

Wirkungsbereich der Bundesministerien für Inneres Justiz

Ausgewählte Ermittlungsmaßnahmen

Die rechtlichen Rahmenbedingungen für die besonderen Ermittlungsmaßnahmen und für die Telekommunikationsüberwachung waren ausreichend. Defizite bestanden vor allem im Fehlen aussagekräftiger statistischer Daten, in der unzureichenden Mitwirkung aller beteiligten Telekommunikationsbetreiber, in der mangelhaften technischen Ausrüstung der Sondereinheit für Observation und in der Übermittlung rechtswidriger Gerichtsbeschlüsse.

Kurzfassung

Prüfungsziel

Zur wirksamen Bekämpfung der allgemeinen und organisierten Kriminalität sowie terroristischer Vereinigungen sah die Strafprozessordnung 1975 besondere Ermittlungsmaßnahmen (großer und kleiner Späh- und Lauschangriff, Videofalle) sowie Maßnahmen zur Überwachung der Telekommunikation vor. (TZ 3, 17)

Ziel der Gebarungüberprüfung war die Beurteilung der Effizienz und Effektivität der Aufgabenerfüllung des BMI und des BMJ sowie des Zusammenwirkens von Justiz- und Sicherheitsbehörden sowie der Sicherheitsexekutive in diesem Bereich. (TZ 1)

Rechtsgrundlagen

Den mit der Einführung besonderer Ermittlungsmaßnahmen verbundenen gravierenden Grundrechtseingriffen wurde durch die Einrichtung eines besonderen Rechtsschutzsystems Rechnung getragen. (TZ 3, 13)

Datenqualität

Die – in den Geschäftsregistern der Verfahrensautomation Justiz – automationsunterstützt erfassten Maßnahmen zur Überwachung der Telekommunikation boten keine Möglichkeit zur Ermittlung detaillierter und aussagekräftiger Informationen. (TZ 23)

Beginn und Beendigung von Überwachungsmaßnahmen

Die Betreiber von Telekommunikationsdiensten erfüllten ihre gesetzlich normierte Mitwirkungspflicht in unzureichendem Ausmaß. Dies führte zum unwiederbringlichen Verlust von Inhaltsdaten (in der Regel Gesprächsinhalten) sowie zur ungesetzlichen Fortführung von Maßnahmen, die Grund- und Freiheitsrechte der Betroffenen verletzen. (TZ 21)

Sondereinheit für Observation

Eine Änderung der Unterstellung der Sondereinheit für Observation wirkte sich zwar nachhaltig negativ auf deren Ressourcen (Budgetmittel, Personal sowie vor allem Ausrüstung) aus, beeinträchtigte jedoch noch nicht die Qualität ihrer Aufgabenerfüllung. (TZ 4 bis 7)

Gerichtsbeschlüsse für Inhaltsüberwachungsmaßnahmen

Die Übermittlung gesetzwidriger Gerichtsbeschlüsse, mit denen Telekommunikationsbetreibern Überwachungsmaßnahmen angeordnet wurden, war geeignet, die Strafverfolgung zu erschweren oder zu verhindern und verletzte überdies das verfassungsmäßig gewährleistete Grundrecht auf Datenschutz. (TZ 19)

Großer Späh- und Lauschangriff

Der große Späh- und Lauschangriff bewährte sich aus ermittlungstaktischer Sicht zur wirksamen Kriminalitätsbekämpfung. Die Gerichte und die Staatsanwaltschaften gingen mit diesem Ermittlungsinstrument, das tiefe Eingriffe in Grund- und Freiheitsrechte der Betroffenen ermöglichte, maßhaltend und verhältnismäßig um. (TZ 8)

Geheimhaltungsvorschriften wurden durch Gerichte nicht ausreichend beachtet. Diese Verletzungen waren geeignet, den Erfolg der Ermittlungsmaßnahmen zu gefährden. (TZ 10)

Kleiner Späh- und Lauschangriff

Die kontinuierlich geringe Anzahl kleiner Späh- und Lauschangriffe führte aufgrund fehlender Erfahrungen zu Qualitätsmängeln. Aus diesem Grund wäre die Konzentration dieser Aufgabe bei der Sondereinheit für Observation erforderlich. (TZ 11)

Technische Ausrüstung für Observationsmaßnahmen

Das BMI beschaffte technische Ausrüstung für Observationsmaßnahmen zentral. Eine inhaltliche Überprüfung anhand konkreter Problemstellungen bei Überwachungsaufgaben – unter Einbindung der vorhandenen Fachkompetenz der Sondereinheit für Observation – erfolgte jedoch nicht. Schritte zur Erlangung externen Wissens (Werkverträge, Kooperationen im wissenschaftlich-technischen Bereich) wurden nicht gesetzt. (TZ 12)

Rechtsschutzbeauftragter des BMJ

Dem Rechtsschutzbeauftragten als unabhängige und objektive Verfahrenspartei oblag die Prüfung und Kontrolle der Anordnung und Durchführung eines großen Späh- und Lauschangriffes sowie eines automationsunterstützten Datenabgleichs (Rasterfahndung). (TZ 14)

Optische Überwachung

Der Ausrüstungsstand nachgeordneter Dienststellen des BMI für optische Überwachungsmaßnahmen (Videofalle) war inhomogen und verbesserungsbedürftig. (TZ 15, 16)

Änderungen durch das Strafprozessreformgesetz

Im strafprozessualen Vorverfahren, das ab 1. Jänner 2008 neu gestaltet wurde, sind Telekommunikationsmaßnahmen ausnahmslos durch den Staatsanwalt nach vorheriger gerichtlicher Bewilligung anzuordnen. (TZ 20)

Statistische Erfassung und Berichterstattung

Das BMJ erfüllte die gesetzliche Verpflichtung zur Berichterstattung an den Nationalrat über den Einsatz von Maßnahmen zur Überwachung einer Telekommunikation nicht ausreichend. Wegen Mängel bei der Datenerfassung und –auswertung waren die im jährlichen Sicherheitsbericht veröffentlichten Zahlen betreffend Maßnahmen zur Überwachung einer Telekommunikation fehlerhaft. (TZ 22)

Kostenersatz für Betreiber von Telekommunikationseinrichtungen

Die Neuregelung des Kostenersatzes für die Mitwirkung der Betreiber an Überwachungsmaßnahmen bewirkte einen wirtschaftlicheren Vollzug und eine Senkung der Kosten für das BMJ. (TZ 24)

Das BMJ konnte die Problematik des – auf Grundlage eines Erkenntnisses des Verfassungsgerichtshofes zu leistenden – Investitionskostenersatzes an die Betreiber noch nicht lösen. (TZ 27)

Abrechnung von Kostenersätzen

Zwischen der Rechnungslegung der Betreiber und der beschlussmäßigen Kostenbestimmung durch die Untersuchungsrichter lagen oftmals mehrere Monate, in Einzelfällen sogar Jahre. (TZ 26)

Maßnahmen zur Überwachung des Internet

Die Nutzung des Mediums Internet konnte aufgrund des Fehlens technischer Voraussetzungen in zunehmendem Maße nicht überwacht werden. (TZ 28)

Kenndaten zu ausgewählten Ermittlungsmaßnahmen

Wesentliche Rechtsgrundlagen

- Vorgaben auf
Europäischer Ebene
- Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation
 - Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden
- nationale
Rechtsgrundlagen
- XII. Hauptstück, Abschnitte V und VI der Strafprozessordnung 1975, BGBl. Nr. 631/1975 i.d.g.F. (Geltungsdauer bis 31. Dezember 2007)
 - 1. Teil, 1. Hauptstück, 5. Abschnitt der Strafprozessordnung 1975 in der Fassung des Strafprozessreformgesetzes, BGBl. I Nr. 19/2004 (Inkrafttreten mit 1. Jänner 2008)
 - § 10a Staatsanwaltschaftsgesetz, BGBl. Nr. 164/1986 i.d.g.F.
 - 12. Abschnitt des Telekommunikationsgesetzes 2003, BGBl. I Nr. 70/2003 i.d.g.F. (Kommunikationsgeheimnis, Datenschutz)
 - Überwachungsverordnung, BGBl. II Nr. 418/2001
 - Überwachungskostenverordnung, BGBl. II Nr. 322/2004

Besondere Ermittlungsmaßnahmen

Angeordnete Fälle einer Überwachung	2001	2002	2003	2004	2005	2006
			Anzahl			
gemäß § 149d Abs. 1 Z 3 Strafprozessordnung 1975 („großer Späh- und Lauschangriff“)	1	2	1	1	2	1
gemäß § 149d Abs. 1 Z 2 Strafprozessordnung 1975 („kleiner Späh- und Lauschangriff“)	3	4	1	4	2	1
gemäß § 149d Abs. 2 Z 1 und 2 Strafprozessordnung 1975 („Videofalle“)	81	77	79	80	75	56

Quelle: jährliche Gesamtberichte über den Einsatz besonderer Ermittlungsmethoden

Überwachungen einer Telekommunikation

	2001	2002	2003	2004	2005	2006
angeordnete Fälle	787	993	2.863	3.760	4.560	3.979
- davon <i>Inhaltsüberwachungen</i>	-	-	838	1.299	1.913	1.866
- davon <i>Standortfeststellungen</i>	-	-	709	980	1.080	798
- davon <i>Feststellung Vermittlungsdaten</i>	-	-	1.316	1.481	1.567	1.315
betroffene Anschlüsse	1.721	2.064	-	-	-	-
- davon <i>Inhaltsüberwachungen</i>	464	641	-	-	-	-
- davon <i>lediglich Rufdatenerfassung</i>	1.257	1.423	-	-	-	-

Quelle: jährliche Sicherheitsberichte; im Jahr 2003 nahm das BMJ eine grundlegende Umstellung bei der statistischen Erhebung vor, die Zahlen ab diesem Zeitpunkt sind aufgrund von Mängeln bei der Datenerfassung fehlerhaft (siehe dazu auch TZ 23)

Ausgaben für die Überwachung der Telekommunikation

	2001	2002	2003	2004	2005	2006
			in Mill. EUR			
Bereich Oberlandesgericht Wien	0,84	1,31	2,84	3,85	3,50	3,98
Bereich Oberlandesgericht Linz	0,44	0,62	1,20	1,45	0,86	1,09
Bereich Oberlandesgericht Graz	0,17	0,48	0,97	0,67	0,63	0,77
Bereich Oberlandesgericht Innsbruck	0,17	0,35	0,81	0,43	0,44	0,66
Summe Ausgaben	1,62	2,76	5,82	6,40	5,43	6,50

Quelle: Auswertungen der Bundesrechnungsabschlüsse

Prüfungsablauf und -gegenstand

- 1 Der RH überprüfte im Mai und Juni 2007 die Gebarung des BMI und des BMJ im Hinblick auf Ermittlungsmaßnahmen im Sinne der Abschnitte V („Überwachung einer Telekommunikation“) und VI („Optische und akustische Überwachung von Personen unter Verwendung technischer Mittel“) des XII. Hauptstückes der Strafprozessordnung 1975 (StPO).

Der Prüfungsgegenstand umfasste die im Dienste der Strafjustiz gesetzten Maßnahmen. Besondere Ermittlungsmaßnahmen ohne richterlichen Auftrag nach dem Sicherheitspolizeigesetz wurden nicht – bzw. nur soweit es Überschneidungen mit dem eigentlichen Prüfungsgegenstand erforderlich machten – einbezogen.

Ziel der Gebarungsüberprüfung war die Beurteilung der Effizienz und Effektivität der Aufgabenerfüllung des BMI und des BMJ sowie des Zusammenwirkens von Justiz- und Sicherheitsbehörden sowie der Sicherheitsexekutive in diesem Bereich.

Die Erhebungstätigkeiten erstreckten sich auf Organisationseinheiten der Zentralstellen BMI und BMJ sowie auf ausgewählte nachgeordnete Dienststellen (Landesgerichte, Landespolizeikommanden).

Zu dem im Oktober 2007 übermittelten Prüfungsergebnis nahmen das BMI und das BMJ im Februar 2008 Stellung. Der RH erstattete seine Gegenäußerungen im März 2008.

Besondere Ermittlungsmaßnahmen

Ausgangslage

- 2 Als Reaktion auf die dynamische Entwicklung primär der organisierten Kriminalität begann Mitte der 90er Jahre die öffentliche und (rechts)politische Diskussion über eine Ausweitung der Ermittlungsinstrumentarien. Nach einer grundsätzlichen Entscheidung für die Implementierung solcher Maßnahmen lag die Herausforderung in der Schaffung spezieller Rechtsgrundlagen sowie in deren Integration in die vorgegebenen Strukturen des Strafverfahrens.

Die neuen Eingriffsbefugnisse der Sicherheitsbehörden sollten ausschließlich auf Basis richterlicher Genehmigung möglich und zur Aufklärung vorher definierter strafbarer Handlungen eingesetzt werden. Zudem sollten sie sich an dem Gebot der Zweckmäßigkeit und Effizienz einerseits, an den Grundsätzen der Verhältnismäßigkeit und Subsidiarität sowie der Vereinbarkeit mit Grundrechten¹⁾ andererseits orientieren.

¹⁾ Garantie der Privatsphäre im Sinne des Art. 8 Abs. 1 Europäische Menschenrechtskonvention (Achtung des Privatlebens, des Familienlebens und der Wohnung)

Rechtsgrundlagen

3.1 Die legislative Umsetzung besonderer Ermittlungsmaßnahmen¹⁾ erfolgte vor allem durch eine Erweiterung der StPO um den großen und kleinen Späh- und Lauschangriff. Weitere dieser Maßnahmen waren die Videofalle sowie der automationsunterstützte Datenabgleich (Rasterfahndung).

¹⁾ Die formal richtige Bezeichnung gemäß Strafprozessordnung 1975 lautet „optische und akustische Überwachung von Personen unter Verwendung technischer Mittel“.

Die Geltung dieser Bestimmungen war zunächst bis 31. Dezember 2001 befristet, um ausreichende praktische Erfahrungen hinsichtlich der Effizienz und Verhältnismäßigkeit dieser Maßnahmen gewinnen zu können. Mit 1. Jänner 2002 erfolgte die Übernahme in den Dauerrechtsbestand.

Angesichts der damit verbundenen gravierenden Grundrechtseingriffe war ein besonderes Rechtsschutzsystem – ein unabhängiger Rechtsschutzbeauftragter im BMJ – erforderlich. Mit einer ebenfalls neu geschaffenen Geheimschutzordnung des BMI sowie einer Verschlusssachenordnung des BMJ sollten der Geheimnisschutz verbessert und Missbräuche verhindert werden.

Die weltweite Zunahme terroristischer Akte – u.a. auch in Folge der Ereignisse des 11. September 2001 – bewirkte eine Erweiterung des Anwendungsbereiches besonderer Ermittlungsmaßnahmen auf den Tatbestand der terroristischen Vereinigung.

3.2 Nach Ansicht des RH war die zeitlich begrenzte Einführung neuer Ermittlungsmaßnahmen eine geeignete Vorgangsweise, um vor allem der damals schwer abschätzbaren Dichte und kriminaltaktischen Umsetzbarkeit dieser Maßnahmen ausreichend Rechnung zu tragen. Wesentlich war in diesem Zusammenhang die Einrichtung des besonderen Rechtsschutzsystems, das sich in der Schaffung eines Rechtsschutzbeauftragten manifestierte.

Der RH empfahl dem BMJ, bei der Neueinführung weiterer Ermittlungsmaßnahmen – vor allem hinsichtlich der zeitlich befristeten Geltung und des besonderen Rechtsschutzsystems – in der bisherigen Weise vorzugehen.

3.3 Laut Mitteilung des BMJ sei es durch das mit 1. Jänner 2008 in Kraft getretene Strafprozessreformgesetz zu einer Ausdehnung des Rechtsschutzes durch die Ausweitung der Aufgaben des Rechtsschutzbeauftragten gekommen. Auch für die Arbeitsgruppe „Online-Durchsuchung“ wäre die Ausweitung der Befugnisse des Rechtsschutzbeauftragten ein wesentliches Thema. Dazu sei vor allem eine angemessene personelle Ausstattung erforderlich.

Sondereinheit für Observation

Organisation und Aufgaben

4.1 Zur taktischen Umsetzung des Kerns dieser neuen Ermittlungsmaßnahmen – dem großen Späh- und Lauschangriff – richtete das BMI die Sondereinheit für Observation (SEO) zunächst in unmittelbarer Unterstellung unter den Generaldirektor für die öffentliche Sicherheit ein. Die operative Einsatzbereitschaft der nach der Sondereinheitenverordnung geschaffenen SEO war Mitte 1998 gegeben.

Die Aufgaben umfassten

- die Durchführung großer sowie (auf Berufsgeheimnisträger eingeschränkte¹⁾) kleiner Späh- und Lauschangriffe (siehe dazu auch TZ 10 und TZ 11),

¹⁾ Darunter sind Verteidiger, Notare, Rechtsanwälte, Wirtschaftstreuhänder, Psychiater, Psychotherapeuten, Psychologen, Bewährungshelfer, eingetragene Mediatoren, Mitarbeiter anerkannter Einrichtungen zur psychosozialen Beratung und Betreuung sowie Medienunternehmen, Medieninhaber, Herausgeber, Medienmitarbeiter und Arbeitnehmer eines Medienunternehmens oder Mediendienstes zu verstehen.

- die Lauschabwehr sowie
- sonstige Assistenzdienstleistungen für andere Sicherheitsdienststellen.

Darüber hinaus entwickelte die SEO auch kontinuierlich technische Nischenlösungen, z.B. im Zuge von Telefonüberwachungen oder Sonderlagen.

Mit Wirksamkeit vom 1. Jänner 2003 wurde die SEO unmittelbar dem Direktor des Bundeskriminalamtes unterstellt.

4.2 Die Einrichtung einer eigenen Sondereinheit zur Durchführung besonderer Ermittlungsmaßnahmen war ein tauglicher Schritt zur Sicherstellung und Bündelung der notwendigen Ressourcen sowie zur Gewährleistung der erforderlichen ressortinternen Geheimhaltung.

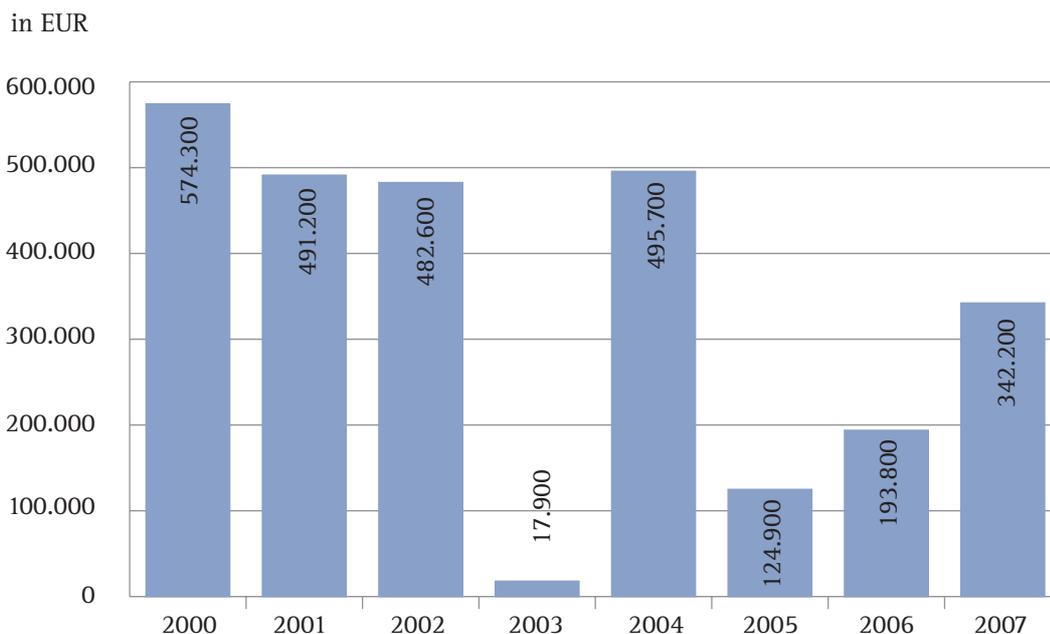
Die ursprüngliche direkte Unterstellung der SEO unter den Generaldirektor für die öffentliche Sicherheit war vor allem in Krisenfällen und wegen der kürzeren Informationswege zweckmäßig. Darüber hinaus bot sie eine taugliche Grundlage zur Schaffung und Erhaltung eines hohen Qualitätsstandards, der dem besonderen Einsatzbereich sowie der Bedeutung des großen Späh- und Lauschangriffes angemessen war. Er empfahl daher dem BMI, dieses ursprüngliche Unterstellungsverhältnis wiederherzustellen.

4.3 Laut Stellungnahme des BMI finde hinsichtlich einer Änderung der Unterstellung der SEO ein Diskussions- und Prüfungsprozess statt.

Ressourcen

Budgetmittel

5.1 Bis 2002 erfolgte die Budgetierung der SEO direkt über die Zentralleitung des BMI. Danach wurde sie aus Mitteln des Bundeskriminalamtes dotiert. Die folgende Grafik zeigt die jährlichen Ausgabenbeträge in EUR:



Quelle: Daten BMI

Sondereinheit für Observation

Im Jahr 2004 war für die SEO ursprünglich ein Betrag von rd. 41.500 EUR veranschlagt, der durch die Finanzierung aus einem Sonderbudget (Sicherheitspaket 2004) auf rd. 495.700 EUR erhöht wurde.

Seit Eingliederung der SEO in das Bundeskriminalamt entsprachen die gewährten Mittel nicht dem von ihr veranschlagten tatsächlichen Budgetbedarf. Nach Aufzeichnungen der SEO wären für notwendige Anschaffungen – vor allem im technischen Bereich – in den Jahren 2003 bis 2006 zusätzlich rd. 3,6 Mill. EUR erforderlich gewesen.

5.2 Nach der Zuordnung der SEO zum Bundeskriminalamt standen dieser die zuvor ausreichenden Budgetmittel nicht mehr zu Verfügung, was sich nachhaltig negativ auf ihre Ausrüstung (siehe dazu auch TZ 7) auswirkte. Dabei verkannte der RH nicht, dass die SEO lediglich eine von mehreren Organisationsteilen des Bundeskriminalamtes war, vermisste aber dennoch eine ausreichende Prioritätensetzung. Er empfahl daher dem BMI eine künftig verbesserte Steuerung der Budgetmittel für die SEO.

5.3 *Laut Mitteilung des BMI sei dem vermehrten Mittelbedarf der SEO 2007 mit rd. 342.200 EUR so weit wie möglich Rechnung getragen worden. Für 2008 seien rd. 538.240 EUR vorgesehen.*

Personal

6.1 Seit Gründung der SEO waren dieser 27 systemisierte Planstellen zur Aufgabenerfüllung zugewiesen. Im Zuge einer Evaluierung des Bundeskriminalamtes im Jahr 2005 reduzierte sich diese Anzahl zugunsten anderer Organisationsteile auf 25 Planstellen.

Mangels gesonderter Erfassung konnte die Feststellung der tatsächlichen Personalkosten nicht ohne unvermeidbaren Aufwand vorgenommen werden.

6.2 (1) Der RH konnte die nach Eingliederung in das Bundeskriminalamt erfolgte Planstellenreduktion der SEO nicht nachvollziehen. Angesichts der kontinuierlichen Ausweitung des Aufgabenspektrums, der erbrachten Leistungen sowie der angeregten zusätzlichen Aufgabewahrnehmung (siehe dazu TZ 11 und TZ 12) empfahl er dem BMI, die Wiederherstellung des ursprünglichen Personalstandes zu prüfen.

(2) Weiters stellte der RH fest, dass die im BMI vorhandenen Daten über den Personalaufwand der SEO keine taugliche Grundlage für Steuerungsmaßnahmen boten. Er empfahl daher dem BMI, im Zuge der Einrichtung einer Kosten- und Leistungsrechnung entsprechende Vorkehrungen zu treffen.

- 6.3 *Das BMI teilte in seiner Stellungnahme mit, dass es aufgrund seiner Personalentwicklungskonzepte gezwungen gewesen sei, entsprechende Umschichtungen durchzuführen. Deshalb seien zwei Planstellen in eine andere Abteilung implementiert worden.*

Technische Ausstattung

- 7.1 Grundlage für die Aufgabenerfüllung der SEO war deren Ausrüstung, die im Wesentlichen aus technischen Einsatzmitteln sowie einem Fuhrpark bestand. Die Ausrüstung der SEO entsprach unmittelbar nach ihrer Einrichtung dem damaligen Stand der Technik. Der Fuhrpark der SEO bestand nahezu ausschließlich aus Fahrzeugen, die das BMI während der Einrichtungsphase der SEO 1998 beschafft hatte.

Als Beurteilungsgrundlage für den aktuellen Ausrüstungsstand dienten dem RH bestehende Inventarlisten sowie eine Aufstellung technischer Einsatzmittel, wobei insbesondere der Einsatzzweck, der Anschaffungszeitpunkt und der Stand der Technik berücksichtigt wurden.

- 7.2 Der RH hielt fest, dass die SEO infolge unzureichender Budgetmittel mit der zwischenzeitlich rasanten technischen Entwicklung – vor allem in den Bereichen Telekommunikation und IT – nicht mehr Schritt halten konnte. Erforderliche neue Ausrüstung konnte daher nicht beschafft werden. Zudem waren zur Zeit der Gebarungsüberprüfung wesentliche Ausrüstungsteile dringend erneuerungsbedürftig.

Dennoch beeinträchtigte die mangelhafte Ausrüstung noch nicht die Qualität der Aufgabenerfüllung. Diese war jedoch im zunehmenden Ausmaß von Improvisationsgeschick, technischen Eigenentwicklungen und Leihgaben anderer Dienststellen abhängig.

Der RH empfahl daher dem BMI, nach vorangehender Bedarfsfeststellung und budgetärer Vorsorge ein Anschaffungsprogramm für eine dem Stand der Technik entsprechende Ausrüstung der SEO zu erarbeiten und einen Zeitplan für dessen Umsetzung festzulegen.

7.3 Laut Mitteilung des BMI erarbeite die SEO jährlich ein Anschaffungsprogramm. Bei der Aufteilung des Budgets für 2008 sei den Bedürfnissen der SEO so weit wie möglich entsprochen worden.

Großer Späh- und Lauschangriff

Einsatzvoraussetzungen und Anzahl

8.1 Unter dem großen Späh- und Lauschangriff sind die Überwachung nichtöffentlicher Verhalten sowie Äußerungen von Personen unter Verwendung technischer Mittel zur Bild- oder Tonübertragung sowie -aufnahme ohne Kenntnis der Betroffenen zu verstehen.

Nach § 149d StPO ist die Durchführung eines großen Späh- und Lauschangriffes für bestimmte Straftatbestände bzw. für Verbrechen mit einem Strafrahmen von mehr als zehn Jahren Freiheitsstrafe und darüber hinaus nur nach einer Prüfung der Verhältnismäßigkeit sowie der Subsidiarität¹⁾ der Maßnahme zulässig.

¹⁾ Grundsatz der Verhältnismäßigkeit: Das Interesse an der Aufklärung der Straftat muss die Nachteile, die mit einer geheimen Überwachung verbunden sind, aufwiegen. Grundsatz der Subsidiarität: Prüfung, ob nicht mit weniger eingriffsintensiven Maßnahmen begründete Aussicht auf den angestrebten Erfolg besteht.

Seit Einführung der Maßnahme war die SEO mit der Prüfung und Durchführung der folgenden Anzahl großer Späh- und Lauschangriffe befasst:

	Große Späh- und Lauschangriffe							
	1999	2000	2001	2002	2003	2004	2005	2006
	Anzahl							
geprüft	2	8	4	5	4	2	3	5
davon durchgeführt	1	4	1	1	1	1	- ¹⁾	1

¹⁾ Zwei Beschlüsse konnten aufgrund der gegebenen Rahmenbedingungen nicht realisiert werden; für den weiteren konnte kein Gerichtsbeschluss erwirkt werden.

Quelle: Aufzeichnungen der SEO; die dargestellten Zahlen weichen aufgrund unterschiedlicher Erfassungszeiträume von jenen der Sicherheitsberichte ab.

- 8.2** Nach Einschätzung des RH war die Grundsatzentscheidung, den großen Späh- und Lauschangriff ausschließlich auf ein enges Deliktsspektrum unter besonderen Voraussetzungen zu beschränken – vor allem angesichts der Tiefe der dadurch ermöglichten Grundrechtseingriffe sowie der Streuwirkung auf unbeteiligte Dritte – aus rechtsstaatlicher Sicht angemessen. Der RH stellte weiters fest, dass sich der große Späh- und Lauschangriff aus ermittlungstaktischer Sicht zur wirksamen Kriminalitätsbekämpfung bewährte.

Der RH teilte die wiederholte Einschätzung des BMJ, dass mit dem Ermittlungsinstrument des großen Späh- und Lauschangriffes maßhaltend und verhältnismäßig umgegangen wurde; dies bestätigte auch die Wirksamkeit der strengen Einsatzvoraussetzungen.

Ablauf eines großen Späh- und Lauschangriffes

- 9.1** Folgende Grafik zeigt die ablauforganisatorische Abwicklung eines großen Späh- und Lauschangriffes durch die SEO:

Großer Späh- und Lauschangriff

Erstkontakt mit der fallführenden Dienststelle			
Grobprüfung rechtlicher Voraussetzungen sowie technische Machbarkeitsstudie			
Beantragung des großen Späh- und Lauschangriffes durch die SEO und die fallführende Exekutivdienststelle bei der Staatsanwaltschaft			
Beschlussfassung durch das Gericht auf Antrag der Staatsanwaltschaft			
Planung des operativen Ablaufes			
Aufbau der Infrastruktur sowie Einbringung der technischen Einsatzmittel ins Zielobjekt			
Verständigung des Gerichts von der Einbringung			
Optische und akustische Aufzeichnung			
Zeitechte Auswertung und Dokumentation			
Beendigung der Maßnahme – Ausbau der Einsatzmittel			
Verständigung des Gerichts von der Beendigung			
Detailauswertung des aufgezeichneten Materials			
Endbericht, Akten- und Datenträgerübergabe an das Gericht			
Löschung aller Datenträger über Antrag des Rechtsschutzbeauftragten und Auftrag des Gerichts			
		<ul style="list-style-type: none"> – Durchgehende Information der Staatsanwaltschaft und des Gerichts – Einbeziehung des Rechtsschutzbeauftragten, fortlaufende und unangemeldete Kontrollen 	<p>Laufende Einbindung und Akkordierung mit der fallführenden Exekutivdienststelle. Beteiligung an der Auswertung</p>

Die polizeitaktische Durchführung eines großen Späh- und Lauschangriffes verlangte von den eingesetzten Ermittlern die Anpassung an im Einzelfall ständig wechselnde Einsatzbedingungen, wie bspw. Arbeitszeiten und räumliche Gegebenheiten. Zur Verhinderung des Verlustes von Überwachungsergebnissen hatte die SEO während laufender Überwachungsmaßnahmen für die Aufrechterhaltung der technischen Infrastruktur zu sorgen.

Die Auswertung und grobe schriftliche Dokumentation der Überwachungsdaten erfolgte, falls erforderlich, unter Beiziehung eines Dolmetschers unmittelbar, um das zeitgerechte Einschreiten bei allenfalls geplanten strafbaren Handlungen sicherstellen zu können. Die endgültige Detailauswertung war – insbesondere bei langen Überwachungen oder bei Einsatz von Dolmetschern – mit mehrmonatigen Auswertungsphasen nach Beendigung der Maßnahmen verbunden.

Die SEO verfügte über interne Vorschriften hinsichtlich Dokumentation und Geheimhaltung sämtlicher Umstände, die mit einer Maßnahme verbunden waren.

Der RH überprüfte stichprobenartig die Ermittlungsakte mehrerer großer Späh- und Lauschangriffe.

- 9.2** Der organisatorische Ablauf eines großen Späh- und Lauschangriffes war nach Beurteilung des RH zwar komplex, aber angesichts der Vielzahl an beteiligten Organisationen erforderlich. Überdies bot er eine taugliche Basis für Geheimhaltung und wechselseitige Kontrolle.

Die von der SEO aufgestellten internen Regelungen bewirkten einen hohen Qualitätsstandard der schriftlichen Auswertungen.

Geheimhaltung;
Beschlüsse

- 10.1** Der RH überprüfte die bei der SEO lückenlos aufliegenden Gerichtsbeschlüsse sowie den Schriftverkehr mit den anordnenden Gerichten für große Späh- und Lauschangriffe. Dabei stellte er fest, dass in einem Fall bei Honoraranweisungen eines Gerichtes für eine Dolmetscherin auf deren Kontoauszügen die Aktenzahl sowie der Name der Zielperson der Überwachungsmaßnahme ersichtlich waren, obwohl der betreffende Akt nach der Verschlusssachenordnung entsprechend klassifiziert war.

In einem weiteren Fall erfolgte die Übermittlung eines Verlängerungsbeschlusses auf dem Faxweg, obwohl die Verschlusssachenordnung ausnahmslos die persönliche Zustellung vorsieht.

Großer Späh- und Lauschangriff

Eine Durchsicht sämtlicher Beschlüsse ergab, dass in den Jahren 2000 bis 2002 mehrmals Nachtrags- und Ergänzungsbeschlüsse wegen inhaltlicher und formeller Mängel gefasst werden mussten.

Seit Dezember 2005 war im Intranet des BMJ ein Leitfaden für den großen Späh- und Lauschangriff verfügbar, der sämtliche für die Beschlussfassung maßgeblichen Rechtsvorschriften (u.a. auch alle Geheimhaltungsvorschriften) und Rahmenbedingungen enthielt.

10.2 (1) Der RH bemängelte, dass Geheimhaltungsvorschriften durch Gerichte nicht ausreichend beachtet wurden. So stellten die Anführung des Namens einer Zielperson eines großen Späh- und Lauschangriffes auf dem Kontoauszug einer Dolmetscherin ebenso wie die Übermittlung eines Beschlusses auf dem Faxweg grobe Verletzungen der Verschlusssachenordnung dar. Darüber hinaus waren sie geeignet, den Erfolg der Ermittlungsmaßnahmen sowie im ersten Fall die körperliche Sicherheit der Dolmetscherin zu gefährden. Er empfahl dem BMJ, für die Einhaltung der Geheimhaltungsvorschriften durch Gerichte verstärkt zu sorgen.

(2) Beschlüsse für große Späh- und Lauschangriffe erwiesen sich hinsichtlich inhaltlicher und formeller Gesichtspunkte – vor allem in der Einführungsphase der Maßnahme – mehrfach als verbesserungsbedürftig. Ein wesentlicher Grund lag darin, dass der große Späh- und Lauschangriff ein gänzlich neues und selten angeordnetes Ermittlungsinstrument darstellte.

(3) Mit der Erstellung des Leitfadens reagierte das BMJ in geeigneter Form.

10.3 *Laut Stellungnahme des BMJ werde die Verschlusssachenordnung anlässlich des Inkrafttretens des Strafprozessreformgesetzes mit 1. Jänner 2008 überarbeitet. Im Rahmen einer internen Kundmachung erfolge der Hinweis auf die unbedingte Notwendigkeit der durchgehenden Einhaltung der Geheimhaltungsvorschriften.*

Kleiner Späh- und Lauschangriff

11.1 Bereits vor Schaffung des kleinen Späh- und Lauschangriffes sah das Sicherheitspolizeigesetz eine ähnliche Maßnahme vor, die jedoch weniger eingriffsintensiv war und durch den Rechtsschutzbeauftragten des BMI überwacht wurde.

Im Zuge eines kleinen Späh- und Lauschangriffes konnten „nicht öffentliches Verhalten und nicht öffentliche Äußerungen von Personen unter Verwendung technischer Mittel zur Bild- oder Tonübertragung sowie -aufnahme überwacht werden“, wobei mindestens ein Gesprächspartner in die Überwachung eingeweiht war.

Nachstehende Organisationseinheiten führten in folgender Anzahl kleine Späh- und Lauschangriffe nach der StPO durch:

	2001	2002	2003	2004	2005	2006
	Anzahl					
Sondereinheit für Observation (SEO)	-	-	-	2	1	1
Zentrale Observation des Bundeskriminalamtes	- ¹⁾	1	1	2	2	1
Bundesamt für Verfassungsschutz und Terrorismusbekämpfung	-	-	-	1	1	-

¹⁾ Vor Schaffung des Bundeskriminalamtes nahmen operative Assistenzbereiche der heutigen Landeskriminalämter diese Aufgaben wahr.

Die dargestellten Zahlen weichen aufgrund unterschiedlicher Erfassungszeiträume von jenen der Sicherheitsberichte ab.

Quelle: Aufzeichnungen der genannten Organisationseinheiten

Laut jährlichem Gesamtbericht des BMJ über den Einsatz besonderer Ermittlungsmaßnahmen war zur Zeit der legislatischen Umsetzung von jährlich 20 kleinen Lauschangriffen ausgegangen worden.

Die SEO führte kleine Späh- und Lauschangriffe auf Ersuchen anderer Dienststellen durch. Zudem war sie wiederholt Anlaufstelle bei technischen Problemen und für die Beseitigung von Qualitätsmängeln im Zuge von Auswertungen kleiner Späh- und Lauschangriffe anderer Organisationseinheiten.

Kleiner Späh- und Lauschangriff

11.2 Angesichts der kontinuierlich geringen Anzahl kleiner Späh- und Lauschangriffe sowie dabei aufgetretener Qualitätsmängel empfahl der RH dem BMI, diese Aufgabe – speziell im Hinblick auf deren technische Problemlösungskompetenz und Fachwissen sowie ihren hohen Dokumentationsstandard – bei der SEO zu konzentrieren.

11.3 *Laut Stellungnahme des BMI sei die technische Durchführung des „kleinen Späh- und Lauschangriffes“ für strafprozessuale Zwecke mit der Maßnahme nach § 54 Abs. 4 Sicherheitspolizeigesetz (Ermittlung personenbezogener Daten mit Bild- und Tonaufzeichnungsgeräten) überwiegend ident; dies setze die gleiche technische Ausrüstung voraus. Mangels Konkretisierung könne es auf Qualitätsmängel und technische Probleme bei der Durchführung solcher Maßnahmen nicht eingehen.*

Eine Konzentration der Maßnahme würde weder zu Einsparungen von Personal oder technischer Ausrüstung führen, noch eine Hebung der Qualität mit sich bringen.

11.4 Der RH betonte, dass die Durchführung kleiner Späh- und Lauschangriffe strafprozessualen Zwecken – insbesondere der Beweissicherung – diene. Demgegenüber erlaube die Maßnahme des § 54 Abs. 4 Sicherheitspolizeigesetz keine Aufzeichnungen und ist daher nicht – wie dies das BMI vermeint – von seiner technischen Durchführung her ident. Darüber hinaus setzen beide Maßnahmen nicht die gleiche technische Ausrüstung voraus. Die Feststellungen des RH über Qualitätsmängel bezogen sich auf zwei Fälle, in denen die zentrale Observation des Bundeskriminalamtes die SEO um Qualitätsverbesserung von Aufnahmen ersucht hatte.

Technische Ausrüstung für Observationsmaßnahmen

12.1 Seit Mitte der 90er Jahre kam es bei technischen Entwicklungen zu einer rasanten Beschleunigung, die vor allem die Bereiche Telekommunikation sowie IT und damit auch das Internet betraf.

Die SEO reagierte auf die für sie veränderte Aufgabenstellung mit einer Vertiefung ihres Spezialisierungsgrades sowie mit technischen Eigenentwicklungen. Darüber hinaus bestand ein erhöhter Bedarf an technischer Ausrüstung, der mit den in den vergangenen Jahren unzureichenden Budgetmitteln nicht mehr abgedeckt werden konnte. Weitere Schritte der SEO, um Zugang zu externem Wissen zu erlangen – wie etwa durch Werkverträge oder Kooperationen im wissenschaftlich-technischen Bereich –, wurden nicht gesetzt.

Das BMI beschaffte technische Ausrüstung für Observationsmaßnahmen zentral. Eine inhaltliche Überprüfung der Beschaffungen anhand konkreter Problemstellungen bei Überwachungsaufgaben – unter Einbindung der vorhandenen Fachkompetenz der SEO – erfolgte nicht. Dies bewirkte einen inhomogenen Ausrüstungsstand.

- 12.2** Das BMI konnte somit mit der technischen Entwicklung nicht Schritt halten; Teile des Internets und der Telekommunikation konnten nicht überwacht werden. Der RH empfahl daher dem BMI, in der SEO ein Kompetenzzentrum für Observationstechnik einzurichten. Dadurch könnte vor allem für ressortweite Projekte sowie für Beschaffungsvorgänge der hohe Spezialisierungsgrad der SEO genutzt werden.

Weiters empfahl er, Anforderungsprofile mit dem Ziel des Zugangs zu externen Wissensquellen (bspw. Universitäten) zu formulieren.

- 12.3** *Das BMI teilte mit, dass eine noch intensivere Zusammenarbeit zwischen Bedarfsträgern und jenen Organisationseinheiten, denen die Budgetierung und Beschaffung von Observationstechnik obliegt, sicherstellen solle, dass benötigte technische Geräte zur Verfügung stehen.*
- 12.4** Der RH anerkannte die vom BMI erwähnte Intensivierung der Zusammenarbeit und des Informationsaustausches und regte dennoch an, den hohen Spezialisierungsgrad der SEO entsprechend für Beschaffungsvorgänge und ressortweite Projekte zu nutzen.

Hinsichtlich des Zugangs zu externen Wissensquellen hielt er die Formulierung derartiger Anforderungsprofile für erforderlich.

Rechtsschutzbeauftragter des BMJ

Allgemeines

- 13.1** Die besonderen Ermittlungsmaßnahmen ermöglichten tiefe Eingriffe in Grund- und Persönlichkeitsrechte. Da der Eingriff zum Zeitpunkt der Durchführung der Ermittlungsmaßnahme für den Betroffenen nicht erkennbar war, schuf der Gesetzgeber zur Wahrung der Rechte von Betroffenen einen Rechtsschutzbeauftragten.

Ein besonderes Auswahlverfahren, die Forderung spezieller Qualifikationen sowie eine – im Gegensatz zu den Rechtsschutzbeauftragten des BMI und BMLV – einfachgesetzlich verankerte Unabhängigkeit und Weisungsfreiheit stellten die ordnungsgemäße Aufgabenerfüllung des Rechtsschutzbeauftragten sicher.

Aufgaben des Rechtsschutzbeauftragten

13.2 Die Einrichtung und Ausgestaltung der Funktion des Rechtsschutzbeauftragten zeigte einerseits grundsätzlich das Bewusstsein des Gesetzgebers für den Grundrechtsschutz und trug andererseits der hohen Eingriffstiefe der besonderen Ermittlungsmaßnahmen Rechnung.

14.1 Dem Rechtsschutzbeauftragten als unabhängige und objektive Verfahrenspartei oblag die Prüfung sowie Kontrolle der Anordnung und Durchführung eines großen Späh- und Lauschangriffes sowie eines automationsunterstützten Datenabgleichs (Rasterfahndung). Bei Telekommunikationsüberwachungen erstreckten sich seine Befugnisse auf den engen Kreis der Berufsgeheimnisträger. Darüber hinaus war für diese Personengruppen seine Ermächtigung zur Durchführung großer und kleiner Späh- und Lauschangriffe erforderlich.

Die Durchführungskontrolle umfasste die Akteneinsicht bei Sicherheitsbehörden, Staatsanwaltschaften und Gerichten, die darüber hinaus auf Verlangen Auskünfte zu erteilen hatten. Gleichzeitig stellte der Rechtsschutzbeauftragte sicher, dass die Maßnahmen den Eingriffsvoraussetzungen – z.B. Bestehen des Tatverdachts, Verhältnismäßigkeit, Subsidiarität – fortwährend entsprachen.

Nach Beendigung einer Überwachung war dem Rechtsschutzbeauftragten der Bericht der Sicherheitsbehörden zu übermitteln. Ferner konnte der Rechtsschutzbeauftragte die Vernichtung bestimmter Bilder oder Aufzeichnungen beantragen.

Der RH stellte bei stichprobenartiger Überprüfung von großen Späh- und Lauschangriffen fest, dass der Rechtsschutzbeauftragte bereits in einem sehr frühen Stadium – nämlich bei Beantragung der Maßnahmen bei Gericht – von der SEO umfassend informiert wurde. Zudem führte er während laufender Maßnahmen zahlreiche, unangemeldete Kontrollen bei der SEO durch.

14.2 Der RH hielt fest, dass der Rechtsschutzbeauftragte seinen umfangreichen Überprüfungs- und Kontrollbefugnissen nachkam und damit die Rechte Betroffener wahrte.

Der RH empfahl dem BMJ, eine legislative Initiative zur Ausweitung der Befugnisse des Rechtsschutzbeauftragten auch auf länger dauernde Maßnahmen zur Telekommunikationsüberwachung – vor allem angesichts ihrer großen Streuwirkung – zu überlegen. Dadurch könnten auch die vom RH aufgezeigten Mängel hinsichtlich der Übermittlung von Anordnungsbeschlüssen (siehe dazu auch TZ 19) künftig vermieden werden.

14.3 Das BMJ teilte in seiner Stellungnahme mit, dass eine Erweiterung der Kontrollbefugnisse seines Rechtsschutzbeauftragten entweder dessen Überlastung oder eine personelle Ausweitung bedeuten würde. Es erwarte, den aufgezeigten Mangel (Anmerkung: hinsichtlich Übermittlung von Anordnungsbeschlüssen) durch konventionelle Kontrolle der staatsanwaltschaftlichen Praxis vermeiden zu können.

Optische Überwachung

Allgemeines

15.1 Als weitere besondere Ermittlungsmaßnahme sah die StPO zwei Fälle der optischen Überwachung (Videofalle) vor, in denen nicht öffentliches Verhalten von Personen auf Basis gerichtlicher Beschlüsse aufgezeichnet werden durfte.

Außerhalb von Wohnungen war die optische Überwachung zur Aufklärung jeglicher strafbaren Handlung zulässig. Innerhalb von Wohnungen oder sonstigen zum Hauswesen gehörigen Räumlichkeiten lagen notwendige Überwachungsvoraussetzungen in der ausdrücklichen Zustimmung des Inhabers. Eine weitere Voraussetzung bildete der Umstand der ohne die Maßnahme wesentlich erschwerten oder aussichtslosen Aufklärung einer strafbaren Handlung, die mit mehr als einem Jahr Freiheitsstrafe bedroht ist.

Seit 2001 wurde folgende Anzahl von Videofallen gerichtlich angeordnet:

	2001	2002	2003	2004	2005	2006
	Anzahl					
Videofallen gemäß § 149d Abs. 2 Z 1 und 2 StPO	81	77	79	80	75	56

Quelle: Sicherheitsberichte

Demgegenüber erlaubte auch das Sicherheitspolizeigesetz die Bildaufzeichnung öffentlichen Verhaltens, allerdings nur zur Abwehr gefährlicher Angriffe, krimineller Verbindungen und zur erweiterten Gefahrenforschung.

Die polizeitaktische Umsetzung von Videofallen nach der StPO und dem Sicherheitspolizeigesetz erfolgte dezentral durch Assistenzbereiche aller neun Landeskriminalämter und des BMI. Diese Bereiche führten die Überwachungen in Kooperation mit den fallführenden Ermittlungsgruppen der Landeskriminalämter und des Bundeskriminalamtes durch.

Basierend auf der Auswertung eines Fragebogens untersuchte der RH den Ausrüstungsstand dieser Assistenzbereiche. In einigen Landeskriminalämtern stand ausreichend Überwachungstechnik zur Verfügung. In anderen bestand – auch nach eigenen Angaben – Verbesserungsbedarf, weil wesentliche Ausrüstungsgegenstände fehlten oder erneuerungsbedürftig waren.

- 15.2** Aus Sicht des RH stellte die dezentrale Wahrnehmung optischer Überwachungen (Videofallen) die unbedingt erforderliche Nähe sowie Kooperation zwischen allen an der Umsetzung beteiligten Fachbereichen sicher. Als Ergebnis seiner Auswertung beurteilte der RH den Ausrüstungsstand nachgeordneter Dienststellen des BMI in diesem Bereich als inhomogen und verbesserungsbedürftig.

Der RH empfahl daher dem BMI, den Ausrüstungsstand sämtlicher Dienststellen für optische Überwachungsmaßnahmen zu evaluieren, in Zusammenarbeit mit der SEO (siehe dazu auch TZ 7) den Ausrüstungsbedarf zu erheben und auf dieser Grundlage ein nachhaltiges Beschaffungsprogramm zu erarbeiten.

- 15.3** *Laut Stellungnahme des BMI seien entsprechende Optimierungs- und Anschaffungsprogramme bereits in Ausarbeitung.*

IT-Unterstützung zur
Auswertung

16.1 Die Auswertung analoger Videoaufzeichnungen gestaltete sich zeitintensiv, weil die Ermittler dazu sämtliche Videoaufzeichnungen durchzusehen hatten.

Im BMI liefen Vorarbeiten zu einem Projekt zur IT-unterstützten Auswertung digitaler Videoaufzeichnungen. Der Einsatz dieser Technik sollte wesentlich verkürzte Auswertungszeiten und dadurch einen geringeren Personaleinsatz ermöglichen. Aufgrund anderer Prioritäten verwarf das BMI dieses Projekt jedoch Mitte des Jahres 2007.

16.2 Der RH teilte die Einschätzung, dass die IT-unterstützte Auswertung digitaler Videoaufzeichnungen Potenzial für Ressourceneinsparungen bietet. Er empfahl daher dem BMI, den Nichteinsatz von IT zu Auswertungszwecken auf Basis einer Wirtschaftlichkeitsberechnung zu überdenken.

16.3 *Laut Stellungnahme des BMI sei der Umstieg auf digitale Aufnahme- und Auswertungsgeräte sinnvoll und würde sukzessive in den nächsten Jahren durchgeführt werden.*

Überwachung einer Telekommunikation

Zulässigkeit

17.1 Nach der bis 31. Dezember 2007 geltenden Fassung der StPO umfasste die „Überwachung einer Telekommunikation“ die Feststellung von Standort-, Verkehrs- und Inhaltsdaten. Überwachungsmaßnahmen waren im Wesentlichen zur Aufklärung von vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlungen zulässig.

Die mit 1. Jänner 2008 in Kraft getretene Fassung der StPO unterscheidet zwischen der „Auskunft über Daten einer Nachrichtenübermittlung“ (Verkehrs-, Zugangs- und Standortdaten) und der „Überwachung von Nachrichten“ (Inhaltsdaten). Die Zulässigkeit wurde auf die Aufklärung oder Verhinderung von im Rahmen krimineller oder terroristischer Vereinigungen begangenen oder geplanten strafbaren Handlungen erweitert.

Eine Novelle des Telekommunikationsgesetzes 2003, welche – in Umsetzung einer EU-Richtlinie – die Verpflichtung der Anbieter und Betreiber öffentlicher Kommunikationsnetze zur Speicherung relevanter Daten für einen Zeitraum von sechs Monaten vorsah, lag erst im Entwurf vor. Die Bereiche Internet und E-Mail waren darin noch nicht einbezogen.

Überwachung einer Telekommunikation

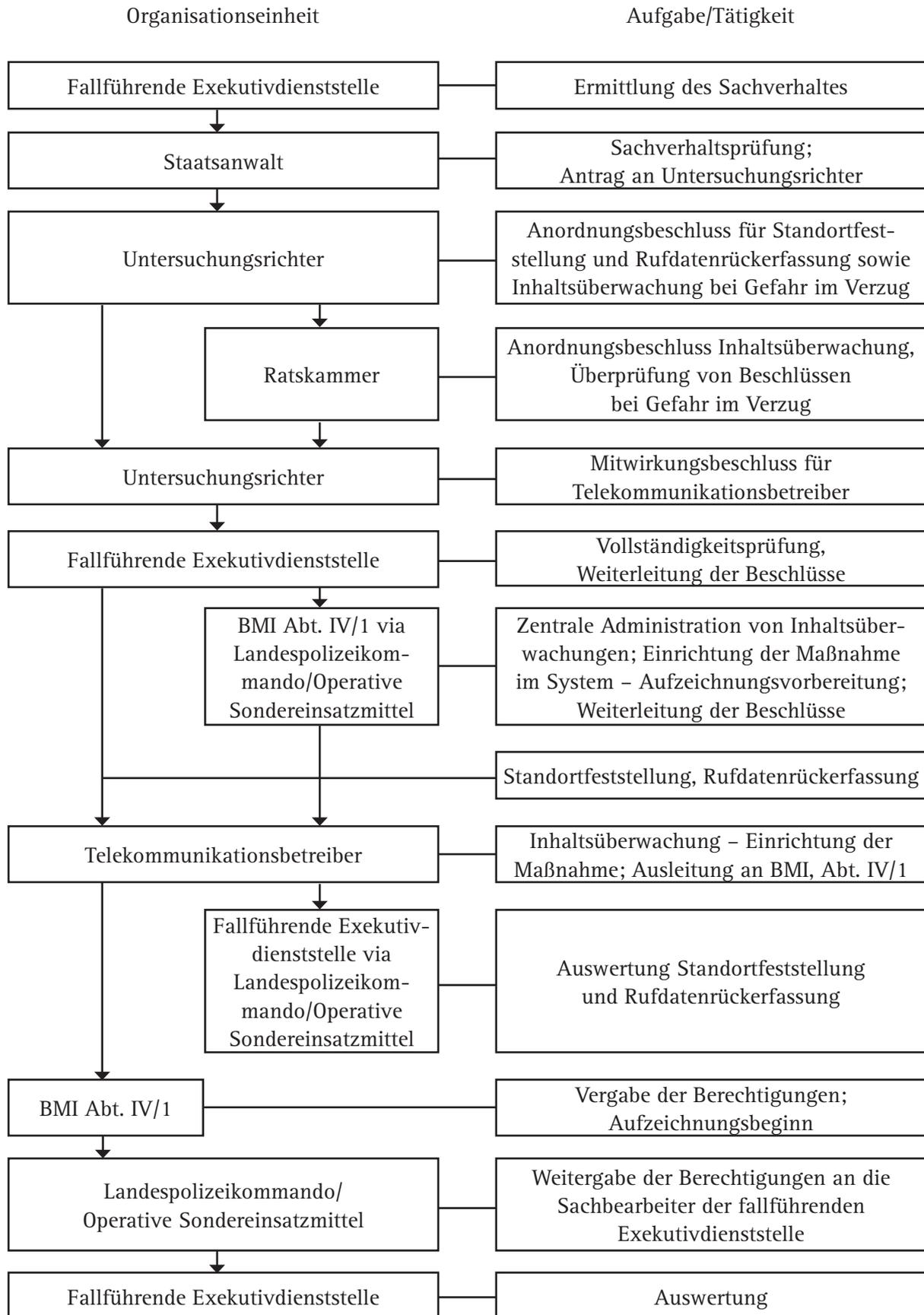
17.2 Der RH hielt die Überwachung der Telekommunikation für die wirksame Kriminalitätsbekämpfung in bestimmten Bereichen (insbesondere Suchtgift, organisierte Kriminalität) für wesentlich.

Die österreichische Gesetzgebung formuliert die Zulässigkeit von Überwachungsmaßnahmen allgemein und benennt keine konkreten, taxativen Straftatbestände wie bspw. die deutsche StPO. Allerdings ist die Erforderlichkeit und Verhältnismäßigkeit der Anwendung jeweils im Rahmen der Anordnung¹⁾ zu prüfen.

¹⁾ bis 31. Dezember 2007 durch den Untersuchungsrichter bzw. die Ratskammer, ab 1. Jänner 2008 durch den Staatsanwalt mit gerichtlicher Bewilligung

Ablauforganisation

18.1 Folgende Grafik zeigt den organisatorischen Ablauf von Telekommunikationsüberwachungsmaßnahmen zur Zeit der Gebarungüberprüfung:



Überwachung einer Telekommunikation

Der Grafik ist zu entnehmen, dass Gerichtsbeschlüsse für sämtliche Inhaltsüberwachungen zwar dezentral von den fallführenden Exekutivdienststellen erwirkt, jedoch (seit 1. Februar 2007) vom BMI zentral administriert wurden. Die zuständige Organisationseinheit des BMI trat an die Telekommunikationsbetreiber heran und übermittelte diesen die betreffenden Gerichtsbeschlüsse.

Das BMI zeichnete die von den Betreibern übermittelten Gesprächsinhalte auf einem zentralen Server zu Dokumentations- und Archivierungszwecken auf. Gleichzeitig stellte es diese Audiodaten vorher definierten Verantwortlichen der fallführenden Exekutivdienststelle auf dezentralen Auswertungseinheiten zur Verfügung. Diese Verantwortlichen übertrugen die derart übermittelten Gesprächsinhalte für das beauftragende Gericht in Bild- oder Schriftform.

Lag hingegen ein Beschluss auf Übermittlung von Verbindungs- und Standortdaten vor, erfolgte die Kommunikation zwischen fallführenden Exekutivdienststellen und Telekommunikationsbetreibern auf direktem Weg. Die Betreiber übermittelten sodann die beauftragten Daten direkt an die Ermittler dieser Dienststellen.

Bei den bisher in geringer Anzahl durchgeführten Internetüberwachungen erwirkten fallführende Dienststellen den gerichtlichen Beschluss, während die operative Durchführung der Maßnahmen gemeinsam mit der Zentralstelle erfolgte.

- 18.2** Aus Sicht des RH war die Vielzahl der an den Überwachungsmaßnahmen beteiligten Organisationseinheiten erforderlich. Die komplexen Informationswege bewirkten darüber hinaus eine wechselseitige Kontrolle und verringerten dadurch die Gefahr von Überwachungsmaßnahmen gegenüber Unbeteiligten.

Weiters stellte der RH fest, dass die in der Zentralstelle vorgenommene Konzentration von Inhaltsüberwachungen zur einheitlichen Abwicklung, Dokumentation und Archivierung von Inhaltsüberwachungsmaßnahmen führte.

Gerichtsbeschlüsse für Inhaltsüberwachungsmaßnahmen

19.1 Zur Zeit der Gebarungsüberprüfung sah die StPO vor, dass neben dem Beschluss auf Anordnung einer Überwachungsmaßnahme ein weiterer Mitwirkungsbeschluss für Telekommunikationsbetreiber zu fassen war.

Dieser Mitwirkungsbeschluss für Betreiber hatte lediglich den Namen des Inhabers des Teilnehmeranschlusses, dessen Bezeichnung sowie den Zeitpunkt des Beginns und der Beendigung der Überwachung zu enthalten. Er war darüber hinaus mit einer Geheimhaltungsklausel zu versehen.

Mitwirkungsbeschlüsse hatten somit keinesfalls – im Gegensatz zu den umfassenderen Anordnungsbeschlüssen¹⁾ – folgende Daten zu enthalten:

- den Namen des Beschuldigten, die Tat, deren er verdächtig war und ihre gesetzliche Bezeichnung,
- die Tatsachen, aus denen sich der Tatverdacht ergab.

¹⁾ Der für Verbindungs- und Standortdaten vom Untersuchungsrichter, für Inhaltsdaten (außer bei Gefahr im Verzug) von der Ratskammer zu fassende Anordnungsbeschluss hatte folgende Daten zu enthalten:

1. den Namen des Beschuldigten, die Tat, deren er verdächtig war und ihre gesetzliche Bezeichnung,
2. den Namen des Inhabers des Teilnehmeranschlusses und dessen Bezeichnung,
3. den Zeitpunkt des Beginns und der Beendigung der Überwachung,
4. die Tatsachen, aus denen sich die Erforderlichkeit und Verhältnismäßigkeit der Überwachung ergab und
5. die Tatsachen, aus denen sich der Tatverdacht ergab.

19.2 Der RH stellte bei seiner Stichprobenprüfung von Inhaltsüberwachungsbeschlüssen fest, dass Gerichte in rd. 90 % der Fälle gesetzwidrig Anordnungs- anstelle von Mitwirkungsbeschlüssen übermittelten, obwohl ein Erlass des BMJ auf die gegenteilige Vorgangsweise hinwies. Diese Vorgangsweise war geeignet, die Strafverfolgung zu erschweren oder zu verhindern, zumal diese Überwachungsmaßnahmen auch in sehr frühen Ermittlungsstadien beschlossen wurden.

Die gesetzwidrigen Handlungen der Gerichte führten auch dazu, dass Mitarbeiter der Telekommunikationsbetreiber Kenntnis von sensiblen Daten erlangten, die nicht für sie bestimmt waren. In mehreren Fällen erfolgte die Preisgabe von Vertrauenspersonen, für die besondere Geheimhaltungs- und Sicherheitsvorkehrungen bestanden. In einem anderen Fall ermöglichte der Wortlaut des Anordnungsbeschlusses Rückschlüsse auf die Person eines verdeckten Ermittlers, zu deren Sicherheit noch strengere Vorschriften bestanden.

Die Hinweise auf den Einsatz eines verdeckten Ermittlers sowie auf Vertrauenspersonen waren aus Sicht des RH geeignet, deren körperliche Integrität und Sicherheit zu gefährden.

Durch die Übermittlung der Anordnungsbeschlüsse wurden darüber hinaus die schutzwürdigen Geheimhaltungsinteressen sämtlicher in diesen Beschlüssen genannter Personen und somit deren verfassungsmäßig gewährleistetes Grundrecht auf Datenschutz verletzt.

Wenngleich der RH anerkannte, dass das BMJ dieser Problematik mit einem entsprechenden Erlass Rechnung trug, hielt er jedoch weitere Schritte zur Abstellung dieses Missstandes für erforderlich.

Er empfahl daher dem BMJ, umgehend im Wege der Präsidenten der Landesgerichte auf eine gesetzmäßige Vorgangsweise – durch die ausschließliche Übermittlung von Mitwirkungsbeschlüssen an Telekommunikationsbetreiber – hinzuwirken und deren Einhaltung zu überwachen.

Der RH empfahl dem BMJ weiters, im Erlassweg dafür Sorge zu tragen, dass Mitwirkungsanordnungen der Staatsanwaltschaften künftig keine Daten enthalten, welche die Strafverfolgung erschweren oder verhindern könnten, und ferner für die Beachtung des Grundrechts auf Datenschutz zu sorgen (siehe dazu auch TZ 20).

19.3 *Laut Stellungnahme des BMJ habe es alle Staatsanwaltschaften im Wege der Oberstaatsanwaltschaften durch Erlass nachdrücklich auf die Notwendigkeit einer gesonderten Anordnung hingewiesen und allen Rechtsanwendern entsprechende Formulare über das Intranet zur Verfügung gestellt.*

Änderungen durch das Strafprozessreformgesetz

20.1 Im ab 1. Jänner 2008 neu gestalteten strafprozessualen Vorverfahren sind Telekommunikationsüberwachungsmaßnahmen ausnahmslos durch den Staatsanwalt – nach vorheriger gerichtlicher Bewilligung – anzuordnen.

Dieser hat den Telekommunikationsbetreibern ihre Mitwirkungsverpflichtung mittels gesonderter Anordnung aufzutragen. Die Anordnung hat die gerichtliche Bewilligung sowie den Umfang der Mitwirkungsverpflichtung und eine Geheimhaltungsklausel zu enthalten. Eine detaillierte Festlegung des Inhaltes dieses Mitwirkungsbeschlusses besteht nach der neuen Rechtslage hingegen nicht mehr.

20.2 Aus Sicht des RH ist die Konzentration des Ermittlungsverfahrens bei der Staatsanwaltschaft geeignet, das Verfahren vom Antrag einer Telekommunikationsüberwachungsmaßnahme bis zu deren faktischen Umsetzung zu beschleunigen. Überdies führt die Nähe des Staatsanwaltes zu den ermittelnden Exekutivdienststellen zu einer Verkürzung der Informationswege.

Der Rechtsschutz wird dadurch nicht geschmälert, weil sowohl gegen die gerichtliche Bewilligung als auch gegen die staatsanwaltschaftliche Anordnung Rechtsmittel ergriffen werden können.

Beginn und Beendigung von Überwachungsmaßnahmen

21.1 Alle Überwachungsmaßnahmen basierten ausnahmslos auf gerichtlicher Anordnung, hatten sofort zu beginnen und waren rund um die Uhr umzusetzen. Dies spiegelte sich auch in der Überwachungskostenverordnung wider, die entsprechende Aufschläge für Tätigkeiten außerhalb der Bürozeiten vorsah. Ebenso sah § 94 des Telekommunikationsgesetzes 2003 vor, dass die Telekommunikationsbetreiber an Überwachungsmaßnahmen im erforderlichen Ausmaß mitzuwirken hatten.

Im Zuge der Gebarungüberprüfung im BMI stellte der RH fest, dass kein Telekommunikationsbetreiber außerhalb der Bürozeiten mit Überwachungsmaßnahmen begonnen hatte. Dies führte bei Inhaltsüberwachungen dazu, dass alle bis zum verspäteten Beginn anfallenden Inhaltsdaten – vorwiegend Gesprächsinhalte aber auch Dateiinhalte – unwiederbringlich verloren waren.

In einigen Fällen wurde vom Gericht am Freitag die Beendigung einer Inhaltsüberwachung mit sofortiger Wirkung angeordnet, die tatsächliche Beendigung erfolgte jedoch erst am darauffolgenden Montag.

Überwachung einer Telekommunikation

21.2 Der RH stellte fest, dass die Telekommunikationsbetreiber ihre gesetzlich normierte Mitwirkungspflicht an Überwachungsmaßnahmen in unzureichendem Ausmaß erfüllten. Der dadurch verursachte Verlust von Inhaltsdaten war geeignet, die Strafverfolgung massiv zu beeinträchtigen. Die beschlusswidrige Fortführung mehrerer Inhaltsüberwachungen verletzte die Grund- und Freiheitsrechte der Betroffenen.

Der RH empfahl daher dem BMJ unter Beteiligung des BMI, durch Verhandlungen mit den Betreibern die sofortige Umsetzung von Überwachungsmaßnahmen sicherzustellen. Darüber hinaus empfahl er, auf eine detaillierte Regelung der Mitwirkungspflichten der Betreiber hinzuwirken.

21.3 *Das BMJ teilte in seiner Stellungnahme mit, dass es wiederholt auf die Sicherstellung einer permanenten Erreichbarkeit der Betreiber hingewirkt habe. Es werde künftig auf Missstände und mögliche Haftungsfragen (etwa bei Schäden durch verspätete Mitwirkung) hinweisen. Eine detaillierte Regelung der Mitwirkungsverpflichtungen der Betreiber strebe es derzeit nicht an.*

Statistische Erfassung und Berichterstattung

22.1 Bis zum Jahr 2003 erhoben die Staatsanwaltschaften detaillierte statistische Daten über die im jeweiligen Zuständigkeitsbereich beantragten bzw. rechtskräftig angeordneten Telefonüberwachungen. Auf dieser Grundlage veröffentlichte das BMJ ausgewählte Daten in komprimierter Form im jährlichen Sicherheitsbericht der Bundesregierung.

Anfang 2003 verfügte das BMJ, dass im Rahmen der Verfahrensautomation Justiz Telefonüberwachungen differenziert nach Verfahrensschritten in den – automationsunterstützt geführten – Geschäftsregistern der Staatsanwaltschaften bzw. der Gerichte zu erfassen sind.

Ab dem Berichtsjahr 2003 nutzte das BMJ die statistischen Auswertungen der Geschäftsregister als Grundlage für die Ermittlung bzw. Veröffentlichung von Daten zur Überwachung der Telekommunikation im Sicherheitsbericht. Aufgrund der geänderten Methodik und Struktur der Erfassung wich der Informationsgehalt der veröffentlichten Daten von jenem der Vorjahre grundlegend ab.

Mit der Einführung besonderer Ermittlungsmaßnahmen zur Bekämpfung organisierter Kriminalität wurde das BMJ gemäß § 10a Staatsanwaltschaftsgesetz verpflichtet, jährlich dem Nationalrat, dem Datenschutzrat und der Datenschutzkommission einen Gesamtbericht über den Einsatz dieser Maßnahmen zu erstatten. Die Berichtspflicht erstreckte sich dezidiert auch auf den vergleichbaren Bereich der Überwachung des Fernmeldeverkehrs.

- 22.2** Die jährlichen Gesamtberichte über den Einsatz besonderer Ermittlungsmaßnahmen enthielten keine Daten betreffend die Überwachung der Telekommunikation. Auch die im jeweiligen Sicherheitsbericht veröffentlichten Informationen entsprachen nicht den Vorgaben des § 10a Staatsanwaltschaftsgesetz. Das BMJ erfüllte seinen gesetzlichen Auftrag somit nicht ausreichend.

Der RH verkannte nicht, dass die gesetzlich festgelegten Berichtspflichten nur mit erheblichem Aufwand vollinhaltlich erfüllbar sind. Er erachtete allerdings ein Mindestmaß an Informationsgehalt für erforderlich, um eine Beurteilung von Effizienz und Verhältnismäßigkeit sowie eine effektive parlamentarische und datenschutzrechtliche Evaluation der Maßnahmen zur Überwachung der Telekommunikation zu ermöglichen. Die relevanten Daten sollten automationsunterstützt erfasst werden.

Der RH empfahl dem BMJ weiters, eine Initiative zur Änderung des Staatsanwaltschaftsgesetzes zu setzen, um die gesetzlichen Informationspflichten betreffend die Überwachung einer Telekommunikation so zu gestalten, dass diese unter vertretbarem Aufwand auch vollinhaltlich erfüllbar sind.

- 22.3** *Gemäß Stellungnahme des BMJ könne es der Empfehlung hinsichtlich der Änderung des Staatsanwaltschaftsgesetzes folgen. Einer besonderen Berichtspflicht über Anordnungen zur Auskunftserteilung über Daten einer Nachrichtenübermittlung sowie auf Überwachung von Nachrichten nach § 13 Abs. 2 und 3 StPO bedürfe es nicht mehr, weil statistische Aufbereitungen durch Auswertung der entsprechenden Registereintragungen möglich seien. Durch isolierte Einsichtnahme in das staatsanwaltschaftliche Register sei ein detaillierter Überblick über Verfahren mit diesen Ermittlungsmaßnahmen und über die Anzahl der einzelnen Maßnahmen möglich.*

Überwachung einer Telekommunikation

22.4 Mit der durch das Strafprozessreformbegleitgesetz II, BGBl. I Nr. 112/2007 vom 28. Dezember 2007, erfolgten Änderung des Staatsanwaltschaftsgesetzes wurde die Berichtspflicht für Überwachungsmaßnahmen im Bereich der Nachrichtenübermittlung zur Gänze aufgehoben. Der RH verblieb allerdings bei seiner Ansicht, dass – im Hinblick auf die effektive parlamentarische und datenschutzrechtliche Evaluation – ein Mindestmaß an Information sichergestellt werden sollte.

Datenqualität

23.1 Bei Einführung der Datenerfassung betreffend Telefonüberwachungen in der Verfahrensautomation Justiz traf das BMJ keine Regelung, in welchen Registern die jeweiligen Maßnahmen (Anträge bzw. Bewilligungen) einzutragen sind.

Im Februar 2006 stellte das BMJ klar, dass Verfahrensschritte für Telefonüberwachungen nur mehr vom Gericht zu erfassen sind und somit eine Eintragung in den Registern der Staatsanwaltschaften zu unterbleiben habe.

23.2 Die Bundesrechenzentrum Gesellschaft mit beschränkter Haftung stellte dem RH – in Absprache mit dem BMJ – ausgewählte Daten hinsichtlich sämtlicher – in den Geschäftsregistern der Verfahrensautomation Justiz – automationsunterstützt erfassten Maßnahmen zur Überwachung einer Telekommunikation der Jahre 2005 und 2006 in einer elektronischen Datei zur Verfügung. Auf Grundlage deren Auswertung und stichprobenmäßiger Überprüfungen stellte der RH fest, dass die Vorgehensweise bei der Erfassung der Verfahrensschritte bei den Staatsanwaltschaften und Gerichten – auch noch nach den erfolgten Klarstellungen durch das BMJ – unterschiedlich war.

Mängel betrafen insbesondere Doppelerfassungen in den Geschäftsregistern der Staatsanwaltschaften und der Gerichte bzw. der Ratskammern sowie in der Erfassung bloßer Anregungen der Sicherheitsbehörden.

Konkrete Folgen waren

- die Ausweisung überhöhter Fallzahlen sowohl bei Anträgen als auch bei Bewilligungen,
- die Darstellung deutlich zu niedriger Prozentwerte für das Verhältnis Anträge zu Bewilligungen bei Standortfeststellungen und Feststellung von Vermittlungsdaten (laut Sicherheitsberichten jeweils rd. 60 % bis 70 %) sowie

- die Darstellung überhöhter Verhältniszahlen betreffend Inhaltsüberwachungen (laut Sicherheitsberichten 2005 und 2006 rd. 120 % bzw. 130 %).

Aufgrund seiner stichprobenartigen Überprüfungen hielt der RH eine tatsächliche Bewilligungsquote jeweils nahe 100 % für realistisch.

Nach Ansicht des RH war die differenzierte Erfassung der Überwachungsmaßnahmen in den Geschäftsregistern der Verfahrensautomation Justiz zu Dokumentationszwecken für die Strafverfahren zweckmäßig. Dieses System war allerdings infolge seiner Struktur für Zwecke statistischer Auswertungen nur bedingt geeignet und bot keine Möglichkeit zur Ermittlung detaillierter und aussagekräftiger Informationen zur Überwachung der Telekommunikation.

Der RH empfahl daher dem BMJ, ein für Zwecke statistischer Auswertungen geeignetes, IT-unterstütztes Instrumentarium zu erarbeiten und die Rahmenbedingungen für die Erstellung entsprechender Auswertungen zu schaffen.

Im Hinblick auf eine weitere Nutzung der Verfahrensautomation Justiz als Basis für statistische Auswertungen empfahl der RH dem BMJ, durch klare Vorgaben sowie Maßnahmen zur Qualitätssicherung die einheitliche (einmalige) und richtige Erfassung der Daten sicherzustellen sowie verstärkte Plausibilitätsprüfungen vorzunehmen.

23.3 *Laut Mitteilung des BMJ entspräche die Doppelerfassung der Maßnahmen zur Überwachung einer Telekommunikation in den Registern der Staatsanwaltschaften und der Gerichte (auch im Ratskammerregister) den Anordnungen des Verfahrensautomation Justiz-Online-Handbuchs und sei – wie auch andere Doppelerfassungen (z.B. Verfahrensausgang) – Ausdruck eines Dokumentationsbedürfnisses der jeweils eintragenden Organisationseinheiten. Divergenzen würden sich hier nicht gänzlich ausschließen lassen.*

23.4 Der RH hielt seine Empfehlungen – im Hinblick auf die Gewinnung aussagekräftiger statistischer Daten – vollinhaltlich aufrecht. Jedenfalls wäre die Richtigkeit der im Sicherheitsbericht veröffentlichten Zahlen zu gewährleisten.

Überwachung einer Telekommunikation

Kostenersatz für
Betreiber

Grundsätzliche Regelung

- 24.1** Für die Mitwirkung an der Überwachung einer Telekommunikation gebührte den Betreibern von Telekommunikationseinrichtungen gemäß dem Telekommunikationsgesetz ein angemessener Kostenersatz.

Die Höhe der angemessenen Kosten war mehrfach Gegenstand von Meinungsverschiedenheiten zwischen Gerichten und Betreibern. Nach der Judikatur waren die Leistungen nach dem durch den gerichtlichen Auftrag entstandenen „tatsächlichen Aufwand“ zu vergüten. Dabei hatten die Betreiber ihre Kosten detailliert aufgliedert geltend zu machen.

Mit dem am 20. August 2003 in Kraft getretenen Telekommunikationsgesetz 2003 (§ 94 Abs. 2) wurde vorgesehen, den angemessenen Kostenersatz durch Verordnung festzulegen. Auf dieser Grundlage erließ das BMJ – nach ausführlichen Verhandlungen mit dem Fachverband und den Betreibern – im Einvernehmen mit dem BMVIT, dem BMF, dem BMI und dem BMLV die Überwachungskostenverordnung, die mit 1. September 2004 in Kraft trat.

In der Verordnung wurden Tarife für Standardleistungen normiert. Diese umfassten im Wesentlichen einmalige Beträge für die Einrichtung einer Überwachungsmaßnahme, zeitraumbezogene Beträge für Auswertungen sowie Kostenersätze für konkret bezeichnete Einzelleistungen.

- 24.2** Die Standardisierung der Kostenersätze bewirkte eine zweckmäßigere und wirtschaftlichere Vollziehung, weil damit eine detaillierte Einzelfallprüfung der Angemessenheit der verrechneten tatsächlichen Kosten durch die Gerichte nicht mehr erforderlich war. Im Endergebnis lagen die Kostenersätze in der Regel auch niedriger als vor Anwendung der Überwachungskostenverordnung.

Die Überwachungskostenverordnung sieht eine Überprüfung der Kostenentwicklung in angemessenen Abständen vor. Der RH empfahl, in diesem Rahmen die Höhe einzelner Tarifsätze – unter Einbindung technischer Sachverständiger sowie Experten des BMI – im Hinblick auf die technischen Weiterentwicklungen sowie auf den mit der jeweiligen Maßnahme verbundenen tatsächlichen Aufwand auf ihre sachliche Rechtfertigung zu prüfen.

- 24.3** *Dem BMJ erschien es noch zu früh, mögliche technische Vorteile bei den einzelnen Arbeitsschritten den gestiegenen Personalkosten gegenüberzustellen oder auch nur inflationäre Bereinigungen vorzunehmen. Weiters verwies das BMJ auf die Verhandlungen zum Investitionskostensatz für die Betreiber.*

Verrechnung von Zuschlägen

- 25.1** Im Bereich der Überwachung einer Telekommunikation waren im Wesentlichen sechs Betreiber von Bedeutung.

Drei davon verrechneten bei Inhaltsüberwachungen für sämtliche im Überwachungszeitraum enthaltenen Samstage, Sonn- und Feiertage einen Zuschlag von 100 % auf den gemäß Überwachungskostenverordnung vorgesehenen Tarif (50 EUR anstatt 25 EUR pro Tag) und erhielten diesen auch vergütet, während die übrigen Betreiber durchgängig den Normalsatz anwendeten.

- 25.2** Der RH hielt fest, dass der Ersatz der Kosten gemäß Überwachungskostenverordnung der Höhe nach im Wesentlichen ordnungsgemäß und einheitlich vollzogen wurde. Es war allerdings nicht nachvollziehbar, dass von drei Betreibern generell ein Zuschlag für außerhalb der Normalzeit erbrachte Leistungen in Anspruch genommen wurde.

Der RH empfahl, die betreffende Regelung klarer zu formulieren und einheitlich zu vollziehen. In diesem Zusammenhang hielt der RH auch die Erbringung eines geeigneten Nachweises der Betreiber, dass die zugrunde gelegte Tätigkeit notwendigerweise außerhalb der regulären Arbeitszeit anfiel, für erforderlich.

- 25.3** *Laut Mitteilung des BMJ sollte eine präziserte Beschreibung des konkreten Kostenersatzes für Samstage, Sonn- und Feiertage in der Überwachungskostenverordnung vor einer Einigung über den Investitionskostensatz nicht angestrebt werden; die im Wesentlichen gut funktionierende Kostenpraxis zwischen Justiz und Betreibern sollte in diesem heiklen Zeitraum nicht gefährdet werden.*

- 25.4** Der RH konnte der Argumentation des BMJ bezüglich der Präzisierung der Überwachungskostenverordnung grundsätzlich folgen. Er hielt es allerdings für geboten, eine einheitliche Vollzugspraxis für alle Betreiber sicherzustellen.

Überwachung einer Telekommunikation

Abrechnung von
Überwachungs-
gebühren

- 26.1** Unmittelbar nach Abschluss der Überwachungsmaßnahmen stellten die Telekommunikationsbetreiber die von ihnen erbrachten Leistungen bei dem die Überwachung anordnenden Gericht in Rechnung. Der Untersuchungsrichter, der die Maßnahmen angeordnet hatte, prüfte die Rechnungen und bestimmte die Kosten mit einem eigenen Beschluss. Während die Betreiber ihre Rechnungen bei sonstigem Verfall binnen vier Wochen nach Abschluss der Maßnahmen zu legen hatten, bestand für die Gebührenbeschlüsse der Gerichte keine besondere Regelung.
- 26.2** Der RH stellte im Zuge einer Stichprobenprüfung fest, dass zwischen Rechnungslegung der Betreiber und Bestimmung der Kosten mittels Beschluss durch die Untersuchungsrichter oftmals ein Zeitraum von mehreren Monaten lag. In einem Fall des Landesgerichts Korneuburg betrug der Zeitraum sogar drei Jahre und betraf die Zahlung von 98.906,22 Euro. Zum Teil mussten die Betreiber die Bezahlung der offenen Kosten mehrmals einmahnen.

In komplexen Ermittlungsfällen waren verschiedene Überwachungsmaßnahmen gegen mehrere Beschuldigte oft bei sämtlichen Betreibern angeordnet worden. Dadurch war die Nachvollziehbarkeit – auch in Ermangelung eines zeitgemäßen Kanzlei- und Aktensystems – erschwert.

Aus Sicht des RH fiel die zeitaufwendige Prüfung der Betreiberrechnungen nicht in den Kernbereich richterlicher Aufgabenerfüllung. Der RH empfahl daher dem BMJ, für die Prüfung der Betreiberrechnungen in Landesgerichten spezialisierte Bedienstete einzusetzen, die ebenso die Kostenbeschlüsse vorzubereiten hätten.

Die vom RH festgestellte – in einigen Fällen um mehrere Jahre – verspätete Fassung von Gebührenbeschlüssen bewirkte, dass der vom BMJ sowohl im Jahresabschluss ausgewiesene, als auch der dem Nationalrat im Sicherheitsbericht angeführte jährliche Aufwand für Telekommunikationsmaßnahmen unrichtig wiedergegeben war.

Der RH empfahl daher, die zeitgerechte Bezahlung von Betreiberrechnungen sicherzustellen, um dadurch den tatsächlichen Aufwand für Überwachungsmaßnahmen periodenecht wiedergeben zu können.

- 26.3** *Das BMJ teilte in seiner Stellungnahme mit, dass verspätete Kostenbestimmungen dann erfolgen würden, wenn Akten nicht verfügbar wären oder mehrere Rechnungen in einem Beschluss zusammengefasst würden. Eine neue Regelung in der Durchführungsverordnung zum Staatsanwaltschaftsgesetz könne künftig Verzögerungen begegnen.*

Hinsichtlich der Empfehlung, für die Prüfung von Betreiberrechnungen spezialisierte Bedienstete einzusetzen, die auch Kostenbeschlüsse vorzubereiten hätten, wies das BMJ darauf hin, dass die bisherige Kostenbestimmung durch Richter aus rein faktischen Erwägungen sinnvoll sei. Seit 1. Jänner 2008 sei durch eine Änderung des Gebührenanspruchsgesetzes eine erhöhte Qualitätskontrolle bei der Kostenbestimmung gegeben.

Investitionskosten
der Betreiber

27.1 Das bis zum 19. August 2003 geltende Telekommunikationsgesetz (§ 89) hatte normiert, dass den Betreibern aus der Verpflichtung, die zur Überwachung des Fernmeldeverkehrs erforderlichen Einrichtungen bereitzustellen, kein Anspruch auf Ersatz der Investitionskosten zukomme. Der Verfassungsgerichtshof hob den Ausschluss der Kostenersatzpflicht als verfassungswidrig auf.

Die Verordnung des BMVIT über die Überwachung des Fernmeldeverkehrs (Überwachungsverordnung) regelt die Gestaltung der technischen Einrichtungen. Gemäß § 4 der Überwachungsverordnung hatten die Betreiber ab 1. Jänner 2005 für die Übergabe der Daten einer überwachten Telekommunikation an die Sicherheitsbehörden eine Schnittstelle nach ETSI-Standard¹⁾ bereitzustellen.

¹⁾ Europäischer Standard ES 201 671 Version 2.1.1 des European Telecommunications Standardisation Institute

In den Verhandlungen mit den Betreibern zur Überwachungskostenverordnung erzielte das BMJ die Vereinbarung, dass die bisher für die Sicherstellung der technischen Durchführbarkeit einer Überwachung generell getätigten Investitionen („Altinvestitionen“) im Wege der – im Einzelfall zu leistenden – Kostenersätze der Überwachungskostenverordnung als abgegolten gelten. Investitionskosten im Zusammenhang mit der Einrichtung einer ETSI-konformen Schnittstelle wurden dezidiert ausgenommen.

Im April 2007 urgierte der Fachverband der Telekommunikations- und Rundfunkunternehmen eine Entscheidung des BMJ in der Frage des Investitionskostenersatzes. Dabei argumentierte er nunmehr auch mit zusätzlich erforderlichen Investitionen aus der künftigen Verpflichtung zur Vorratsdatenspeicherung.

27.2 Ein Erkenntnis des Verfassungsgerichtshofes beurteilte den Ausschluss einer Kostenersatzpflicht für den Staat als nicht verhältnismäßig. Nach Auffassung des RH wäre allerdings auch eine angemessene Beteiligung der Betreiber zu prüfen.

Überwachung einer Telekommunikation

Der RH empfahl dem BMJ, im Rahmen von Verhandlungen mit Vertretern der Betreiber eine Übereinkunft in der Frage des Investitionskostenersatzes zu treffen.

Zur bloßen Abdeckung der Investitionen im Zusammenhang mit der Implementierung des ETSI-Standards hielt der RH Direktzahlungen für geeignet. Im Hinblick auf neuerliche Investitionen aufgrund von Änderungen in der Technologie bzw. des Auftretens potenzieller neuer Anbieter wäre allerdings in Hinkunft mit – vorerst nicht abschätzbaren – weiteren Forderungen von Betreibern zu rechnen. Es sollte daher eine Lösung getroffen werden, die derartige künftige Forderungen ausschließt. Der RH hielt in diesem Zusammenhang die Vereinbarung eines – maßvollen – Zuschlages auf die Tarife der Überwachungskostenverordnung für überlegenswert.

27.3 *Das BMJ verwies auf umfassende Bemühungen, eine Übereinkunft in der Frage des Investitionskostenersatzes zu treffen, die – wenn möglich – durch eine einmalige Direktzahlung künftige Forderungen ausschließen sollte. Die Verhandlungen mit den einzelnen Betreibern würden sich allerdings schwierig gestalten. Bislang sei kein Gutachter zu finden gewesen, der die Verhältnismäßigkeit bzw. Angemessenheit der Höhe der Kosten beurteilen würde. Zuletzt sei eine umfassende Stellungnahme des Verfassungsdienstes im Bundeskanzleramt eingeholt worden.*

Maßnahmen zur
Überwachung des
Internet

28.1 Überwachungsmaßnahmen im Internet galten als Überwachung der Telekommunikation.

Infolge des Fehlens entsprechender technischer Voraussetzungen war die Anzahl an Internetüberwachungsmaßnahmen zur Zeit der Gebärungsüberprüfung gering. Zudem führten mehrere Organisationseinheiten Internetüberwachungsmaßnahmen durch, so dass weder eine einheitliche Vorgangsweise noch die zentrale Koordinierung dieser Überwachungsmaßnahmen möglich war. Mangels konkreter Statistiken wäre die Erhebung der genauen Anzahl der Internetüberwachungen nur mit unvertretbarem Aufwand möglich gewesen.

In Ermangelung einer mit der Überwachungskostenverordnung korrespondierenden Vorschrift erfolgte die Abrechnung der Leistungen der Internetprovider uneinheitlich und einzelfallbezogen.

28.2 Der RH stellte fest, dass hinsichtlich der Einrichtung der technischen Voraussetzungen zur Internetüberwachung dringender Handlungsbedarf bestand, weil die Nutzung dieses Mediums in zunehmendem Maße nicht überwacht werden konnte. Trotz mehrjähriger Kenntnis dieses Missstandes reagierten weder die Einsatzabteilung, noch das Bundeskriminalamt, noch die Technikabteilung des BMI angemessen auf diesen Mangel.

Der RH empfahl daher dem BMI, durch die Einrichtung einer Arbeitsgruppe unverzüglich die technischen Möglichkeiten für die Überwachung des Internetverkehrs zu schaffen und diese Maßnahmen zentral auszurichten. Dem BMJ empfahl er die Erlassung einer entsprechenden Verordnung, die auch für die Abgeltung von Leistungen der Internetprovider fixe Kostensätze vorzusehen hat.

28.3 *Das BMI teilte in seiner Stellungnahme mit, dass die Möglichkeiten zur Überwachung des Internetverkehrs durch den Ankauf eines Gerätes für die SEO geschaffen worden seien. Seither führe die SEO diese Überwachung zentral im gesamten Bundesgebiet für alle Organisationseinheiten durch.*

28.4 Aus Sicht des RH kann angesichts der wachsenden Bedeutung der Internetkommunikation mit der Anschaffung lediglich eines Internetüberwachungsgeräts sowie den begrenzten Personalressourcen der SEO schon mittelfristig nicht das Auslangen gefunden werden. Unter zentraler Ausrichtung verstand der RH daher eine am Vorbild der Telefonüberwachungsmaßnahmen orientierte Lösung.

Sonstige Feststellungen

29 Sonstige Feststellungen und Empfehlungen des RH betrafen:

(1) Europäische Übermittlungsstandards für Telekommunikationsinhalte durch Telekommunikationsbetreiber wurden verzögert umgesetzt. Die letzten beiden Betreiber setzten diese Verpflichtung erst während der Gebarungsüberprüfung – also rd. zwei Jahre verspätet – um. Die dem BMI dadurch entstandenen zusätzlichen Kosten konnten mit vertretbarem Aufwand nicht quantifiziert werden.

(2) Für die SEO sollte ein Peilgerät für Mobiltelefone beschafft werden. Die bei der SEO und dem Bundesamt für Verfassungsschutz und Terrorismusbekämpfung vorhandenen zwei Geräte waren nur eingeschränkt einsetzbar und veraltet, jenes des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung zudem unzureichend ausgelastet.

(3) Nach Durchführung einer Wirtschaftlichkeitsberechnung sollte die SEO mit einem Gerät zur betreiberunabhängigen Standortfeststellung von Mobiltelefonen ausgestattet werden.

Schlussbemerkungen/Schlussempfehlungen

30 Zusammenfassend hob der RH folgende Empfehlungen hervor:

BMI

(1) Die Sondereinheit für Observation sollte direkt dem Generaldirektor für die öffentliche Sicherheit unterstellt werden. (TZ 4)

(2) Die Steuerung von Budgetmitteln zugunsten der Sondereinheit für Observation wäre künftig zu verbessern. (TZ 5)

(3) Die Wiederherstellung des ursprünglichen Personalstandes der Sondereinheit für Observation sollte geprüft werden. (TZ 6)

(4) Im Zuge der Einrichtung einer Kosten- und Leistungsrechnung wären entsprechende Vorkehrungen für Steuerungsmaßnahmen zu treffen. (TZ 6)

(5) Ein Anschaffungsprogramm für eine dem Stand der Technik entsprechende Ausrüstung der Sondereinheit für Observation wäre nach vorangehender Bedarfsfeststellung und budgetärer Vorsorge zu erarbeiten sowie ein Zeitplan für dessen Umsetzung festzulegen. (TZ 7)

(6) Die Durchführung kleiner Späh- und Lauschangriffe sollte bei der Sondereinheit für Observation konzentriert werden. (TZ 11)

(7) In der Sondereinheit für Observation sollte ein Kompetenzzentrum für Observationstechnik eingerichtet werden. (TZ 12)

(8) Es wären Anforderungsprofile mit dem Ziel des Zugangs zu externen Wissensquellen (bspw. Universitäten) zu formulieren. (TZ 12)

(9) Der Ausrüstungsstand sämtlicher Dienststellen für optische Überwachungsmaßnahmen wäre zu evaluieren, der Ausrüstungsbedarf zu erheben und ein nachhaltiges Beschaffungsprogramm zu erarbeiten. (TZ 15)

BMJ

(10) Basierend auf einer Wirtschaftlichkeitsberechnung sollte der Nichteinsatz von IT zur Auswertung von Ergebnissen optischer Überwachungsmaßnahmen überdacht werden. (TZ 16)

(11) Die technischen Möglichkeiten für die Überwachung des Internetverkehrs wären zu schaffen und diese Maßnahmen zentral auszurichten. (TZ 28)

(12) Ein für Zwecke statistischer Auswertungen geeignetes IT-unterstütztes Instrumentarium sollte erarbeitet und die Rahmenbedingungen für die Erstellung entsprechender Auswertungen sollten geschaffen werden. (TZ 23)

(13) Durch klare Vorgaben und Maßnahmen zur Qualitätssicherung wären die einheitliche (einmalige) und richtige Erfassung der Daten in der Verfahrensautomation Justiz sicherzustellen sowie verstärkte Plausibilitätsprüfungen vorzunehmen. (TZ 23)

(14) Durch Verhandlungen mit Betreibern sollte die sofortige Umsetzung von Überwachungsmaßnahmen sichergestellt sowie auf eine detaillierte Regelung der Mitwirkungspflichten der Betreiber hingewirkt werden. (TZ 21)

(15) Im Rahmen von Verhandlungen wäre eine Lösung für den Ersatz der Investitionskosten der Betreiber zu treffen. (TZ 27)

(16) Es wäre auf die ausschließliche Übermittlung von Mitwirkungsbeschlüssen an Telekommunikationsbetreiber hinzuwirken. (TZ 19)

(17) Bei der Neueinführung weiterer Ermittlungsmaßnahmen wäre – vor allem hinsichtlich der zeitlich befristeten Geltung und des besonderen Rechtsschutzsystems – in der bisherigen Weise vorzugehen. (TZ 3)

(18) Für die Einhaltung der Geheimhaltungsvorschriften durch Gerichte wäre verstärkt zu sorgen. (TZ 10)

(19) Eine legislative Initiative zur Befugnisausweitung des Rechtsschutzbeauftragten auf länger dauernde Telekommunikationsüberwachungen sollte überlegt werden. (TZ 14)

Schlussbemerkungen/ Schlussempfehlungen

(20) Im Erlassweg wäre dafür Sorge zu tragen, dass Mitwirkungsanordnungen der Staatsanwaltschaften künftig keine Daten enthalten, welche die Strafverfolgung erschweren oder verhindern könnten. Darüber hinaus wäre für die Beachtung des Grundrechts auf Datenschutz zu sorgen. (TZ 19, 20)

(21) Die für eine effektive parlamentarische und datenschutzrechtliche Evaluation der Maßnahmen zur Überwachung der Telekommunikation relevanten Daten sollten automationsunterstützt erfasst werden. (TZ 22)

(22) Eine Initiative zur Änderung des Staatsanwaltschaftsgesetzes sollte gesetzt werden, um die gesetzlichen Informationspflichten betreffend die Überwachung einer Telekommunikation so zu gestalten, dass diese unter vertretbarem Aufwand auch vollinhaltlich erfüllbar sind. (TZ 22)

(23) Hinsichtlich der Überwachungskostenverordnung sollte die Höhe einzelner Tarifsätze auf ihre sachliche Rechtfertigung geprüft werden. Weiters sollte die Regelung betreffend des Zuschlages für Leistungen außerhalb der Normalzeit eindeutig formuliert bzw. dessen einheitlicher Vollzug sichergestellt werden. (TZ 24, 25)

(24) Die Prüfung von Betreiberrechnungen in den Landesgerichten sollte auf spezialisierte Bedienstete konzentriert werden, die auch Kostenbeschlüsse vorzubereiten hätten. (TZ 26)

(25) Die zeitgerechte Bezahlung von Betreiberrechnungen wäre sicherzustellen, um dadurch den tatsächlichen Aufwand für Überwachungsmaßnahmen periodenecht wiedergeben zu können. (TZ 26)

(26) Für die Abgeltung von Leistungen der Internetprovider sollten im Rahmen einer Verordnung fixe Kostensätze vorgesehen werden. (TZ 28)