittlung über automatisierte Hilfsmittel, unabhängig vom Ort des Geschehens. Für die Durchführung einer solchen Massnahme ist die Bewilligung des Ministers erforderlich, welche auf Gesuch des Dienstvorstehers erteilt wird. Massnahmen betreffend Konversationen, Telekommunikation oder Datenverkehr via automatisierte Hilfsmittel darf der Verteidigungs-, Nachrichten- und Sicherheitsdienst nur dann ergreifen, wenn hierfür eine Bewilligung vom Minister für Inneres und Königliche Angelegenheiten erteilt wurde. **Gesuche hierfür werden vom Dienstvorsteher gestellt** und enthalten mindestens: eine Angabe der Massnahme, welche vom Dienst ergriffen werden soll; Nummern, welche die Identifizierung des Nutzers²⁵³ ermöglichen könnten sowie Information zur von der in Frage stehenden Massnahme mitbeteiligten Person oder Organisation und der Grund, welcher die Ergreifung der in Frage stehenden Massnahme erforderlich macht.²⁵⁴

Gestützt auf Artikel 28 des Gesetzes über den Nachrichten- und Sicherheitsdienst **können die Anbieter von Dienstleistungen ein Gesuch** um Herausgabe/Bekanntgabe von Nutzerdaten und Informationen über den Telekommunikationsverkehr eines Nutzers **direkt bei einem Telekommunikationsanbieter** im Sinne des Telekommunikationsgesetzes **einreichen**. Das Gesuch kann sowohl Daten, die zum Zeitpunkt seiner Einreichung schon verarbeitet wurden als auch solche, die künftig zu bearbeiten sind, betreffen. Um ein Gesuch bei einem Telekommunikationsanbieter einreichen zu können, ist keine Bewilligung nach Artikel 19 des Gesetzes erforderlich. Das Gesuch hat schriftlich durch den Dienstvorsteher zu ergehen und folgende Angaben zu enthalten: die Nummer oder Information zu Name und Wohnsitz oder Aufenthaltsort der Person bzw. die zur Nummer gehörende registrierte Organisations-Dienststelle; eine Beschreibung der gewünschten Information sowie eine Angabe des Zeitraumes, über welchen die Information ergehen soll. Die Anbieter von Dienstleistungen sind ausserdem befugt (Artikel 29 des Gesetzes über den Nachrichten- und Sicherheitsdienst), die **Telekommunikationsanbieter um Bekanntgabe von Informationen** zu Name, Adresse, Postleitzahl, Aufenthaltsort sowie den von der Person genutzten Telekommunikations-Dienstleistungen zu ersuchen. Auch hierfür ist keine Bewilligung nach Artikel 19 des Gesetzes erforderlich und das Gesuch ist vom Vorsteher des zuständigen Dienstes, oder in seinem Namen, einzureichen.

²⁵² Eine Dienstleistung nach dem Gesetz über den Nachrichten- und Sicherheitsdienst ist entweder der Allgemeine Nachrichten- und Sicherheitsdienst oder der Verteidigungs-, Nachrichten- und Sicherheitsdienst.

²⁵³ Die Definition des Begriffes „Zahl“ ist in Artikel 1.1 bb des Telekommunikationsgesetzes enthalten. Der Begriff „Zahl“ umfasst demnach Zahlen, Buchstaben sowie Symbole – einzeln oder in Kombination, welche dazu dienen, Zugang zu geben oder Nutzer und Netzwerkelemente zu identifizieren (z.B. Anbieter von Netzwerkdienstleistungen).

²⁵⁴ Für kabellose Telekommunikation sind zwei verschiedenen Zulassungsverfahren vorgesehen (Artikel 26 und 27 des Gesetzes über den Nachrichten- und Sicherheitsdienst).

Verfügt der Anbieter nicht über die ersuchte Information und ist Artikel 25 oder 28 des Gesetzes einschlägig, so kann der Anbieter von Dienstleistungen den Telekommunikationsanbieter dazu anhalten, die Information zu beschaffen und auszuhändigen. Die Anbieter von Dienstleistungen sind befugt, technische Hilfsmittel zu benutzen, sofern dies für die Beschaffung der Nummer notwendig ist.

3. Kosten und Finanzflüsse

3.1. Rechtsgrundlage für Finanzierung

Artikel 13.6 des Telekommunikationsgesetzes regelt die Kosten und die Finanzierung der Telekommunikationsüberwachung. Artikel 13.6 (3) sieht vor, dass in einem ministeriellen Erlass ('ministeriële regeling') weitere Vorschriften über die Festsetzung und den Ersatz von Telekommunikationsüberwachungskosten im Sinne dieser Bestimmung festgesetzt werden können. Am 30. März 2005 trat der ministerielle Erlass bezüglich Abhörungskosten und Informationsbeschaffung in Kraft. Diese Regelung enthält detaillierte Information über die Kosten und die Entschädigung, welche bei Telekommunikationsüberwachungsmassnahmen anfallen.

Neben den einschlägigen Rechtsvorschriften existiert eine **Abfindungsvereinbarung** über die Entschädigung für Telekommunikationsüberwachung, welche die niederländische Regierung **mit den fünf grössten niederländischen Telekomaniern** (T-Mobile, KPN, UPC, Ziggo und Vodafone) ausgemacht hat (siehe 3.4). Die rechtliche Grundlage für diese Vereinbarung ist in Artikel 3.3 des Erlasses bezüglich Abhörungskosten und Informationsbeschaffung zu finden, welcher die Behörden ermächtigt, zur Regelung der zurückzuerstattenden Kosten sowie über die Bedingungen solcher Rückzahlungen ein Sonderabkommen zu treffen.

3.2. Entscheidstrukturen über Kostentragung einer Überwachung im Einzelfall

3.2.1. Allgemeines

Gemäss Artikel 13.6 (1) des Telekommunikationsgesetzes sind die **Investitions-, Nutzungs- und Instandhaltungskosten**, welche den Anbietern öffentlicher Telekommunikationseinrichtungen bei der Erfüllung ihrer gesetzlichen Pflichten zur Telekommunikationsüberwachung anfallen, **durch die Anbieter zu tragen**. Für die in diesem Zusammenhang anfallenden **Verwaltungs- und Personalkosten** haben die Anbieter einen Anspruch auf **Kompensation durch den niederländischen Staat**. Der ministerielle Erlass bezüglich Abhörungskosten und Informationsbeschaffung enthält Richtwerte für die Kompensation der mit den verschiedenen Überwachungsmassnahmen verbundenen Handlungen:

Anhang III des Erlasses bezüglich Abhörungskosten und Informationsbeschaffung enthält folgende Angaben:

Richtwerte²⁵⁵:

1.	Installierung von Überwachungsmassnahmen	€ 15,07
2.	Ausweitung der Überwachungsmassnahme	€ 15,07

²⁵⁵ Dies ist eine inoffizielle Übersetzung der einschlägigen Bestimmung. Die niederländische Regelung zu den aktuellen Kompensationsbeträgen vom 1. Juni 2011 – 1. Juni 2012 (die jährliche Indexierung findet jeweils am 1. Juni jedes Kalenderjahres statt; die jüngste Indexierung mit den fraglichen Beträgen per 1. Juni 2012 wurde noch nicht veröffentlicht) ist verfügbar unter:
<https://zoek.officielebekendmakingen.nl/stcrt-201110165.html?zoekcriteria=%3fzkt%3dUitgebreid%26pst%3dStaatscourant%26vrt%3dindexering%26bafta%26p%26kd%3dInDeGeheleText%26dpr%3dAlle%26spd%3d20120606%26epd%3d20120606%26sdt%3dDatumPublicatie%26ap%3d%26pnr%3d1%26rpp%3d10&resultIndex=0&sorttype=1&sortorder=4>
 (31.05.2012).

3.	Vorzeitiger Abschluss einer Überwachungsmassnahme	€ 15,07
4.	Lösung technischer Probleme (pro Stunde)	€ 30,12
5.	Regelmässige Zulieferung von Dateien an CIOT (pro Tag)	€ 30,12
6.	Beschaffung von Informationen basierend auf aktuellen, identifizierenden Daten	€ 7,52
7.	Beschaffung von Informationen basierend auf alten, identifizierenden Daten	€ 7,52
8.	Beschaffung von Informationen basierend auf alten Nutzerverkehrsdaten	€ 7,52
9.	Beschaffung von Informationen basierend auf einer identifizierenden Tatsache	€ 30,12
10.	Datenanalyse	€ 30,12
11.	Beschaffung von Informationen auf der Grundlage von Mastdaten	€ 30,12
12.	Kooperation in allen in dieser Liste nicht enthaltenen komplexen Suchanfragen (pro Stunde)	€ 30,12

Gemäss Anhang I des Erlasses sind diese Kosten rückerstattbar, soweit es sich dabei um **Personalkosten** handelt. Diese Personalkosten werden um 5% erhöht für „andere Kosten“ bezüglich die in Anhang III aufgelisteten Handlungen, soweit diese zusätzlichen Handlungen eine der folgenden Tätigkeiten umfassen: Entgegennahme der Frage/des Auftrages, administrative/technische Prüfung, Eingabe von Daten in das System, Offenhalten der Verbindung, Kontrolle im System, Aktualisierung der Datei, das Senden einer Antwort, Aktenablage und Rechnungsstellung.

Alle Beträge nach Anhang III werden um 50% bzw. um 100% erhöht, wenn die Anfrage **dringend** ist und **ausserhalb der Geschäftszeiten, an Wochenenden oder an nationalen Feiertagen** gestellt wird.

3.2.2. Praxis

Der Telekommunikationsanbieter gibt der Behörde, welche die Überwachung anordnete, eine **Auflistung der Kosten**, welche nach Beendigung einer Überwachung rückerstattet werden können. Jeder Kostenvoranschlag enthält eine genaue Angabe der ausgeführten Tätigkeiten (unter Bezugnahme auf die Handlungskategorien aus der Übersicht über die Richtwerte in Anhang III) sowie der dafür aufgewendeten Zeit (Artikel 3 des ministeriellen Erlasses).

Der **Kostenvoranschlag sollte folgende Informationen enthalten** (Anhang II des ministeriellen Erlasses):

1. Referenznummer der Staatsanwaltschaft oder Referenznummer, wenn es sich um ein Gesuch des Allgemeinen Nachrichten- und Sicherheitsdienstes handelt;
2. Identifizierung des Gegenstandes (die Telefonnummer der Telefonleitung, welche abgehört werden soll, die „International Mobile Equipment Identity“ Nummer (IMEI Nummer), Information zum Login, IP-Adresse, E-Mail Adresse, usw.);
3. Auftraggeber (Name des mit der Sache befassten Staatsanwalts oder Untersuchungsrichters oder des zuständigen Beamten);
4. Eingangsdatum und -zeit (für Abhörvorgänge und Versorgung mit künftigen Verkehrsdaten);
5. Enddatum und Zeit (für Abhörvorgänge und Versorgung mit künftigen Verkehrsdaten);
6. Verwaltungsbezirk des Auftraggebers;
7. Auftraggeber (gesuchstellende Behörde);
8. Kontaktdaten der bei der gesuchstellenden Behörde zuständigen Person.

Wenn die Kosten des Anbieters die **einschlägigen Richtwerte übersteigen**, muss der Anbieter diesen höheren Betrag begründen. Ausserdem muss der Anbieter auf Gesuch der beteiligten Behörde ergänzende Informationen über die verrichtete Arbeit und den verwendeten Stundenansatz sowie die Erklärung eines Rechnungsprüfers zur Kostenübersicht aushändigen.

Wenn es dem Anbieter gelingt, einen höheren Betrag einzufordern, so wird dieser Betrag zurückerstattet, soweit diese Kosten – im Rahmen der Angemessenheit – als nötig erachtet werden.

3.3. Kostenverteilung

Siehe oben Ziffer 3.2.

3.4. Finanzierungsmechanismen ausserhalb der einzelnen Verfahren

Für die erste **Abfindungsvereinbarung** zwischen der niederländischen Regierung und den fünf grössten niederländischen Anbietern wurde eine Gültigkeitsdauer von drei Jahren vereinbart, namentlich von 2005 bis 2008. Nach Ablauf dieser Gültigkeitsdauer wurde eine neue Abfindungsvereinbarung mit einer Gültigkeit von drei Jahren getroffen. Der Inhalt dieser Vereinbarung ist **aus Sicherheitsgründen geheim**. Die Regierung erklärte aber, die vereinbarte Datenbeschaffungsqualität sei in einer ausführlichen Dienstgütevereinbarung festgehalten worden. In dieser Dienstgütevereinbarung ist der Schwerpunkt auf die Geschwindigkeit der Datenbeschaffung gelegt worden. Auch ist die Leistungserfüllung Teil der Vereinbarung sowie der Einbau eines Anreizes für die effizientere Herstellung von **Abhören, Aufnehmen und das Liefern von Daten**. Es ist in der Vereinbarung keine spezielle, separate Regel auf den Privatbereich vorgesehen, da die Vereinbarung unter die existierenden legalen Verpflichtungen des Privatbereichs fällt.²⁵⁶

²⁵⁶

TK 32500 VII, nr. 6 Verslag houdende een lijst van vragen en antwoorden. 'Vaststelling van de begrotingsstaten van het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties voor het jaar 2010' from 10 november 2010, verfügbar (auf Niederländisch) unter https://zoek.officielebekendmakingen.nl/kst-32500-VII-6.html?zoekcriteria=%3fzkt%3dUitgebreid%26pst%3dStaatsblad%257cStaatscourant%257cTractatenblad%257cParlementaireDocumenten%26vrt%3dVodafone%2ben%2bZiggo%2ben%2bvergoedingen%26zkd%3dInDeGeheleText%26dpr%3dAlle%26sdt%3dDatumPublicatie%26ap%3d%26pnr%3d2%26rpp%3d10%26_page%3d1%26sorttype%3d1%26sortorder%3d4&resultIndex=3&sorttype=1&sortorder=4 (06.06.2012).

4. Tarifvergleich Schweiz – Niederlande

Schweiz					Niederlande				
Massnahme	Gebühren		Entschädigungen		Massnahme	Gebühren		Entschädigungen	
	CHF	Anm.	CHF	Anm.		€	Anm.	€	Informationsgewinn
TELEFONÜBERWACHUNG AKTIV (Überwachung leitungsvermittelte Fernmeldedienste)	2410	CS 1-3: Nutzinformationen und Verkehrsdaten	1330	Art. 16 lit. a, b und c VÜPF: 1. die verfügbaren Adressierungselemente (Rufnummern der abgehenden und ankommenden Kommunikationsvorgänge), 2. die tatsächliche bekannte Zielrufnummer und die eingeschalteten verfügbaren Rufnummern, falls der Anruf um- oder weitergeleitet wurde, 3. die erzeugten Signale, einschliesslich der Zeichengabe für den Bereitschaftszustand, die Parameter der Fernmeldeanlagen (z.B. IMSI-Nummer, IMEI-Nummer) und die erzeugten Signale für die Aktivierung der Konferenzschaltung oder der Anrufumleitung, 4. bei Mobiltelefonie: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist, 5. das Datum und die Uhrzeit	Telefonüberwachung		Gebühren werden im Gesetz nicht gesondert angeführt	15,07	Annex III Regulation: Nr.1 Einrichtung der Überwachungsverbindung (placing a tap)
								7,52	Nr. 6: Datenübermittlung (information supply based on actual identifying data)
					Auskunft über Verkehrsdaten			30,12	Nr. 10: Standortbestimmung (information supply based on data from the data mast)

TELEFONÜBERWACHUNG RÜCKWIRKEND	700	CS 4: Historische Verkehrsdaten	540	Art. 16 lit. d VÜPF: 1. die verfügbaren Adressierungselemente (Rufnummern der abgehenden und eingehenden Kommunikationsvorgänge, sofern diese der Fernmeldediensteanbieterin bekannt sind), 2. die Kommunikationsparameter des Endgerätes der Mobiltelefonie und die Parameter zur Teilnehmeridentifikation (wie die IMSI-Nummer und die IMEI-Nummer), 3. bei Mobiltelefonie: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist, 4. das Datum, die Zeit und die Dauer der Verbindung	Auskunft über historische Daten und historische Verkehrsdaten			7,52	Nr. 7: Übermittlung historischer Identifikationsdaten (information supply based on historical identifying information)
	2200	CS 5: Antennensuchlauf (Geografische Koordinaten)	2000	Art. 16 lit. e VÜPF: der Antennensuchlauf: rückwirkende Eruiierung aller an einem bestimmten Standort angefallenen mobilen Kommunikationsvorgänge während eines bestimmten Zeitraumes, sofern es zum Aufbau einer Kommunikation gekommen ist.				7,52	Nr. 8: Übermittlung historischer Verkehrsdaten (information supply based on historical traffic data of a user)
	600	CS 6: Antennensuchlauf (Cell ID)	600	Definition nach Art. 16 lit. e VÜPF (siehe oben)					
INTERNETÜBERWACHUNG (Überwachung paketvermittelte Fernmeldedienste)	4160	PS 1: Nutzinformationen und Verkehrsdaten gemäss Art. 24a lit. a und b VÜPF	1330	Art. 24a lit. a und b: a. die Übermittlung sämtlicher Daten, die über den überwachten Zugang gesendet oder empfangen werden; b. die Bereitstellung und die simultane oder periodische Übermittlung der folgenden Angaben über den Internetzugang: 1. das Datum und die Uhrzeit, zu der die Datenverbindung hergestellt und getrennt wird, 2. die Art der Datenverbindung oder des Anschlusses, 3. die verwendeten Anmeldungsdaten (Log-in),	Internetüberwachung			7,52	Nr. 6: Datenübermittlung anhand von Identifikationsdaten (information supply based on actual identifying data)

	800	PS 2: Verkehrsdaten gemäss Art. 24a lit. b VÜPF	640	4. die verfügbaren Adressierungselemente, insbesondere des Ursprungs der Kommunikation, 5. die Kommunikationsparameter der Endgeräte und die Parameter zur Teilnehmeridentifikation (z.B. MAC-Adresse, IMEI-Nummer, IMSI-Nummer), 6. bei Zugang über ein Mobilfunknetz: die Bestimmung und die periodische Übertragung des Zell-Identifikators (Cell ID), des Standortes und der Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person momentan verbunden ist Art. 24a lit. b VÜPF: b. die Bereitstellung und die simultane oder periodische Übermittlung der folgenden Angaben über den Internetzugang: 1. das Datum und die Uhrzeit, zu der die Datenverbindung hergestellt und getrennt wird, 2. die Art der Datenverbindung oder des Anschlusses, 3. die verwendeten Anmeldungsdaten (Log-in), 4. die verfügbaren Adressierungselemente, insbesondere des Ursprungs der Kommunikation, 5. die Kommunikationsparameter der Endgeräte und die Parameter zur Teilnehmeridentifikation (z.B. MAC-Adresse, IMEI-Nummer, IMSI-Nummer), 6. bei Zugang über ein Mobilfunknetz: die Bestimmung und die periodische Übertragung des Zell-Identifikators (Cell ID), des Standortes und der Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person momentan verbunden ist, 7. die technischen Änderungen, die während der Verbindung stattfinden,				7,52	Nr. 7: Übermittlung historischer Identifikationsdaten (information supply based on historical identifying information)
--	-----	---	-----	--	--	--	--	------	--

				und, falls bekannt, ihre Ursachen;					
	2410	PS 3: Nutzerinformationen und Verkehrsdaten gemäss Art. 24a lit. c VÜPF	1330	Art. 24a lit. c VÜPF: die Übermittlung der Nutzerinformationen, die über die überwachte Anwendung gesendet oder empfangen werden;				7,52	Nr. 8: Datenübermittlung anhand von historischen Verkehrsdaten (information supply based on historical traffic data of a user)
	800	PS 4: Verkehrsdaten einer Anwendung gemäss Art. 24a lit. d VÜPF	640	Art. 24a lit. d VÜPF: die Bereitstellung und die simultane oder periodische Übermittlung folgender Angaben über die überwachte Anwendung: 1. das Datum und die Uhrzeit der Kommunikation (Beginn und Ende), 2. die verfügbaren Adressierungselemente, insbesondere diejenigen des Ursprungs und des Ziels der Kommunikation, 3. die verwendeten Anmeldungsdaten (Log-in), 4. bei der Überwachung von E-Mail-Verkehr: die Umschlaginformationen gemäss dem benutzten Protokoll, 5. die anderen verfügbaren Kommunikationsparameter, 6. die technischen Änderungen während der Kommunikation und ihre Ursachen, falls bekannt.				30,12	Nr. 9: Datenübermittlung anhand von identifizierenden Dateien (file analysis)

	700 250	PS 5: Verkehrsdaten nach Art. 24b lit. a VÜPF - Angaben nach Ziffern 1-6 - Angaben nach Ziffern 2,3, 4 und 5 (jede Kombination möglich)	540 250	Art. 24b lit. a VÜPF: a. die Übermittlung der folgenden Angaben über den überwachten Zugang: 1. das Datum und die Uhrzeit, zu der die Datenverbindung hergestellt und getrennt wurde, 2. die Art der Datenverbindung oder des Anschlusses, 3. die verwendeten Anmeldungsdaten (Log-in), 4. die verfügbaren Adressierungselemente, insbesondere des Ursprungs der Kommunikation, 5. die Kommunikationsparameter der Endgeräte und die Parameter zur Teilnehmeridentifikation (z.B. MAC-Adresse, IMEI-Nummer, IMSI-Nummer), 6. bei Zugang über ein Mobilfunknetz: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist.					
	700	PS 6: Benutzeridentifikation des asynchronen Postdienstes nach Art. 24b lit. b VÜPF	540	Art. 24b lit. b VÜPF: b. die Übermittlung der folgenden Angaben bei Versand oder Empfang von Meldungen durch einen asynchronen elektronischen Postdienst: 1. das Datum und die Uhrzeit des Versands oder des Empfangs von Mitteilungen bei der Internetzugangsanbieterin, 2. bei der Überwachung von E-Mail-Verkehr: die Umschlaginformationen gemäss benutztem Protokoll, 3. die IP-Adressen der sendenden und empfangenden Fernmeldeanlagen der asynchronen elektronischen Postdienste, 4. die anderen verfügbaren Adressierungselemente.					

EINFACHE AUSKÜNFTE: Telefon	4	A 0: Basisinformationen wie Rufnr., Teilnehmeradresse, SIM-Nr.	4	Auskünfte über Identifikationsdaten			30,12	Nr. 5: CIOT-Abfrage (zentrale Datenverwaltung) pro Tag
	360	A1-A4: versch. Angaben zu Fernmeldeanschlüssen	250				7,52	Nr. 6: Informationsübermittlung basierend auf Identifikationsdaten
	10	A 0.1: Basisinformationen Internet	10				7,52	Nr. 7: Informationsübermittlung basierend auf historischen Identifikationsdaten
Internet	250	A 0.2 Basisinformation Internet (z.B. Dynamische IP Adresse)	250	nicht gesondert angeführt: wie Auskunft über Identifikationsdaten				

ZUSÄTZLICHE KOSTEN: Zusätzliche Pauschalen für Dienstleistungen ausserhalb der Normalarbeitszeit	250	Art. 3 GebV-ÜPF: Für Dienstleistungen, die ausserhalb der Zeit von Montag bis Freitag zwischen 8 und 17 Uhr erbracht werden Fallpauschale wird hälftig dem Dienst und den Post- und Fernmeldedienstanbieterinnen sowie den Internetzugangsanbieterinnen gutgeschrieben.		ZUSÄTZLICHE KOSTEN: Zusätzliche Pauschalen für Dienstleistungen ausserhalb der Normalarbeitszeit					
Zusätzliche Auslieferung von Datenträgern	125	Art. 3a GebV-ÜPF: Für die Lieferung von zusätzlichen Datenträgern mit bereits ausgelieferten Daten pro Datenträger						- 50% 100%	Zuschlag auf alle in Annex III genannten Tarife sofern die Massnahmen - ausserhalb der Normalarbeitszeiten oder an Wochenenden oder gesetzlichen Feiertagen durchgeführt werden.
Gebühren für nicht aufgeführte Dienstleistungen	160	Art. 4 GebV-ÜPF: - Gebühren für nicht angeführte Dienstleistungen werden im Einzelfall nach Zeit- und Sachaufwand nach einem Stundensatz festgelegt - Kosten für die Bereitstellung von Geräten und Material werden durch den Dienst zusätzlich in Rechnung gestellt	160	Art. 4a GebV-ÜPF: - Entschädigungen für nicht angeführte Dienstleistungen werden im Einzelfall nach Zeit- und Sachaufwand nach Stundensatz festgesetzt; Entschädigungen werden als Teil der Gebühr nach Art. 4 [GebV-ÜPF] in Rechnung gestellt - Einreichung einer detaillierten Abrechnung ihres Aufwands - Entschädigungen decken 80 % des gesamten Zeit- und Sachaufwands	Gebühren für nicht aufgeführte Dienstleistungen			30,12	Nr. 11: Gebühren für nicht angeführte Dienstleistungen pro Stunde

F. ÖSTERREICH

1. Übersicht über die strafprozessualen Grundlagen der Fernmeldeüberwachung

Die Fernmeldeüberwachung (auch Telekommunikationsüberwachung) ist nur in den vom Gesetz vorgesehenen Fällen zulässig. Relevante Rechtsgrundlage ist neben der Strafprozessordnung das 2003 erlassene **Telekommunikationsgesetz** (öTKG). Die Strafverfolgungsbehörden haben bei der Verwendung personenbezogener Daten ferner die Bestimmungen des **Datenschutzgesetzes** (öDSG) zu beachten (§ 74 öStPO) und hierbei insbesondere den Grundsatz der Gesetz- und Verhältnismässigkeit zu wahren. Hierbei ist insbesondere auf Geheimhaltungsinteressen Rücksicht zu nehmen.

Mit dem Strafrechtsänderungsgesetz 2002 erfolgte eine Anpassung der Regelungen der Überwachung eines Fernmeldeverkehrs an die **modernen Begriffe** – vor allem an den Begriff „Telekommunikation“ – des öTKG und der Überwachungsverordnung (ÜVO). Es wurde festgehalten, dass sich die Bestimmungen der StPO auf die Überwachung sämtlicher Formen der Telekommunikation beziehen.

1.1. Fernmelde- und Kommunikationsgeheimnis

Das Fernmeldegeheimnis ist ein grundrechtlich geschütztes Recht.²⁵⁷ Dieses Grundrecht wird in § 93 öTKG gesetzlich näher ausgeführt. Einschränkungen sind unter bestimmten Voraussetzungen zulässig (Grundsatz der Gesetzmässigkeit).

Die nachstehende Zusammenfassung behandelt ausschliesslich den strafprozessualen Rahmen der Telekommunikationsüberwachung. Diese zulässigen Überwachungsmassnahmen sind im Abschnitt zum Ermittlungsverfahren (§ 134 ff. öStPO) geregelt.²⁵⁸ Die öStPO differenziert zwischen:

- Auskunft über Daten einer Nachrichtenübermittlung (Verkehrs- und Standortdaten, siehe 1.2.) und
- Überwachung von Nachrichten (sog. Inhaltsdaten, siehe 1.3.)

In 1.4. werden ferner jene Sachverhalte behandelt, die nicht unter das Kommunikationsgeheimnis fallen.

Vom Fernmeldegeheimnis ausgenommen ist die Ablesung von Daten aus einem beschlagnahmten Beweismittel. Denn die Bestimmungen zur Telekommunikationsüberwachung sind von jenen der Sicherstellung abzugrenzen. Die Differenzierung erfolgt danach, wo die Daten erhoben werden: Werden die Daten beim Telekommunikationsteilnehmer selbst erhoben, gilt die Datenerhebung als Sicherstellung im Sinne von § 111 öStPO. Demnach hat der Betroffene auf Verlangen den Gegenstand – in der Regel den Datenträger – herauszugeben sowie zugänglich zu machen, etwa durch Bekanntgabe eines Codewortes (so genannte Editions- oder Mitwirkungspflicht).²⁵⁹ Im Falle von

²⁵⁷ Art. 10a Staatsgrundgesetz in der Fassung des BGBl 1974/8 und Art. 8 EMRK (diese steht im Verfassungsrang). Der Straftatbestand zur Verletzung des Telekommunikationsgeheimnisses findet sich in § 119 und § 119 a öStGB (Strafgesetzbuch).

²⁵⁸ Soweit nicht anders angeführt, beziehen sich die nachstehenden Bestimmungen auf die öStPO.

²⁵⁹ Als Beispiel werden hier etwa das Abrufen der in einem Telefonspeicher abgelegten Daten (Telefonlisten) sowie das Auslesen einer SIM-Card genannt. Anderes gilt beim Lesen noch ungeöffneter Nachrichten (SMS/MMS), zumal die Daten sich Soweit nicht anders angeführt, beziehen sich die nachstehenden Bestimmungen auf die öStPO.

²⁵⁹ Als Beispiel werden hier etwa das Abrufen der in einem Telefonspeicher abgelegten Daten (Telefonlisten) sowie das Auslesen hier in gewisser Weise noch beim Betreiber befinden, vgl. E. E. FABRIZY, Die ös-

Verweigerung sind Zwangsgewalt und Beugemittel gemäss § 93 öStPO zulässig. Werden die Daten **beim Betreiber der Telekommunikation** ermittelt, gilt die Datenerhebung als Telekommunikationsüberwachung, die den jeweiligen Voraussetzungen unterliegen muss (§ 135 Abs. 2 und 3 öStPO).²⁶⁰

1.2. Datenauskunft

1.2.1. Definition

Die Auskunft über Daten einer Nachrichtenübermittlung ist in § 134 Z. 2 öStPO geregelt. Hiervon erfasst sind Verkehrsdaten, Zugangsdaten und Standortdaten eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft. Die Legaldefinitionen dieser Daten sind dem ÖTKG zu entnehmen:

- **Verkehrsdaten** sind Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zweck der Fakturierung dieses Vorgangs verarbeitet werden (§ 92 Abs. 3 Ziff. 4 ÖTKG) und umfassen damit jene Informationen, die die gesamte Weiterleitung der Informationen über das elektronische Kommunikationsnetz betreffen²⁶¹: darunter fallen insbesondere die aktive und passive Teilnehmernummer, die Art des Endgeräts, den Tariffcode, die Gesamtzahl der für den Abrechnungszeitraum zu berechnenden Einheiten, die Art, das Datum, den Zeitpunkt und die Dauer der Verbindung oder sonstigen Nutzung, die übermittelte Datenmenge, die Leitwege, das verwendete Protokoll, das Netz (von dem die Nachricht ausgeht oder an das sie gesendet wird), das Format der Nachricht sowie andere Zahlungsinformationen (Vorauszahlung, Ratenzahlung, Sperren des Anschlusses oder Mahnungen).
- **Zugangsdaten** sind Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind (§ 92 Abs. 3 Ziff. 4a ÖTKG).
- **Standortdaten** sind Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben (§ 92 Abs. 3 Ziff. 6 ÖTKG).

Diese Begriffsbestimmungen orientieren sich an der europäischen Richtlinie 2002/58/EG, die mit dem Telekommunikationsgesetz 2003 umgesetzt wurde. Bei der Auslegung der Begriffe ist die Richtlinie heranzuziehen.²⁶²

Die Datenauskunft nach § 134 Ziff. 2 öStPO erfasst nach herrschender Meinung auch die Rufdaten(rück)erfassung und Standortbestimmung.²⁶³ Mit der Rufdatenerfassung wird festgestellt, welche Teilnehmeranschlüsse Ursprung und Ziel einer Telekommunikation sind oder waren. Die Standortfeststellung bestimmt den räumlichen Bereich, in dem sich ein durch einen bestimmten Teilnehmeranschluss gekennzeichnetes Endgerät befindet oder befunden hat, von dem die zu überwachende Verbindung abgewickelt wird oder werden soll. Dies betrifft insbesondere auch die Bekanntgabe der Funkzelle, in der sich ein Mobiltelefon befindet, auch wenn mit diesem nicht telefoniert wird.²⁶⁴

terreichische Strafprozessordnung. Kurzkommentar, 10. Auflage, Wien 2008, § 111 StPO Rz 1 sowie § 134 Rz 5.

²⁶⁰ E. E. FABRIZY, Die österreichische Strafprozessordnung. Kurzkommentar, 10. Auflage, Wien 2008, § 134 öStPO Rz 5.

²⁶¹ Erläuternde Regierungsvorlage, 128 dBlg NR, XXII. GP, S. 18.

²⁶² C. SINGER, in A. Stratil (Hrsg.), Telekommunikationsgesetz 2003, 3. Auflage, Wien 2004, S. 291.

²⁶³ C. BERTEL & A. VENIER, Strafprozessrecht, 5. Auflage, Wien 2011, Rz 335.

²⁶⁴ E. E. FABRIZY, Die österreichische Strafprozessordnung. Kurzkommentar, 10. Auflage, Wien 2008, § 134 StPO Rz 3.

1.2.2. Rechtsgrundlage und Voraussetzungen

Die Datenauskunft ist zulässig:

- Wenn der dringende Verdacht einer Entführung oder Geiselnahme besteht, sofern sich die Auskunft auf Daten einer solchen Nachricht beschränkt, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung vom Beschuldigten übermittelt, empfangen oder gesendet wird (§ 135 Abs. 2 Ziff. 1 öStPO).
- Bei ausdrücklicher Zustimmung des Inhabers der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird und damit die Förderung der Aufklärung einer mit mehr als sechsmonatigen Freiheitsstrafe bedrohten Straftat zu erwarten ist (§ 135 Abs. 2 Ziff. 2 öStPO).
- Wenn dies zur Aufklärung einer mit mehr als einem Jahr Freiheitsstrafe bedrohte Vorsatztat beitragen kann und mit Grund anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können (§ 135 Abs. 2 Ziff. 3 öStPO).

Die in § 135 Abs. 2 Ziff. 2 und 3 öStPO genannte Förderung der Aufklärung umfasst die Erhebung des Sachverhaltes und die Feststellung von Beweismitteln.²⁶⁵

1.3. Nachrichtenüberwachung

1.3.1. Definition

Die „Überwachung von Nachrichten“ oder Nachrichtenüberwachung (§ 134 Ziff. 3 öStPO) umfasst nach der Gesetzesdefinition das Ermitteln des Inhalts von Nachrichten (im Sinne von § 92 Abs. 3 Ziff. 7 ÖTKG), die über ein Kommunikationsnetz oder einen Dienst der Informationsgesellschaft ausgetauscht oder weitergeleitet werden. Dies betrifft insbesondere das Abhören, Abfangen und die Aufzeichnung von Telefongesprächen sowie E-Mails.²⁶⁶ Ausgenommen vom Nachrichtenbegriff sind Informationen, die als Teil eines Rundfunkdienstes über ein Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden und nicht individuell identifizierbar sind (§ 92 Abs. 3 Ziff. 7 ÖTKG).

1.3.2. Rechtsgrundlage und Voraussetzungen

Die Nachrichtenüberwachung ist in ähnlichen Fällen wie die Auskunft über Daten zulässig:

- Im Fall einer Entführung oder Geiselnahme (Verweis auf § 135 Abs. 2 Ziff. 1 öStPO);
- Mit ausdrücklicher Zustimmung zur Förderung der Aufklärung einer mit mehr als sechsmonatiger Freiheitsstrafe bedrohten Vorsatztat (Verweis auf § 135 Abs. 2 Ziff. 2 öStPO);
- Zur Aufklärung einer mit mehr als einem Jahr Freiheitsstrafe bedrohten Vorsatztat sowie
- Wenn die Aufklärung oder Verhinderung einer begangenen oder geplanten strafbaren Handlung im Rahmen einer kriminellen oder terroristischen Vereinigung oder kriminellen Organisation (§§ 278 bis 278b öStGB) ansonsten wesentlich erschwert wäre. Nach dem Gesetzeswortlaut ist überdies erforderlich, dass der Anlageninhaber der Straftat dringend verdächtig (§ 135 Abs. 3 Ziff. 3 lit. a öStPO) ist oder auf Grund bestimmter Tatsachen anzunehmen ist, dass eine der Tat dringend verdächtige Person die technische Einrichtung benutzen wird oder mit ihr eine Verbindung herstellen wird (§ 135 Abs. 3 Ziff. 3 lit. b öStPO);
- Wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig, ermittelt werden kann (§ 135 Abs. 3 Ziff. 4 öStPO).

²⁶⁵ E. E. FABRIZY, Die österreichische Strafprozessordnung. Kurzkommentar, 10. Auflage, Wien 2008, § 135 StPO Rz 8.

²⁶⁶ C. BERTEL & A. VENIER, Strafprozessrecht, 5. Auflage, Wien 2011, Rz 335.

1.4. Auskunft und Verarbeitung von Stammdaten

1.4.1. Definition

Stammdaten umfassen alle personenbezogenen Daten, die für die Begründung, Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter erforderlich sind. Das Gesetz nennt hier in abschliessender Form (§ 92 Abs. 3 Ziff. 3 öTKG):

- a. Familienname und Vorname
- b. Akademischer Grad
- c. Wohnadresse
- d. Teilnehmernummer und sonstige Kontaktinformation für die Nachricht
- e. Information über Art und Inhalt des Vertragsverhältnisses
- f. Bonität

Unter Wohnadresse nach lit. c fällt die postalische Wohn- und Zustelladresse. Andere Kontaktinformationen, wie E-Mail, Netzwerk- oder IP-Adresse, sind von lit. d oder Ziff. 4 (Verkehrsdaten) umfasst. Lit. e wurde hinzugefügt, um Informationen über die konkreten Vertragsinhalte (darunter etwa Tarifoptionen, Vertragslaufzeiten und vereinbarte Nebenleistungen) zu berücksichtigen, die sich aus dem Wettbewerb im Telekommunikationsbereich ergeben.²⁶⁷ Stammdaten unterliegen **nicht dem Fernmeldegeheimnis** gemäss Art. 10a des Staatsgrundgesetzes^{268 269}.

1.4.2. Rechtsgrundlage und Voraussetzungen

Für die Auskunft von Stammdaten kommen **zwei Rechtsgrundlagen** in Betracht.

Gemäss § 76a Abs. 1 öStPO können die kriminalpolizeilichen Behörden, Staatsanwaltschaften und Gerichte zur **Aufklärung eines konkreten Verdachts einer Straftat** einer bestimmten Person Auskunft über Stammdaten verlangen. Anbieter öffentlicher Kommunikationsdienste sind auf deren schriftliches Verlangen verpflichtet, diese Daten zu übermitteln (§ 90 Abs. 7 öTKG).

Dieselbe Pflicht ergibt sich aus § 90 Abs. 7 öTKG in Verbindung mit § 53 Abs. 3a Sicherheitspolizeigesetz (SPG). Dieses regelt ganz allgemein die Organisation der **Sicherheitsverwaltung** und die Ausübung der Sicherheitspolizei (§ 1 SPG). Die genannte Bestimmung ermächtigt die Sicherheitsbehörden von Betreibern öffentlicher Telekommunikationsdienste gemäss § 92 Abs. 3 Ziff. 1 öTKG und sonstigen Diensteanbietern im Sinne des E-Commerce-Gesetzes Auskunft zu verlangen über:

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

Voraussetzung hierfür sind das Vorliegen einer konkreten Gefahrensituation und der Bedarf der Daten zur Erfüllung der nach dem SPG übertragenen Aufgaben. Diese sind insbesondere die erste allgemeine Hilfeleistungspflicht (§ 19 SPG), die Aufrechterhaltung der öffentlichen Sicherheit (§ 20 ff. SPG), Aufrechterhaltung der öffentlichen Ordnung (§ 27 SPG) sowie der Besondere Überwachungsdienst (§ 27a SPG).

²⁶⁷ C. SINGER, in A. Stratil (Hrsg.), Telekommunikationsgesetz 2003, 3. Auflage, Wien 2004, S. 291.

²⁶⁸ Staatsgrundgesetz vom 21.12.1867, über die allgemeinen Rechte der Staatsbürger für die im Reichsrathe [sic] vertretenen Königreiche und Länder.

²⁶⁹ E. E. FABRIZY, Die österreichische Strafprozessordnung. Kurzkommentar, 10. Auflage, Wien 2008, § 134 Rz 4.

Diese Daten sind vom Betreiber unverzüglich und **kostenlos** bekannt zu geben (§ 53 Abs. 3a SPG).

2. Übersicht über Prozess- und Organisationsstrukturen

2.1. Prozess- und Organisationsstrukturen

Wie in der ersten Frage ausgeführt, wird die Telekommunikationsüberwachung von den Sicherheitsbehörden im Ermittlungsverfahren durchgeführt. Gemäss der Organisationsstruktur des österreichischen Strafprozessrechts wirken hier die folgenden Behörden zusammen: die Kriminalpolizei, die Staatsanwaltschaft und die Gerichte.

Die Ermittlungsmassnahmen werden von der Kriminalpolizei **auf Anordnung der Staatsanwaltschaft** durchgeführt (§ 103 öStPO). Die Staatsanwaltschaft kann überdies auch selbst ermittelnd tätig werden (§ 103 Abs. 2 i.V.m. § 91 Abs. 2 öStPO).

Für sämtliche oben dargestellten Massnahmen – mit Ausnahme der Auskunft über die Stammdaten – hat die Anordnung der Staatsanwaltschaft auf Grund einer **gerichtlichen Bewilligung** zu erfolgen (§ 137 Abs. 1 zweiter Satz öStPO; Richtervorbehalt). Diese ist daher bei sonstiger Nichtigkeit²⁷⁰ als Eingriff in das grundrechtlich geschützte Kommunikationsgeheimnis (1.1.) unbedingte Voraussetzung. Die Gerichte haben gemäss dem Grundsatz der Gesetzes- und Verhältnismässigkeit die anzuordnenden Massnahmen zu prüfen. Hierbei sind die Massnahmen insbesondere im Verhältnis zur Schwere der Straftat zum Grad des Verdachts und zum angestrebten Erfolg abzuwägen. Es müssen insbesondere auch die Erfolgsaussichten weniger eingreifender Massnahmen geprüft werden.²⁷¹

Die Staatsanwaltschaften haben den zur Mitwirkung verpflichteten Betreiber mittels einer gesonderten Anordnung über den Umfang seiner Pflicht und seine Verschwiegenheitspflicht zu informieren (§ 138 Abs. 3 StPO). Der Betreiber kann dagegen Einspruch beim Gericht erheben (§ 106 StPO).

2.2. Mitwirkungspflicht auf Seiten der Anbieter

Die Anbieter sind verpflichtet, alle Einrichtungen bereitzustellen, die zur Überwachung von Nachrichten (siehe 1.2.) sowie zur Auskunft über Daten einer Nachrichtenübermittlung (siehe 1.3.) nach den Bestimmungen der StPO erforderlich sind. Die Gestaltung der technischen Einrichtung sind gem. § 94 TKG durch Verordnung festzulegen. Diese **Überwachungsverordnung**²⁷² (kurz ÜVO) wurde am 30.11.2001 veröffentlicht und die Mehrzahl der Regelungen trat am 1.12.2011 in Kraft.

Sie richtet sich an Betreiber öffentlicher Kommunikationsdienste. Der persönliche Anwendungsbereich umfasst demnach Unternehmen, die einen öffentlichen Telefondienst anbieten und in deren Netz physikalische Teilnehmeranschlüsse – dies sind durch eine Adresse eindeutig gekennzeichnete Anschlüsse – vorhanden sind (§ 2 Abs. 1 ÜVO).

Ziel der Verordnung ist die Festlegung eines einheitlichen Standards für die Schnittstellen, an denen die Betreiber öffentlicher Telekommunikationsdienste die auf Grund des gerichtlichen Beschlusses

²⁷⁰ Dies ergibt sich aus dem ausdrücklichen Beweisverwertungsverbot des § 140 öStPO.

²⁷¹ D. Damjanovic et al., Handbuch des Telekommunikationsrechts, Wien 2006, S. 270 f.

²⁷² Verordnung der Bundesministerien für Verkehr, Innovation und Technologie über die Überwachung des Fernmeldeverkehrs (Überwachungsverordnung, kurz ÜVO), BGBl II Nr 418/2001 in der Fassung des BGBl II Nr. 559/2003. Die Verordnung wurde auf Grundlage des § 89 TKG alte Fassung erlassen (heute entspricht dieser im Wesentlichen § 94 öTKG neue Fassung).

spezifizierten Daten den Strafverfolgungsbehörden zur Verfügung zu stellen haben (§ 3 Abs. 4 ÜVO schreibt eine zweifelsfreie Zuordnung vor).

Die technischen Anforderungen müssen dergestalt sein, dass folgende Funktionen über die aktive Mitwirkung des Betreibers im Einzelfall zur Verfügung gestellt werden können:

- 1) Die Überwachung und Aufzeichnung der Telekommunikation die von dem zu überwachenden Teilnehmeranschluss ausgeht oder für diesen bestimmt ist als auch jene Telekommunikation die zu Datenspeichern weitergeleitet oder von diesen abgerufen wird, die dem Teilnehmeranschluss (kurz TA) zugeordnet sind (§ 3 Abs. 1 Z 1 und 2 ÜVO).

Zur Bereithaltung dieser Funktionen, die Standort- und Verkehrsdaten betreffend, sind die Betreiber **in jedem Fall** verpflichtet (§ 3 Abs. 3 ÜVO *e contrario*).

- 2) Ausserdem sind folgende taxativ aufgezählten Inhaltsdaten oder weitere mit der Überwachung stehende Informationen zur Verfügung zu stellen (§3 Abs. 2 Z 1-10 ÜVO): Adresse des zu überwachenden TAs; die gewählten Adressen (auch wenn keine Verbindung zu Stande kommt oder der Verbindungsversuch vorzeitig beendet wird); die Adresse der TAs von denen gewählt wird; Adressen etwaiger Um- oder Weiterleitungen (jeweils die physikalischen Anschlüsse); Adressen dem der TAs fallweise zugeordnet werden kann; der angeforderte/in Anspruch genommene Dienst; technische Ursache für Abbruch/Nichtzustandekommen der Verbindung; im Falle von Mobilanschlüssen die betroffenen Funkzellen sowie Angaben aus denen Datum und Uhrzeit sowie Dauer der Verbindung hervorgeht.

Diese Verpflichtungen, die Inhaltsdaten betreffen, sind vom Betreiber nur zu erfüllen, soweit ihm dies auf Grund wirtschaftlicher und technischer Gegebenheiten **zumutbar** ist (§ 3 Abs. 3 ÜVO). Die Zumutbarkeit ergibt sich aus der in der Investitionskostenverordnung (IKEV, siehe unten, 3.) genannten Umsatzschwelle der Anbieter (§ 3 IKEV).

Die Auflagen nach 1) und 2) gelten sinngemäss für Telekommunikationsverbindungen mit mehr als einer Gegenstelle, an denen der überwachte TA teilnimmt (§ 3 Abs. 5 Ziff. 1 ÜVO); Verbindungen die für den überwachten TA bestimmt sind oder von diesem aufgebaut werden, wenn er fallweise einem anderen TA zugeordnet ist oder von einem anderen TA angenommen wird (§ 3 Abs. 5 Ziff. 2 ÜVO) sowie für den Fall dass mehrere Telekommunikationsverbindungen gleichzeitig bestehen (§ 3 Abs. 5 Ziff. 3 ÜVO).

- 3) Die Betreiber haben diese Informationen an einer festgelegten technischen Schnittstelle für die gesamte Dauer der angeordneten Überwachungsmassnahme bereitzustellen, wobei bestimmte technische Standards einzuhalten sind (§ 4 Abs. 1 Ziff. 1 - 4 ÜVO).

Zur Festlegung einheitlicher technischer Standards betreffend der Übermittlung der Daten wurde auf Grundlage der §§ 94 Abs. 4 sowie § 102c TKG die **Datensicherheitsverordnung (DSVO)**²⁷³ erlassen. Der Anwendungsbereich der Verordnung erstreckt sich auf die Verwendung von Verkehrsdaten, Zugangsdaten und Standortdaten sowie Stammdaten (§ 1 Abs. 2 DSVO). Sie trifft etwa nähere Bestimmungen für die zu verwendende Übertragungs- und Verschlüsselungstechnologie (§ 5 DSVO) und legt fest, dass die Übermittlung der Daten über eine beim Bundesrechenzentrum einzurichtende **zentrale Durchlaufstelle** zu erfolgen hat (§ 8 ff. DSVO).

²⁷³ Verordnung der Bundesministerien für Verkehr, Innovation und Technologie betreffend die Datensicherheit, BGBl II Nr. 402/2011.

3. Kosten und Finanzflüsse

3.1. Rechtsgrundlage für Finanzierung

Hinsichtlich der Finanzierung und dem Kostenersatz ist zu differenzieren zwischen jenen Ausgaben, die getätigt wurden, um die einheitlichen technischen Standards zu gewährleisten und jenen Kosten, die für bewilligte Überwachungsmassnahmen anfallen.

3.1.1. Kostenersatz für getätigte Investitionen zur Bereithaltung der Einrichtungen

Für die Investitionen, welche die Anlagenbetreiber aus der Umsetzung der DSVO für die Bereitstellung der technischen Einrichtungen getroffen haben, gebührt ihnen Kostenersatz gemäss der Investitionskostenersatzverordnung²⁷⁴ (IKEV). Diese auf Grundlage von § 94 Abs. 4 öTKG erlassene Verordnung gilt auch für Investitionen, die im Sinne dieser Bestimmung vor Inkrafttreten der Verordnung (1.4.2012) angefallen sind (§ 6 IKEV).

Als Bemessungsgrundlage sind insbesondere (exemplarische Aufzählung) folgende Ausgaben zu berücksichtigen (§ 2 Abs. 1 Ziff. 1 bis 4 IKEV):

- Anschaffungskosten
- Einrichtungskosten
- Netzanpassungskosten
- Lizenzkosten

Die Anbieter haben binnen drei Monaten diese Ausgaben betreffende Angaben an die zuständigen Bundesministerien zu übermitteln. Mangels Übermittlung der Angaben, hat die Bundesministerin für Verkehr, Innovation und Technologie die Bemessungsgrundlage zu schätzen (§ 3 Abs. 1 IKEV). Nach Ablauf der Frist hat sie gemäss § 4 IKEV per Bescheid die Höhe der zu ersetzenden Kosten festzustellen. Den **Anbietern gebührt 80 % der Bemessungsgrundlage** abzüglich der gemäss § 5 IKEV geleisteten Vorauszahlung und der **von allen Anbietern anteilig zu tragenden Investitionskosten für die Einrichtung der zentralen Durchlaufstelle** (§ 4 Abs. 2 ÜKVO).

3.1.2. Kostenersatz für die Mitwirkung an der Telekommunikationsüberwachung

Die Rechtsgrundlagen für den Kostenersatz für die angeordneten Überwachungsmassnahmen sind § 94 StPO sowie die auf deren Grundlage erlassene Überwachungskostenverordnung²⁷⁵ (ÜKVO).

Der Kostenersatz betrifft sowohl die Auskunftserteilung über Stamm- und Zugangsdaten nach § 76a Abs. 2 StPO als auch die Datenauskunft und Überwachung von Nachrichten (Inhaltsdaten) nach § 135 Abs. 2 und 3 StPO (§ 1 ÜKVO). Ersatz gebührt nur für jene Leistungen, die gem. der genannten Anspruchsgrundlagen angeordnet und auch tatsächlich erbracht wurden (§ 1 Abs. 2 ÜKVO). Blieb die Massnahme ergebnislos – aus Gründen der Rufnummernportierung oder aus Verschulden des Anbieters – ist ein Ersatz ausgeschlossen. Gemäss § 94 Abs. 1 öTKG beläuft sich der Kostenersatz auf **80 % der Personal- und Sachaufwendungen**. Die Bemessungsgrundlage für den Prozentsatz wird in der ÜKVO geregelt (s. folgende Seite).

²⁷⁴ Verordnung der Bundesministerien für Verkehr, Innovation und Technologie über den Ersatz der Investitionskosten der Anbieter für die Bereitstellung der Einrichtungen, die zur Auskunft über Daten einer Nachrichtenübermittlung einschliesslich der Auskunft über Vorratsdaten erforderlich sind, BGBl II Nr. 107/2012.

²⁷⁵ Überwachungskostenverordnung, BGBl 322/2004, zuletzt geändert durch BGBl II Nr. 133/2012.

§ 7. Die Kosten einer Standortbestimmung betragen

1. für eine Funkzellenauswertung	
a) Ermittlung der Funkzelle	Euro 148,00
b) Einrichtung pro Funkzelle	Euro 64,00
c) Datensortierung und Auswertung pro Verbindungsdatensatz	Euro 00,40
2. für eine Ermittlung von historischen Standortdaten bei zustande gekommenen Verbindungen	
a) Einrichtung	Euro 64,00
b) Auswertung pro überwachten Tag	Euro 06,50
3. für eine Auswertung von Standortdaten für einen zukünftigen Überwachungszeitraum	
a) Einrichtung	Euro 64,00
b) Auswertung pro überwachten Tag	Euro 06,50
4. für eine Ermittlung aktueller Standortdaten	
a) Einrichtung pro Rufnummer	Euro 37,00
b) Auswertung und Versand pro Abfrage ohne Plandarstellung/Landkarte	Euro 16,00
c) Plandarstellung/Landkarte pro Abfrage	Euro 16,00

Ermittlung von Verkehrsdaten**§ 8. Die Kosten für die Ermittlung von Vermittlungsdaten auf Basis der Rufnummer, IMEI- Nummer oder IMSI- Nummer betragen**

1. für die Ermittlung von historischen Verkehrsdaten	
a) Einrichtung	Euro 64,00
b) Auswertung pro überwachten Tag	Euro 06,50
c) Zusätzliche Ermittlung einer verwendeten IMEI-Nummer (im Mobilnetz)	Euro 60,00
2. für die laufende Ermittlung von Verkehrsdaten für einen zukünftigen Überwachungszeitraum	
a) Einrichtung	Euro 64,00
b) Auswertung pro überwachten Tag	Euro 06,50
3. für die Ermittlung von Rufnummern auf Basis von IMEI- oder IMSI-Nummern	
a) Datenrasterung	Euro 60,00
b) Laufende Ermittlung von Rufnummern auf Basis von IMEI- oder IMSI-Nummern für einen zukünftigen Überwachungszeitraum pro überwachten Tag	Euro 06,50

Ermittlung von Vorratsdaten**§ 8a. Die Kosten für die Ermittlung von Vorratsdaten betragen:**

a) Einrichtung	Euro 64,00
b) Auswertung pro überwachten Tag	Euro 06,50
c) für die Datenrasterung im Zusammenhang mit der Ermittlung von Rufnummern oder Nummern Teilnehmerkennungen oder auf Basis von IMEI- öffentlicher oder IMSI- IP-Adressen	Euro 60,00

Ermittlung von Stamm- und Zugangsdaten**§ 8b. Die Kosten für die Ermittlung von Stamm- und Zugangsdaten betragen Euro 40,00.****Beachte für folgende Bestimmung**

Zum Bezugszeitraum vgl. § 13 Abs. 3.

Überwachung von Nachrichten**§ 9. Die Kosten für die Überwachung von Nachrichten betragen**

1. für die Einrichtung und Herstellung der Überwachungsverbindung	Euro 128,00
2. für das Aufrechterhalten der Verbindung, die Kontrolle und Auswertung der Daten pro überwachten Tag	Euro 25,00

PUK- Code**§ 10. Die Kosten für die Bekanntgabe des PUK- Codes betragen**

für die Ermittlung und Weiterleitung	Euro 32,00
--------------------------------------	------------

Beachte für folgende Bestimmung

Zum Bezugszeitraum vgl. § 13 Abs. 3.

Transportkosten

§ 11. Ist zur Durchführung der Auskunftserteilung oder der Überwachung ein Transport von Zusatzgeräten erforderlich, so sind dem Betreiber die Kosten für die Benützung eines Kraftfahrzeuges zu ersetzen. Als Ersatz dieser Kosten gebührt die nach § 10 Abs. 3 der Reisegebührenvorschrift 1955, BGBl. Nr. 133, hierfür vorgesehene Vergütung.

Beachte für folgende Bestimmung

Zum Bezugszeitraum vgl. § 13 Abs. 3.

Sekretariatspauschale

§ 12. Die Sekretariatspauschale umfasst die Kosten für die Aufbereitung und Übermittlung der Daten, sofern diese nicht bereits in den vorhergehenden Tarifsätzen umfasst sind, sowie für die Herstellung sonstiger Unterlagen und Kostennoten. Sie beträgt

1. pro Anordnung	Euro 15,20
2. pro Ergänzungsanordnung	Euro 05,60

Zusätzlich gebührt ein Zuschlag von 100% für Leistungen, die an Samstagen, Sonntagen und gesetzlichen Feiertagen sowie Werktagen zwischen 22.00 und 6.00 Uhr erbracht wurden, sofern diese nicht ohne Nachteil für die Überwachung auch zu einem anderen Zeitpunkt hätten erbracht werden können.

Die Anbieter sind verpflichtet, den **Kostenersatz in Pauschalbeträgen** binnen vier Wochen nach Beendigung der Ermittlungsmassnahmen bei sonstigem Verlust **bei der Staatsanwaltschaft oder dem Gericht**, das die Massnahmen angeordnet bzw. bewilligt hat, in **schriftlicher Form geltend** zu machen (§ 6 ÜKVO). Gegebenenfalls können die Betreiber dazu aufgefordert werden, eine Aufschlüsselung der die Kosten in einzelne Kostenbestandteile sowie eine Begründung für Notwendigkeit und Umfang der Leistungen nachzureichen (§ 6 Abs. 2 ÜKVO).

3.2. Entscheidungsstrukturen über Kostentragung einer Überwachung im Einzelfall

Die Überwachungskosten fliessen in die Kosten des Strafverfahrens ein. Diese sind erschöpfend im § 381 öStPO geregelt. Vorausgesetzt das Strafverfahren endet mit einem Schuldspruch, können die Kosten daher auf den Angeklagten übergewälzt werden (§ 391 öStPO). Das österreichische Strafprozessrecht ist als Mischsystem eines Einzel- und Pauschalgebührens systems zu charakterisieren.²⁷⁶

Das Gericht hat – unter Beachtung einer gesetzlich festgelegten Obergrenze – einen **Pauschalkostenbeitrag** zu bestimmen. Jene Gebühren, die gesondert in Rechnung zu stellen sind, sind vom § 381 öStPO erschöpfend aufgezählt (**Einzelgebührens system**). Darunter fallen auch die Überwachungsmassnahmen. Soweit diese im Ermittlungsverfahren einen erheblichen Beitrag zur Aufklärung der Tat geleistet haben, sind sie gemäss § 381 Abs. 1 Ziff. 5 öStPO als Kosten des Strafverfahrens anzusetzen.

3.3. Kostenverteilung

Wird das Strafverfahren auf andere Weise als durch einen Schuldspruch beendet, sind die Kosten vom Bund zu tragen. Dies gilt allerdings nicht für Strafverfahren, die auf Begehren eines Privatanklägers oder auf Antrag eines Privatbeteiligten geführt wurden. Diesfalls sind ihnen die angefallenen Kosten aufzutragen (§ 390 öStPO).

3.4. Finanzierungsmechanismen ausserhalb der einzelnen Verfahren

Eine Vergütung oder Entschädigung von Telekommunikationsanbietern ausserhalb der genannten Bestimmungen ist ausgeschlossen. Die Recherche hat keine weiteren Finanzierungsmechanismen zu Tage gefördert.

²⁷⁶

E. E. FABRIZY, Die österreichische Strafprozessordnung. Kurzkommentar, 10. Auflage, Wien 2008, § 381 Rz. 1.

4. Tarifvergleich Schweiz – Österreich

Schweiz					Österreich				
Massnahme	Gebühren		Entschädigungen		Massnahme	Gebühren		Entschädigungen	
	CHF	Anm.	CHF	Anm.		€	Anm.	€	Informationsgewinn
TELEFONÜBERWACHUNG AKTIV (Überwachung leitungsvermittelte Fernmeldedienste)	2410	CS 1-3: Nutzinformationen und Verkehrsdaten	1330	Art. 16 lit. a, b und c VÜPF: 1. die verfügbaren Adressierungselemente (Rufnummern der abgehenden und ankommenden Kommunikationsvorgänge), 2. die tatsächliche bekannte Zielrufnummer und die eingeschalteten verfügbaren Rufnummern, falls der Anruf um- oder weitergeleitet wurde, 3. die erzeugten Signale, einschliesslich der Zeichengabe für den Bereitschaftszustand, die Parameter der Fernmeldeanlagen (z.B. IMSI-Nummer, IMEI-Nummer) und die erzeugten Signale für die Aktivierung der Konferenzschaltung oder der Anrufumleitung, 4. bei Mobiltelefonie: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist, 5. das Datum und die Uhrzeit	Nachrichtenüberwachung gemäss § 91 Abs. 3 Z 7 umfasst diese das Ermitteln des Inhalts von Nachrichten (Inhaltsdaten), die über ein Kommunikationsnetz oder einen Dienst der Informationsgesellschaft ausgetauscht oder weitergeleitet werden Bsp: Telefongespräche, E-Mails		Gebühren werden im Gesetz nicht gesondert angeführt	128	§ 9 ÜKVO: Z 1 für Einrichtung und Herstellung der Überwachungsverbindung
								25	Z 2 für Aufrechterhalten der Verbindung, Kontrolle und Auswertung der Daten pro Tag
					Datenauskunft (Verkehrsdaten, Standortdaten) Def. Verkehrsdaten gemäss § 92 Abs 3 Z. 4 TKG: Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein			148 64 0,4	§ 7 ÜKVO Kosten einer Standortbestimmung: - Ermittlung der Funkzelle für eine Funkzellenauswertung - Einrichtung pro Funkzelle

TELEFONÜBERWACHUNG RÜCKWIRKEND	700	CS 4: Historische Verkehrsdaten	540	Art. 16 lit. d VÜPF: 1. die verfügbaren Adressierungselemente (Rufnummern der abgehenden und eingehenden Kommunikationsvorgänge, sofern diese der Fernmeldediensteanbieterin bekannt sind), 2. die Kommunikationsparameter des Endgerätes der Mobiltelefonie und die Parameter zur Teilnehmeridentifikation (wie die IMSI-Nummer und die IMEI-Nummer), 3. bei Mobiltelefonie: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist, 4. das Datum, die Zeit und die Dauer der Verbindung	Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden Bsp: Teilnehmernr., Art Endgerät, Datum, Zeitpunkt und Dauer der Verbindung, übermittelte Datenmenge, verwendetes Protokoll, Format der Nachricht Def. Standortdaten gemäss § 92 Abs 3 Z. 6 TKG: Daten, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben, im Fall von festen Telekommunikationsendeinrichtungen sind Standortdaten die Adresse der Einrichtung				- Datensortierung und Auswertung pro Verbindungsdatensatz Auswertung für einen zukünftigen Überwachungszeitraum: 64 6,5 - Einrichtung - Auswertung pro Tag 37 16 Ermittlung aktueller Standortdaten - Einrichtung pro Rufnr. - Auswertung und Versand pro Abfrage ohne Plandarstellung 16 - Plandarstellung pro Abfrage § 8 ÜKVO Kosten Ermittlung Verkehrsdaten 64 - Z. 2 lit. a für die laufende Ermittlung für einen zukünftigen Überwachungszeitraum für die Einrichtung 6,5 - für die Auswertung pro überwachtem Tag § 7 historische Standortdaten 64 6,5 - Einrichtung - Auswertung pro Tag
					Auskunft über historische Daten oder Vorratsdaten: Def. Vorratsdaten nach § 92 Abs. 3 Z. 6b TKG: Daten die aufgrund der Speicherverpflichtung nach § 102a gespeichert werden; derzeit Individualantrag beim Verfassungsgerichtshof anhängig.				

	2200	CS 5: Antennensuchlauf (Geografische Koordinaten)	2000	Art. 16 lit. e VÜPF: der Antennensuchlauf: rückwirkende Eruiierung aller an einem bestimmten Standort angefallenen mobilen Kommunikationsvorgänge während eines bestimmten Zeitraumes, sofern es zum Aufbau einer Kommunikation gekommen ist.				64 6,5 60	§ 8 historische Verkehrsdaten: - Einrichtung - Auswertung pro überwachten Tag - zusätzliche Ermittlung IMEI Nr.
	600	CS 6: Antennensuchlauf (Cell ID)	600	Definition nach Art. 16 lit. e VÜPF (siehe oben)				64 6,5 60	§ 9 Vorratsdaten: - Einrichtung - Auswertung pro Tag - Datenrasterung Ermittlung von Rufnr. auf Basis IMEI oder IMSI-Nr. oder öffentlich IP Adressen
INTERNETÜBERWACHUNG (Überwachung paketvermittelte Fernmeldedienste)	4160	PS 1: Nutzinformationen und Verkehrsdaten gem. Art. 24a lit. a und b VÜPF	1330	Art. 24a lit. a und b VÜPF: a. die Übermittlung sämtlicher Daten, die über den überwachten Zugang gesendet oder empfangen werden; b. die Bereitstellung und die simultane oder periodische Übermittlung der folgenden Angaben über den Internetzugang: 1. das Datum und die Uhrzeit, zu der die Datenverbindung hergestellt und getrennt wird, 2. die Art der Datenverbindung oder des Anschlusses, 3. die verwendeten Anmeldungsdaten (Log-in), 4. die verfügbaren Adressierungselemente, insbesondere des Ursprungs der Kommunikation, 5. die Kommunikationsparameter der Endgeräte und die Parameter zur Teilnehmeridentifikation (z.B. MAC-Adresse, IMEI-Nummer, IMSI-Nummer), 6. bei Zugang über ein Mobilfunknetz: die Bestimmung und die periodische Übertragung des Zell-Identifikators (Cell ID), des Standortes und der Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person momentan verbunden ist	nicht gesondert angeführt: wie Nachrichtenüberwachung				

	800	PS 2: Verkehrsdaten gemäss Art. 24a lit b VÜPF	640	Art. 24a lit. b VÜPF: b. die Bereitstellung und die simultane oder periodische Übermittlung der folgenden Angaben über den Internetzugang: 1. das Datum und die Uhrzeit, zu der die Datenverbindung hergestellt und getrennt wird, 2. die Art der Datenverbindung oder des Anschlusses, 3. die verwendeten Anmeldungsdaten (Log-in), 4. die verfügbaren Adressierungselemente, insbesondere des Ursprungs der Kommunikation, 5. die Kommunikationsparameter der Endgeräte und die Parameter zur Teilnehmeridentifikation (z.B. MAC-Adresse, IMEI-Nummer, IMSI-Nummer), 6. bei Zugang über ein Mobilfunknetz: die Bestimmung und die periodische Übertragung des Zell-Identifikators (Cell ID), des Standortes und der Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person momentan verbunden ist, 7. die technischen Änderungen, die während der Verbindung stattfinden, und, falls bekannt, ihre Ursachen; und, falls bekannt, ihre Ursachen;						
	2410	PS 3: Nutzerinformationen und Verkehrsdaten gem. Art. 24a lit. c VÜPF	1330	Art. 24a lit. c VÜPF: die Übermittlung der Nutzinformationen, die über die überwachte Anwendung gesendet oder empfangen werden;						

	800	PS 4: Verkehrsdaten einer Anwendung gem. Art. 24a lit. d VÜPF	640	Art 24a lit. d VÜPF: die Bereitstellung und die simultane oder periodische Übermittlung folgender Angaben über die überwachte Anwendung: 1. das Datum und die Uhrzeit der Kommunikation (Beginn und Ende), 2. die verfügbaren Adressierungselemente, insbesondere diejenigen des Ursprungs und des Ziels der Kommunikation, 3. die verwendeten Anmeldungsdaten (Log-in), 4. bei der Überwachung von E-Mail-Verkehr: die Umschlaginformationen gemäss dem benutzten Protokoll, 5. die anderen verfügbaren Kommunikationsparameter, 6. die technischen Änderungen während der Kommunikation und ihre Ursachen, falls bekannt. Art. 24b lit. a VÜPF: a. die Übermittlung der folgenden Angaben über den überwachten Zugang: 1. das Datum und die Uhrzeit, zu der die Datenverbindung hergestellt und getrennt wurde, 2. die Art der Datenverbindung oder des Anschlusses, 3. die verwendeten Anmeldungsdaten (Log-in), 4. die verfügbaren Adressierungselemente, insbesondere des Ursprungs der Kommunikation, 5. die Kommunikationsparameter der Endgeräte und die Parameter zur Teilnehmeridentifikation (z.B. MAC-Adresse, IMEI-Nummer, IMSI-Nummer), 6. bei Zugang über ein Mobilfunknetz: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommuni-					
	700 250	PS 5: Verkehrsdaten nach Art. 24b lit. a VÜPF - Angaben nach Ziffern 1-6 - Angaben nach Ziffern 2,3,4, und 5 (jede Kombination möglich)	540 250						

	700	PS 6: Benutzeridentifikation des asynchronen Postdienstes nach Art. 24b lit. b VÜPF	540	kation verbunden ist. Art. 24b lit. b VÜPF: b. die Übermittlung der folgenden Angaben bei Versand oder Empfang von Meldungen durch einen asynchronen elektronischen Postdienst: 1. das Datum und die Uhrzeit des Versands oder des Empfangs von Mitteilungen bei der Internetzugangsanbieterin, 2. bei der Überwachung von E-Mail-Verkehr: die Umschlaginformationen gemäss benutztem Protokoll, 3. die IP-Adressen der sendenden und empfangenden Fernmeldeanlagen der asynchronen elektronischen Postdienste, 4. die anderen verfügbaren Adressierungselemente.					
EINFACHE AUSKÜNFTE: Telefon	4	A 0: Basisinformationen wie Rufnr., Teilnehmeradresse, SIM-Nr.	4		Auskünfte über Stammdaten Def. Stammdaten gemäss § 92 Abs 3 Z. 3 TKG: alle personenbezogenen Daten, die für die Begründung, Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter erforderlich sind (Name, akadem. Grad, Wohnadresse, Teilnehmernr., Art u Inhalt Vertragsverhältnis, Bonität) Def. Zugangsdaten gemäss § 92 Abs 3 Z. 4a TKG: Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind.			40	§ 8b ÜKVO: Ermittlung von Stamm- und Zugangsdaten

Internet	360	A1-A4: versch. Angaben zu Fernmeldeanschlüssen	250	Art. 14 Abs. 1 lit. a-c BÜPF: a. Name, Adresse und, sofern vorhanden, Beruf der Teilnehmerin oder des Teilnehmers; b. Adressierungselemente nach Artikel 3 Buchstabe f des Fernmeldegesetzes vom 30. April 1997; c. Art der Anschlüsse	nicht gesondert angeführt: wie Auskünfte über Stammdaten			32	§ 10 Bekanntgabe PUK-Code
	10	A 0.1: Basisinformationen Internet	10	Art. 27 Abs. 1 VÜPF: a. bei IP-Adressen: die Art des Anschlusses, das Datum und die Uhrzeit der Zuteilung oder das Datum und die Uhrzeit des Anfangs und gegebenenfalls des Endes des Zuteilungszeitraumes, den Namen, die Adresse, die Anmeldungsdaten (Log-in) und, soweit bekannt, den Beruf der Teilnehmerin oder des Teilnehmers, sowie weitere IP-Adressen, die die Internetzugangsanbieterin dieser oder diesem zugeteilt hat; b. bei EDV-Systemen: sofern verfügbar, zusätzlich die Domainnamen und weitere Adressierungselemente unter denen diese der Internetzugangsanbieterin bekannt sind c. bei elektronischen Postdiensten, sofern sie von den Internetzugangsanbieterin zur Nutzung durch Kunden eingerichtet sind: soweit bekannt, den Namen, die Adresse und den Beruf der Teilnehmerin oder des Teilnehmers.					
	250	A 0.2 Basisinformation Internet (z.B. Dynamische IP Adresse)	250	Art. 14 Abs. 4 BÜPF: Wird eine Straftat über das Internet begangen, so ist die Internet-Anbieterin verpflichtet, der zuständigen Behörde alle Angaben zu machen, die eine Identifikation des Urhebers oder der Urheberin ermöglichen					

ZUSÄTZLICHE KOSTEN: Zusätzliche Pauschalen für Dienstleistungen aus- serhalb der Normalar- beitszeit	250	Art. 3 GebV-ÜPF: Für Dienstleistungen, die ausserhalb der Zeit von Mon- tag bis Freitag zw. 8 u 17 Uhr erbracht werden Fallpauschale wird hälftig dem Dienst und den Post- und Fernmeldedienstanbieterinnen sowie den Internetzugangs- anbieterinnen gutgeschrieben.			ZUSÄTZLICHE KOSTEN: Leistungen ausserhalb der Normalar- beitszeiten			100%	§ 5 ÜkVO: Für Leistungen an Samstagen, Sonntagen und gesetzlichen Feiertagen sowie an Werktagen zwischen 22.00 und 6.00 Uhr gebührt dem Anbieter ein Zuschlag von 100% für die in den Tarifen des 2. Ab- schnitts [Anm: die oben genannten Ent- schädigungstarife] enthaltenen Personal- kosten, es sei denn, dass die Leistungen ohne Nachteil für die Überwachung auch zu einem anderen Zeitpunkt hätten erbracht werden können.
Zusätzliche Auslieferung von Datenträgern	125	Art. 3a GebV-ÜPF: Für die Lieferung von zusätzli- chen Datenträgern mit bereits ausgelieferten Daten pro Datenträger							
Gebühren für nicht aufge- führte Dienstleistungen	160	Art. 4 GebV-ÜPF: - Gebühren für nicht angeführ- te Dienstleistungen werden im Einzelfall nach Zeit- und Sach- aufwand nach einem Stunden- satz festgelegt - Kosten für die Bereitstellung von Geräten und Material werden durch den Dienst zusätzlich in Rechnung gestellt	160	Art. 4a GebV-ÜPF: - Entschädigungen für nicht ange- führte Dienstleistungen werden im Einzelfall nach Zeit- und Sachauf- wand nach Stundensatz festgesetzt; Entschädigungen werden als Teil der Gebühr nach Art. 4 [GebV-ÜPF] in Rechnung gestellt - Einreichung einer detaillierten Abrechnung ihres Aufwands - Entschädigungen decken 80 % des gesamten Zeit- und Sachaufwands	Sekretariatspauschale			- 15,20 - 5,60	§ 12 Sekretariatspauschale für die Aufberei- tung und Übermittlung der Daten sofern nicht bereits erfasst; für die Herstellung sonstiger Unterlagen und Kostennoten - pro Anordnung - pro Ergänzungsanordnung

G. VEREINIGTES KÖNIGREICH (ENGLAND)

1. Übersicht über die strafprozessualen Grundlagen

Nach Art. 8 Abs. 1 EMRK ist das Recht auf die Achtung des Privat- und Familienlebens garantiert. Behördliche Eingriffe in dieses Recht sind nur mit gesetzlicher Grundlage und soweit für verschiedene ausdrücklich aufgezählte öffentliche Interessen notwendig möglich (Art. 8 Abs. 2 EMRK). Das Vereinigte Königreich hat die EMRK unterzeichnet und ratifiziert und danach durch den **Human Rights Act 1998** umgesetzt.

Soweit keine gesetzliche Grundlage für verdeckte Ermittlungen besteht, würden Fernmeldeüberwachungsmaßnahmen den *Human Rights Act 1998* verletzen. Aus diesem Grund besteht nach Teil III des *Police Act 1997* die gesetzliche Möglichkeit, verdeckte Eingriffe in das Eigentum oder in kabellose Telegraphie durch die Polizei, Steuer- und Zollbehörden und andere Behörden zu genehmigen. Für die Nachrichtendienste (*intelligence services*) müssen physische Eingriffe in das Eigentum (z.B. zum Installieren einer Abhörvorrichtung) nach dem *Intelligence Services Act 1994* durch den *Secretary of State* genehmigt werden.²⁷⁷

Alle Formen verdeckter Überwachung, welche keine verdeckte Zutritte oder Eingriffe in Eigentum oder kabellose Telegraphie verlangen, fallen unter den ***Regulation of Investigatory Powers Act 2000 (RIPA)***²⁷⁸, der am 2. Oktober 2000 (zusammen mit dem *Human Rights Act 1998*) in Kraft getreten ist und den *Interception of Communications Act 1985* ersetzt. Sowohl das Abhören als auch das Aufzeichnen und Überwachen von Telekommunikation wird durch RIPA geregelt. Dabei werden die Regeln durch sogenannte ***Codes of Practice***²⁷⁹ des *Home Office* (Innenministeriums) ergänzt.

1.1. Abhörmassnahmen

Teil I, 1. Kapitel von RIPA regelt die Möglichkeit, vom Inhalt einer Kommunikation (E-mail, Telefonie, SMS) Kenntnis zu nehmen. Auch wenn in seltenen Fällen das rechtmässige Abhören von Telekommunikation ohne eine entsprechende Verfügung (*warrant*) erlaubt ist (z.B. wenn eine oder mehrere Parteien zugestimmt haben, oder nach den auf Gefängnissen anwendbaren Regeln²⁸⁰), wird das rechtmässige Abhören gemäss section 5 RIPA grundsätzlich nur gemäss einem vom ***Secretary of State*** (d.h. in der Regel dem Innenminister) erlassenen *warrant* genehmigt.

Die Zahl der ***intercepting agencies***, d.h. der Institutionen und Organisationen, welche einen Antrag für die Genehmigung einer Überwachung stellen (oder stellen lassen) können, ist **begrenzt**. Es handelt sich dabei um den *Security Service* (Inlandsnachrichtendienst), den *Secret Intelligence Service* (Auslandsnachrichtendienst), die *Government Communications Headquarters* (Telekommunikationsnachrichtendienst), die auf gewisse organisierte Verbrechen spezialisierte *Serious Organised Crime Agency*, die Polizei, *HM Revenue & Customs* (Steuerbehörde), die *Defence Intelligence* oder andere nationale Sicherheitsbehörden, welche eine entsprechende vertragliche Verpflichtung haben.²⁸¹

²⁷⁷ Section 5, Intelligence Service Act 1994.

²⁷⁸ Verfügbar unter <http://www.legislation.gov.uk/ukpga/2000/23/contents> (24.01.13).

²⁷⁹ *Acquisition and Disclosure of Communications Data Code of Practice* und *Interception of Communications, Home Office Codes of Practice* (2007), verfügbar unter <http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-acquisition?view=Binary> und <http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/interception-comms-code-practice?view=Binary>, (24.01.13).

²⁸⁰ Siehe sections 3 und 4 RIPA.

²⁸¹ Section 6 (2) RIPA.

1.1.1. Gründe für das Abhören

Das Erlangen eines *warrant* führt dazu, dass die Überwachungsmassnahme als gerechtfertigter Eingriff in die Rechte gemäss Art. 8 EMRK gilt, sofern die Massnahme notwendig und verhältnismässig ist. Gemäss RIPA muss der *Secretary of State* annehmen, dass die Massnahme für einen der folgenden Gründe **notwendig** ist:²⁸²

- im Interesse der nationalen Sicherheit,
- zur Prävention und Aufklärung ernsthafter Verbrechen (*serious crime*),
- zur Wahrung des ökonomischen Wohlstands des Vereinigten Königreichs,
- in Anwendung einer internationalen Rechtshilfevereinbarung, soweit die Umstände dem *Secretary of State* mit der Prävention oder Aufklärung ernsthafter Verbrechen im Inland vergleichbar erscheinen.

Als **ernsthafte Verbrechen** im erwähnten Zusammenhang gelten nach *section 81 (2) und (3) RIPA* die Straftat oder eine der Straftaten, welche durch das Verhalten begründet wird, für welches eine mindestens 21-jährige Person ohne Vorstrafen zu **voraussichtlich drei oder mehr Jahren** Freiheitsstrafe verurteilt würde, oder Verhalten, welches die Anwendung von **Gewalt** beinhaltet, einen wesentlichen **finanziellen Gewinn** hervorbringt oder von einer grossen Zahl von Personen in Verfolgung eines gemeinsamen Zwecks gezeigt wird.

Falls die Massnahme notwendig ist, muss der *Secretary of State* auch davon ausgehen, dass diese **verhältnismässig** zu dem damit verfolgten Zweck ist. Dies bedeutet, dass die Einschränkung durch die Abhörung gegenüber der Notwendigkeit der Massnahme abgewogen werden muss.

1.1.2 Das Verwenden der Informationen im Strafverfahren

Grundsätzlich spielt weder die Möglichkeit von Abhörmassnahmen noch das abgehörte Material selbst eine Rolle im Strafverfahren. Nach Ansicht der Regierung würde das Zulassen von durch Abhören erlangter Beweismittel vor Gericht von der Effizienz dieser Technik ablenken. Somit wird das abgehörte Material **ausschliesslich für aufklärerische Zwecke** (*intelligence purpose*) verwendet. Dies ergibt sich aus *section 17 RIPA*, wonach Beweise, Fragen, Bekräftigungen oder Aussagen in rechtlichen Verfahren nicht zulässig sind, soweit diese den Inhalt einer überwachten Kommunikation betreffen oder auf das Vorliegen (oder Fehlen) eines Überwachungs-*warrant* (und damit auf das Vorliegen von Überwachungsmassnahmen) deuten.²⁸³ Dies bedeutet, dass das durch Abhören erlangte

²⁸² *Section 5 (3) RIPA.*

²⁸³ *Section 17 RIPA: "Exclusion of matters from legal proceedings.*

(1) Subject to section 18, no evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings or Inquiries Act proceedings which (in any manner)

(a)discloses, in circumstances from which its origin in anything falling within subsection (2) may be inferred, any of the contents of an intercepted communication or any related communications data; or

(b)tends (apart from any such disclosure) to suggest that anything falling within subsection (2) has or may have occurred or be going to occur.

(2)The following fall within this subsection

(a)conduct by a person falling within subsection (3) that was or would be an offence under section 1(1) or (2) of this Act or under section 1 of the Interception of Communications Act 1985;

(b)a breach by the Secretary of State of his duty under section 1(4) of this Act;

(c)the issue of an interception warrant or of a warrant under the Interception of Communications Act 1985;

Material weder von der Anklage noch von der Verteidigung verwendet werden kann. Damit wird die Waffengleichheit (Art. 6 EMRK) gewährleistet.

Ausnahmen von dieser Regel sind gemäss *section 18 RIPA* streng begrenzt auf (i) Staatsanwälte, soweit diese damit die *fairness* eines Verfahrens zu gewährleisten (aber nicht zum Aufbau eines Kreuzverhörs) und um abzusichern, dass die Anklage nicht ungerecht vorgeht; und (ii) auf einen Richter, soweit dieser in Ausnahmefällen die Funktionen des Staatsanwalts überprüfen muss und diesem über die Fairness des Verfahrens Weisungen geben muss, wobei dabei weder der Umstand der Abhörung noch deren Gegenstand einer Jury mitgeteilt werden darf.

1.2. Das Erlangen und Übermitteln von Kommunikationsdaten

Das Erlangen und Übermitteln von Kommunikationsdaten, d.h. des „**Wer, Wann, Wo**“ einer Kommunikation (und nicht des Inhalts einer Kommunikation) wird durch Teil I, Kapitel II RIPA geregelt. Nur Personen, welche zu einer der in RIPA speziell bezeichneten öffentlichen Behörde gehören, können den Zugang zu solchen Verkehrs- und Standortdaten gewähren. Die entsprechenden Personen können dies aber nur für gewisse Zwecke (je nach Art der betroffenen Behörde) tun.

Als entsprechende **öffentliche Behörde** gelten die Polizei, die *Serious Organised Crime Agency*, die schottische *Crime and Drug Enforcement Agency*, *HM Revenue & Customs*, sowie durch *Order* des *Secretary of State* bezeichnete Behörden. In der Tat hat der *Secretary of State* verschiedene solche *Order* erlassen, so dass die Zahl der Behörden, welche Zugang zu Kommunikationsdaten haben, bedeutend gestiegen ist. Im Jahr 2008 handelte es sich dabei um 52 Polizeikräfte, 12 zusätzliche Vollzugsbehörden, 474 lokale Behörden und 110 andere öffentliche Behörden.²⁸⁴

RIPA definiert Kommunikationsdaten als Daten, welche beim Erbringen und Unterhalt von Kommunikationsdienstleistungen (Post und Telekommunikation) entstehen, geschaffen oder erhalten werden. Dabei können drei Arten von Kommunikationsdaten gesammelt werden:

- **Benutzerdaten** (*Subscriber Data*), d.h. Informationen, die ein Dienstleistungsanbieter über einen Klienten hat (z.B. Name und Adresse).
- **Verkehrsdaten** (*Service Use Data*), d.h. Informationen über die Benutzung der Kommunikationsdienstleistung durch eine Person (z.B. Liste mit den Telefonanrufen unter Angabe von Datum und Zeit sowie der angerufenen Rufnummern).
- **Daten zum Verkehr** (*Traffic Data*), d.h. Angaben, welche bei einer Kommunikation zum Zwecke der Kommunikationsübermittlung mitgeliefert werden (z.B. alles, was aussen auf einer Postsendung angebracht ist, betreffend deren Versandroute).

Kommunikationsdaten können gemäss *section 22 (2) RIPA* für eine Vielzahl von Zwecken konsultiert werden, inkl. zum **Zwecke der Aufklärung und Verhinderung von Straftaten** oder zur Vermeidung öffentlicher Aufruhr oder zur Wahrung öffentlicher Sicherheit. Ein solcher Zugang stellt aber ein Eingriff in die Privatsphäre von Einzelpersonen dar und muss deshalb die Prinzipien der Notwendigkeit und Verhältnismässigkeit respektieren. Zusätzliche Restriktionen ergeben sich aus dem Code of Practice des Innenministeriums.²⁸⁵ Dabei geht es insbesondere darum, welche erfahrenen Mitarbeiter innerhalb einer öffentlichen Behörde über den Zugang zu Daten beschliessen können und welche

(d)the making of an application by any person for an interception warrant, or for a warrant under that Act;

(e)the imposition of any requirement on any person to provide assistance with giving effect to an interception warrant.”

²⁸⁴ Siehe dazu den Bericht des *Interception of Communications Commissioner* 2006, verfügbar unter <http://www.official-documents.gov.uk/document/hc0708/hc02/0252/0252.asp> (24.01.13).

²⁸⁵ Acquisition and Disclosure of Communications Data, Home Office Code of Practice, zit., S. 20 ff.

Personen die Datenerhebung durchführen. In der Polizei muss die Genehmigung von einem Superintendenten oder einem höheren Rang erteilt werden.²⁸⁶

1.2.1 Verwendung der Kommunikationsdaten im Strafverfahren

Gemäss dem *Code of Practice* des *Home Office*²⁸⁷ müssen öffentliche Behörden die Unterlagen über Mitteilungen, Anträge und Genehmigungen aufbewahren. Es bestehen hingegen keine besonderen strafprozessualen Regeln zu Beweismitteln im Bereich der Telekommunikation. Anders als die durch Abhören erlangten Informationen können die gemäss den oben ausgeführten Grundsätzen erhaltenen Telekommunikationsdaten (**Verkehrsdaten und Kundendaten**) durchaus als **Beweismittel in einem Strafverfahren verwendet werden**.

Nach dem *Criminal Procedure and Investigations Act 1996* (CPIA)²⁸⁸ besteht eine Pflicht, dass alles Material, welches im Rahmen einer Untersuchung erlangt worden ist und für die Untersuchung relevant erscheint, aufgezeichnet und dem Staatsanwalt (*prosecutor*) übermittelt werden muss.

Schliesslich ist noch darauf hinzuweisen, dass Teil III RIPA sich auf die Untersuchung von **verschlüsselten elektronischen Daten** bezieht.²⁸⁹ Dabei gilt die Prävention und Aufklärung von Straftaten als Grund, welcher zur Entschlüsselung solcher Daten berechtigt. Gemäss *section 49* RIPA kann jede öffentliche Behörde in der Regel einen Richter um einen Entscheid ersuchen, wonach eine Person oder Organisation zur Entschlüsselung der geschützten Information beauftragt (*to serve notice*) wird.

2. Übersicht über Prozess- und Organisationsstrukturen

2.1. Abhörungsverfahren

2.1.1 Genehmigung einer Abhörungsmassnahme

Vor der Durchführung einer Abhörungsmassnahme muss ein Antrag auf Erlass eines “**warrant**” an den *Secretary of State* gerichtet werden. Abhörungsverfügungen sind an die Person der „abhörenden“ Organisation gerichtet, welche den Antrag eingereicht hat. Diese Person kann dann eine Kopie der Verfügung an jede Person richten, welche bei der Durchführung der Massnahme behilflich sein könnte. Eine solche Verfügung enthält zwei Teile: erstens eine vom *Secretary of State* unterzeichnete Bezeichnung des von der Massnahme betroffenen Gegenstands oder der betroffenen Örtlichkeiten, und zweitens einen Anhang (*schedule*), der die abzuhörenden Gespräche auflistet.

Der **Anhang** sollte zudem den Namen des Telekommunikationsanbieters enthalten, welcher die Massnahme durchführen soll, eine Referenznummer und schliesslich die Bezeichnung der Art und Weise, wie die abzuhörenden Gespräche identifiziert werden können. Dies kann durch die Angabe von Adressen, Telefonnummern, Apparaten oder anderen Faktoren sowie durch eine Kombination dieser Faktoren erfolgen.

Es besteht auch die Möglichkeit **dringender Verfügungen** (*urgent warrants*). Diese können erlassen werden, wenn der *Secretary of State* nicht verfügbar ist. Ein solcher *warrant* wird in einem Dringlich-

²⁸⁶ Für genauere Angaben, siehe *Regulation of Investigatory Powers (Communications Data) Order SI 2010/480*.

²⁸⁷ *Acquisition and Disclosure of Communications Data, Home Office Code of Practice*, zit., S. 46.

²⁸⁸ Siehe Teil II CPIA und *Home Office Code of Practice, Acquisition and Disclosure of Communications Data*, zit.

²⁸⁹ Das entsprechende Verfahren gemäss dem III. Teil RIPA liegt ausserhalb des vorliegenden Gutachtens und wird deshalb nicht genauer beschrieben.

keitsverfahren erlassen und gilt nur während fünf Tagen. Die ordentlichen *warrants*, welche zu Zwecken der Verbrechensaufklärung oder -verhütung erlassen werden, gelten jeweils drei Monate, wobei sofern notwendig die Möglichkeit der Verlängerung besteht.²⁹⁰

2.1.2 Die Anforderungen an die Telekommunikationsanbieter

Nachdem ein *warrant* erlassen wurde, wird er dem Adressaten zugestellt, d.h. in der Regel der antragsstellenden Organisation. Diese Organisation kann danach die Kommunikationen selbst abhören oder von anderen Personen (wie z.B. von Telekommunikationsanbietern) die Unterstützung bei der Umsetzung des *warrant* verlangen. Gemäss *section 11 (4)* RIBA müssen Post- und **Telekommunikationsanbieter** alle Schritte unternehmen, um einen zugestellten *warrant* umzusetzen. Ausgenommen sind allerdings Massnahmen, welche für den Anbieter nicht **mit vernünftigem Aufwand möglich** sind („*not reasonably practicable*“).²⁹¹

Was genau mit vernünftigem Aufwand möglich ist, sollte durch **Konsultation** zwischen der Regierung und den Telekommunikationsanbietern vereinbart werden. Wird keine Einigung erreicht, kann der *Secretary of State* gemäss *section 11 (8)* RIBA entscheiden, ob er ein ziviles Verfahren zur Aussprache einer **Anordnung** (*injunction*) oder ein Gesuch um Anordnung der Ausführung der Massnahme anstreben möchte. Zudem begeht ein Telekommunikationsanbieter, der wissentlich seine Pflicht zur Umsetzung eines *warrant* verletzt, gemäss *section 11 (7)* RIBA eine **Straftrat** und kann zu einer Freiheitsstrafe von bis zu zwei Jahren oder einer Busse oder beidem verurteilt werden (s. dazu auch zwei Absätze weiter unten).

Alle Telekommunikationsanbieter, die zum Aufrechterhalten angemessener Abhörfähigkeiten verpflichtet sind, erhalten ein **Handbuch**, in welchem die Grundinformationen enthalten sind, die zur Behandlung einer Anordnung zur Unterstützung beim Durchführen einer Abhörmassnahme notwendig sind.²⁹² Die durchführende Behörde, welche die Mitwirkung eines Telekommunikationsanbieters verlangt, sollte dem Anbieter zudem die folgenden Informationen geben:²⁹³

- Eine vom *Secretary of State* unterzeichnete und datierte Kopie des „warrant instrument“;
- Den Anhang mit den Faktoren, welche die Identifikation der abzuhörenden Kommunikationsvorgänge erlaubt;
- Ein Deckblatt, mit welchem die abhörende Behörde den Anbieter zur Unterstützung auffordert und in dem allfällige andere Angaben zur Überwachung gemacht werden. Die Kontaktinformationen zur Behörde werden entweder ebenfalls in diesem Dokument angegeben oder sind im oben erwähnten Handbuch erwähnt.

Während alle Telekommunikationsanbieter verpflichtet sind, eine spezifische Überwachungsmassnahme umzusetzen, kann von gewissen Anbietern ganz allgemein verlangt werden, dass diese das rechtmässige Abhören ihres Netzwerks erlauben. Dies kann das Einhalten von Vorgaben wie diese des **European Telecommunications Standards Institute** (ETSI) beinhalten.²⁹⁴ Nach den *Lawful Intercept standards* des ETSI²⁹⁵ sollten z.B. Überwachungsgeräte spezifische Funktionen wie z.B. die Echt-

²⁹⁰ Siehe *section 9* RIPA.

²⁹¹ *Section 11 (5)* RIPA.

²⁹² Dieses Dokument gilt als private Vereinbarung zwischen einem Anbieter und der Regierung des Vereinigten Königreichs und ist deshalb nicht öffentlich verfügbar oder zugänglich.

²⁹³ *Interception of Communications, Home Office Code of Practice*, zit., S. 8-9.

²⁹⁴ Z.B. die ETSI ES 201 671 v.3.1.1 (May 2007) verfügbar unter http://www.etsi.org/deliver/etsi_es/201600_201699/201671/03.01.01_60/es_201671v030101p.pdf (24.01.13).

²⁹⁵ S. dazu <http://www.etsi.org/index.php/technologies-clusters/technologies/security/lawful-interception>.

zeitüberwachung beinhalten und andere gleichzeitig bestehende Abhörvorrichtungen sollten von anderen abhörenden Organisationen verborgen werden.

Die ***Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002***²⁹⁶ führt aus, welche Verpflichtungen nach Ansicht des *Secretary of State* einem Anbieter auferlegt werden können um sicherzustellen, dass diese solche Massnahmen umsetzen können. Der Order ist auf Anbieter mit mehr als 10'000 Kunden anwendbar (*section 12 RIBA*). Den betroffenen Anbietern kann eine Mitteilung (*notice*) zugestellt werden, welche diejenigen Massnahmen ausführt, welche der Anbieter zur Erfüllung seiner Verpflichtungen ergreifen muss. Vor Zustellung einer solchen formellen Mitteilung wird jedoch zwischen Regierung und Anbieter über den Inhalt der Mitteilung verhandelt. Zudem hat der Anbieter die Möglichkeit, die Angemessenheit der in einer Mitteilung verlangten technischen Vorgaben und Fähigkeiten durch das Technical Advisory Board zu verlangen, also durch eine nicht departementale (und damit wohl unabhängige) Regierungsbehörde.²⁹⁷

2.2. Verfahren zum Erlangen und Mitteilen von Kommunikationsdaten

Zwar könnten Polizeikräfte theoretisch gemäss dem *Police and Criminal Evidence Act 1984* die Herausgabe von Kommunikationsdaten aufgrund eines gerichtlichen „*production order*“ verlangen. Es entspricht jedoch der Praxis und *Policy* des *Home Office*, dass der Zugang zu diesen Informationen **gemäss den Bestimmungen des RIPA** beantragt wird. Dabei ist in der Regel (anders als bei Anordnungen zur Vorlage – *production orders*) **keine gerichtliche Genehmigung** nötig, und die Daten können für mehr Zwecke genutzt werden als nach dem *Police and Criminal Evidence Act 1984*. Lediglich Gemeindebehörden (*local councils*) müssen gemäss dem kürzlich erlassenen *Protection of Freedoms Act 2012*²⁹⁸ eine gerichtliche (*magistrate*) Genehmigung beantragen, um Zugang zu solchen Daten erhalten.

2.2.1 Gesuch auf Zugang zu Kommunikationsdaten

Ein Gesuch um Zugang zu Kommunikationsdaten geht in der Regel von einer Person aus, die eine Untersuchung oder andere Operation für eine berechnigte öffentliche Behörde führt. Das Gesuch muss die Notwendigkeit und die Verhältnismässigkeit des Zugangs zu den Kommunikationsdaten aufführen. Es wird dann einer eigens dafür bezeichneten Person (*designated person*), die in der entsprechenden Behörde eine definierte Funktion innehat, zugestellt. Diese Person beurteilt das Gesuch.

Die öffentliche Behörde sollte zudem noch einen „*single point of contact*“ (SPoC) haben, d.h. eine zugelassene Einzelperson oder eine Gruppe von zugelassenen Personen, welche im Zugang und Erhalt von Kommunikationsdaten und der Zusammenarbeit mit den Anbietern ausgebildet sind. Die Anbieter haben Zugang zu den Angaben über alle zugelassenen Personen, um die Echtheit einer Anfrage überprüfen zu können. Der SPoC erlaubt eine objektive Beurteilung und Beratung sowohl für den Gesuchsteller als auch für die bezeichnete Person. SPoC sollte insbesondere folgende Fähigkeiten haben:²⁹⁹

- Beurteilung, ob das Erlangen spezifischer Kommunikationsdaten von einem Anbieter vernünftigerweise als möglich erscheint oder ob die verlangten Daten notwendigerweise mit anderen Daten verbunden sind;

²⁹⁶ Verfügbar unter http://www.legislation.gov.uk/ukxi/2002/1931/pdfs/ukxi_20021931_en.pdf (24.01.13).

²⁹⁷ Für weitere Informationen, s. <http://www.homeoffice.gov.uk/agencies-public-bodies/tab/> (24.01.13).

²⁹⁸ *Section 37, Protection of Freedoms Act 2012.*

²⁹⁹ *Acquisition and Disclosure of Data, Home Office Code of Practice*, zit., S. 24.

- Beratung der Gesuchsteller zur besten Datenerlangungsmethode in den Fällen, in welchen die gesuchten Daten von mehreren Anbietern stammen;
- Versicherung gegenüber dem Anbieter, dass die Genehmigungen und Mitteilungen echt und legal sind;
- Beurteilung, ob die vom Anbieter übermittelten Daten die Anforderungen einer Genehmigung / Mitteilung erfüllen;
- Beurteilung der Kosten und Ressourcen für die öffentliche Behörde und den Anbieter.

Kommunikationsdaten können auf zwei Arten erlangt werden:

Zunächst kann eine Genehmigung (**authorisation**) ausgestellt werden. Eine solche Genehmigung erlaubt es den Personen innerhalb einer öffentlichen Behörde, gegenüber einem Anbieter ein gewisses Verhalten an den Tag zu legen, d.h. es ist die rechtliche Grundlage für das Einholen von Kommunikationsdaten beim Anbieter, die dieser bereits hat. Falls ein Anbieter z.B. technisch nicht in der Lage ist, gewisse Daten zu erfassen, kann gemäss der Gesetzgebung eine untersuchende Behörde die Daten selbst sammeln, in der Regel in Zusammenarbeit mit dem Anbieter.

Mitteilungen (**notices**) sind dann angemessen, wenn es sicher ist, dass ein Anbieter in der Lage ist, spezifische Daten zu finden oder zu ermitteln, und diese mitzuteilen. In diesem Fall wird die bezeichnete Person dem Inhaber der Daten eine entsprechende Mitteilung zuteilen und von diesem das Erfüllen der in der Mitteilung genannten Bedingungen verlangen.

Mitteilungen und Genehmigungen sind höchstens **ein Monat gültig** und können auf erneutes Gesuch um einen Monat verlängert werden.

In jeder betroffenen öffentlichen Behörde muss ein Beamter der oberen Hierarchiestufe (*senior responsible officer*) – eine Person, welche das Amt oder die Funktion der zuständigen Person innerhalb der Behörde innehat – für die Integrität des Prozesses zum Erlangen von Kommunikationsdaten zuständig und verantwortlich sein, insbesondere für das Einhalten der *Codes of Practice* sowie für die Übersicht über Fehlermeldungen an das *Interception of Communications Commissioner's Office* (IOCCO).³⁰⁰

2.2.2 Anforderungen an die Anbieter

Gemäss *section 22 (6)* RIPA muss ein Anbieter eine Mitteilung befolgen, sofern dies vernünftigerweise möglich ist. Gemäss dem entsprechenden Code of Practice³⁰¹ muss der Anbieter in der Regel die Kommunikationsdaten in schriftlicher oder elektronischer Form innerhalb von 10 Arbeitstagen nach Erhalt der Mitteilung kommunizieren.

Falls ein Anbieter die verlangten Kommunikationsdaten nicht liefert, kann der *Secretary of State* ein ziviles Verfahren gegen den Anbieter anstreben. Dies kann unter anderem zu einer Anordnung (*injunction*) führen, die den Anbieter zum Liefern der Daten zwingt.³⁰²

Gemäss europäischen Rechtsakten müssen Anbieter Kommunikationsdaten speichern. Ursprünglich war RIPA nur auf Daten anwendbar, welche nach Ausstellen einer entsprechenden Genehmigung gesammelt worden waren. Strafverfolgungsbehörden verlangten jedoch auch Zugang zu historischen Daten als Beweismittel um erfolgreiche Strafverfolgung zu ermöglichen, da bei Entdeckung einer Handlung diese bereits fortgeschritten sein könnte. Die in Umsetzung des europäischen Rechts erlas-

³⁰⁰ Appointed under section 57 RIPA for the purpose of keeping under review the exercise of powers and duties under Chapter II RIPA.

³⁰¹ *Acquisition and Disclosure of Communications Data, Home Office Code of Practice*, zit., S. 31.

³⁰² *Sections 22 (7) und (8) RIPA.*

sene *Data Retention (EC Directive) Regulations* SI 2009/859³⁰³ sind am 6. April 2009 in Kraft getreten. Demnach müssen auch Internetaktivitäten als Kommunikationsdaten jeweils **ein Jahr lang** von den Anbietern **aufbewahrt** werden.

Ein Anhang der 2009 *Regulations* führt genauer aus, welche Daten aufbewahrt werden müssen. Zur Anwendbarkeit dieser Verpflichtung ist allerdings erforderlich, dass der Anbieter vom *Secretary of State* schriftlich darüber informiert worden ist (*Regulation 10* der 2009 *Regulations*). Im September 2009 bestätigte das Innenministerium, seit Inkrafttreten der *Regulations* entsprechende Mitteilungen (*notices*) für „mehrere“ Anbieter erlassen zu haben.³⁰⁴

3. Kosten und Finanzflüsse

3.1. Rechtsgrundlage für Finanzierung

3.1.1 Abhörmassnahmen

Gemäss *section 14* RIPA muss der *Secretary of State* sicherstellen, dass die notwendigen Vorkehrungen (*arrangements*) bestehen, wonach die Kommunikationsanbieter einen angemessenen Anteil (*fair contribution*) an den effektiven oder wahrscheinlichen Kosten der Ausführung von Abhörungsverfügungen (*warrants*) erstattet erhalten. Nach *section 14 (3)* RIPA kann der *Secretary of State* zur Erfüllung seiner Pflicht Vorkehrungen dafür treffen, dass Zahlungen aus parlamentarisch gesprochenen Geldern erfolgen. Gemäss den Erklärungen zum RIPA müssen solche Vorkehrungen sicherstellen, dass die Anbieter einen in jedem einzelnen Fall angemessenen Betrag erhalten – einerseits angesichts der Kosten für die Sicherstellung der Abhörungs-fähigkeit und andererseits angesichts der Unterstützung bei einzelnen Abhörmassnahmen (*warrants*).

3.1.2 Erlangen und Übermitteln von Kommunikationsdaten

Section 24 RIPA ist eine analoge Vorschrift zu *section 14*. Diese Bestimmung anerkennt, dass bei den Anbietern auch bei der Ausführung von Mitteilungen bzw. Anordnungen zum Gewähren von Zugang zu und Übermitteln von Kommunikationsdaten Kosten entstehen. Die Vorschrift ermöglicht das Treffen von Vorkehrungen, dass den Dienstleistern angemessene Zahlungen an die Dienstleistungsanbieter ausgerichtet werden können, um so die zeitgerechte Mitteilung von Kommunikationsdaten zu erleichtern.

Nach dem *Home Office Code of Practice*³⁰⁵ werden den Kommunikationsanbietern erhebliche öffentliche Gelder verfügbar gemacht um sicherzustellen, dass diese auch ausserhalb ihrer ordentlichen Geschäftstätigkeit die entsprechenden (gesetzlichen, notwendigen und verhältnismässigen) Anforderungen der öffentlichen Behörden auf Ermitteln und Mitteilen von Kommunikationsdaten in einer effektiven und effizienten Art behandeln können. Nur so können die Untersuchungen und Operationen der Behörden zum Schutz der Öffentlichkeit und zur Bekämpfung der Kriminalität unterstützt werden

Der *Code of Practice* bestätigt zudem, dass es für die Kommunikationsanbieter durchaus legitim ist, eine Kostenbeteiligung zu verlangen. Diese könne auch einen Teil zur Finanzierung der allgemeinen, zum Befolgen von Mitteilungen oder zum Sicherstellen des Erfassens und rechtzeitigen Übermittels von Kommunikationsdaten notwendigen Kosten („business overheads“) umfassen. Die Möglichkeit

³⁰³ Verfügbar unter <http://www.legislation.gov.uk/ukSI/2009/859/contents/made> (28.01.13).

³⁰⁴ Siehe P. WARD & A. HORNE, *Interception of communications*, 17.05.2012 (SN/HA/6332) House of Commons Library, S. 10.

³⁰⁵ *Acquisition and Disclosure of Communications Data, Home Office Code of Practice*, zit., S. 37.

des Ersetzens dieser Kosten ist insbesondere für diese Anbieter relevant, welche Leute spezifisch dafür anstellen, das Erfüllen der Vorgaben von RIPA zu überwachen, und welche auch entsprechende Informationssysteme haben. Finanzielle Beiträge können auch für Kosten eines Anbieters angemessen sein, der seine Systeme erneuern muss um die Übermittlungsprozesse aufrechtzuerhalten oder effizienter zu gestalten, oder wo neue Technologien wiederum Investitionen in begleitende Technologien erfordern um die Vorgaben für die Übermittlung und Erfassung von Kommunikationsdaten auch für die dank den neuen Technologien angebotenen Dienstleistungen zu erfüllen.

Anbieter, welche die Erstattung angemessener Beiträge beantragen, sollten Zusicherungen abgeben und jede weitere vom Innenministerium verlangte Information erteilen, damit dieses sich versichern kann, dass der beantragte Ersatz eine angemessene Beteiligung an den effektiven Kosten darstellt.

3.1.3 Aufbewahren von Kommunikationsdaten

Für die Verpflichtung Kommunikationsdaten aufzubewahren sieht Regulation 11 der *Data Retention Regulations*³⁰⁶ vor, dass der *Secretary of State* Kosten eines öffentlichen Kommunikationsanbieters ersetzen kann, die durch das Befolgen der *Regulations* entstanden sind. Dabei kann der Ersatz davon abhängen, dass die Kosten dem *Secretary of State* im Voraus mitgeteilt worden sind und dass dieser damit einverstanden war. Zudem kann der *Secretary of State* verlangen, dass der Anbieter mit einer für die Überprüfung des Erstattungsanspruchs angemessenen **Revision (audit)** einverstanden ist.

3.2. Entscheidungsstrukturen über Kostentragung einer Überwachung im Einzelfall

Auch wenn der *Secretary of State* nach den oben zitierten Vorschriften des RIPA die Möglichkeit hat, „Vorgehensweisen zu treffen“ um die Beiträge an die Kosten der Anbieter festzusetzen, ist dies mindestens nicht in generell-abstrakter Form erfolgt. Vielmehr lässt das *Home Office* mitteilen, dass das genaue Verfahren für Zahlungen und die Berechnung der Beiträge zur Erstattung von Kosten des **Abhörens der Telekommunikation vertraulich** sind.³⁰⁷

Das *Home Office* hat immerhin bestätigt, dass die Regierung sich dazu verpflichtet hat, die **gesamten Grenzkosten** (*the full marginal costs*) im Zusammenhang mit Zugang und Aufbewahrung von Kommunikationsdaten zurückzuerstatten. Dies bedeutet, dass den Anbietern die direkt auf die Erfüllung der Verpflichtung zurückzuführenden Kosten zurückerstattet werden, nicht aber allgemeine Kosten (*wider business overheads*). Gemäss dem *Home Office* beinhalten direkt auf die Erfüllung zurückzuführende Kosten einerseits im Zusammenhang mit dem Unterhalt der Datenaufbewahrungssysteme entstehende Kosten, und andererseits Personalkosten für Anspruchs- und Kontaktpersonen der Strafverfolgungs- und Vollzugsbehörden.

Das Innenministerium führt dazu aus, dass das Gesetz zwar nicht eine Bezahlung der vollen Grenzkosten verlangt (sondern lediglich die Möglichkeit angemessener Anteile an den Kosten der Anbieter vorsieht). Die Regierung habe aber die **strategische Entscheidung** gefällt hat, dies zu tun. Dabei geht es einerseits darum sicherzustellen, dass die Wirtschaft des Vereinigten Königreichs nicht durch Vollzugsvorschriften der Regierung benachteiligt wird, andererseits erlaubt es der Regierung auch, verschiedene zusätzliche Elemente auszuformulieren, welche in der Gesetzgebung nicht vorgesehen sind, so z.B. Sicherheitsstandards und zeitliche Vorgaben („*service level agreements that industry are expected to meet in terms of timeliness of response to law enforcement queries.*“) Der strategische Entscheid soll somit sicherstellen, dass die Vollzugsbehörden des Vereinigten Königreichs die bestmögliche Dienstleistung erhalten.

³⁰⁶ Data Retention (EC Directive) Regulations 2009.

³⁰⁷ Die Information in diesem Abschnitt wurde von Robert Foss, Pursue Policy and Strategy Unit, Office for Security and Counter-Terrorism, The Home Office erteilt.

Gemäss dem Innenministerium werden die Kosten durch eine **Vielzahl verschiedener Mechanismen** erstattet. Bis vor kurzer Zeit war das hauptsächlich verwendete Modell ein marktbasiertes System, bei welchem jeder Anbieter seine Produkte (d.h. z.B. die verschiedenen Arten von Kommunikationsdaten) aufführte und für jede Aktivität einen **bestimmten Tarif** verlangte. Dies setzte jedoch eine komplizierte Einschätzung jedes Anbieters der im nächsten Jahr zu erwartenden Kosten für das Zurückbehalten und Übermitteln von Kommunikationsdaten voraus, zusammen mit einer Berechnung der erwarteten Nachfrage für verschiedene Produkte, damit die Tarife auch eine Deckung der zu erwartenden Kosten ermöglichten.

Während der letzten drei Jahre ist man im Vereinigten Königreich deshalb zu einem zentralisierten Modell übergegangen, wobei die grösseren Telekommunikationsanbieter ihre für den Betrieb der Datenrückbehaltung und -übermittlung notwendigen **jährlichen Kosten einschätzen** müssen. Diese Einschätzung wird dann dem *Home Office* übermittelt, welches die Kosten revidieren lässt, mit den öffentlichen Behörden und Vollzugsorganen diskutiert und genehmigt. Die Vollzugsbehörden tragen am Ende die Kosten. Die Anbieter werden zwar vom *Home Office* entschädigt, doch stellt das *Home Office* die Kosten der öffentlichen Behörde bzw. den Strafverfolgungsbehörden wiederum in Rechnung. Zur Ermittlung dieser Rechnung wird ein (nicht veröffentlichtes) **Vereinbarungsmodell** verwendet, wobei die Kosten jeder öffentlichen und Vollzugsbehörde gemäss der im Vorjahr in Anspruch genommenen Daten ermittelt werden.

Für die **spezifischen Kosten**, welche bei den Anbietern beim Bearbeiten der Anfragen entstehen, werden nach Angaben des Innenministeriums angemessene Methoden zur Bestimmung der Tarife nach Verhandlungen zwischen den Anbietern und dem Innenministerium festgelegt. Sofern die Telekommunikationsbranche ihre eigenen Berechnungsmodelle aufstellt, behält sich das Innenministerium deren Überprüfung vor und verlangt allenfalls Änderungen, sofern das Modell als nicht angemessen erscheint.

3.3. Kostenverteilung

Die Kosten, welche die öffentlichen Behörden durch zentrale Fonds zurückerstatten, hängen von den durch die einzelnen Anbieter festgesetzten Tarifen ab. Dabei sind die Tarife oder Ansätze der individuellen Anbieter, welche ihre Kosten zur Sicherung der angemessenen Überwachungsfähigkeit und zur Erfüllung der aus Abhörungs-, Aufzeichnungs- und Übermittlungsverpflichtungen bestätigen würden, **nicht öffentlich verfügbar**, und die Anbieter sind auch nicht bereit, diese auf Anfrage mitzuteilen.

Das Innenministerium hat bestätigt, dass es aus Gründen der Vollzugsmethode (*for reasons of sensitivity of law enforcement methodology*) die Liste der Produkte nicht veröffentlicht. Wie bereits oben erwähnt werden das genaue Verfahren für die Zahlungen und die Art der Berechnung für das Abhören von Telekommunikation **vertraulich** behandelt. Zudem scheint das Innenministerium gemäss verschiedenen Informationsanfragen an die Regierung nicht bereit, eine Aufschlüsselung der Kosten gemäss Telekommunikationsanbieter oder gemäss der Art der Anfrage / Überwachungsmassnahme öffentlich zu machen. Die Informationen beschränken sich auf die globalen Kosten für Dienstleistungen, welche von Anbietern unter RIPA angefordert worden sind.

Das Innenministerium macht zur Rechtfertigung des Zurückhaltens dieser Informationen geltend, dass Partner aus der Industrie nicht identifiziert werden möchten, da sie das Risiko fürchten, dass die **Klienten zu Konkurrenzunternehmen wechseln** würden, welche nicht aktiv mit dem Innenministerium zusammenarbeiten würden (abgesehen vom rechtlich notwendigen). Das Veröffentlichen von Namen der Unternehmen, welche mit dem Innenministerium zusammenarbeiten, würde finanzielle und rufschädigende Auswirkungen für die betroffenen Unternehmen haben.

Somit würde die **Zusammenarbeit zwischen Innenministerium und den Kommunikationsanbietern** leiden. Bei einer Veröffentlichung könnten Anbieter ihre Zusammenarbeit reduzieren, so dass weniger Kommunikationsdaten verfügbar wären. Dies wiederum würde die öffentliche Sicherheit beeinträchtigen. Das Nichtveröffentlichen von solcher Information war früher auch mit den Nachteilen für die wirtschaftlichen Interessen gerechtfertigt.³⁰⁸

Schliesslich würde gemäss dem Innenministerium das Veröffentlichen von Informationen über die Anbieter hervorheben, wo die operationellen Ressourcen fokussiert würden. Damit würde wiederum die Effizienz der Vollzugsbehörden im Verhüten und Aufklären von Verbrechen leiden und ein inakzeptables **Risiko** für die Fähigkeit des Vereinigten Königreichs **zur Sicherung der nationalen Sicherheit** darstellen. Aus diesen Gründen sei die entsprechende Information von den Transparenz- und Veröffentlichungsvorschriften des *Freedom of Information Act 2000* gemäss dessen *sections 24 (1)* und *31(1)(a)* ausgenommen.³⁰⁹

3.4. Finanzierungsmechanismen ausserhalb der einzelnen Verfahren

Siehe oben, 3.1. und 3.2.

³⁰⁸ Section 43 (2) *Freedom of Information Act 2000*.

³⁰⁹ Siehe die Antwort zu einem entsprechenden Informationsgesuch, verfügbar unter <http://www.whatdotheyknow.com/request/119572/response/296749/attach/3/attachment.pdf> (24.01.13).

V. SCHLUSSFOLGERUNG

Die Kosten der Fernmeldeüberwachung und deren Verteilung auf die Akteure stehen im Vordergrund des vorliegenden Rechtsvergleichs (s. oben, I.). Aus diesem Grund fokussieren sich die die Folgerungen zu den verschiedenen Fragen auf den Aspekt der Kosten.

Zunächst ist zu bemerken, dass sich Unterschiede bei den **strafprozessualen Grundlagen** nur sehr beschränkt auf die Kostenverteilung auswirken. Die Ausnahme ist das Vereinigte Königreich, wo das Durchführen von Überwachungsmassnahmen und die entsprechenden Informationen nicht im Strafprozess verwendet bzw. erwähnt werden darf, so dass eine Überwälzung der Kosten auf einen allfällig verurteilten Straftäter bereits aus diesem Grund entfällt. Im französischen Recht ist eine solche Überwälzung ganz grundsätzlich nicht vorgesehen. In den übrigen Staaten ist eine Kostentragung durch die verurteilte Person mindestens nicht ausgeschlossen, wird aber oft nicht ausdrücklich angesprochen. Als Ausnahme ist neben Deutschland das österreichische Recht zu erwähnen, welches die Überwälzung der Kosten einer entsprechenden Massnahme ausdrücklich nur dann vorsieht, wenn diese einen erheblichen Beitrag zur Aufklärung der Straftat geleistet hat.

Stärker verknüpft sind Kostenfragen mit den **Prozess- und Organisationsstrukturen**. Hier erscheint die in der Schweiz vorgesehene zentralisierte Behandlung der Gesuche der Ausnahmefall zu sein. Lediglich in den Niederlanden besteht für die meisten Datenauskünfte ebenfalls eine Zentralstelle, welche direkt eine entsprechende Datenbank unterhält auf welche die Strafverfolgungsbehörden Zugriff haben. In Österreich hat die Datenübermittlung aus Sicherheits- und Qualitätsgründen über eine zentrale Stelle zu erfolgen. In den meisten übrigen Rechtsordnungen kontaktieren die Strafverfolgungsbehörden die Telekom-Unternehmen. Allfällig bestehende zentralisierte Stellen haben entweder eine Kontrollfunktion (so im Vereinigten Königreich oder, bezüglich technischer Anforderungen in Deutschland) oder erleichtern allenfalls die Kontaktaufnahme mit den Anbietern (so in Deutschland). Dementsprechend ist auch die in der Schweiz vorgesehene Rechnungsstellung an die Endnutzer für die staatlich erbrachten Dienstleistungen die Ausnahme. Allerdings ist nicht auszuschliessen, dass in anderen Staaten eine entsprechende Rechnungsstellung trotz fehlender ausdrücklicher Grundlage ebenfalls stattfindet (z.B. im Vereinigten Königreich im Rahmen der Abrechnungen zwischen Innenministerium und den entsprechenden Behörden). Insbesondere wo verhandelte Tarife oder umfassende Abkommen über die Vergütung zwischen staatlichen Stellen und den Telekom-Anbietern bestehen wie im Vereinigten Königreich, in Dänemark und teilweise in den Niederlanden sowie in Frankreich (für Vorhalte- und Instandhaltungskosten) sind die Kostenflüsse weniger transparent.

Bei der Verteilung der Kosten **zwischen den staatlichen Institutionen** fällt auf, dass in gewissen Staaten die Kosten und insbesondere deren Rückerstattung an die Telekom-Unternehmen durch unterschiedliche Ministerien getragen werden. So übernimmt in Österreich das Bundesministerium für Verkehr, Innovation und Technik den Ersatz gewisser (Vorhalte und Instandhaltungs-) Kosten, die Strafverfolgungsbehörden erstatten die Kosten der einzelnen Massnahmen. In anderen Rechtsordnungen tritt mindestens gegenüber den Telekom-Unternehmen lediglich eine Behörde auf (z.B. in Frankreich durch das Justizministerium, im Vereinigten Königreich das Innenministerium), wobei – wie bereits erwähnt – eine (teilweise) Überwälzung auf die anfragenden Behörden erfolgt. In einer dritten Gruppe von Rechtsordnungen (soweit ersichtlich in Deutschland, wohl auch in Italien) übernehmen – wie in der Schweiz – unmittelbar (und ausschliesslich) die anfragenden Behörden die staatlichen Kosten. Dieser Aspekt ist auch mit der Frage verbunden, ob eine Rechtsordnung die staatliche Kostenbeteiligung nur für die konkreten Massnahmen oder auch für allgemeine Kosten (Vorhalte- und Instandhaltungskosten) vorsieht.

Bezüglich der **Kostenverteilung zwischen dem Staat und dem Telekom-Unternehmen** entspricht der in der Schweiz vorgesehene Ansatz demjenigen in Deutschland, Dänemark und den Niederlanden. - Eine staatliche Kostentragung ist nur für die einzelnen, konkreten Massnahmen vorgesehen. Andere Rechtsordnungen sehen eine staatliche Kostenbeteiligung auch für Vorhaltekosten- oder Instandhaltungskosten vor (z.B. das Vereinigte Königreich, Österreich, Frankreich). In diesem Sinn scheint das Schweizer System für die Telekom-Unternehmen im internationalen Vergleich eher weniger vorteilhaft, wenn auch nicht isoliert.

Betrachtet man hingegen das **Preisniveau**, deutet ein *prima facie* Vergleich darauf hin, dass die Ansätze in der Schweiz im Vergleich eher hoch sind. Es ist diesbezüglich jedoch hervorzuheben, dass angesichts der unterschiedlichen Kategorisierungen in den verschiedenen nationalen Tarifsystemen sowie angesichts der Vertraulichkeit der Informationen in anderen Rechtsordnungen keine eindeutige Beurteilung und damit auch keine abschliessende Schlussfolgerung zum Preisniveau möglich ist.

SCHWEIZERISCHES INSTITUT FÜR RECHTSVERGLEICHUNG

Dr. Lukas Heckendorn Urscheler
Vize-Direktor