

**Bericht der Bundesregierung zu den Auswirkungen der nach Artikel 22 Abs. 2 des Terrorismusbekämpfungsgesetzes befristeten Änderungen des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes, des Artikel 10-Gesetzes, des Sicherheitsüberprüfungsgesetzes und des § 7 Abs. 2 des BKA-Gesetzes**

Inhaltsverzeichnis

	Seite
A. Anlass und Gegenstand der Evaluierung	2
B. Wesentliche Ergebnisse	3
C. Gesetzesfolgenauswertung	5
I. Nachrichtendienstgesetze	5
(Artikel 1 bis 3 Terrorismusbekämpfungsgesetz)	
1. Beobachtung völkerverständigungswidriger Bestrebungen	5
2. Betroffenenangaben bei Übermittlungersuchen	7
3. Auskünfte von Banken, Finanzdienstleistern und Finanzunternehmen	7
4. Auskünfte von Postdienstleistern	13
5. Auskünfte von Luftfahrtunternehmen	13
6. Auskünfte von Telekommunikations- und Teledienstleistern	15
7. Anordnungsverfahren zu den neuen Auskunftsbefugnissen und zum IMSI-Catcher	20
8. Löschung, Kennzeichnung, Übermittlungseinschränkung bei den neuen Auskunftsregelungen und beim IMSI-Catcher	22
9. Vertraulichkeitspflicht des Auskunftsgewährenden	25
10. Mitteilung an Auskunftsbetroffene	26
11. Erweiterung der technischen Wohnungsüberwachung (Eigensicherung)	27
12. IMSI-Catcher	28
13. Regellöschungsfrist beim Bundesamt für Verfassungsschutz	31
14. Spontanübermittlungen durch das Bundesamt für Migration und Flüchtlinge an das Bundesamt für Verfassungsschutz	33
15. Spontanübermittlungen durch Ausländerbehörden an Landesverfassungsschutzbehörden	39
16. Weiterübermittlung der Spontanübermittlungen des Bundesamtes für Migration und Flüchtlinge durch den Militärischen	41

Abschirmdienst und den Bundesnachrichtendienst	
17. Übermittlung zur Gewährleistung der Sicherheit von lebens- oder verteidigungswichtigen Einrichtungen	42
18. Übermittlung an Private durch den Militärischen Abschirmdienst	42
19. Mitteilung an Betroffene von einer Übermittlung an Private	43
20. Ausschluss der Übermittlungsregelungen für die Fälle „bei Erhebung“	43
II. Artikel 10-Gesetz – G 10 – (Artikel 4 Terrorismusbekämpfungsgesetz)	44
III. Sicherheitsüberprüfungsgesetz (Artikel 5 Terrorismusbekämpfungsgesetz)	45
IV. § 7 Abs. 2 BKAG (Artikel 10 Nr. 2 Terrorismusbekämpfungsgesetz)	51
D. Ausblick	53
Anhang: Statistische Auswertung und Kosten im BfV zu Abschnitt C.III	54

## **A. Anlass und Gegenstand der Evaluierung**

Die Anschläge vom 11. September 2001 markieren eine neue Dimension der terroristischen Bedrohung. Um dieser Bedrohung effektiv zu begegnen, hat der Gesetzgeber umgehend mit dem Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361, 3142) die gesetzlichen Instrumente fortentwickelt.

Bereits der Gesetzentwurf der Bundesregierung enthielt dabei eine Befristung der neuen nachrichtendienstlichen Befugnisse und Zuständigkeiten, um deren Evaluation sicherzustellen (Begründung zu Artikel 22 Abs. 2, BT-Drs. 14/7386, S. 69), also eine Überprüfung von Gesetzesfolgen, insbesondere der Praktikabilität und der Erreichung der gesetzgeberischen Ziele. Der Gesetzgeber hat diese Befristung auf § 7 Abs. 2 BKA-Gesetz erstreckt. Mit dem neuen Artikel 22 Abs. 3 hat er zudem das mit der Befristung bezweckte Evaluierungserfordernis verdeutlicht (Bericht des Innenausschusses, BT-Drs. 14/7864, S. 7f.). Zusätzlich hat der Gesetzgeber für einzelne der befristeten Regelungen in § 8 Abs. 10 BVerfSchG – auch in Verbindung mit § 9 Abs. 4 Satz 6 BVerfSchG, § 5 und § 10 Abs. 3 Satz 6 MAD-Gesetz sowie § 2 Abs. 1a Satz 4 und § 8 Abs. 3a Satz 6 BND-Gesetz – vorgesehen, dass das Parlamentarische Kontrollgremium den Deutschen Bundestag jährlich und nach drei Jahren zusammenfassend zum Zweck der Evaluierung unterrichtet. Das Kontrollgremium hat seine ersten beiden Berichte bereits vorgelegt (BT-Drs. 15/981, 15/3391).

Die Bundesregierung hat die Gesetzesfolgen der nach Artikel 22 Abs. 2 befristeten Regelungen ausgewertet und in diesem Bericht dargestellt, um eine angemessene Entscheidungsgrundlage dafür zu schaffen, inwieweit eine Entfristung sachgerecht ist und welche Modifikationen dabei womöglich vorgenommen werden sollten. Diese Entscheidungen sind in einem komplexen Beziehungsfeld von Freiheit und Sicherheit zu treffen.

- Effektive Terrorismusbekämpfung dient dem Schutz der Menschen und ihrer Freiheit. Sie ist eine freiheitssichernde Staatsaufgabe.
- Für die Befugnisse zur Terrorismusbekämpfung ist bei Eingriffen in Grundrechte der Bürger deren Eignung, Erforderlichkeit und Verhältnismäßigkeit zu gewährleisten.

Um zu einer fundierten Würdigung beizutragen, hat die Bundesregierung einer möglichst transparenten Gesetzesfolgenabschätzung hohes Gewicht beigemessen und sich deshalb dafür entschieden, möglichst weitgehend offen zu berichten. Gleichwohl bleiben bei der Darstellung nachrichtendienstlicher Tätigkeit Geheimschutzgesichtspunkte besonders zu berücksichtigen. Soweit aus Geheimschutzgründen keine konkreten Angaben gemacht werden konnten, ist versucht worden, wesentliche Informationen über abstrakte, aber realitätsnahe Darstellungen zu vermitteln.

Die Angaben des Berichts gelten jeweils zum Auswertungstichtag 31. Dezember 2004.

## **B. Wesentliche Ergebnisse**

Die festgestellten Gesetzesfolgen bestätigen ganz überwiegend die gesetzgeberischen Entscheidungen.

- Die spezielle Aufgabe des Bundesamtes für Verfassungsschutz (BfV) zur Sammlung und Auswertung von Informationen über völkerverständigungswidrige Bestrebungen (§ 3 Abs. 1 Nr. 4 BVerfSchG) hat zu einem verbesserten Informationsstand über extremistische Organisationen und deren effektiveren Bekämpfung beigetragen. So konnte das BfV das Verbotsverfahren gegen die antijüdische/antiisraelische „Hizb ut-Tahrir“ – ein Verein, der sich gegen den Gedanken der Völkerverständigung richtet (§ 3 Abs. 1 VereinsG) – effektiver unterstützen. Gegen die „Hizb ut-Tahrir“ hat das Bundesministerium des Innern am 15. Januar 2003 ein Betätigungsverbot erlassen.
- Die neuen Auskunftsbefugnisse der Dienste (§ 8 Abs. 5ff. BVerfSchG; § 10 Abs. 3 MADG; §§ 2 Abs. 1a, 8 Abs. 3a BNDG) haben relevante Informationen erbracht, beispielsweise bei der Aufklärung von Finanztransaktionen zur indirekten Unter-

stützung des islamistischen Terrorismus, bei der Aufdeckung von Netzwerkstrukturen und der Ermittlung von Kontaktpersonen. Dabei ist von diesen Befugnissen zurückhaltend und verantwortungsvoll Gebrauch gemacht worden.

- Ebenso verantwortungsvoll zurückhaltend ist der Einsatz des sogenannten IMSI-Catchers (§ 9 Abs. 4 BVerfSchG) erfolgt. Bei drei der vom BfV durchgeführten 19 Maßnahmen konnten unbekannte IMSI-Nummern ermittelt und auf Grundlage dieser Nummern die vorgesehene G 10-Maßnahme ermöglicht werden. In den übrigen Fällen wurde festgestellt, dass die Zielpersonen entweder dem BfV bereits bekannte oder keine Mobiltelefone in Gebrauch hatten (was ebenfalls für die operative Bearbeitung einer Zielperson wichtige Erkenntnisse sind).
- Die erweiterte Zusammenarbeit des Bundesamtes für Migration und Flüchtlinge (BAMF) mit dem BfV nach § 18 Abs. 1a BVerfSchG hat das Informationsaufkommen deutlich erhöht. Dabei konnte trotz offenerer Fassung der Spontanübermittlungspflicht die Verwertbarkeitsquote der übermittelten Erkenntnisse hoch gehalten werden.
- Die Verfahrensvereinfachung für die Fälle, in denen das Bundeskriminalamt (BKA) als Zentralstelle zur Ergänzung vorhandener Sachverhalte Auskünfte von anderen Stellen benötigt (§ 7 Abs. 2 BKAG), trägt zur Beschleunigung der Informationsbeschaffung und zur Verwaltungsentlastung bei.

In der Situation raschen Handlungsbedarfs nach den Anschlägen vom 11.9.2001 hat der Gesetzgeber insbesondere bei der Ausgestaltung von Verfahrenssicherungen risikosensibel entschieden und bis zur vorgesehenen Evaluierung vorsichtshalber eher aufwendigere als womöglich zu kurz greifende Lösungen gewählt. Die Evaluation bietet die Grundlage für eine Überprüfung dieser Entscheidungen.

- Dabei sollte geprüft werden, ob und ggf. wie bei den aufwendigen Verfahrenssicherungen Differenzierungen nach dem Eingriffsgehalt der verschiedenen neuen Auskunftsbefugnisse vorgenommen werden können, ohne dabei unangemessene Risiken für Rechte von Betroffenen hinzunehmen.

Im Übrigen hat die Praxis auch Prüfbedarf zu Ergänzungen aufgezeigt:

- Auskünfte zu Geldbewegungen und –anlagen nach § 8 Abs. 5 BVerfSchG setzen die Kenntnis der kontoführenden Stelle voraus. Hierzu sollte unter Berücksichtigung der laufenden verfassungsgerichtlichen Verfahren geprüft werden, ob und ggf. wie die zentralen Kontostammdatenauskünfte auch den Verfassungsschutzbehörden und dem BND erteilt werden können.

**C. Gesetzesfolgenauswertung**

**I. Nachrichtendienstgesetze**

**(Artikel 1 bis 3 Terrorismusbekämpfungsgesetz)**

**1. Beobachtung völkerverständigungswidriger Bestrebungen**

**a) Bundesamt für Verfassungsschutz**

Mit Artikel 1 Nr. 1 Terrorismusbekämpfungsgesetz haben die Verfassungsschutzbehörden durch die neue Regelung des § 3 Abs. 1 Nr. 4 BVerfSchG die Aufgabe erhalten, Bestrebungen im Geltungsbereich dieses Gesetzes zu beobachten, die gegen den Gedanken der Völkerverständigung (Artikel 9 Abs. 2 des Grundgesetzes), insbesondere gegen das friedliche Zusammenleben der Völker (Artikel 26 Abs. 1 des Grundgesetzes) gerichtet sind. Der Gesetzgeber hat solches Schüren von Hass als gefährlichen Nährboden auch für terroristische Gewalt angesehen (BT-Drs. 14/7386, S. 36, 38). Deshalb sollten die Verfassungsschutzbehörden auf klarer Rechtsgrundlage über solche Bestrebungen Informationen sammeln und auswerten.

**aa) Auswertung**

Informationsgewinnung

Das unmittelbare Ziel, Informationen über gefährliche Bestrebungen zu gewinnen, wurde erreicht. Beispielsweise sind im Bereich des Islamismus sechs Organisationen nach Inkrafttreten des Terrorismusbekämpfungsgesetzes gestützt auf § 3 Abs. 1 Nr. 4 BVerfSchG zu Beobachtungsobjekten des BfV geworden. Diese Organisationen verfügen zusammen über rund 800 Mitglieder bzw. Anhänger in Deutschland. Beispielsweise wurde die multinationale „Hizb ut-Tahrir al Islami“ (HuT) im Jahre 2002 aufgrund ihrer in islamistischen Positionen wurzelnden antijüdischen/antiisraelischen und generell antiwestlichen Agitation Beobachtungsobjekt und im Jahre 2004 eine islamistische Bildungseinrichtung. Auch im Bereich des sonstigen Ausländerextremismus ist die neue Aufgabenregelung zum Tragen gekommen, beispielsweise bei einer Organisation, die mit rassistischen Äußerungen in Erscheinung getreten war.

Auf der Grundlage der gewonnenen Informationen wurden zudem konkrete Bekämpfungsmaßnahmen möglich. Herauszuheben ist das vereinsrechtliche Betätigungsverbot gegenüber der HuT, das das Bundesministerium des Innern gem. § 3 Abs. 1 in Verbindung mit § 15 Abs. 1 Satz 2 und § 18 Satz 2 VereinsG mit Verfügung vom 15.01.2003 erlassen hat. Auch für die von den zuständigen Landesbehörden

vorgenommenen Vollzugs- und weiteren vereinsrechtlichen Ermittlungsmaßnahmen (z.B. Durchsuchungsmaßnahmen) wurde auf die Erkenntnisse des BfV aus der Beobachtung der Organisation zurückgegriffen.

### Gerichtliche Überprüfung

Bislang hat sich keine der - auch - aufgrund § 3 Abs. 1 Nr. 4 BVerfSchG beobachteten und im Verfassungsschutzbericht oder einer Publikation des BfV genannten Organisationen rechtlich gegen die Beobachtung gewendet.

### Kosten

Zu den finanziellen Auswirkungen speziell der neuen Aufgabennorm ist eine Aussage nicht möglich.

## **bb) Schlussfolgerungen**

Die praxisbewährte Regelung sollte unverändert beibehalten werden.

## **b) Militärischer Abschirmdienst**

Mit Artikel 2 Nr. 1 Terrorismusbekämpfungsgesetz hat der Militärische Abschirmdienst (MAD) durch den neuen § 1 Abs. 1 Satz 2 MAD-Gesetz die entsprechende Aufgabe für seinen Zuständigkeitsbereich erhalten.

## **aa) Auswertung**

### Informationsgewinnung

Das Ziel, Informationen über gefährliche Bestrebungen zu gewinnen, wurde erreicht. Nähere Angaben sind aus Geheimschutzgründen nicht möglich; die operative Bearbeitung ist zum Teil noch nicht abgeschlossen.

Auch die vom MAD gesammelten Informationen haben zudem bereits konkrete Maßnahmen ermöglicht, insbesondere die Entfernung von Extremisten aus der Bundeswehr und ihren Einrichtungen.

## Kosten

Eine Zuordnung von aufgewandten Kosten zu den im Rahmen der neuen Aufgabe getätigten Maßnahmen ist nicht möglich. Zusätzliches Personal ist wegen des mit der neuen Aufgabe nach § 1 Abs. 1 Satz 2 MADG verbundenen Aufgabenzuwachses im MAD nicht eingestellt worden. Allerdings sind drei Personen aus dem vorhandenen Personalbestand der MAD-Stellen in das MAD-Amt versetzt worden.

### **bb) Schlussfolgerungen**

Die praxisbewährte Regelung sollte unverändert beibehalten werden.

## **2. Betroffenenangaben bei Übermittlungersuchen**

Mit Artikel 1 Nr. 3 Buchstabe a Terrorismusbekämpfungsgesetz sind dem § 8 Abs. 1 BVerfSchG zwei Sätze angefügt worden, wonach ein Ersuchen des BfV um Übermittlung personenbezogener Daten nur diejenigen personenbezogenen Daten enthalten darf, die für die Erteilung der Auskunft unerlässlich sind; schutzwürdige Interessen des Betroffenen dürfen nur in unvermeidbarem Umfang beeinträchtigt werden. Damit sollte einer Forderung des Bundesbeauftragten für den Datenschutz Rechnung getragen und durch ausdrückliche Regelung klargestellt werden, dass solche Übermittlungen auch ohne Zustimmung des BMI (§ 19 Abs. 4 S. 2 BVerfSchG) zulässig sind, dabei aber auf das Unerlässliche beschränkt werden müssen.

Die bezweckten Klarstellungen wurden unmittelbar durch den Gesetzeswortlaut erreicht.

Die klaren Regelungen sollten unverändert beibehalten werden.

## **3. Auskünfte von Banken, Finanzdienstleistern und Finanzunternehmen**

### **a) Bundesamt für Verfassungsschutz**

Mit Artikel 1 Nr. 3 Buchstabe b Terrorismusbekämpfungsgesetz ist in § 8 BVerfSchG ein neuer Absatz 5 eingefügt worden. Das BfV darf danach im Einzelfall bei Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen unentgeltlich Auskünfte zu Konten, Konteninhabern und sonstigen Berechtigten sowie weiteren am Zahlungsverkehr Beteiligten und zu Geldbewegungen und Geldanlagen einholen,

wenn dies zur Erfüllung seiner Aufgaben nach § 3 Abs. 1 Nr. 2 bis 4 BVerfSchG<sup>1</sup> erforderlich ist und tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die in den Aufgabennormen genannten Schutzgüter vorliegen.

Die Regelung soll Auskünfte der Kreditinstitute gewährleisten, um Informationen über Geldströme und Kontobewegungen zur Feststellung von Tätern und Hintermännern zu gewinnen (BT-Drs. 14/7386, S. 36) und eine bessere Einschätzung von finanziellen Ressourcen und Gefährlichkeit vornehmen zu können (BT-Drs. 14/7386, S. 39).

## aa) Auswertung

### Informationsgewinnung

Die Befugnis wurde 29 Mal angewendet (davon 2 Verlängerungen, 2 Verlängerungen mit Erweiterung, 2 Erweiterungen und 1 Änderung):

Quartal	III/02	IV/02	I/03	II/03	III/03	IV/03	III/04	IV/04
Anordnungen	4	4	5	1	4	4	4	3

Es ist umstritten, ob das Gesetz eine Auskunftspflicht begründet (vgl. einerseits Gesetzesbegründung, BT-Drucksache 14/7386, allgemeine Begründung, S. 36; andererseits BfD, 19. TB. BT-Drs. 15/888, S. 110). Sanktionsmöglichkeiten im Falle der Auskunftsverweigerung sind jedenfalls nicht vorgesehen. Dies hat bislang zu keinen Problemen geführt. In keinem Fall wurde die Auskunftserteilung von den Instituten abgelehnt.

Ziel von Anträgen nach § 8 Abs. 5 BVerfSchG war es u.a., finanzielle Transaktionen „Arabischer Mujahedin“ aufzudecken, um finanzielle Unterstützungen für den von ihnen betriebenen gewaltsamen „Jihad“, insbesondere die Förderung terroristischer Anschläge, zu erkennen. Ein Antrag diene z.B. der Verifizierung der Annahme der indirekten finanziellen Unterstützung des islamistischen Terrorismus durch Überweisung von Geldbeträgen an eine oder mehrere arabische Non-Governmental Organizations (NGO).

---

<sup>1</sup> Dies sind:

- sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht (Nr. 2),
- Bestrebungen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden (Nr. 3) und
- Bestrebungen im Geltungsbereich des Gesetzes, die gegen den Gedanken der Völkerverständigung gerichtet sind (Nr. 4).



Auch wurden zu mehreren Spendenvereinen, die im Bundesgebiet in Moscheen und Islamischen Zentren Spendengelder sammeln, Auskünfte bei Kreditinstituten eingeholt. Die Anträge basierten auf der Annahme einer Einbindung dieser Organisationen in das Finanzierungsnetzwerk der Hamas. Im Rahmen der Auswertung der Unterlagen wurde festgestellt, dass Gelder sowohl direkt als auch indirekt über verschiedene Finanzierungsnetzwerke innerhalb Europas an Organisationen der Hamas im Nahen Osten geflossen sind. Ferner ergaben sich aus den Unterlagen neue Ermittlungsansätze, da festgestellt werden konnte, dass oftmals Personen, die an eine der betreffenden Organisation gespendet haben, auch als Spender für andere Vereine auftraten. Die gewonnenen Erkenntnisse waren insbesondere auch im Hinblick auf das Verbotverfahren gegen „Al Aqsa e.V.“ relevant; sie dienten u. a. der Vorbereitung von Exekutivmaßnahmen, die nach der Urteilsverkündung des Bundesverwaltungsgerichts zur Abweisung der Klage des „Al Aqsa e.V.“ am 3. Dezember 2004 eingeleitet wurden.

In einem Fall aus dem Bereich Spionageabwehr wurde festgestellt, dass der Betroffene neben dem überwachten Konto ein weiteres Bankkonto bei einem anderen Kreditinstitut unterhält. Weiter konnten anhand der Kontoauskunft Reisetätigkeiten festgestellt werden, die finanzielle Situation und Verbindungen zu Dritten wurden transparent. In einem weiteren Fall - in dem die Ermittlungen noch andauern – besteht der Verdacht, ein hauptamtlicher Angehöriger eines Nachrichtendienstes wickle Geldtransfers an islamistische Gruppierungen ab.

### Eingriff in Persönlichkeitsrechte

Die Auskunftersuchen bezogen sich auf insgesamt 33 Betroffene.

Beispielhaft für die Befugnisschwelle der „schwerwiegenden Gefahr“ sind Fälle von Geldersammlungen oder gezielten Geldtransfers, die terroristische Anschläge ermöglichen oder eine Gruppierung, die im Ausland auch gewalttätig/terroristisch tätig ist (z.B. Hamas), unterstützen sollen. Eine „schwerwiegende Gefahr“ könnte ferner im Falle einer Organisation gegeben sein, die mit militärischen Strukturen eine Drohkulisse gegenüber anderen Volksgruppen aufbaut. Im Hinblick auf proliferationsrelevante Sachverhalte besteht eine schwerwiegende Gefahr typischerweise darin, dass – aufgrund bestehender internationaler Verpflichtungen, die auch die Bundesrepublik Deutschland eingegangen ist – solche von deutschem Boden ausgehende Aktivitäten nachhaltig die auswärtigen Beziehungen, die politische Glaubwürdigkeit und das Ansehen der deutschen Außenpolitik schädigen. Im Bereich der Spionageabwehr wird das Vorliegen einer „schwerwiegenden Gefahr“ für das Schutzgut der Sicherheit der Bundesrepublik Deutschland regelmäßig bejaht, wenn tatsächliche Anhalts-

punkte dafür vorliegen, dass Firmen maßgeblich von einem fremden Nachrichtendienst gesteuert werden und diesem dadurch umfassende Einreise- und Geldbewegungsmöglichkeiten zur Verfügung stehen.

### Praktikabilität

Eine Anfrage setzt die Kenntnis voraus, bei welchem der ca. 3.000 Kreditinstitute in Deutschland der Betroffene ein Konto unterhält. Als Erkenntnisquellen können hier z.B. Quellenmeldungen, G 10-Maßnahmen, in Ausnahmefällen offen zugängliche Flugblätter oder Internetseiten oder die Auswertung von Asservaten dienen, nicht jedoch ein zentraler Abruf von Kontostammdaten. Dies bedeutet, dass die für die praktische Durchführung des § 8 Abs. 5 BVerfSchG erforderlichen Informationen eher zufällig anfallen. Verbleibende Kenntnisdefizite können die Normpraktikabilität beeinträchtigen. Es sind bereits wiederholt Fälle aufgetreten, in denen die Einholung einer Auskunft angezeigt gewesen wäre, mangels Kontoinformationen jedoch unterblieben ist.

Dies kann sich z.B. bei Geldbeschaffungsaktivitäten für ausländische extremistische Organisationen auswirken, wenn zwar Hinweise auf konkrete Personen, die in derartige Sammelaktivitäten eingebunden sein sollen, vorliegen, jedoch nicht auf eine Kontonummer oder eine konkrete Bank. So konnte z.B. in einem Fall dem Verdacht der indirekten Unterstützung des islamistischen Terrorismus durch Überweisung von Geldern an eine NGO nicht weiter nachgegangen werden. Auch ließen sich Hinweise auf Geldtransfers für Passfälschungen mangels ausreichender Kontoinformationen nicht durch ein Auskunftsverfahren nach § 8 Abs. 5 BVerfSchG verifizieren.

In anderen Regelungszusammenhängen – deren rechtliche Bewertung freilich nicht vollständig auf den hier vorliegenden Sachverhalt übertragen werden kann – hat der Gesetzgeber den Verfassungsschutzbehörden eine zentrale Abfrage von Bestandsdaten eingeräumt. So erhalten die Verfassungsschutzbehörden nach § 112 Abs. 2 Nr. 4 TKG zentral von der Regulierungsbehörde für Telekommunikation und Post Auskunft zu Rufnummern und Identifizierungsangaben zu Telekommunikationskunden.

### **bb) Schlussfolgerungen**

- Die Befugnis hat aufgabendienliche Erkenntnisse erbracht, ohne dass damit unangemessen breite Überwachungsfolgen verbunden waren. Sie sollte beibehalten werden.

- Ergänzend sollte unter Berücksichtigung der laufenden verfassungsgerichtlichen Verfahren geprüft werden, ob und ggf. wie die zentralen Kontostammdatenauskünfte auch den Verfassungsschutzbehörden erteilt werden können.

## b) Bundesnachrichtendienst

Mit Artikel 3 Nr. 1 Terrorismusbekämpfungsgesetz ist in § 2 BND-Gesetz ein neuer Absatz 1a eingefügt worden, wonach der Bundesnachrichtendienst (BND) im Einzelfall bei Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen unentgeltlich Auskünfte zu Konten, Konteninhabern und sonstigen Berechtigten sowie weiteren am Zahlungsverkehr Beteiligten und zu Geldbewegungen und Geldanlagen einholen darf, soweit dies im Rahmen seiner Aufgaben für die Sammlung von Informationen über bestimmte Gefahrenbereiche<sup>2</sup> erforderlich ist und tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die außen- und sicherheitspolitischen Belange der Bundesrepublik Deutschland vorliegen.

### Informationsgewinnung

Insgesamt wurden drei vom BND gestellte Anträge genehmigt (in den Quartalen III/02, I/03, II/03), wobei zehn Konten bei sechs unterschiedlichen Banken betroffen waren. Zwei Anträge betrafen ausschließlich den Gefahrenbereich des internationalen Terrorismus gemäß § 5 Abs. 1 Satz 3 Nr. 2 G 10, ein Antrag darüber hinaus den Gefahrenbereich der Geldwäsche gemäß § 5 Abs. 1 Satz 3 Nr. 6 G 10.

In keinem Fall ist die Auskunft verweigert worden.

Es wurden relevante Beiträge zur Aufklärung terroristischer Netzwerke erlangt. Hierzu gehören Erkenntnisse zu Geldtransfers aus dem Ausland über Zwischenkonten, Erkenntnisse zu Überweisungen von Zielgruppen untereinander und Hinweise auf die zur Verfügung stehenden Geldmittel und ihre Herkunft; ferner konnten Erkenntnisse zu weiteren verdächtigen Personen und Kontaktpersonen gewonnen

---

<sup>2</sup> Die in § 5 Abs. 1 Satz 3 Nr. 1 bis 4 und 6 G 10 genannten Gefahrenbereiche, nämlich die Gefahr

- eines bewaffneten Angriffs auf die Bundesrepublik Deutschland (Nr. 1),
- der Begehung internationaler terroristischer Anschläge mit unmittelbarem Bezug zur Bundesrepublik Deutschland (Nr. 2),
- der internationalen Verbreitung von Kriegswaffen im Sinne des Gesetzes über die Kontrolle von Kriegswaffen sowie des unerlaubten Außenwirtschaftsverkehrs mit Waren, Datenverarbeitungsprogrammen und Technologien in Fällen von erheblicher Bedeutung (Nr. 3),
- der unbefugten Verbringung von Betäubungsmitteln in nicht geringer Menge in die Bundesrepublik Deutschland (Nr. 4) und
- der international organisierten Geldwäsche in Fällen von erheblicher Bedeutung (Nr. 6).

werden. Die erteilten Auskünfte haben Vermutungen über die Zusammenarbeit bei der Terrorismusfinanzierung bestätigt.

### Eingriff in Persönlichkeitsrechte

Die Auskunftersuchen bezogen sich auf insgesamt sechs Personen.

Als eingriffsrechtfertigende „schwerwiegende Gefahr“ wurden drohende potenzielle terroristische Anschläge (auch bereits im Planungs- und Finanzierungsstadium) angesehen. Eine schwerwiegende Gefahr wurde jedenfalls dann bejaht, wenn aufgrund tatsächlicher Anhaltspunkte von einer grundsätzlichen Anschlagsbereitschaft der zu überprüfenden Betroffenen ausgegangen werden musste. Zu bedenken ist in einem solchen Zusammenhang ferner der mögliche Ansehens- und Vertrauensverlust Deutschlands, wenn nachrichtendienstlichen Hinweisen auf Finanzierung von Terroranschlägen oder vermutete Geldwäscheaktivitäten von großem Umfang nicht mit allen rechtlich zur Verfügung stehenden Mitteln nachgegangen wird.

### Praktikabilität

Hier gilt das bereits zum BfV Ausgeführte ebenso. In zwei Fällen existierten die Konten, zu denen die Auskünfte erbeten worden waren, bei den betreffenden Finanzunternehmen nicht bzw. nicht mehr. Da dem BND kein zentraler Abruf von Kontostammdaten zur Verfügung stand, waren in diesen Fällen keine weiterführenden Erkenntnisse durch rechtzeitige Anfrage beim richtigen Unternehmen zu gewinnen .

### **bb) Schlussfolgerungen**

- Der BND hat von der Befugnis in geringerem Umfang Gebrauch gemacht als das BfV, was angesichts der aufgabenspezifisch divergierenden Bedarfslage von Auslands- und Inlandsnachrichtendienst indes nicht überrascht. Die Befugnis hat dabei aufgabendienliche Erkenntnisse erbracht, indem aus der Auslandsaufklärung gewonnene einschlägige Erkenntnisse zu solchen Personen, die inländische Bankverbindungen unterhalten, weiter vertieft werden konnten. Unangemessen breite Überwachungsfolgen waren damit nicht verbunden. Die Befugnis sollte beibehalten werden.
- Ergänzend sollte ebenso wie zum BfV (vgl. bereits oben) unter Berücksichtigung der laufenden verfassungsgerichtlichen Verfahren geprüft werden, ob und ggf. wie die zentralen Kontostammdatenauskünfte auch dem BND erteilt werden können.

#### **4. Auskünfte von Postdienstleistern**

Mit Artikel 1 Nr. 3 Buchstabe b Terrorismusbekämpfungsgesetz ist in § 8 BVerfSchG auch ein neuer Absatz 6 eingefügt worden. Das BfV darf danach im Einzelfall zur Erfüllung seiner Aufgaben nach § 3 Abs. 1 Nr. 2 bis 4 BVerfSchG (vgl. oben Fn. 1) unter den Voraussetzungen des § 3 Abs. 1 G 10 (tatsächliche Anhaltspunkte, dass jemand bestimmte schwere Straftaten plant, begeht oder begangen hat) bei Personen und Unternehmen, die geschäftsmäßig Postdienstleistungen erbringen, sowie bei denjenigen, die an der Erbringung dieser Dienstleistungen mitwirken, unentgeltlich Auskünfte zu Namen, Anschriften, Postfächern und sonstigen Umständen des Postverkehrs einholen.

Die Regelung soll der Gewinnung von Informationen über Kommunikationswege zur Vorbereitung von G 10-Maßnahmen dienen. Hierzu sollen Auskünfte der Postdienstleister gewährleistet werden (BT-Drs. 14/7386, S. 39).

##### **a) Auswertung**

Bislang wurden keine Anträge auf Auskunftersuchen an Postdienstleister gem. § 8 Abs. 6 BVerfSchG gestellt.

##### **b) Schlussfolgerungen**

Die Befugnis hat sich in der geltenden Ausformung nicht bewährt, da wegen der Voraussetzungen des § 3 Abs. 1 G 10 kein praktischer Bedarf für isolierte Auskünfte nach § 8 Abs. 6 BVerfSchG aufgetreten ist und solcher Bedarf auch künftig absehbar nicht auftreten wird. Deshalb könnte erwogen werden, an dieser Regelung nicht festzuhalten.

#### **5. Auskünfte von Luftfahrtunternehmen**

Mit Artikel 1 Nr. 3 Buchstabe b Terrorismusbekämpfungsgesetz ist in § 8 BVerfSchG auch ein neuer Absatz 7 eingefügt worden. Das BfV darf danach im Einzelfall bei Luftfahrtunternehmen unentgeltlich Auskünfte zu Namen, Anschriften und zur Inanspruchnahme von Transportleistungen und sonstigen Umständen des Luftverkehrs einholen, wenn dies zur Erfüllung seiner Aufgaben nach § 3 Abs. 1 Nr. 2 bis 4 BVerfSchG (vgl. oben Fn. 1) erforderlich ist und tatsächliche Anhaltspunkte für

schwerwiegende Gefahren für die in den Aufgabennormen genannten Schutzgüter vorliegen.

Die Regelung soll gewährleisten, dass Luftfahrtunternehmen Auskünfte erteilen, die zur frühzeitigen und umfassenden Gewinnung von Informationen über Reisewege und dadurch zur Analyse internationaler terroristischer Gruppen beitragen können, insbesondere hinsichtlich Ruhe- und Vorbereitungsräumen sowie Zielgebieten ( BT-Drs. 14/7386, S. 40).

## **a) Auswertung**

### Informationsgewinnung

Bislang wurden in drei Fällen Auskunftsersuchen gem. § 8 Abs. 7 BVerfSchG an Luftfahrtunternehmen gestellt, eines im Quartal IV/02 und zwei im Quartal III/03. In keinem Fall wurde die Auskunft verweigert.

Wenn das BfV erfährt, dass eine Person aus dem Umfeld einer ausländischen terroristischen Gruppierung von einem Land X nach einem Zwischenstopp in Deutschland in ein Drittland reist, um dort möglicherweise Angehörige der Terrororganisation zu treffen (Beschaffungsprojekte), ist es wegen der Gefahr weiterer Terroraktionen wichtig, den modus operandi - in diesem Fall Reisemodalitäten mutmaßlicher Kontaktleute - zu überprüfen (z.B.: Reise mit Falschpapieren oder mit Klarnamen?). Dazu müssen die Passagierlisten mit den dem BfV bekannten Erkenntnissen verglichen werden. Der Abgleich ist wichtig für die Bewertung der reisenden Person. Das Fehlen des Klarnamens auf der Liste, trotz gesicherter Erkenntnisse über seine Ankunft, verdichtet den Verdacht auf Einbindung in illegale Aktivitäten.

Die Auskünfte haben dazu beigetragen, Anhaltspunkte für Reisebewegungen von Personen aus Netzwerken „Arabischer Mujahedin“ zu verifizieren.

Der zurückhaltende Gebrauch der Befugnis erklärt sich zum einen durch einen verantwortungsvollen Umgang mit ihr. So wurde auf eine Antragstellung verzichtet, wenn dies zum Schutz der Betroffenen gegenüber ausländischen staatlichen Stellen erforderlich erschien. Im Übrigen scheidet ein Auskunftsantrag auch dann aus, wenn die Vertraulichkeit der Behandlung durch das Luftfahrtunternehmen nicht hinreichend gewährleistet ist.

## Eingriff in Persönlichkeitsrechte

Die Auskunftersuchen bezogen sich auf insgesamt fünf Betroffene. Tatsächliche Anhaltspunkte für „schwerwiegende Gefahren“ im Sinne der Norm wurden im Falle von Flugreisen im Zusammenhang mit bevorstehenden terroristischen Anschlägen oder zu deren Vorbereitung gesehen, ferner auch im Falle der Einbindung der betroffenen Flugreisenden in islamistische terroristische Netzwerkstrukturen sowie bei Anhaltspunkten für die Unterstützung einer terroristischen Organisation, etwa mit der Durchführung logistischer Aufgaben.

### **bb) Schlussfolgerungen**

Die Befugnis hat aufgabendienliche Erkenntnisse erbracht, ohne dass damit unangemessen breite Überwachungsfolgen verbunden waren. Sie sollte beibehalten werden.

## **6. Auskünfte von Telekommunikations- und Teledienstleistern**

### **a) Bundesamt für Verfassungsschutz**

Mit Artikel 1 Nr. 3 Buchstabe b Terrorismusbekämpfungsgesetz ist in § 8 BVerfSchG auch ein neuer Absatz 8 eingefügt worden. Das BfV darf danach im Einzelfall zur Erfüllung seiner Aufgaben nach § 3 Abs. 1 Nr. 2 bis 4 BVerfSchG (vgl. oben Fn. 1) unter den Voraussetzungen des § 3 Abs. 1 G 10 (tatsächliche Anhaltspunkte, dass jemand bestimmte schwere Straftaten plant, begeht oder begangen hat) bei denjenigen, die geschäftsmäßig Telekommunikationsdienste und Teledienste erbringen oder daran mitwirken, unentgeltlich Auskünfte über Telekommunikationsverbindungsdaten und Teledienstnutzungsdaten einholen<sup>3</sup>. Sie können auch zur zukünftigen Telekommunikation und zukünftigen Nutzung von Telediensten verlangt werden.

Die Regelung soll Auskünfte der Diensteanbieter gewährleisten. Hierdurch sollen Informationen über den Aufenthaltsort, Kommunikationsprofile und –beziehungen

---

<sup>3</sup> Telekommunikationsverbindungsdaten und Teledienstnutzungsdaten sind gemäß § 8 Abs. 8 Satz 3 BVerfSchG:

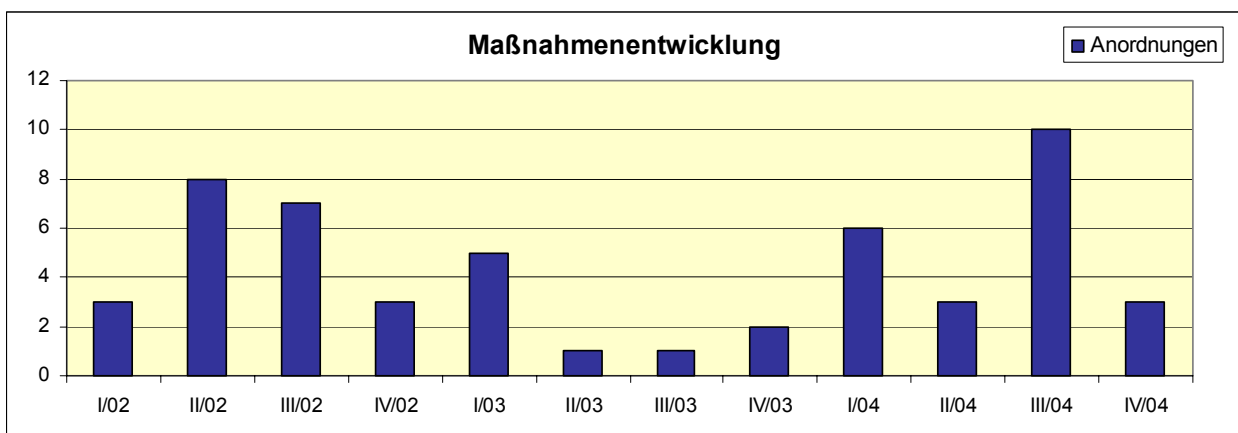
- Berechtigungskennungen, Kartennummern, Standortkennung sowie Rufnummer oder Kennung des anrufenden und angerufenen Anschlusses oder der Endeinrichtung,
- Beginn und Ende der Verbindung nach Datum und Uhrzeit,
- Angaben über die Art der vom Kunden in Anspruch genommenen Telekommunikations- und Teledienst-Dienstleistungen,
- Endpunkte festgeschalteter Verbindungen, ihr Beginn und ihr Ende nach Datum und Uhrzeit.

sowie das Umfeld der Zielperson, z.B. über weitere Beteiligte terroristischer Netzwerke, gewonnen werden (BT-Drs. 14/7386, S. 40).

**aa) Auswertung**

Informationsgewinnung

Bislang wurden in 35 Fällen Auskunftersuchen gem. § 8 Abs. 8 BVerfSchG an Telekommunikationsdienstleister gestellt. Zusammen mit Erweiterungs- und Verlängerungsanträgen beträgt die Gesamtzahl der Auskunftersuchen 52 (davon 13 Verlängerungen und vier Erweiterungen):



Quartal	I/02	II/02	III/02	IV/02	I/03	II/03	III/03	IV/03	I/04	II/04	III/04	IV/04
Anordnungen	3	8	7	3	5	1	1	2	6	3	10	3

In keinem Fall wurden Auskünfte verweigert.

Die Auskünfte haben insbesondere zur Aufdeckung von Netzwerkstrukturen „Arabischer Mujahedin“ beigetragen, indem hierdurch Gesprächskontakte verschiedener Personen belegt werden konnten.

Im Rahmen der Beobachtung völkerverständigungswidriger Bestrebungen aus dem rechtsextremistischen Bereich konnten zuvor unbekannte Kontaktpersonen ermittelt werden. Ein Antrag diente dazu, die Nutzer von 40 IP-Adressen zu ermitteln, da von diesen Internetadressen aus völkerverständigungswidrige Musiktitel im Internet zum Download angeboten worden waren.

Auch bei der Spionageabwehr konnten relevante Informationen erlangt werden, insbesondere zur Verdachtserhärtung, zur Konkretisierung von Anlaufadressen und zur



Erstellung eines Teilbewegungsbildes (ohne aufwendige und enttarnungsanfällige Observationsmaßnahmen), das Rückschlüsse auf die methodische Arbeitsweise des nachrichtendienstlichen Gegners zulässt.

### Eingriff in Persönlichkeitsrechte

Die Auskunftersuchen bezogen sich auf insgesamt 45 Betroffene. Hinzu kommt ein Auskunftersuchen, bei dem die Bestandsdaten von Internetnutzern anhand von 40 IP-Adressen bei den jeweiligen Internet-Providern angefragt wurden<sup>4</sup>. Zu 35 IP-Adressen konnten die Nutzerdaten recherchiert werden. Dabei handelte es sich – wegen Mehrfachnutzung – um insgesamt 28 Betroffene.

Zum Anordnungszeitraum:	Betroffene	Anordnungsdauer
	5	
	(+ 28 betroffene Nutzer von IP-Adressen)	bis zu 1
	Woche	
	1	10 Tage
	3	1 Monat
	25	12 - 13 Wochen
	8	24 Wochen
	3	26 Wochen

### **bb) Schlussfolgerungen**

Die Befugnis hat aufgabendienliche Erkenntnisse erbracht, ohne dass damit unangemessen breite Überwachungsfolgen verbunden waren. Sie sollte beibehalten werden.

### **b) Militärischer Abschirmdienst**

Mit Artikel 2 Nr. 4 Buchstabe b ist in § 10 MAD-Gesetz ein neuer Absatz 3 eingefügt worden. Die Regelung entspricht der betreffenden BfV-Befugnis.

---

<sup>4</sup> Bei Nutzerdaten hinter dynamischen IP-Adressen handelt es sich nach Ansicht der berechtigten Stellen um Bestandsdaten. Die Mehrheit der Betreiber steht allerdings auf dem Standpunkt, es handle sich um Verbindungsdaten und verlangt das Vorliegen einer entsprechenden Anordnung (hier gem. § 8 Abs. 8 BVerfSchG). Die Frage wird in der Rechtsprechung derzeit uneinheitlich bewertet.

## aa) Auswertung

### Informationsgewinnung

Bislang wurden in sechs Fällen Auskunftersuchen gem. § 10 Abs. 3 MADG gestellt.

Quartal	III/02	IV/02	I/03	II/04
Anordnungen	1	2	2	1

In keinem Fall wurden Auskünfte verweigert. Teilweise bestand jedoch zuvor rechtlicher Erläuterungsbedarf zu der neuen Befugnis.

Mit den Auskünften konnten vorliegende Informationen verifiziert und der Kontakt zu bislang nicht bekannten Personen aus dem islamistischen Umfeld nachgewiesen werden. Ferner konnten aus den erhobenen Telekommunikationsverbindungsdaten methodische Erkenntnisse gewonnen werden.

### Eingriff in Persönlichkeitsrechte

Die Auskunftersuchen bezogen sich auf sieben Anschlussinhaber und 38 Anschlüsse sowie einen Zeitraum von jeweils drei Monaten (soweit die Auskunft in Bezug auf zukünftige Telekommunikation oder zukünftige Nutzung von Telediensten verlangt worden ist).

## bb) Schlussfolgerungen

Die Befugnis hat aufgabendienliche Erkenntnisse erbracht, ohne dass damit unangemessen breite Überwachungsfolgen verbunden waren. Sie sollte beibehalten werden.

## c) Bundesnachrichtendienst

Mit Artikel 3 Nr. 2 Terrorismusbekämpfungsgesetz ist in § 8 BNDG ein neuer Absatz 3a eingefügt worden. Die Regelung entspricht der betreffenden BfV-Befugnis. Der BND darf danach im Einzelfall, soweit dies im Rahmen seiner Aufgaben für die Sammlung von Informationen über bestimmte Gefahrenbereiche<sup>5</sup> erforderlich ist, bei

<sup>5</sup> Die in § 5 Abs. 1 Satz 3 Nr. 1 bis 4 und 6 G 10 genannten Gefahrenbereiche, nämlich die Gefahr

- eines bewaffneten Angriffs auf die Bundesrepublik Deutschland (Nr. 1),
- der Begehung internationaler terroristischer Anschläge mit unmittelbarem Bezug zur Bundesrepublik Deutschland (Nr. 2),

denjenigen, die geschäftsmäßig Telekommunikationsdienste und Teledienste erbringen oder daran mitwirken, unentgeltlich Auskünfte über Telekommunikationsverbindungsdaten und Teledienstnutzungsdaten einholen. Sie können auch zur zukünftigen Telekommunikation und zukünftigen Nutzung von Telediensten verlangt werden.

## aa) Auswertung

### Informationsgewinnung

Bislang wurden vom BND sechs Anträge (davon ein Ergänzungsantrag) für insgesamt 18 Anschlussnummern bei fünf verschiedenen Telekommunikationsunternehmen gestellt, die ausschließlich den Gefahrenbereich des internationalen Terrorismus gem. § 5 Abs. 1 Satz 3 Nr. 2 G 10 betrafen.

Quartal	III/02	I/03	II/03	I/04
Anordnungen	2	2	1	1

Zu Anfang waren gewisse Vorbehalte einiger Diensteanbieter zu überwinden, teilweise bestand auch rechtlicher und tatsächlicher Erläuterungsbedarf zu der neuen Befugnis. Zwischenzeitlich ist die Zusammenarbeit mit den Diensteanbietern aber durchaus konstruktiv. In keinem Fall wurden Auskünfte verweigert.

Durch Auskünfte über Verbindungsdaten kann zum Einen mittels eines Abgleichs mit bereits bekannten Anschlussnummern festgestellt werden, ob die verdächtigen Anschlussinhaber in Deutschland tatsächlich in regelmäßigem Kontakt zu mutmaßlichen Mitgliedern terroristischer Vereinigungen stehen. Zum Anderen können aus der Liste der Verbindungsdaten Erkenntnisse über weitere Anschlussnummern im Ausland ermittelt werden, die möglicherweise von terroristischen Vereinigungen genutzt werden. Dies ermöglicht dem BND, seine Beschränkungsmaßnahmen nach § 5 Abs. 1 Satz 3 Nr. 2 G 10 zum Gefahrenbereich des internationalen Terrorismus um die entsprechenden Anschlussnummern im Ausland als formale Suchbegriffe zu erweitern. Dadurch kann das Mittel der Fernmeldeaufklärung im Bereich des internationalen Terrorismus gezielter eingesetzt werden.

- 
- der internationalen Verbreitung von Kriegswaffen im Sinne des Gesetzes über die Kontrolle von Kriegswaffen sowie des unerlaubten Außenwirtschaftsverkehrs mit Waren, Datenverarbeitungsprogrammen und Technologien in Fällen von erheblicher Bedeutung (Nr. 3),
  - der unbefugten Verbringung von Betäubungsmitteln in nicht geringer Menge in die Bundesrepublik Deutschland (Nr. 4) und
  - der international organisierten Geldwäsche in Fällen von erheblicher Bedeutung (Nr. 6).

## Eingriff in Persönlichkeitsrechte

Die Ersuchen bezogen sich auf insgesamt zwölf Betroffene (18 Anschlussnummern) bei fünf verschiedenen Telekommunikationsunternehmen. Bei drei Betroffenen betrug der Zeitraum vier Monate, bei den restlichen neun Betroffenen fünf Monate. Sämtliche Anträge wurden zum Gefahrenbereich Internationaler Terrorismus gestellt (§ 5 Abs. 1 Satz 3 Nr. 2 G 10). Sie bezogen sich überwiegend auf Anschlussnummern, die Netzwerken islamistischer Extremisten zuzuordnen sind.

### **bb) Schlussfolgerungen**

Die Befugnis hat aufgabendienliche Erkenntnisse erbracht, ohne dass damit unangemessen breite Überwachungsfolgen verbunden waren. Sie sollte beibehalten werden.

## **7. Anordnungsverfahren zu den neuen Auskunftsbefugnissen (und zum IMSI-Catcher)**

Mit Artikel 1 Nr. 3 Buchstabe b Terrorismusbekämpfungsgesetz ist in § 8 BVerfSchG auch ein neuer Absatz 9 eingefügt worden, dessen Sätze 1 bis 8 das Anordnungsverfahren festlegen (gilt im Verweisungswege entsprechend für die entsprechenden Befugnisse von MAD und BND und den Einsatz des IMSI-Catchers, dazu C.I.12 / Fn. 8). Danach gilt Folgendes:

- Auskünfte dürfen nur auf Antrag eingeholt werden. Der Antrag ist durch den Präsidenten des Bedarfsträgers (BfV, MAD bzw. BND) oder seinen Vertreter schriftlich zu stellen und zu begründen.
- Über den Antrag entscheidet in den Fällen des BfV und MAD das vom Bundeskanzler beauftragte Bundesministerium des Innern, im Falle des BND der Chef des Bundeskanzleramts.
- Das Bundesministerium des Innern bzw. der Chef des Bundeskanzleramtes unterrichten monatlich die G 10-Kommission über die beschiedenen Anträge vor deren Vollzug. Bei Gefahr im Verzuge können sie den Vollzug der Entscheidung auch bereits vor der Unterrichtung der Kommission anordnen. Die G 10-Kommission prüft von Amts wegen oder auf Grund von Beschwerden die Zulässigkeit und Notwendigkeit der Einholung von Auskünften.
- § 15 Abs. 5 G 10 (Entscheidung der G 10-Kommission über Zulässigkeit und Notwendigkeit von Beschränkungsmaßnahmen) ist mit der Maßgabe entsprechend anzuwenden, dass die Kontrollbefugnis der Kommission sich auf die gesamte Erhebung, Verarbeitung und Nutzung der nach den Absätzen 5 bis 8 erlangten per-

sonenbezogenen Daten erstreckt. Entscheidungen über Auskünfte, die die G 10-Kommission für unzulässig oder nicht notwendig erklärt, haben das Bundesministerium des Innern bzw. der Chef des Bundeskanzleramtes unverzüglich aufzuheben.

Zweck der Regelung ist es, durch Verfahren zu sichern, dass die Einholung der Auskünfte zulässig und notwendig ist.

Die getroffenen Maßgaben stehen in einem gewissen normativen Spannungsverhältnis zu Vergleichsregelungen des Bundesverfassungsschutzgesetzes mit teilweise wohl deutlich stärkerem Eingriffsgehalt bei zugleich deutlich minderen Verfahrensmaßgaben. So genügt zum Einsatz nachrichtendienstlicher Mittel gemäß § 8 Abs. 2 BVerfSchG eine Zuständigkeitsfestlegung beim BfV, zu der die Zustimmung des Bundesministeriums des Innern und eine Unterrichtung des Parlamentarischen Kontrollgremiums (PKGr) erforderlich ist. Selbst bei Maßnahmen, die in ihrer Art und Schwere einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses gleichkommen (insbesondere das Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes mit dem verdeckten Einsatz technischer Mittel), sieht § 9 Abs. 3 BVerfSchG lediglich noch ergänzend vor, das Parlamentarische Kontrollgremium auch von der konkreten Maßnahme zu unterrichten. Die Auskunftseinholung etwa bei einem Luftfahrtunternehmen hat dagegen einen anderen Eingriffsgehalt, ist aber mit sehr viel aufwendigeren Verfahrenssicherungen versehen.

#### **a) Auswertung**

Die Ergebnisse der Zweckverfolgung lassen sich nur begrenzt und mittelbar messen. Bislang ist keine Anordnung in einer nachfolgenden Verwaltungstreitsache aufgehoben worden. Von den insgesamt 124 Anträgen wurden zwei durch das BMI und ein weiterer durch die G 10-Kommission abgelehnt.

Die Entscheidungsbildung zum Auskunftersuchen ist aufwendig gestaltet. Verfahrensmäßige Sicherungen sind dabei insoweit geboten, wie sie zum Schutz des Betroffenen unter Berücksichtigung von Gegenstand und Wirkungen des Ersuchens erforderlich sind. Soweit die Regelung über das grundrechtlich Gebotene hinausgeht, sollten auch Praktikabilitätsgesichtspunkte in die Gesetzesfolgenabschätzung eingehen. Dies betrifft auch die Verfahrensdauer bei der Anordnung operativer Maßnahmen. Insoweit ist in der aktuellen Durchführungspraxis der Auskunftsantragsverfahren vom Entschluss der Fachebene bis zur Entscheidung der G 10-Kommission bzw. bis zur Eilanordnung der Obersten Bundesbehörde eine breite Streuung zwischen

zwölf Werktagen und – häufig – mehreren Wochen feststellbar (die auch mit den Sitzungsterminen der G 10-Kommission zusammenhängt).

Von den 121 Anordnungen beruhen 17 (14 %) auf Eilanträgen im Sinne von § 8 Abs. 9 Satz 5 BVerfSchG gestellt worden (13 Anträge auf Telekommunikationsverbindungsdaten und vier Anträge auf IMSI-Catcher-Einsatz).

Der hohe Verfahrensaufwand führt in der Praxis zu einer eingeschränkten Nutzung dieser Befugnisse. In der Entscheidungssituation des nach den Anschlägen vom 11.9.2001 rasch handelnden Gesetzgebers war gut begründbar, bei der Ausgestaltung von Verfahrenssicherungen bis zur vorgesehenen Evaluierung risikosensibel zu entscheiden und vorsichtshalber eher zu weitgehende als womöglich zu kurz greifende Lösungen zu wählen. Nunmehr könnte eine Überprüfung dieser Entscheidung erfolgen.

## **b) Schlussfolgerungen**

Zur Optimierung der Praktikabilität der neuen Auskunftsregelungen durch Verfahrensvereinfachungen könnte geprüft werden, ob und ggf. wie Differenzierungen nach dem Eingriffsgehalt der verschiedenen Befugnisse vorgenommen werden können, ohne dabei unangemessene Risiken für Rechte von Betroffenen hinzunehmen.

## **8. Löschung, Kennzeichnung, Übermittlungseinschränkung** (bei den neuen Auskunftsregelungen und beim IMSI-Catcher)

Für die Verarbeitung der nach den neuen Auskunftsregelungen erhobenen Daten bestimmt § 8 Abs. 9 Satz 9 BVerfSchG (und entsprechend die Verweisungsregelungen zum IMSI-Catcher und zu MAD und BND) die entsprechende Anwendung der Prüf-, Kennzeichnungs-, Löschungspflichten und Übermittlungseinschränkungen nach § 4 G 10. Danach gilt insbesondere Folgendes:

- Die erhebende Stelle prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die erhobenen personenbezogenen Daten im Rahmen ihrer Aufgaben für zulässige Erhebungszwecke erforderlich sind. Soweit die Daten für diese Zwecke nicht erforderlich sind und nicht für eine Übermittlung an andere Stellen benötigt werden, sind sie unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen. Die Löschung ist zu protokollieren.
- Die verbleibenden Daten sind zu kennzeichnen.

- Die Daten dürfen nur übermittelt werden zur Verhinderung, Aufklärung oder Verfolgung bestimmter schwerer Straftaten und zur Vorbereitung und Durchführung eines Partei- oder Vereinsverbotsverfahrens.

#### **a) Löschung**

Eine Besonderheit dieser Regelung gegenüber der allgemeinen Löschungspflicht nach § 12 Abs. 2 und 3 BVerfSchG besteht darin, dass von Anfang an terminlich engmaschige Prüfroutinen erfolgen (maximal nach jeweils sechs Monaten), die auch unabhängig von laufender Bearbeitung eine Überprüfung gewährleisten, ob eine Speicherung weiterhin erforderlich ist. Im Übrigen sind die Daten unter besonderer Beaufsichtigung zu löschen, was auch zu protokollieren ist.

#### **aa) Auswertung**

Die Regelüberprüfungen haben bislang lediglich Verwaltungsroutinen veranlasst, jedoch zu keinen Löschungen geführt<sup>6</sup>.

Dies liegt auch darin begründet, dass eine kurzfristige Löschung der Erkenntnisse über Kontaktpersonen bei der Aufklärung der äußerst konspirativ arbeitenden Netzwerkstrukturen „Arabischer Mujahedin“ wegen der Erforderlichkeit der Weiternutzung nicht sachgerecht wäre. Verbindungen bzw. Vernetzungen werden erst dann erkennbar, wenn ein größerer, aus verschiedenen Quellen stammender Datenbestand auf Überschneidungen hin überprüft werden kann. Gerade auch zur angestrebten Intensivierung der Aufklärung der Finanzierungswege des internationalen Terrorismus ist das längerfristige Vorhalten von Kontobewegungsdaten, insbesondere von Einzählern und Geldempfängern, erforderlich. Deshalb ist einerseits mit Lösungsfolgen der Prüfroutinen erst bei länger gespeicherten Daten zu rechnen, andererseits wirft dies die Frage auf, ob der Verwaltungsaufwand der vorgesehenen besonderen Prüfroutinen angemessen ist.

Bereits § 12 Abs. 3 BVerfSchG (auch in Verbindung mit § 7 Abs. 1 MADG und § 5 Abs. 1 BNDG) sieht allgemein vor, dass das BfV (bzw. MAD/BND) Erforderlichkeitsprüfungen nach festgesetzten Fristen vornimmt. Die Fristfestlegung erfolgt dabei in den Arbeitsplänen und Dateianordnungen des BfV, die der Zustimmung des Bundesministeriums des Innern unterliegen und an deren Erstellung der Bundesbeauftragte für den Datenschutz beteiligt wird (zu Dateianordnungen speziell geregelt in § 14 BVerfSchG). Dieses flexiblere System könnte den sachlich gerechtfertigten Dif-

---

<sup>6</sup> Löschungen sind zwar erfolgt, resultierten aber aus Überprüfungen bei der laufenden Sachbearbeitung.

ferenzierungen im Anwendungsbereich von § 8 Abs. 5 bis 8 BVerfSchG angemessener sein.

## **bb) Schlussfolgerungen**

Die Praxis hat bislang nicht die Erwartung bestätigt, dass ein relevanter Bedarf besteht, durch Prüfroutinen zum Schutz von Persönlichkeitsrechten beizutragen. Wie bereits allgemein zu den Verfahrensregelungen (bei C.I.7.b) ausgeführt, könnte auch hier geprüft werden, ob und ggf. wie diese Verfahrenssicherung differenziert nach dem Eingriffsgehalt der verschiedenen Befugnisse ausgestaltet, d.h. teilweise auf die besonders engmaschigen Prüfroutinen verzichtet werden könnte.

## **b) Kennzeichnung**

### **aa) Auswertung**

Die Kennzeichnung erfordert erheblichen Verwaltungsaufwand. Im BfV sind mit der Unterlagenverwaltung aktuell zwei Mitarbeiter des mittleren Dienstes (Teilzeit, 50 %) befasst<sup>7</sup>. Die Unterlagenverwaltung schließt neben der Kennzeichnung weitere Aufgaben ein, die jedoch überwiegend zur effektiven Ausformung der Kennzeichnungszwecke in Anlehnung an die Verfahrensweise in G 10-Sachen erfolgen und somit in die Gesamtwürdigung einzubeziehen sind.

### **bb) Schlussfolgerungen**

Auch hier (siehe bereits C.I.8.a.bb) könnte angesichts differenziert zu betrachtender Eingriffswirkungen eine entsprechend differenzierte Regelung zum optimierten Ausgleich von Aufwand und Nutzen geprüft werden.

## **c) Übermittlungseinschränkung**

Die Übermittlungsregelung ist - einschränkende - lex specialis gegenüber den allgemeinen Übermittlungsbefugnissen des Bundesverfassungsschutzgesetzes. Demgemäß waren die Rechtstatsachen zu erheben, die den einschränkenden Normgehalt betreffen. Hiernach ist untersucht worden, ob Fälle aufgetreten sind, bei denen eine

---

<sup>7</sup> Die betreffenden Mitarbeiter werden allerdings je nach Arbeitsanfall auch in der G 10-Unterlagenverwaltung zur Unterstützung der dortigen Mitarbeiter eingesetzt, wie auch umgekehrt von dort erforderlichenfalls personelle Unterstützung bei der Kennzeichnung nach § 8 Abs. 9 Satz 9 BVerfSchG erfolgt, so dass dieser flexible Einsatz bei einer groben Würdigung nicht wesentlich ins Gewicht fällt.



Übermittlung nach §§ 19, 20 BVerfSchG erfolgt wäre, nach § 8 Abs. 9 Satz 9 BVerfSchG i.V.m. § 4 Abs. 4 G 10 aber unterbleiben musste.

#### **aa) Auswertung**

Bislang sind Übermittlungen lediglich im Bereich der Beobachtung von islamistischen Bestrebungen und im Bereich der Spionageabwehr erfolgt. Es sind keine Fälle aufgetreten, in denen eine Übermittlung fachlich wünschenswert gewesen wäre und nach den allgemeinen Übermittlungsregelungen auch hätte erfolgen dürfen, jedoch nach den speziellen Übermittlungsbeschränkungen unterbleiben musste. Solche Fälle sind aber für die Zukunft nicht auszuschließen.

#### **bb) Schlussfolgerungen**

Die Evaluierung gibt keinen Anlass, die Übermittlungsbeschränkungen in Frage zu stellen.

### **9. Vertraulichkeitspflicht des Auskunftsgewährenden**

Der neue § 8 Abs. 9 S. 10 BVerfSchG enthält zu den neuen Auskunftsregelungen ein Verbot für den Auskunftsgewährender, das Auskunftersuchen und die übermittelten Daten dem Betroffenen oder Dritten mitzuteilen. Dieses Verbot ist allerdings nicht sanktionsbewehrt, anders als die entsprechenden Mitteilungsverbote nach § 17 G 10 durch § 18 G 10. Insoweit stellt sich die Frage, ob Bedarf besteht, das gesetzliche Verbot vergleichbar zu bewehren.

Bislang sind keine gesetzwidrigen Indiskretionen bekannt. Allerdings wirkt ein spezifisches Risiko, dass die Vertraulichkeit nicht gewahrt werden wird, bereits auf das Antragsverhalten dergestalt, dass eine Auskunft in solchen Fällen erst gar nicht eingeholt wird (vgl. oben C.I.5.a). In solchen Fällen würde eine Sanktionsbewehrung des Mitteilungsverbots die Risikoeinschätzung typischerweise nicht wesentlich ändern.

Die Evaluierung gibt keinen Anlass, die Verletzung des Mitteilungsverbots durch spezielle Sanktionen zu bewehren.

## 10. Mitteilung an Betroffene

Nach § 8 Abs. 9 Satz 11 BVerfSchG ist Auskunftsbetroffenen entsprechend den G 10-Regelungen die Auskunftseinholung mitzuteilen, sobald dies ohne Gefährdung des Auskunftszwecks möglich ist. Ist dies fünf Jahre nach Maßnahmebeendigung immer noch nicht der Fall und kann dies praktisch auch für die Zukunft ausgeschlossen werden, dann kann die G 10-Kommission die Mitteilungspflicht aufheben, wenn die Daten zu löschen sind.

Das BfV holt nach Abschluss der jeweiligen Maßnahme und Auswertung des erlangten Materials die Entscheidung des Bundesministeriums des Innern über eine Mitteilung an den Betroffenen ein. Das Bundesministerium des Innern bittet im Falle des (auch vorläufigen) Absehens von einer Mitteilung die G 10-Kommission um Zustimmung. Bisher ist in zwei Fällen entschieden worden, dass eine Mitteilung zu erfolgen hat. In einem Fall läuft die Adressermittlung noch, in dem anderen Fall ist die Mitteilung an einen Nebenbetroffenen bereits erfolgt.

In 31 Fällen ist entschieden worden, dass vorerst bzw. weiterhin keine Mitteilung erfolgen soll und die Prüfung zu einem jeweils festgelegten späteren Termin wiederholt wird. In zwei weiteren Fällen (einer nach § 8 Abs. 7 BVerfSchG, einer nach § 8 Abs. 8 BVerfSchG) ist mit Zustimmung der G 10-Kommission entschieden worden, dass die Betroffenen endgültig keine Mitteilung erhalten sollen, da diese nicht namentlich identifiziert werden konnten.

Auch der MAD prüft unmittelbar nach Abschluss einer Maßnahme die Frage, ob die Gefährdung ihres Zwecks einer Mitteilung an den Betroffenen entgegensteht, und verfährt im Weiteren wie das BfV. Im Berichtszeitraum hat die G 10-Kommission in einem Fall der Mitteilung der Maßnahme an den Betroffenen zugestimmt und in zwei weiteren Fällen gebilligt, dass vorerst keine Mitteilung erfolgen, sondern die Prüfung zu einem späteren Zeitpunkt erneut durchgeführt werden soll.

Mit Zustimmung des Bundeskanzleramtes unterrichtet der BND die G 10-Kommission bereits ein Jahr nach Maßnahmenbeendigung über die Gründe für die Zurückstellung der Mitteilung und bittet um Einverständnis. Er wird das Verfahren unaufgefordert wiederholen, falls sich die Gründe für die Zurückstellung vor Ablauf der fünf Jahre ändern. Dies soll der G 10-Kommission eine dichtere Kontrolle über vorerst zurückgestellte Mitteilungen an Betroffene ermöglichen.

Da das Gesetz noch keine fünf Jahre in Kraft ist, hat sich die Frage eines endgültigen Absehens von Mitteilung bislang nicht gestellt.

Die Regelung zielt darauf, den Betroffenen über den Eingriff zu informieren, dies jedoch nur, wenn eine Gefährdung des Zwecks der Maßnahme ausgeschlossen werden kann. Angesichts dieser Einschränkung und der beschränkten Normanwendungsdauer überrascht zwar nicht, dass bislang erst wenige Auskunftsfälle zu verzeichnen sind, so dass sich aus der Evaluierung gegenwärtig kein Änderungsbedarf ergibt. Es sollte aber beobachtet werden, wie sich die Balance zwischen Mitteilungsinteresse und Aufgabengewährleistung in der Praxis weiter entwickelt.

Sofern das Verfahrensmodell des G 10 künftig differenziert übertragen werden soll (Beschränkung auf Maßnahmen, die ebenfalls in das Grundrecht aus Artikel 10 GG eingreifen), könnte es zur inneren Wertungshomogenität beitragen, hierbei auch die Mitteilungspflicht einzubeziehen. Auch nach der allgemeinen Regelung in § 9 Abs. 3 Nr. 1 BVerfSchG bestehen Mitteilungspflichten nur beim Einsatz nachrichtendienstlicher Mittel und nur dann, wenn die Erhebung in ihrer Art und Schwere einer Beschränkung des Brief-, Post- und Fernmeldegeheimnis gleichkommt. Bei der Auskunftseinholung bei Kreditinstituten und Luftfahrtunternehmen nach § 8 Abs. 5 bzw. 7 BVerfSchG ist das nicht der Fall.

## **11. Erweiterung der technischen Wohnungsüberwachung (Eigensicherung)**

Mit Artikel 1 Nr. 4 Buchstabe a Terrorismusbekämpfungsgesetz sind der Regelung zur technischen Wohnungsüberwachung in § 9 Abs. 2 BVerfSchG neue Bestimmungen angefügt worden, die insbesondere einschließen, dass die Maßnahme auch zum Schutz der bei einem Einsatz in Wohnungen tätigen Personen erfolgen darf, soweit dies zur Abwehr von Gefahren für deren Leben, Gesundheit oder Freiheit unerlässlich ist. Außerdem sind Zweckbindungs- und Verfahrensregelungen ergänzt worden. Die Regelung gilt im Verweisungswege auch für den MAD (§ 5 MADG) und in Deutschland für den BND (§ 1 Abs. 2 Satz 2 i.V.m. § 3 Satz 2 BNDG).

BfV, MAD und BND haben von der Befugnis bislang keinen Gebrauch gemacht.

- Die bisherige Praxis hat die Erforderlichkeit der Befugnis nicht bestätigt.
- Die Regelung war jedoch durch konkrete Vorkommnisse der Vergangenheit veranlasst. Entsprechende Fälle können bei der operativen Arbeit in einem gewalttätigen Umfeld auch künftig auftreten. Wenngleich denkbare Einsatzfälle sicher begrenzt bleiben, spricht dies dafür, die Eigensicherungsbefugnis beizubehalten.

## 12. IMSI-Catcher

### a) Bundesamt für Verfassungsschutz

Mit Artikel 1 Nr. 4 Buchstabe c Terrorismusbekämpfungsgesetz ist in dem neuen § 9 Abs. 4 BVerfSchG eine spezielle Befugnis zum Einsatz des sogenannten „IMSI-Catchers“ geschaffen worden. Der Einsatz des IMSI-Catchers dient der Ermittlung der Geräte- und Kartenummer von Mobiltelefonen, die zur Vorbereitung einer Telekommunikationsüberwachung nach dem G 10 benötigt werden, und auf dieser Basis auch zur Lokalisierung des Standortes des Gerätes<sup>8</sup>.

Der neue § 9 Abs. 4 BVerfSchG lässt den Einsatz des IMSI-Catchers zur Erfüllung der Aufgaben nach § 3 Abs. 1 Nr. 2 bis 4 BVerfSchG (vgl. oben Fn. 1) zu, wenn die Voraussetzungen des § 3 Abs. 1 G 10 vorliegen (tatsächliche Anhaltspunkte, dass jemand bestimmte schwere Straftaten plant, begeht oder begangen hat). Für die Verarbeitung der Daten gelten die Prüf-, Kennzeichnungs- und Löschungspflichten sowie die Übermittlungs- und Zweckbindungsregelung nach § 4 G 10 entsprechend (vgl. oben C.I.8).

Personenbezogene Daten eines Dritten dürfen nur im technisch unvermeidbaren Umfang erhoben werden. Sie unterliegen einem absoluten Verwendungsverbot und sind nach Beendigung der Maßnahme unverzüglich zu löschen. Demgemäß erfolgt

---

<sup>8</sup> Mit dem IMSI-Catcher ist es möglich, in seinem Einzugsbereich die IMSI (International Mobile Subscriber Identity) eines eingeschalteten Mobiltelefons zu ermitteln. Diese IMSI ist eine weltweit einmalige Kennung, die die sogenannte SIM-Karte (SIM = Subscriber Identity Module) eindeutig identifiziert. Die IMSI ist auf der SIM-Karte gespeichert, die ein Mobilfunkteilnehmer bei Abschluss eines Mobilfunkvertrages, dem Kauf eines Mobiltelefons mit Prepaid-Karte oder dem Kauf einer Prepaid-Karte allein erhält. Mit Hilfe der IMSI können durch Anfrage beim jeweiligen Netzbetreiber die Mobilfunknummer und die Anschlussinhaberdaten ermittelt werden.

Zur Ermittlung der IMSI simuliert ein IMSI-Catcher die Basisstation einer regulären Funkzelle eines Mobilfunknetzes. Eingeschaltete Mobiltelefone im Einwirkungsbereich dieser „vermeintlichen“ Basisstation buchen sich nun automatisch beim IMSI-Catcher ein. Durch einen speziellen Befehl des IMSI-Catchers wird dabei die Herausgabe der IMSI veranlasst und das Mobiltelefon in das Mobilfunknetz zurück gewiesen.

Ist der von der Zielperson genutzte Netzbetreiber nicht bekannt – was den Regelfall darstellt – muss diese Suche in allen Mobilfunknetzen durchgeführt werden. In Funkzellen mit vielen Teilnehmern ist es zudem erforderlich, mehrere Messungen durchzuführen, bis die gesuchte IMSI aus der Vielzahl der gesammelten Daten – gleichsam als Schnittmenge – herausgefiltert werden kann.

Durch die Simulation einer Funkzelle werden bestehende Verbindungen nicht unterbrochen. Die auf dem IMSI-Catcher eingebuchten Mobiltelefone werden lediglich für die Dauer des eigentlichen Messvorgangs dem normalen Mobilfunknetz entzogen. Während dieser sehr kurzen Zeit ist eine Kommunikation mit diesem Mobiltelefon nicht möglich.

zu IMSI-Nummern Dritter bereits keine Anfrage bei den Netzbetreibern, so dass hier bereits keine Rückschlüsse auf die entsprechenden Mobilfunknummern und die dazugehörigen Anschlussinhaberdaten gewonnen werden. Dies ist auch organisatorisch dadurch gewährleistet, dass einerseits diese Daten nicht in hausinterne Datenbanken des BfV eingespeist werden und die Anfragen bei den Netzbetreibern bzw. der Regulierungsbehörde für Telekommunikation und Post nicht unmittelbar durch den IMSI-Catchertrupp erfolgt, sondern durch eine gesonderte Organisationseinheit.

## aa) Auswertung

### Informationsgewinnung

Bislang sind 21 Anordnungen nach § 9 Abs. 4 BVerfSchG ergangen (20 Grundanordnungen, eine Verlängerung), davon wurden bisher 19 durchgeführt (davon eine als Verlängerung). Eine Maßnahme wurde auf Grund höherer Priorität von zwei anderen, im selben Anordnungszeitraum laufenden Maßnahmen sowie der späteren Abgabe des Falles an die Strafverfolgungsbehörden nicht durchgeführt. Eine weitere Maßnahme wurde zum Ende des Berichtszeitraums genehmigt, aber noch nicht durchgeführt.

Quartal	III/02	I/03	II/03	III/03	IV/03	I/04	II/04	III/04	IV/04
Anordnungen	3	3	1	1	4	2	4	2	1

Bei drei Maßnahmen konnte anhand der festgestellten IMSI-Nummern der Gebrauch eines bis dahin nicht bekannten Mobiltelefons festgestellt werden. In zwei Fällen wurden anschließend Maßnahmen nach G 10 angeordnet. In dem dritten Fall wurde zu dem ermittelten Mobilfunkanschluss eine G 10-Maßnahme beantragt. Über den Antrag ist noch nicht entschieden worden.

In den übrigen Fällen wurde festgestellt, dass die Zielpersonen entweder bereits bekannte oder keine Mobiltelefone in Gebrauch hatten. Dieses Ergebnis ist jedoch nicht als „erfolglos“ zu betrachten, da im Vorfeld nur der Verdacht der Nutzung eines unbekanntes Mobiltelefons bestand. Insofern konnte dieser Verdacht durch die Maßnahme – zumindest im Rahmen des Genehmigungs- bzw. Einsatzzeitraums des IMSI-Catchers – ausgeräumt werden. Auch dieser Umstand ist für die operative Bearbeitung einer Zielperson eine wichtige Erkenntnis.

## Eingriff in Persönlichkeitsrechte

Von den Maßnahmen waren 20 Zielpersonen betroffen<sup>9</sup>. Beim IMSI-Catcher-Einsatz werden daneben in seinem Einzugsbereich ggf. auch IMSI-Nummern Dritter mit dem Request-Befehl technisch abgerufen. Gemäß dem absoluten Verwendungsverbot erfolgt zu diesen Daten jedoch keine Anfrage bei den Netzbetreibern, so dass Rückschlüsse auf die entsprechenden Mobilfunknummern und die dazugehörigen Anschlussinhaberdaten nicht gewonnen werden. Die Daten werden nur technisch zwischengespeichert, um durch einen Abgleich verschiedener Messungen anhand der Schnittmenge die IMSI-Nummer gerade der Zielperson zu erkennen. Eine Anfrage ergeht nur in dem Fall, in dem durch mehrfach übereinstimmende Messungen des IMSI-Catchertrupps bestätigt wird, dass die Zielperson ein bis dahin unbekanntes Mobiltelefon nutzt und – falls bei den einzelnen Messungen mehrere IMSI-Nummern angefallen sind – nur mit der als Treffer des Abgleichs ermittelten Nummer der Zielperson. Um diesen Abgleich durchführen zu können, bleiben die erfassten IMSIs unbeteiligter Personen vom IMSI-Catchertrupp längstens solange gespeichert, bis der Einsatz beendet ist und die Daten damit nicht mehr benötigt werden. Sie werden nur für besagten technischen Abgleich genutzt und anschließend gelöscht. Eine Einspeicherung der Daten in hausinterne Datenbanken des BfV findet nicht statt. Die Drittbetroffenen bleiben also anonym und für sie sind – über die technische Zwischenerfassung hinausgehende – nachteilige Folgen ausgeschlossen; Kommunikationsinhalte werden mit der Maßnahme ohnehin nicht erfasst. Die Eingriffsintensität der technischen Zwischenerfassung ist insgesamt sehr gering.

### **bb) Schlussfolgerungen**

Die Befugnis hat sich in der Praxis bewährt. Belange Dritter sind durch das absolute Verwertungsverbot und die Pflicht zu unverzüglicher Löschung im Ergebnis nur durch den technischen Erhebungsvorgang und insoweit marginal berührt. Unangemessene Überwachungsfolgen sind damit nicht verbunden. Die Regelung sollte beibehalten werden.

### **b) Militärischer Abschirmdienst**

Die neue Regelung des § 9 Abs. 4 BVerfSchG findet nach § 5 MADG auf den MAD entsprechende Anwendung. Der MAD hat bislang in einem Fall von dieser Befugnis Gebrauch gemacht. Von der Maßnahme war eine Person betroffen. Durch den Einsatz des IMSI-Catchers konnte die Nutzung bereits bekannter Mobiltelefone festge-

---

<sup>9</sup> Bei einer der 21 Anordnungen handelte es sich um eine Verlängerung mit demselben Betroffenen; da eine Anordnung nicht durchgeführt wurde, waren durchführungsbetroffen 19 Personen.

stellt und der Verdacht der Nutzung eines bis dahin nicht bekannten Mobiltelefons ausgeschlossen werden.

Das zum BfV Angemerkte gilt hier ebenso.

### **c) Bundesnachrichtendienst**

Die neue Regelung des § 9 Abs. 4 BVerfSchG findet nach § 3 Satz 2 BNDG auf den BND – für die Datenerhebung im Inland (§ 1 Abs. 2 Satz 2 BNDG) – entsprechende Anwendung. Der BND hat von dieser Befugnis jedoch noch keinen Gebrauch gemacht.

Nach der positiven Praxiserfahrung bei BfV und MAD sollten die Befugnis gleichwohl beibehalten bleiben. Nach dem speziellen Aufgabenbereich des BND ist zwar auch künftig mit einer geringen Zahl von Bedarfsfällen zu rechnen. Solche Fälle können bei der Vorbereitung von Individualkontrollen nach § 3 G 10 gegenüber Mobiltelefon-Inhabern jedoch auch für den Zuständigkeitsbereich des BND künftig durchaus auftreten.

## **13. Regellöschungsfrist beim Bundesamt für Verfassungsschutz**

§ 12 Abs. 3 Satz 2 BVerfSchG sieht für die Extremismusbeobachtung (nicht für die Spionageabwehr) Regellöschungsfristen vor: Ist die letzte relevante Information älter, dann sind die Daten zur betreffenden Person zu löschen, es sei denn der Präsident des BfV oder sein Vertreter ordnen im Einzelfall ausnahmsweise weitere Speicherung an. Mit Artikel 1 Nr. 5 Terrorismusbekämpfungsgesetz ist diese Regellöschungsfrist für den Beobachtungsbereich nach § 3 Abs. 1 Nr. 3 BVerfSchG (gewalt-same Bestrebungen, die auswärtige Belange gefährden, d.h. insbesondere islamisti-scher Terrorismus) von 10 auf 15 Jahre heraufgesetzt worden. Für den neuen Auf-gabenbereich der völkerverständigungswidrigen Bestrebungen (§ 3 Abs. 1 Nr. 4 BVerfSchG, etwa antisemitische Hetze) ist die Regellöschungsfrist ebenfalls auf 15 Jahre festgesetzt worden, also ebenfalls 5 Jahre höher als für die allgemeine Extre-mismusbeobachtung nach § 3 Abs. 1 Nr. 1 BVerfSchG (weiterhin 10 Jahre).

### **a) Auswertung**

Konkrete Zahlenangaben zur Normanwendung können unter Geheimschutzerwä- gungen nicht publiziert werden. Allgemein ist jedoch in diesem Zusammenhang zum Regelungshintergrund anzumerken, dass es gerade im Beobachtungsbereich „Isla-

mismus, Islamistischer Terrorismus“ – im Ergebnis vergleichbar mit der Spionageabwehr – einer möglichst langfristigen Vorhaltung von Informationen beim BfV bedarf, um dem hochkonspirativen Verhalten islamistischer Terroristen, den oft langdauernden individuellen Radikalisierungsprozessen im islamistischen Milieu und dem daraus erwachsenden enormen Bedrohungspotenzial ausreichend Rechnung zu tragen. Die Verlängerung der Speicherfristen ist dabei in erster Linie für Datensätze von Personen von Bedeutung, die bis zum Ablauf der Frist (noch) keine besondere Bedeutung erlangt haben.

Zu Personen aus dem Spektrum „Arabischer Mujahedin“ liegen dem BfV häufig am Anfang nur bruchstückhafte Grunddaten, z.B. Aliasnamen, vor. Eine Identifizierung solcher Personen ist daher oftmals nicht oder nur mit erheblichem Zeitverzug möglich. Denkbar sind beispielsweise Fälle, in denen das BfV, z.B. durch einen Partnerdienst, Informationen bezüglich des Aufenthalts einer Person, die über die vorhandenen Grunddaten (z.B. Aliasnamen) zunächst nicht zu identifizieren ist, in einem Ausbildungslager „Arabischer Mujahedin“ in Afghanistan im Jahre 1993 erhält. Die Identifizierung einer solchen Person könnte möglicherweise erst Jahre nach dem Aufenthalt, z.B. im Rahmen von Ermittlungen zur Aufklärung eines Terroranschlags im Jahre 2003, möglich werden. Durch eine zwischenzeitliche Löschung des Datensatzes wegen Ablauf der Zehnjahresfrist würden wertvolle Ermittlungsansätze hinsichtlich der Kontaktpersonen des Attentäters aus der Zeit in Afghanistan (potenzielle Komplizen) untergehen.

Wie die nachrichtendienstliche Erfahrung zeigt, verlaufen Radikalisierungsprozesse im islamistischen Milieu zudem häufig langsam und schrittweise. Vor diesem Hintergrund ist folgende Situation denkbar: Eine Person wird beim BfV als Anhänger einer zwar gegen den Gedanken der Völkerverständigung gerichteten, aber nicht militanten Organisation - z.B. als Verteiler von Flugblättern der Hizb ut-Tahrir (HuT) - gespeichert. Diese Person entwickelt sich über Jahre der „Reifung in der Parteikultur“ (so die Selbstdarstellung der „HuT“) vom Flugblattverteiler zum gewaltbereiten Islamisten und reist in der Absicht, aktiv am „Jihad“ teilzunehmen, von Deutschland aus in Richtung Tschetschenien. Nach dem Tod dieser Person im Rahmen von Kampfhandlungen in Tschetschenien und entsprechender Presseberichterstattung richten sich verschiedene Stellen an das BfV, um Informationen hinsichtlich der Vergangenheit dieser Person in Deutschland zu erhalten. Nach alter Rechtslage wäre ein Bezug zur Hizb ut-Tahrir nicht mehr herstellbar, wenn seit dem letzten Erkenntnisdatum (Flugblattverteilung) bereits mehr als zehn Jahre vergangen wären und der Datensatz des Betroffenen entsprechend gelöscht wurde.



Ein noch größeres Bedrohungspotenzial stellen Personen dar, die nach einer Teilnahme am „Jihad“ etwa in Tschetschenien oder dem Irak, nach Deutschland zurückkehren. Diese Personen sind hochradikalisiert, mit Hass erfüllt und im Untergrundkampf bereits erfahren. Bei einer nur 10-jährigen Speicherfrist von Daten zu solchen Personen könnten hier wichtige Erkenntnisse verloren gehen.

## **b) Schlussfolgerungen**

Die Regelung sollte beibehalten werden.

### **14. Spontanübermittlungen durch das Bundesamt für Migration und Flüchtlinge an das Bundesamt für Verfassungsschutz**

Artikel 1 Nr. 6 Buchstabe c Terrorismusbekämpfungsgesetz enthält mit dem neuen §18 Abs. 1a BVerfSchG eine spezielle Regelung für Übermittlungen, die das Bundesamt für Migration und Flüchtlinge (BAMF) an das BfV von sich aus (ohne Ersuchen, „spontan“) vornimmt. Zuvor war das BAMF gemäß § 18 Abs. 1 BVerfSchG bereits verpflichtet gewesen, von sich aus das BfV über Tatsachen zu unterrichten, die Spionage oder gewalttätigen Extremismus erkennen lassen. Diese Zusammenarbeitspflicht ist mit dem neuen Absatz 1a in Satz 1 erweitert worden, indem

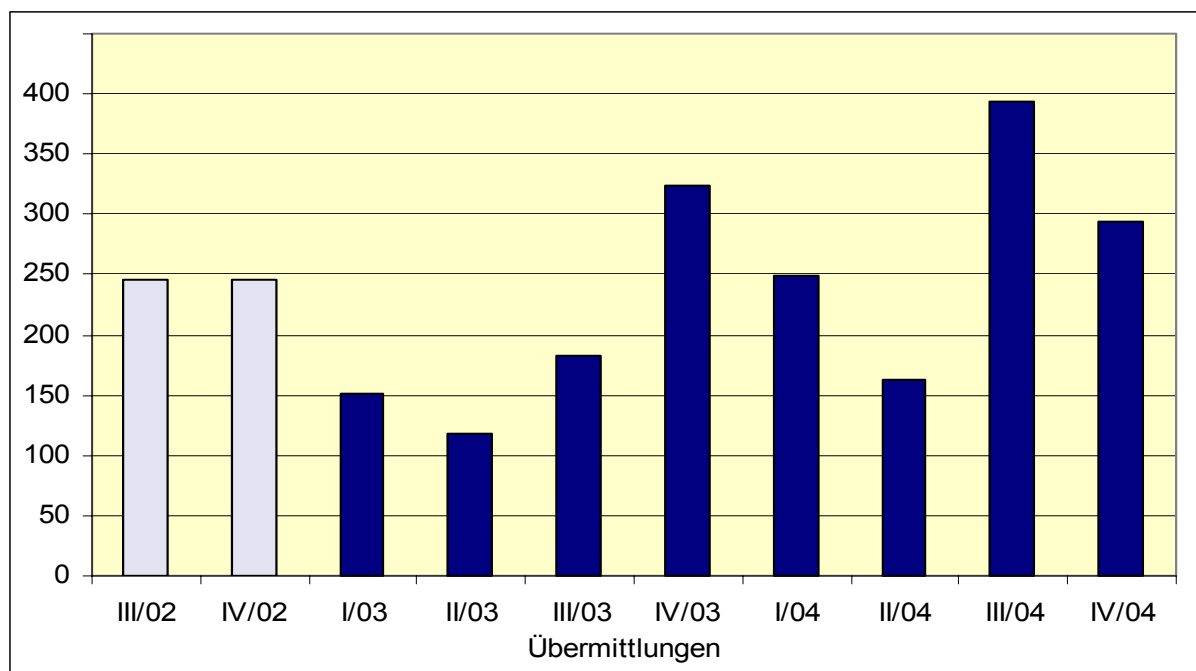
- für die Aufgaben der Extremismusbeobachtung die Einschränkung auf gewalttätige Bestrebungen entfällt und
- bereits tatsächliche Anhaltspunkte die Übermittlung veranlassen.

Satz 2 des neuen Absatzes enthält ein grundsätzliches Verbot der Weiterübermittlung an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen und lässt eine Ausnahme nur für den Fall zu, dass die Übermittlung völkerrechtlich geboten ist. Ohne diese Regelung wäre eine Weiterübermittlung nach § 19 Abs. 3 BVerfSchG für Aufgaben des BfV oder zur Wahrung erheblicher Sicherheitsinteressen des Empfängers zulässig, wenn keine auswärtigen Belange Deutschlands oder überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. Der wesentliche Unterschied besteht also darin, dass eine konkrete Abwägung, ob überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen, nicht erfolgt, sondern die Übermittlung generell unterbleibt (vorbehaltlich völkerrechtlicher Übermittlungsgebote).

**a) Auswertung**

Übermittlungen an das BfV

Für 2002/2003 liegen statistische Angaben vor, die jedoch nicht zwischen Ersuchens- und Spontanübermittlungen und nicht danach unterscheiden, ob die Übermittlung erst aufgrund der Regelungserweiterung erfolgt ist:



Quartal	III/02	IV/02	I/03	II/03	III/03	IV/03	I/04	II/04	III/04	IV/04
Übermittlungen (nach § 18 Abs. 1a und 3 BVerfSchG)	490 <sup>10</sup>		151	118	182	323	249	163	394	294

Der Rückgang der Meldungen im ersten Halbjahr 2003 ist auf die allgemeine Verringerung der Zahl der Asylantragsteller, mit dem Krieg im Irak und mit der Veränderung der Situation in Afghanistan zu erklären. Der Anstieg der Meldungen ab dem 3. Quartal 2003 dürfte auf die kontinuierliche Sensibilisierung der Einzelentscheider zurückzuführen sein. Daneben wurden in diesem Zeitraum auch erstmalig Erkenntnisse aus den verwaltungsgerichtlichen Verfahren statistisch erfasst. Die auffällig hohe Zahl im 4. Quartal 2003 beruht auch darauf, dass in diesem Zeitraum bereits zuvor erfolgte Meldungen statistisch nacherfasst wurden, die Zahl also nicht lediglich dieses Quartal abbildet. Das hohe Ergebnis des 3. Quartals 2004 dürfte einerseits mit einer Abarbeitung von Rückständen nach der Sommerpause, andererseits aber auch damit

<sup>10</sup> Die quartalsweise Erfassung ist erst ab 2003 erfolgt. In dem Diagramm ist die Gesamtzahl des zweiten Halbjahres 2002 auf die beiden Quartale hälftig verteilt aufgenommen.

zu erklären sein, dass die neuen Arbeitshilfen (näher unten) nunmehr in der Durchführungspraxis voll zum Tragen kommen. Letzteres wird von dem Ergebnis des 4. Quartals 2004 untermauert.

Seit 2004 werden die Übermittlungen und die anschließende Verwendung beim BfV differenzierter erfasst, wobei insbesondere auch danach unterschieden wird, ob die Daten hypothetisch bereits nach altem Recht gemäß § 18 Abs. 1 BVerfSchG übermittelt worden wären oder erst aufgrund der weiter gefassten Regelung des § 18 Abs. 1a BVerfSchG ohne Ersuchen zu übermitteln waren (Quasi-Vorher-Nachher-Vergleich zur Ermittlung des Mehrwerts des neuen § 18 Abs. 1a BVerfSchG):

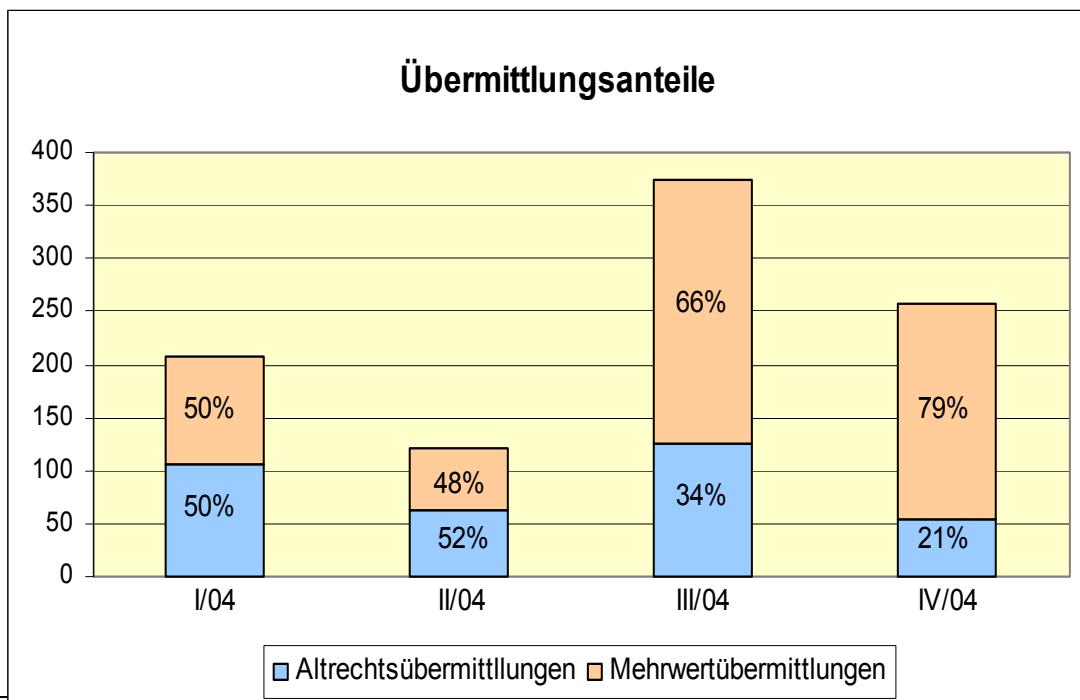
In 41 der 249 Fälle des ersten Quartals 2004 hat das BAMF auf Ersuchen übermittelt, in 208 Fällen von sich aus, wobei in 105 Fällen die Übermittlung auch nach altem Recht aufgrund § 18 Abs. 1 BVerfSchG erfolgt wäre, in 103 Fällen jedoch erst aufgrund der mit § 18 Abs. 1a BVerfSchG erweiterten Übermittlungspflicht. Die Fälle der Spontanübermittlungen sind durch die Rechtsänderung also um 98 % gesteigert worden. Die Zahlen im zweiten Quartal bestätigen den Erfolg: Von den 121 Spontanübermittlungen wären 63 auch nach altem Recht erfolgt, wohingegen 58 erst aufgrund der Rechtsänderung übermittelt worden sind (Mehrwert des § 18 Abs. 1a BVerfSchG: 92 %). Im dritten Quartal ist sogar noch ein deutlicherer Mehrwertzugewinn angefallen: Von den 374 Spontanübermittlungen wären lediglich 126 nach altem Recht erfolgt, das heißt die Rechtsänderung hat zu 248 zusätzlichen Übermittlungen geführt (Mehrwert: 197 %). Diese Steigerung dürfte darauf zurückzuführen sein, dass die neuen Arbeitshilfen (näher unten) nunmehr in der Durchführungspraxis voll zum Tragen kommen. Der sehr hohe „Mehrwert“-Anteil im vierten Quartal – 203 von 257 Spontanübermittlungen – dürfte dagegen eher auf eine geringe Fallzahl der nach altem Recht zu übermittelnden Sachverhalte zurückzuführen sein (nur 54): In absoluten Zahlen sind die „Mehrwertfälle“ gegenüber dem vorausgegangenen Quartal sogar gesunken (203 gegenüber zuvor 248; wobei die Übermittlungszahlen des dritten Quartals infolge Abarbeitung von Rückständen nach der Sommerpause insgesamt außergewöhnlich hoch lagen).

### Speicherung

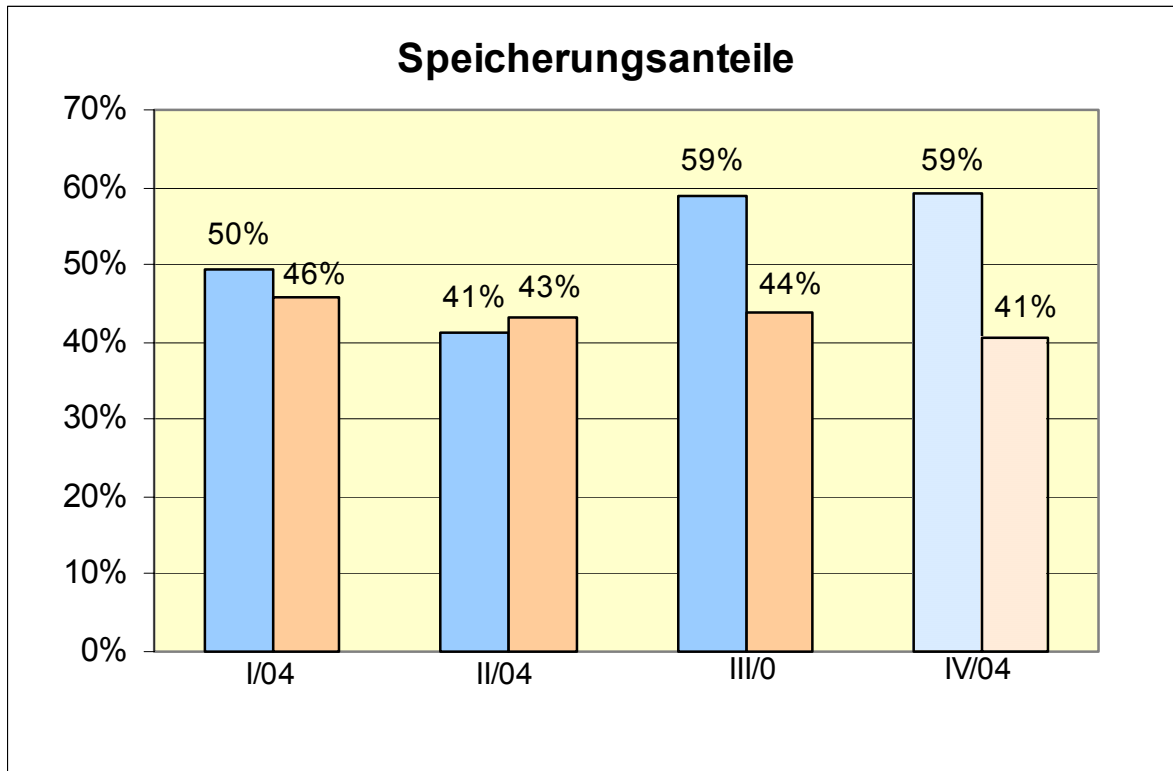
Im ersten Quartal 2004 haben von den 105 Fällen, die auch nach altem Recht übermittelt worden wären, 52 zu einer Speicherung beim BfV geführt (50 %; in 29 Fällen Ersterfassungen). Aus den 103 Fällen, die erst infolge der Rechtsänderung zu übermitteln waren, resultierten 47 Speicherungen (46 %; in 35 Fällen Ersterfassungen). Obgleich die Übermittlungsregelung des § 18 Abs. 1 BVerfSchG mit dem Tatsachen- und Gewaltkriterium deutlich umgrenzter ist als die neue Regelung, konnte die Quote

der Fälle, in denen die Übermittlungen der fachfremden Behörde für Aufgaben des Verfassungsschutzes im Ergebnis verwendbar sind, also erstaunlich hoch gehalten werden (46 % zu 50 %). Die nachfolgenden Quartale mit etwa gleich hohen Speicherquoten bei den zusätzlichen Übermittlungen (jeweils über 40%) bestätigen die kontinuierliche Relevanz des Zusatzaufkommens.

Quartal	I / 04	II / 04	III / 04	IV / 04 <sup>11</sup>
Spontanübermittlungen insgesamt, davon	208	121	374	257 ausgewertet: 238
○ „Altrechtsübermittlungen“	105	63	126	54 ausgewertet: 49
○ „Mehrwertübermittlungen“	103	58	248	203 ausgewertet: 189
Übermittlungsmehrwert des neuen Rechts	98%	92%	197%	376%
Speicherung bei				ausgewertet:
○ „Altrechtsübermittlungen“	52	26	74	29
○ „Mehrwertübermittlungen“	47	25	109	ausgewertet: 78
Speicheranteil bei				ausgewertet:
○ „Altrechtsübermittlungen“	50%	41%	59%	59 %
○ „Mehrwertübermittlungen“	46%	43%	44%	ausgewertet: 41%



<sup>11</sup> Bis zum Stichtag 31. Dezember 2004 waren die im letzten Quartal übermittelten Erkenntnisse beim BfV noch nicht vollständig ausgewertet.



Der eher überraschende Befund, dass trotz des offeneren Übermittlungstatbestandes ein kontinuierlich hoher Erkenntnisnutzen zu erzielen war, ist auch nicht mit einer generell eher restriktiven Übermittlungspraxis zu erklären, wie die absoluten Zahlen und die Relation von Übermittlungen nach altem und neuem Recht ausweisen. Dies spricht für die Bedeutung und Qualität der ergriffenen durchführungssichernden Maßnahmen. Im Vordergrund stehen dabei Maßnahmen, die die gesetzlichen Übermittlungsvoraussetzungen (tatsächliche Anhaltspunkte für extremistische Bestrebungen bzw. Spionage) für die im BAMF befassten Mitarbeiter handhabbar machen sollen.

#### Durchführungssicherung

Zunächst wurde Ende Mai 2002 die einschlägige Dienstanweisung aktualisiert und zusammen mit Kriterienkatalogen des BfV den Einzelentscheidern zur Verfügung gestellt. Die Kriterienkataloge beinhalten sämtliche im Verfassungsschutzbericht 2002 erwähnten extremistischen Organisationen. Ergänzend haben die Außenstellen Auswertungen der Verfassungsschutzberichte 2001 und 2002 erhalten. Zum 01.03.2004 ist eine neue Dienstanweisung (DA-EE-Sicherheit) mit aktualisierten Kriterienkatalogen von BfV und BND in Kraft getreten. Bei der halbjährlichen Kriterienaktualisierung werden auch Rückmeldungen aus der Anwendungspraxis zur Handhabbarkeit berücksichtigt.

Im Zeitraum Juli 2002 bis April 2003 wurden Informationsveranstaltungen zur Sensibilisierung der Mitarbeiter im Hinblick auf die Übermittlungspflichten durchgeführt. Die am 01.03.04 in Kraft getretene DA-EE-Sicherheit wurde im Zeitraum Januar bis April 2004 in Informationsveranstaltungen erläutert. Auch künftig sind neben der periodischen Anpassung der Kriterienkataloge laufende Schulungen vorgesehen, um auf jeweils aktuelle Aspekte der Bekämpfung des islamistischen Terrorismus und Fragen der Einzelentscheider einzugehen.

Im BAMF ist ein Fachreferat als zentrale Organisationseinheit für die Koordination der Zusammenarbeit mit dem BfV zuständig. Dies gewährleistet eine einheitliche Verfahrensweise der Informationsweitergabe, auch durch laufende Rückkopplung mit dem Verfahrensbereich (Referatsleiter, Einzelentscheider, Prozess-Bereich der Außenstellen). Zugleich besteht damit ein zentraler Ansprechpartner für die Außenstellen.

#### Weiterübermittlung an auswärtige öffentliche Stellen

Seit dem ersten Quartal 2004 werden die vom Gesetzgeber als besonders sensibel angesehenen Weiterübermittlungen nach § 18 Abs. 1a Satz 2 i.V.m § 19 Abs. 3 BVerfSchG statistisch erfasst. Bislang sind keine solchen Weiterübermittlungen erfolgt.

#### **b) Schlussfolgerungen**

Die erweiterte Spontanübermittlungspflicht hat das relevante Informationsaufkommen wesentlich verbessert. Die praxisbewährte Regelung sollte beibehalten werden.

Die Evaluierung gibt keinen Anlass, die Übermittlungsbeschränkungen in Frage zu stellen.

Unabhängig davon könnte überprüft werden, ob in Fällen, in denen überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen, eine Weiterübermittlung zugelassen werden sollte, wenn sie zum Schutz zentraler deutscher Sicherheitsinteressen oder entsprechender Sicherheitsinteressen eines Partnerstaates erforderlich ist.

## 15. Spontanübermittlungen durch Ausländerbehörden an Landesverfassungsschutzbehörden

Mit dem neuen § 18 Abs. 1a BVerfSchG ist ergänzend zu der Regelung von Spontanübermittlungen des BAMF an das BfV zugleich eine inhaltlich parallele Übermittlungspflicht der Ausländerbehörden an die Landesverfassungsschutzbehörden bundesgesetzlich eingeführt worden. Die Gesetzesfolgen wurden an zwei Landesstichproben untersucht. Dazu wurden Nordrhein-Westfalen als bevölkerungsreichster Flächenstaat und Berlin als Stadtstaat (mit einer Konzentration von Zielobjekten für fremde Geheimdienste oder terroristische Anschläge) gebeten, ihre Durchführungspraxis unter bestimmten Fragestellungen auszuwerten.

### a) Auswertung

#### Nordrhein-Westfalen

In Nordrhein-Westfalen sind Übermittlungen nach § 16 Abs. 1 Satz 2 VSG-NRW (entspricht § 18 Abs. 1a Satz 1 BVerfSchG) ab dem vierten Quartal 2003 erfasst worden. Ab dem zweiten Quartal wurden auch resultierende Speicherungen in der Amtsdatei des Verfassungsschutzes erfasst. Dabei ergaben sich folgende Zahlen:

Quartal	IV/03	I/04	II/04	III/04	IV/04
Übermittlungen	16	14	14	9	3
Speicherungen	k.A.	k.A.	6 (43 %)	6 (67 %)	1 (33 %)

Angesichts der geringen Grundgesamtheit sind die Speicheranteile allerdings jeweils nur begrenzt aussagekräftig.

Bereits vor Inkrafttreten des § 18 Abs. 1a BVerfSchG bestand landesrechtlich eine entsprechende Übermittlungsbefugnis. Inwieweit die Verdichtung zur Übermittlungspflicht zu einer Veränderung des Mitteilungsverhaltens geführt hat, ließ sich nicht konkret untersuchen, da zum alten Recht keine Übermittlungsstatistik geführt worden war. Allerdings hat das Land mitgeteilt, es habe sich der Eindruck verfestigt, dass die Rechtsänderung zur Sensibilisierung der Ausländerbehörden beigetragen hat. Dazu hat speziell ein Erlass vom 29. August 2003 beigetragen, mit dem das Landesinnenministerium den Ausländerbehörden unter anderem die Informationspflichten erläutert und mit einem Merkblatt Anhaltspunkte und Auffälligkeiten darstellt, die womöglich eine Übermittlung veranlassen.

Weiterübermittlungen an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen nach § 17 Abs. 3 VSG-NRW sind bislang nicht erfolgt und auch für die Zukunft kaum zu erwarten, da die Zusammenarbeit mit auswärtigen Stellen im Verfassungsschutzverbund grundsätzlich über das BfV erfolgt.

### Berlin

Für Berlin ergeben sich bei der Durchführung des § 18 Abs. 1a BVerfSchG bislang folgende Ergebnisse:

Quartal	bis 2004	I/04	II/04	III/04	IV/04
Übermittlungen	0	2	0	2	0
Speicherungen	0	0	0	0	0

Das Land hatte zunächst keine begleitenden Maßnahmen zur Umsetzung der neuen Übermittlungsregelung getroffen. Während des Evaluierungsdialogs hat es eine gemeinsame ganztägige Informationsveranstaltung für die Berliner Ausländerbehörde angekündigt. Das Land erwartet, dass sich mit der resultierenden Sensibilisierung der Mitarbeiter der Berliner Ausländerbehörde die Anzahl der Spontanübermittlungen nach § 18 Abs. 1a BVerfSchG erhöhen wird.

Eine Weiterübermittlung an auswärtige öffentliche Stellen ist nicht erfolgt.

### **b) Schlussfolgerungen**

Die sehr begrenzte Datenbasis lässt nur sehr zurückhaltende Aussagen zu. Ein unmittelbarer Vergleich zu den deutlich höheren Übermittlungszahlen des BAMF ist nicht aussagekräftig, da bereits nach betroffenem Personenkreis und unterschiedlichen behördlichen Aufgaben nachvollziehbar ist, wenn beim BAMF in höherem Maße verfassungsschutzrelevante Informationen anfallen.

Allerdings spricht einiges dafür, dass der praktische Mehrwert der neuen Regelung wesentlich auch von ergänzenden untergesetzlichen Maßnahmen abhängt, da den Normadressaten des § 18 Abs. 1a BVerfSchG in den Ausländerbehörden der für sie fachfremde Übermittlungstatbestand angemessen erläutert werden muss, um eine effektive Gesetzesdurchführung zu gewährleisten. Aus Sicht des Bundes sprechen dafür auch die guten Erfahrungen im Bereich des BAMF mit durchführungssichernden Maßnahmen, wie Dienstanweisungen/Merkblättern und Informationsveranstaltungen.



Vor dem Hintergrund der Erfahrungen mit der Landesstichprobe Nordrhein-Westfalen/Berlin hat das Bundesministerium des Innern im April 2004 sämtliche Länder um Informationen zur Durchführung des § 18 Abs. 1a BVerfSchG in ihrem Bereich gebeten. Die Antworten waren nur begrenzt aussagekräftig, teils mangels entsprechender Statistiken, teils wegen geringen Ausländeranteils in der Bevölkerung (Beitrittsgebiet). Tendenziell werden jedoch einerseits geringe Anwendungszahlen, andererseits Optimierungspotenzial im Bereich begleitender Durchführungsmaßnahmen bestätigt. Der Bund hat seine positiven Erfahrungen mit solchen begleitenden Maßnahmen dargestellt. Im Übrigen ist im Rahmen der Innenministerkonferenz eine Arbeitsgruppe eingerichtet worden, die unter anderem dem Erfahrungsaustausch auf dem Gebiet ganzheitlicher Terrorismusbekämpfung dient.

#### **16. Weiterübermittlung der Spontanübermittlungen des Bundesamtes für Migration und Flüchtlinge durch den Militärischen Abschirmdienst und den Bundesnachrichtendienst**

Mit Artikel 2 Nr. 5 ist im MADG eine Regelung (§ 11 Abs. 1 Satz 3) aufgenommen worden, wonach solche Daten, die die Verfassungsschutzbehörden nach § 18 Abs. 1a BVerfSchG erlangt und an den MAD weiter übermittelt haben, auch vom MAD gemäß § 18 Abs. 1a Satz 2 BVerfSchG grundsätzlich – vorbehaltlich völkerrechtlicher Gebote – nicht an auswärtige öffentliche Stellen übermittelt werden dürfen. Eine entsprechende Verlängerung des Weiterübermittlungsverbots gilt auch für den BND nach § 9 Abs. 2 Satz 2 BNDG, angefügt durch Artikel 3 Nr. 3 Terrorismusbekämpfungsgesetz.

MAD und BND haben bislang von Verfassungsschutzbehörden keine Daten übermittelt erhalten, die die Verfassungsschutzbehörden ihrerseits nach § 18 Abs. 1a BVerfSchG erlangt hatten. Insoweit ist bislang keine auswertbare Gesetzespraxis angefallen.

Dies spricht allerdings noch nicht gegen die Beibehaltung der Regelung. Wenn der Gesetzgeber an seiner mit § 18 Abs. 1a Satz 2 BVerfSchG zunächst vorläufig – befristet – getroffenen Entscheidung festhält, bliebe es konsequent, auch an dem entsprechenden Weiterübermittlungsverbot für MAD und BND festzuhalten, auch wenn der Anwendungsfall des Verbotes nur sehr selten auftreten sollte.

## **17. Übermittlung zur Gewährleistung der Sicherheit von lebens- oder verteidigungswichtigen Einrichtungen**

Mit Artikel 1 Nr. 7 Terrorismusbekämpfungsgesetz ist die Befugnis des BfV erweitert worden, personenbezogene Daten auch an Private zu übermitteln (von § 19 Abs. 4 Satz 1 BVerfSchG n.F.). Dies ist jetzt auch zulässig, wenn es erforderlich ist zur Gewährleistung der Sicherheit von lebens- oder verteidigungswichtigen Einrichtungen (im Sinne von § 1 Abs. 4 Sicherheitsüberprüfungsgesetz). Dadurch sollen die betreffenden Einrichtungen die Möglichkeit erhalten, angemessen auf die von einzelnen Mitarbeitern ausgehenden Gefährdungen zu reagieren (BT-Drs. 14/7864, S. 4f.). Für den engeren Bereich der sicherheitsempfindlichen Stellen wird dies durch das Erfordernis von Sicherheitsüberprüfungen gewährleistet (§ 1 Abs. 4 SÜG). Auch im Übrigen können aber von Mitarbeitern unter Umständen besondere Sabotagegefahren ausgehen.

Von der Befugnis hat das BfV bislang lediglich in einem Fall Gebrauch gemacht. Empfänger war der Sicherheitsbeauftragte einer Firma aus dem u.a. militärtechnischen Entwicklungsbereich. Die Informationen betrafen Erkenntnisse über das Engagement eines Mitarbeiters dieser Firma in einer islamistischen Organisation. Der Sicherheitsbeauftragte sicherte zu, dies bei der zukünftigen Personaleinplanung präventiv zu berücksichtigen.

Auch für die Zukunft ist zu erwarten, dass – in begrenztem Umfang – Bedarfsfälle auftreten. Die Regelung sollte deshalb beibehalten werden, um neben dem engeren Schutz sicherheitsempfindlicher Stellen auch im Übrigen zur Vorbeugung von Sabotagerisiken bei lebens- oder verteidigungswichtigen Einrichtungen beizutragen.

## **18. Übermittlung an Private durch den Militärischen Abschirmdienst**

Mit Artikel 2 Nr. 5 Terrorismusbekämpfungsgesetz ist die bisherige Verweisung in § 11 Abs. 1 Satz 1 MADG auf die Übermittlungsvorschriften in § 19 BVerfSchG nunmehr auch auf dessen Absatz 4 – Übermittlung an Private – erstreckt worden. Hintergrund ist insbesondere die Privatisierung von Teilen der Wehrverwaltung im Zuge der Bundeswehrreform (BT-Drs. 14/7386, S. 42).

Der MAD hat von dieser Befugnis bislang keinen Gebrauch gemacht.

Gleichwohl sollte die Regelung unter den Erwägungen, die ihr zugrunde liegen, beibehalten bleiben. Dabei bleibt insbesondere durch das Erfordernis einer Zustimmung

des BMVg (§ 11 Abs. 1 Satz 2 MADG) gewährleistet, dass auch künftig keine unangemessenen Übermittlungen an Private erfolgen.

## 19. Mitteilung an Betroffenen von einer Übermittlung an Private

Mit Artikel 1 Nr. 7 ist in § 19 Abs. 4 BVerfSchG eine ergänzende Regelung für den Fall aufgenommen worden, dass das BfV „anderen Stellen“ (gemeint sind im Ergebnis Private bzw. nicht-öffentliche Stellen) personenbezogene Daten übermittelt hat. Nach dem neuen Satz 7 muss das BfV dem Betroffenen diese Übermittlung mitteilen, sobald eine Gefährdung seiner Aufgabenerfüllung durch die Mitteilung nicht mehr zu besorgen ist.

Bislang sind solche Mitteilungen noch nicht erfolgt.

Der Regelungszweck, Betroffene über die Übermittlung zu informieren, wurde bislang nicht erreicht. Angesichts der gesetzlichen Voraussetzung, dass dabei der Auskunftszweck nicht gefährdet werden darf, überrascht das Ergebnis im Hinblick auf die kurze Normanwendungsdauer nicht, da mit der Mitteilung zugleich offen gelegt wird, dass das BfV personenbezogene Daten zum Betroffenen gespeichert hat. Die Evaluierung hat insoweit keinen Änderungsbedarf ergeben.

## 20. Ausschluss der Übermittlungsregelungen für die Fälle „bei Erhebung“

Datenübermittlungen erfolgen auch zur Durchführung einer Datenerhebung, z.B. wenn einer Auskunftsperson Identifizierungsangaben zu der Person gemacht werden, zu der Auskunft gewünscht ist. Spezielle Regelungen zu diesem Sachverhalt trifft das BVerfSchG wegen des spezifischen Sachzusammenhangs bei den Erhebungsvorschriften mit § 8 Abs. 1 Satz 2 und 3 (vgl. C.I.2). Ergänzend ist mit Artikel 1 Nr. 7 Terrorismusbekämpfungsgesetz in der Vorschrift zu Übermittlungen an Private bzw. nicht-öffentliche Stellen (§ 19 Abs. 4 BVerfSchG) eine Bestimmung eingefügt worden (neuer Satz 8), wonach § 19 Abs. 4 Sätze 2 und 3 BVerfSchG – Erfordernis der Zustimmung des Bundesministeriums des Innern und besondere Übermittlungsdokumentation – auf den Erhebungssachverhalt keine Anwendung finden. Hintergrund dieser Regelung war, dass zur Anwendbarkeit dieser Vorschriften auf den Erhebungssachverhalt zuvor Meinungsunterschiede bestanden (vgl. BT-Drs. 14/7386, S. 39 [zu § 8 Abs. 1]), die mit einer klarstellenden Regelung ausgeräumt werden sollten.

Die getroffene Regelung ist unter dem Zeitdruck des Entwurfsverfahrens zum Terrorismusbekämpfungsgesetz allerdings redaktionell verfehlt gefasst worden, da der Eindruck entsteht, die übrigen nicht angeführten Sätze des § 19 Abs. 4 BVerfSchG seien – im Umkehrschluss – anwendbar. Dies war jedoch bereits vor der Anfügung des neuen Satzes 8 nicht der Fall und sollte mit dessen Anfügung auch nicht geändert werden.

Beispielsweise ist bei den Übermittlungszwecken nach § 19 Abs. 4 Satz 1 BVerfSchG nicht der Beobachtungsbereich nach § 3 Abs. 1 Nr. 3 BVerfSchG aufgeführt (gewalttätige Bestrebungen, die auswärtige Belange gefährden). Wäre § 19 Abs. 4 Satz 1 BVerfSchG auch auf Erhebungssachverhalte anwendbar, hätte das z.B. die absurde Konsequenz, dass in diesem Aufgabengebiet einer Auskunftsperson nicht mitgeteilt werden dürfte, zu welcher Zielperson sie Auskunft geben soll. Bei Anwendung des § 19 Abs. 4 Satz 6 BVerfSchG müsste auch bei der Informationsbeschaffung unter Legende gleichwohl ein Zweckbindungshinweis erfolgen.

Wäre die Mitteilungspflicht aus § 19 Abs. 1 Satz 7 BVerfSchG auf den Erhebungssachverhalt anwendbar, müsste einer nachrichtendienstlichen Zielperson danach grundsätzlich mitgeteilt werden, dass und wem ihre Daten (zum Zwecke der Auskunftseinholung) übermittelt worden sind. Danach wäre Quellenschutz ausgerechnet gegenüber Extremisten und Spionen grundsätzlich unzulässig. Auch wenn die Mitteilung erst zu erfolgen hätte, sobald dadurch keine Aufgaben gefährdet werden, wäre gleichwohl zu besorgen, dass Auskunftspersonen einer Zusammenarbeit mit dem BfV reserviert bis ablehnend gegenüberstehen, da sie befürchten müssten, dass ihre Befragung dem Betroffenen bekannt wird. Der Erfolg nachrichtendienstlicher Arbeit hängt in diesem Bereich wesentlich vom Vertrauen der befragten Personen in die vertrauliche Behandlung der Angelegenheit durch das BfV ab.

Dass § 19 Abs. 4 Satz 8 BVerfSchG nur einzelne Sätze des Absatzes 4 für den Erhebungssachverhalt von der Anwendung ausnimmt, kann daher verständigerweise nur als eine Klarstellung zu diesen, zuvor strittigen Regelungen verstanden werden, die aber nichts daran ändern sollte, dass Absatz 4 hier auch im Übrigen unanwendbar ist. Diese Klarstellung ist wegen des möglichen Umkehrschlusses jedoch redaktionell verunglückt. Dieses Versehen sollte durch eine eindeutige Regelung behoben werden.

## **II. Artikel 10-Gesetz – G 10 – (Artikel 4 Terrorismusbekämpfungsgesetz)**

Bei den Änderungen handelt es sich um bloße Folgeänderungen.

- In Artikel 4 Nr. 1 Terrorismusbekämpfungsgesetz wird die Änderung in Artikel 1 Nr. 1 Buchstabe a (Einfügung einer Nummer 4 in § 3 Abs. 1 BVerfSchG) nachvollzogen, indem die Verweisung in § 7 Abs. 2 Nr. 1 G 10 auf § 3 Abs. 1 BVerfSchG entsprechend ergänzt wird. Dabei regelt § 7 Abs. 2 Nr. 1 G 10 die Weitergabe von Erkenntnissen aus der strategischen Fernmeldeüberwachung des BND für sämtliche Aufgaben des BfV mit Ausnahme der Spionageabwehr, die in § 7 Abs. 2 Nr. 2 G 10 gesondert geregelt ist. Dass die spezielle Aufgabe nach § 3 Abs. 1 Nr. 4 BVerfSchG (völkerverständigungswidrige Bestrebungen) dabei sachlich in den Zusammenhang der Extremismusbeobachtung und nicht in den Zusammenhang der Spionageabwehr gehört, erschließt sich ohne weiteres.

Eine Befristung der Änderung war - als Folgeänderung zu einer befristeten Regelung - gleichwohl geboten, da bei einem Wegfall von § 3 Abs. 1 Nr. 4 BVerfSchG auch § 7 Abs. 2 Nr. 1 G 10 in der früheren Fassung aufleben müsste. Für eine isolierte Evaluierung der Folgeänderung ergibt sich daraus aber kein Bedarf. Die Übermittlungsregelung ist in der Praxis maßvoll angewendet worden. Näheres kann indes nicht öffentlich mitgeteilt werden, da Angaben zur Verwendung der übermittelten Erkenntnisse durch das BfV dessen Arbeitsmethoden offen legen würden, was aus zwingenden Gründen des Geheimnisses nicht in Betracht kommt. Übermittlungen nach § 7 Abs. 2 Nr. 1 G 10 unterliegen jedoch der Kontrolle der G 10-Kommission nach § 15 Abs. 5 G 10.

Da § 3 Abs. 1 Nr. 4 BVerfSchG beibehalten werden sollte, sollte ebenso § 7 Abs. 2 Nr. 1 G 10 in der angepassten Fassung fortgelten.

- Artikel 4 Nr. 2 Terrorismusbekämpfungsgesetz (Änderung der Bußgeldrahmenvorschrift in § 19 Abs. 2 G 10) betrifft lediglich die Währungsumstellung von DM auf Euro, wobei der Bußgeldrahmen geglättet wird. Die Regelung sollte mithin beibehalten werden.

### **III. Sicherheitsüberprüfungsgesetz (Artikel 5 Terrorismusbekämpfungsgesetz)**

Mit Artikel 5 Terrorismusbekämpfungsgesetz ist das Sicherheitsüberprüfungsgesetz (SÜG), das zuvor nur den vorbeugenden personellen Geheimschutz geregelt hat, um den vorbeugenden personellen Sabotageschutz erweitert worden. Hiernach werden Personen, die an sicherheitsempfindlichen Stellen von lebens- oder verteidigungs-

wichtigen Einrichtungen<sup>12</sup> beschäftigt sind, auf Sicherheitsrisiken überprüft, um einer Sabotage durch „Innentäter“ vorzubeugen.<sup>13</sup>

Das vom Gesetzgeber aufgegriffene Instrument der Sicherheitsüberprüfung wird beim Geheimschutz zur Klärung personeller Risiken seit Jahrzehnten eingesetzt. Zum Sabotagesschutz wird die unterste Stufe („einfache Sicherheitsüberprüfung“) durchgeführt, die standardmäßig lediglich eine Sicherheitserklärung des Betroffenen und Abfragen vorhandener Erkenntnisse beim Bundeszentralregister und den Sicherheitsbehörden vorsieht. Diese Informationen werden von der mitwirkenden Behörde – BfV bzw. MAD – bewertet. Falls die mitwirkende Behörde zu der Einschätzung eines Sicherheitsrisikos gelangt, teilt sie dies dem zuständigen Geheimschutzbeauftragten der Beschäftigungsbehörde bzw. – im nicht-öffentlichen Bereich – dem zuständigen Bundesministerium mit, die darüber entscheiden, ob ein Sicherheitsrisiko vorliegt, das der sicherheitsempfindlichen Tätigkeit des Betroffenen entgegensteht. Auch sonstige sicherheitserhebliche Erkenntnisse unter der Schwelle eines Sicherheitsrisikos werden mitgeteilt, um der Entwicklung von Sicherheitsrisiken vorzubeugen.

Mit dem bestehenden Verfahren nach dem SÜG wird dessen hoher Datenschutzstandard übernommen, insbesondere strenge Zweckbindungen (die auch durch besondere organisatorische Vorkehrungen zu gewährleisten sind) sowie Transparenz für die Betroffenen, einschließlich Auskunftsrechten gegenüber den beteiligten Stellen.

---

<sup>12</sup> Definiert in § 1 Abs. 5 SÜG:

„Lebenswichtig sind solche Einrichtungen,

1. deren Beeinträchtigung auf Grund der ihnen anhaftenden betrieblichen Eigengefahr die Gesundheit oder das Leben großer Teile der Bevölkerung erheblich gefährden kann oder
2. die für das Funktionieren des Gemeinwesens unverzichtbar sind und deren Beeinträchtigung erhebliche Unruhe in großen Teilen der Bevölkerung und somit Gefahren für die öffentliche Sicherheit oder Ordnung entstehen lassen würde.

Verteidigungswichtig sind außerhalb des Geschäftsbereiches des Bundesministeriums der Verteidigung solche Einrichtungen, die der Herstellung oder Erhaltung der Verteidigungsbereitschaft dienen und deren Beeinträchtigung auf Grund

1. fehlender kurzfristiger Ersetzbarkeit die Funktionsfähigkeit, insbesondere die Ausrüstung, Führung und Unterstützung der Bundeswehr und verbündeter Streitkräfte sowie der Zivilen Verteidigung, oder
2. der ihnen anhaftenden betrieblichen Eigengefahr die Gesundheit oder das Leben großer Teile der Bevölkerung

erheblich gefährden kann. Sicherheitsempfindliche Stelle ist die kleinste selbständig handelnde Organisationseinheit innerhalb einer lebens- oder verteidigungswichtigen Einrichtung, die vor unberechtigtem Zugang geschützt ist und von der im Falle der Beeinträchtigung eine erhebliche Gefahr für die in den Sätzen 1 und 2 genannten Schutzgüter ausgeht.“

Die Feststellung der betreffenden Einrichtungen ist durch die Sicherheitsüberprüfungsfeststellungsverordnung vom 30. Juli 2003 (BGBl I, S. 1553) erfolgt.

<sup>13</sup> Gesetzesbegründung BT-Drs.14/7386, S. 37 und 43

## 1. **Durchführungspraxis** (ergänzende Angaben im Anhang<sup>14</sup>)

Die weitaus größte Zahl von Sicherheitsüberprüfungen sind zu Militärischen Sicherheitsbereichen durchgeführt worden. Ein Grund hierfür ist, dass diese Bereiche bereits bei Aufnahme des vorbeugenden personellen Sabotageschutzes fest umrissen waren und zudem weitgehend als sicherheitsempfindlich einzustufen sind. Für die nicht-militärischen Bereiche war zunächst die Festlegung der lebens- oder verteidigungswichtigen Einrichtungen erforderlich, was durch die am 9. August 2003 in Kraft getretene Sicherheitsüberprüfungsfeststellungsverordnung (SÜFV)<sup>15</sup> erfolgt ist. In einem weiteren Schritt waren sodann die sicherheitsempfindlichen Stellen dieser Einrichtungen zu bestimmen. Entsprechend kürzer ist der faktische Durchführungszeitraum der neuen Regelungen in den nicht-militärischen Bereichen.

Relativ hohe Fallzahlen sind dort bisher im Bereich des Bundesministeriums für Wirtschaft und Arbeit nach § 7 SÜFV festzustellen. Sie spiegeln den Überprüfungsbedarf im IT-Bereich der Bundesagentur für Arbeit (BA) wider. Die Bearbeitung und Auszahlung der unterhaltssichernden Leistungen – die für zahlreiche Familien und Einzelpersonen die Existenzgrundlage bilden – erfolgen über ein ausgedehntes effizientes Netzwerk, das die nachgeordneten Dienststellen der BA mit der Bundesagentur in Nürnberg verbindet. Die Komplexität des IT-Systems und seine technische Ausgestaltung bedingt den Einsatz einer entsprechenden Zahl von in die Überprüfung einzubeziehenden Fachkräften. Gemessen an der Gesamtzahl der Beschäftigten bei der BA relativiert sich diese Zahl. Der Anteil des in diesem Zusammenhang sicherheitsüberprüften Personals beträgt etwa 2% der Beschäftigten.

Im nichtöffentlichen Bereich sind Sicherheitsüberprüfungen bislang nur in der Zuständigkeit des Bundesministeriums für Wirtschaft und Arbeit (§ 10 SÜFV) durchgeführt worden. Beim Bundesministerium für Verkehr, Bau- und Wohnungswesen (§ 11 SÜFV) wurden im Berichtszeitraum dagegen noch keine Anträge bearbeitet. Die vorgesehene Liste der gefährlichen Güter mit hohem Gefahrpotenzial konnte erst nach der Umsetzung der in der 13. Ausgabe der UN-Modellvorschriften enthaltenen Festlegung solcher Güter und Regeln zu ihrer Sicherung in die Vorschriften für die europäischen Landverkehrsträger bekannt gemacht werden<sup>16</sup>. Dadurch wurden Divergenzen zwischen den auf internationaler und europäischer Ebene erarbeiteten neuen Sicherungsanforderungen im Gefahrgutbereich und den Anforderungen des vorbeu-

---

<sup>14</sup> Die im Anhang aufgenommenen Angaben könnten von terroristischen Tätern oder gegnerischen Nachrichtendiensten bei Anschlagplanungen zu Risikoabschätzung herangezogen werden. Sie sind daher als „Verschlussache – Nur für den Dienstgebrauch eingestuft“ und – um eine Einstufung des Berichts im Übrigen zu vermeiden – in einen Anhang ausgegliedert.

<sup>15</sup> BGBl I, S. 1553

<sup>16</sup> Liste vom 10. September 2004, Verkehrsblatt vom 15. September 2004, Seite 459

genden personellen Sabotageschutzes vermieden. Die Einführung der neuen Sicherungsanforderungen in das deutsche Recht erfolgte mit der 17. ADR-Änderungsverordnung vom 27. August 2004<sup>17</sup> sowie der 12. RID-Änderungsverordnung vom 28. September 2004<sup>18</sup>. Die Regelungen sind seit dem 1. Januar 2005 in Kraft. Erst seit der Veröffentlichung der Liste und der Verkündung der Vorschriften über die Sicherung ist eine abschließende Bestimmung des zu überprüfenden Personenkreises möglich und konnten sich die Unternehmen auf die Pflicht zur Überprüfung ihrer Mitarbeiter vorbereiten. Daher ist ein entsprechender Antragseingang erst seit Anfang des Jahres 2005 zu verzeichnen.

## **2. Erfolgsbewertung**

### **a) Öffentlicher Bereich**

Der Vollzug des vorbeugenden personellen Sabotageschutzes im öffentlichen Bereich verläuft ohne Schwierigkeiten. Umsetzungshindernisse sind bisher nicht bekannt geworden. Die Fallzahlen lassen Rückschlüsse auf die Tauglichkeit des Instruments der Sicherheitsüberprüfung und somit auch des Instituts des vorbeugenden personellen Sabotageschutzes zu: Es fielen nicht nur in Einzelfällen sicherheits-erhebliche Erkenntnisse an. Darüber hinaus wurden auch in einer Reihe von Fällen Sicherheitsrisiken festgestellt.

Erwartungsgemäß betrifft dies nur einen relativ sehr kleinen Teil der überprüften Beschäftigten, da von den Beschäftigten ganz überwiegend keine Sabotagerisiken ausgehen; der geringe Anteil von Negativ-Voten ist also eher ein Beleg dafür, dass die mitwirkenden Behörden mit der erforderlichen Sorgfalt bei der Erstellung von Voten verfahren. Es ist dabei allerdings wichtig, den relativ kleinen Kreis potenzieller Innentäter von Stellen fern zu halten, an denen Gesundheit oder Leben großer Teile der Bevölkerung erheblich gefährdet werden kann, die für das Funktionieren des Gemeinwesens unverzichtbar sind oder an denen die Verteidigungsbereitschaft erheblich gefährdet werden kann. Im Übrigen ist davon auszugehen, dass die Einführung der Überprüfungsverfahren potenzielle Innentäter bereits davon abhält, sich um eine Verwendung an sicherheitsempfindlichen Stellen zu bewerben, so dass der Erfolg des Instruments sich nicht erst in durchgeführten Überprüfungen niederschlägt.

---

<sup>17</sup> BGBl. II S. 1274

<sup>18</sup> BGBl. II S.1434



## b) Nichtöffentlicher Bereich

Auch im nichtöffentlichen Bereich zeigt sich anhand der bisher festgestellten Erkenntnisfälle, dass das Instrument der Sicherheitsüberprüfung geeignet ist, Personen festzustellen, die nicht mit sicherheitsempfindlichen Tätigkeiten betraut werden dürfen. Hier ist bislang der Anteil von Erkenntnisfällen und festgestellten Sicherheitsrisiken sogar deutlich höher als im öffentlichen Bereich. Dies kann jedoch auch auf Verzerrungseffekten beruhen, die womöglich aus der begrenzten, selektiven Durchführung von Sicherheitsüberprüfungen im nichtöffentlichen Bereich resultieren.

In der Startphase verlief die Antragstellung im nichtöffentlichen Bereich allerdings eher schleppend. Die Zahl der Anträge und Überprüfungen bleibt hinter den Erwartungen zurück. Aus diesem Grund wurde unter Leitung des Bundesministeriums des Innern im Juli 2004 ein Gespräch mit den Vertretern der Verbände betroffener Unternehmen geführt. Die Anhörung der Verbände hat gezeigt, dass es keine grundsätzliche Ablehnung des Instituts der Sicherheitsüberprüfungen gibt; die Erforderlichkeit wurde mehrfach betont. Die Vertreter der Verbände legten aus ihrer Sicht die Ursachen der stockenden Umsetzung des vorbeugenden personellen Sabotageschutzes dar. Sie monierten, dass unklar sei, ob die Durchführung des vorbeugenden personellen Sabotageschutzes eine gesetzliche Verpflichtung darstelle. Zudem sei nicht klar erkennbar, wie eine sicherheitsempfindliche Stelle im betroffenen Unternehmen zu identifizieren sei. Außerdem sei das Problem der Behandlung von Fremdfirmen nicht hinreichend geklärt.

Im Ergebnis eines intensiven Dialogs mit den Verbänden hat das Bundesministerium des Innern – abgestimmt mit Bundesministerium für Wirtschaft und Arbeit, Bundesministerium für Verkehr, Bau- und Wohnungswesen sowie Bundesministerium der Verteidigung – einen Leitfaden erstellt, der die thematisierten Fragen klärt. Der Leitfaden ist den Verbänden mit Schreiben vom 31. Dezember 2004 übermittelt worden. Auswirkungen sind mithin im Berichtszeitraum nicht mehr zu erfassen. Da auch bei den Verbänden die Einsicht in die Erforderlichkeit der Sicherheitsüberprüfungen besteht, ist allerdings davon auszugehen, dass durch die Berücksichtigung des Leitfadens<sup>19</sup> der vorbeugende personelle Sabotageschutz in einem stärkeren Maß umgesetzt wird. Die weitere Entwicklung bleibt jedoch zu beobachten.

## 3. Nebenfolgen

„Überschießende“ Überprüfungstendenzen zu Lasten der Mitarbeiter sind nicht feststellbar. Im öffentlichen Bereich zeigt der begrenzte Überprüfungsumfang, dass kei-

---

<sup>19</sup> Im Internet abrufbar unter: [https://www.bmwa-sicherheitsforum.de/shb/template/js\\_page.php?id=1](https://www.bmwa-sicherheitsforum.de/shb/template/js_page.php?id=1)

nesfalls flächendeckende Verdachts- bzw. Vorratsüberprüfungen durchgeführt worden sind. Dies gilt erst recht für den nichtöffentlichen Bereich. Es ist kein Fall bekannt geworden, in dem ein Unternehmen Sicherheitsüberprüfungen bewusst missbräuchlich eingesetzt hätte, um Teile der Belegschaft für verfahrensfremde Zwecke „kontrollieren“ zu lassen. Im Gegenteil: Es ist bekannt geworden, dass Unternehmen, insbesondere der chemischen Industrie, zusammen mit Arbeitnehmervertretern vorrangige Konzepte zur Gefährdungsminimierung, z.B. zusätzliche materielle und organisatorische Sicherungen, zunehmend verwirklichen. Es sind deshalb weniger Personen als erwartet zu überprüfen, weil sicherheitsempfindliche Stellen besser als bisher durch technische oder organisatorische Maßnahmen geschützt werden. Geringere Überprüfungszahlen als erwartet lassen daher nicht von vornherein auf weniger Sicherheit schließen.

#### **4. Kosten (ergänzende Angaben im Anhang<sup>20</sup>)**

Beim MAD werden die anfallenden Sicherheitsüberprüfungen ohne Einrichtung oder Forderung zusätzlicher Dienstposten abgearbeitet.

Beim BfV konnten die Personalkosten im genannten Rahmen begrenzt gehalten werden, da das BfV angesichts der hinter den Erwartungen zurückbleibenden Fallzahlen Mitarbeiter in anderen Bereichen – im Rahmen der Terrorismusbekämpfung – eingesetzt hat.

Zum nichtöffentlichen Bereich lässt sich im Ergebnis der Verbändeanhörung festhalten, dass die Unternehmen die Frage der Kosten nicht als ernstes Problem beim Vollzug des vorbeugenden personellen Sabotageschutzes betrachten.

#### **5. Schlussfolgerungen**

- Im öffentlichen Bereich haben sich die Regelungen uneingeschränkt bewährt. Im nichtöffentlichen Bereich hat sich das Instrument der Sicherheitsüberprüfung zum Sabotageschutz im Grundsatz ebenfalls bewährt.
- Die Regelungen sollten beibehalten werden. Ob zum nichtöffentlichen Bereich angesichts des bisher geringen Aufkommens an Überprüfungen ergänzende Regelungen erwogen werden sollten, kann fundiert erst nach weiteren Erfahrungen mit den ergriffenen untergesetzlichen Maßnahmen (Leitfaden) beurteilt werden.

---

<sup>20</sup> Angaben zu Personal- und Sachkosten im BfV bedürfen der Verschlusssacheneinstufung und sind daher in den Anhang ausgegliedert.

#### IV. § 7 Abs. 2 BKAG (Artikel 10 Nr. 2 Terrorismusbekämpfungsgesetz)

Das BKA ist Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei. In dieser Funktion unterstützt es die Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder sonst erheblicher Bedeutung. Unter anderem sammelt es alle hierfür erforderlichen Informationen und wertet sie aus (§ 2 Abs. 2 Nr. 1 BKAG). Dabei benötigt das BKA insbesondere für Auswertungszwecke zu vorhandenen Sachverhalten häufig noch ergänzende Informationen. Die notwendige Erhebungsbefugnis dazu enthält § 7 Abs. 2 BKAG.

Mit Artikel 10 Nr. 2 Terrorismusbekämpfungsgesetz ist diese Erhebungsregelung dahingehend geändert worden, dass das BKA befugt ist, ergänzende Daten unmittelbar bei nicht-polizeilichen Stellen zu erheben. Nach altem Recht war das nur subsidiär möglich, soweit es die Daten nicht von anderen Polizeibehörden erhalten konnte. Mit der Änderung sollten diese Datenerhebungen vereinfacht und beschleunigt werden (BT-Drs. 14/7386, S. 52).

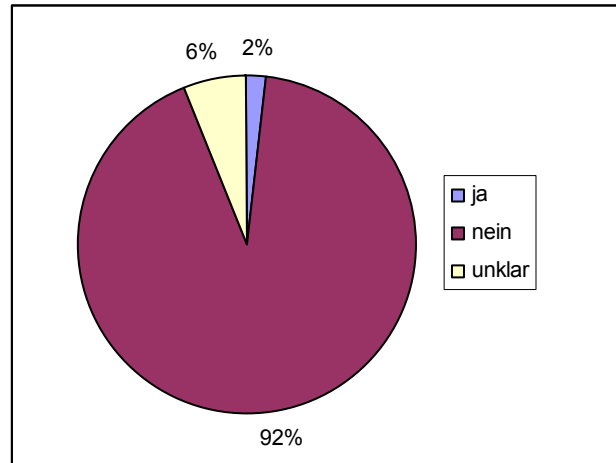
##### a) Auswertung

Im BKA sind die Gesetzesfolgen der neuen Datenerhebungsregelung anhand einer Stichprobe von 744 Anfragen untersucht worden. Die Stichprobe bezog sämtliche Abteilungen des BKA, die Zentralstellenfunktionen wahrnehmen, ein und verteilte sich in 2003 über einen Zeitraum von sieben Monaten, wobei in jedem Monat der jeweilige Sachbearbeiter je eine Woche lang sämtliche Anfragen nach einem Fragebogen ausgewertet hat. Somit liegt ein Erfassungszeitraum von 35 Tagen zugrunde.

Auf sämtliche Sachbearbeiter hochgerechnet erfolgten im Stichprobenzeitraum 11.496, im ganzen Jahr 2003 ca. 67.500 Anfragen. Zur Aufwandsbeschränkung wurden allerdings Anfragen beim Ausländerzentralregister und beim Zentralen Verkehrsinformationssystem (ZEVIS, insbesondere zu Fahrzeug- und Halterdaten aus dem Zentralen Fahrzeugregister) nicht einbezogen; allein beim ZEVIS erfolgen jährlich ca. 60.000 Anfragen.

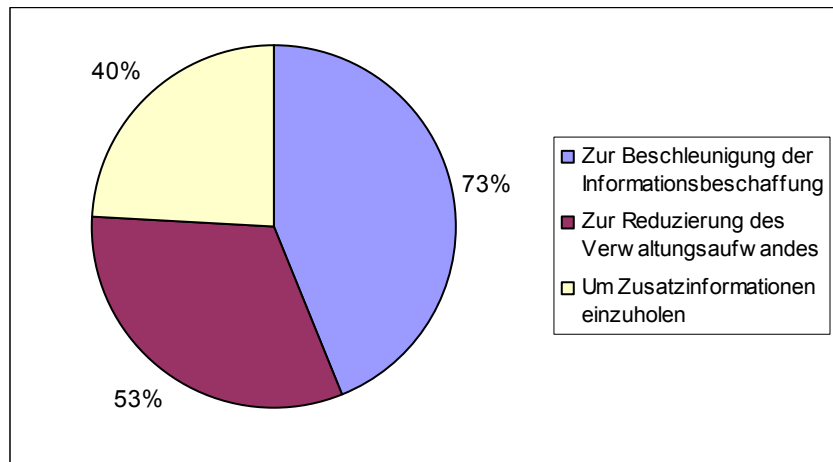
Nach dem Fragebogen war vom Sachbearbeiter zunächst zu erfassen, ob die gewünschten Informationen auch bei einer Polizeibehörde vorliegen. Dies ergab folgendes Ergebnis:

Antwort	Anzahl	in %
ja	15	2 %
nein	684	92 %
unklar	45	6 %



In den Fällen, in denen der Sachbearbeiter davon ausgehen konnte, dass die benötigten Informationen nicht bei einer Polizeibehörde vorhanden sind, hätte er auch nach altem Recht unmittelbar bei der nicht-polizeilichen Stelle anfragen dürfen (BT-Drs. 13/7208, S. 39), so dass sich insoweit mit dem neuen Recht keine weitere Erleichterung ergeben hat. Eine Erleichterung hat sich durch die Rechtsänderung also nur für 8 % der ausgewerteten Fälle ergeben. Bei Einbezug der ZEVI- und AZR-Abfragen wäre dieser Anteil noch deutlich geringer. In absoluten Zahlen ergibt sich allerdings angesichts der hohen Anfragezahlen des BKA gleichwohl eine spürbare Verfahrenserleichterung für – hochgerechnet – etwa 5400 Fälle pro Jahr.

Für die Fälle, in denen der Sachbearbeiter davon ausging, dass die Information auch bei einer Polizeibehörde vorgelegen hätte, ist weiter danach gefragt worden, weshalb gleichwohl unmittelbar bei einem Dritten angefragt wurde (15 Fälle, Angabe mehrerer Gründe war aber möglich).



Antwort	Anzahl	in %
Beschleunigung	11	73 %
Aufwandsverringern	8	53 %
Um Zusatzinformationen einzuholen	6	40 %

## b) Schlussfolgerungen

Die neue Regelung hat nur in einem relativ begrenzten Umfang zu Änderungen der Verwaltungspraxis geführt. Angesichts der hohen absoluten Anfragezahlen resultiert daraus gleichwohl eine ins Gewicht fallende Verbesserung durch Beschleunigung der Informationsbeschaffung und Reduzierung des verbundenen Verwaltungsaufwandes. Die Regelung sollte deshalb beibehalten werden.

## D. Ausblick

Die Evaluierung hat die gesetzgeberischen Entscheidungen ganz überwiegend bestätigt, zu einzelnen Punkten aber auch weitere Verbesserungsmöglichkeiten aufgezeigt.

Auch neue Regelungen werden im Hinblick auf ihre Praxisbewährung zu beobachten sein, wie dies bei der Gesetzgebung allgemein der Fall ist, ohne dass dazu spezielle gesetzliche Evaluierungsmaßgaben oder Befristungen erforderlich wären. Im Terrorismusbekämpfungsgesetz waren solche Vorkehrungen als Korrektiv zum sehr beschleunigten Gesetzgebungsverfahren, gleichsam als Übereilungsschutz, aufgenommen worden. Als generelle Maßgaben zu gesetzlichen Neuregelungen erscheinen sie dagegen nicht veranlasst.