Die Landesbeauftragte
für den Datenschutz
Nordrhein-Westfalen
Bettina Sokol

29. August 2002

Stellungnahme

zum

„Gesetz zur Stärkung des Verfassungsschutzes und seiner Kontrollorgane"
(Gesetzentwurf der Landesregierung – Drucksache 13/2625)
sowie zum
„Gesetz zur Stärkung der parlamentarischen Kontrolle des Verfassungsschutzes, der Justiz und der Polizei" (Gesetzentwurf der Fraktion der FDP – Drucksache 13/1715)

Zu den datenschutzrechtlich einschlägigen Punkten des Fragenkatalogs wird wie folgt Stellung genommen. Darüber hinaus wird die aufgrund der Verfahrensweise nach § 22 Abs. 3 S. 2 DSG NRW gegenüber dem Innenministerium abgegebene Stellungnahme vom 02.05.2002 nebst Anlage beigefügt, die allein die vorgesehenen Befugniserweiterungen für den Verfassungsschutz zum Gegenstand hat.

1. (Frage 1):
Wie bewerten Sie eine Bündelung der Berichtspflichten sowie die Zusammenführung der Gremien wie der FDP-Gesetzentwurf sie vorsieht, insbesondere die Einbeziehung der Aufgaben der G 10-Kommission in ein parlamentarisches Kontrollgremium?

Wenn das Anliegen so verstanden werden kann, dass es darum geht, den Abgeordneten einen Gesamtüberblick über die tatsächlich im Lande stattfindenden Überwachungsmaßnahmen zu erleichtern, so ist dieses Anliegen uneingeschränkt zu begrüßen und zu unterstützen. Das Wissen um Zahl und Art der Eingriffe in die Grundrechte aus Art. 10 GG (Fernmelde-

geheimnis), Art. 13 GG (Unverletzlichkeit der Wohnung) und Art. 2 Abs. 1 i. V. m. Art. 1 Abs.1 GG (Grundrecht auf informationelle Selbstbestimmung) ist nicht nur notwendige Voraussetzung einer effektiven parlamentarischen Kontrolle, sondern dient auch der rationalen Beurteilung rechtspolitischer Forderungen und gesetzgeberischer Initiativen in diesem Bereich.

Das Anliegen eines Gesamtüberblicks ist allerdings nicht von dem Vorhandensein eines in gewisser Weise „allzuständigen" Gremiums abhängig. Aus datenschutzrechtlicher – also grundrechtlicher – Sicht ist die Erstellung zweier jährlicher, schriftlicher Überwachungsberichte der Landesregierung empfehlenswert. Der eine Bericht sollte alle diejenigen Überwachungsmaßnahmen darstellen, über die schon jetzt in öffentlicher Sitzung in den jeweils zuständigen Ausschüssen berichtet wird. Diese Zusammenstellung sollte allen Abgeordneten zugänglich gemacht werden und auch von interessierten Bürgerinnen und Bürgern angefordert werden können.

Die bislang a) in nicht-öffentlicher Sitzung der Ausschüsse, b) gegenüber dem parlamentarischen Kontrollgremium nach § 23 VSG NRW sowie c) der G 10-Kommission erstatteten Berichte und gegebenen Informationen sollten auf ihre weitere Geheimhaltungsbedürftigkeit geprüft werden. Bei fehlender Geheimhaltungsbedürftigkeit sollten diese Informationen in den allgemein zugänglichen Bericht aufgenommen werden. Die weiterhin geheimhaltungsbedürftigen Informationen sollten in dem zweiten oder gegebenenfalls in weiteren Berichten zusammengestellt und den informationsberechtigten Personen zur Verfügung gestellt werden. Vor dem Hintergrund eines solchen Modells verliert die Frage, ob es ein Gremium oder mehrere Gremien geben sollte, an Bedeutung. Maßgeblich sind in erster Linie die Intensität der Diskussion und Kontrolle sowie – gegebenenfalls – etwaige Konsequenzen des Landtags.

2. (Frage 2):
Wie bewerten Sie die Zusammensetzung der G 10-Kommission - augenblicklich ohne Parlamentarier - im Hinblick auf das Ziel: Stärkung der parlamentarischen Kontrolle?

Nach der Rechtsprechung des Bundesverfassungsgerichts verlangt Art. 10 Abs. 2 S. 2 GG, dass das zu seiner Ausführung ergehende Gesetz unter den von der Volksvertretung zu bestellenden Organen ein Organ vorsehen muss, das in richterlicher Unabhängigkeit und für alle an der Vorbereitung, verwaltungsmäßigen Entscheidung und Durchführung der

Überwachung Beteiligten verbindlich über die Zulässigkeit der Überwachungsmaßnahme und über die Frage, ob die betroffene Person zu benachrichtigen ist, entscheidet und die Überwachungsmaßnahme untersagt, wenn es an den rechtlichen Voraussetzungen dafür fehlt. Dieses Organ kann innerhalb oder außerhalb des Parlaments gebildet werden (vgl. BVerfGE 30, 1/23 f.). Danach dürfte es verfassungsrechtlich unbedenklich sein, wenn die Mitglieder der G 10-Kommission nicht Parlamentarierinnen und Parlamentarier sind. Gleichwohl sollten sie zur Vermeidung von Interessenkollisionen nicht der Exekutive angehören. Da die Kontrolle Rechtskontrolle ist, muß das Kontrollorgan außerdem über die dafür erforderliche Sach- und Rechtskunde verfügen.

3. (Frage 7):

Halten Sie es für sinnvoll, die Landesbeauftragte für den Datenschutz an den Sitzungen der G 10-Kommission sowie des parlamentarischen Kontrollgremiums bzw. des Kontrollgremiums (FDP-Gesetzentwurf) zu beteiligen?

Die im Gesetzentwurf der Landesregierung vorgesehene Regelung, dass die G 10-Kommission der Landesbeauftragten für den Datenschutz Gelegenheit zur Stellungnahme in Fragen des Datenschutzes geben kann, kann ein erster Schritt zu einer gegenseitigen Unterstützung der Arbeit der G 10-Kommission und der Landesbeauftragten für den Datenschutz sein. Unabhängig davon, ob es auch weiterhin ein parlamentarisches Kontrollgremium und eine G 10-Kommission geben wird oder nur ein einziges parlamentarisches Kontrollgremium mit erweiterten Zuständigkeiten, wäre eine Mitgliedschaft der Landesbeauftragten für den Datenschutz in diesen Gremien aus verschiedenen Gründen problematisch. Eine beratende Teilnahme an den Unterrichtungen und Beratungen der Kommission dürfte den Zweck einer gegenseitigen Unterstützung zur effektiveren Kontrolle ebenfalls erfüllen.

Die derzeitige Situation im Hinblick auf die Kontrollmöglichkeiten der Landesbeauftragten für den Datenschutz ist jedenfalls verbesserungsbedürftig. Der Verfassungsschutz bestreitet nämlich zur Zeit jedwede Kontrollmöglichkeit der Landesbeauftragten für den Datenschutz betreffend Vorgänge, die im Bereich des G 10-Gesetzes liegen. Es ist zudem in der Praxis zu befürchten, dass die vorgesehenen erweiterten Kontrollmöglichkeiten der G 10-Kommission vom Verfassungsschutz als Argument dafür herangezogen werden, der Landesbeauftragten für den Datenschutz in eben diesem Umfang die Kontrollkompetenz abzusprechen. Ein Gesetz, mit dem Kontrollmöglichkeiten gestärkt werden sollen, sollte jedoch nicht zugleich

dafür nutzbar sein, bestehende Kontrollmöglichkeiten der Landesbeauftragten für den Datenschutz zu beschneiden. Sowohl insoweit als auch in Bezug auf die derzeitige Situation bedarf es eines klärenden Wortes des Gesetzgebers.

Es wird daher vorgeschlagen:

1. Im Gesetzentwurf der Landesregierung (Art. 2, § 3 Abs. 5) werden nach Satz 4 (Die G 10-Kommission kann der oder dem Landesbeauftragten für den Datenschutz Gelegenheit zur Stellungnahme in Fragen des Datenschutzes geben.) folgende Sätze 5-8 angefügt:

   „Dies erfolgt, wenn ein Mitglied es beantragt. Sie kann sie oder ihn zur Teilnahme an ihren Unterrichtungen und Beratungen einladen. Dies erfolgt, wenn ein Mitglied es beantragt. Die oder der Landesbeauftragte für den Datenschutz ist aus Gründen ihrer oder seiner Unabhängigkeit befugt, in diesem Zusammenhang erlangte Informationen auch im Rahmen der Datenschutzkontrolle zu nutzen."

2. Im Gesetzentwurf der Landesregierung (Art. 1, § 25) wird nach Absatz 4 als neuer Absatz 5 eingefügt:

   „Das Kontrollgremium kann der oder dem Landesbeauftragten für den Datenschutz Gelegenheit zur Stellungnahme geben. Dies erfolgt, wenn ein Mitglied es beantragt. Es kann sie oder ihn zur Teilnahme an ihren Unterrichtungen und Beratungen einladen. Dies erfolgt, wenn ein Mitglied es beantragt. Die oder der Landesbeauftragte für den Datenschutz ist aus Gründen ihrer oder seiner Unabhängigkeit befugt, in diesem Zusammenhang erlangte Informationen auch im Rahmen der Datenschutzkontrolle zu nutzen."

Die im Gesetzesentwurf der Landesregierung bisher vorgeschlagenen Absätze 5-7 werden entsprechend Absätze 6-8.

Wortgleich wird insoweit eine Ergänzung des FDP-Entwurfs vorgeschlagen.

4. (Frage 8):

Halten Sie die Speicherung von personenbezogenen Daten gemäß § 10 VSG über 5 Jahre bzw. von Daten über 10 bzw. 15 Jahre für angemessen (bereits nach dem bestehenden Recht konnte im Einzelfall eine längere Speicherung angeordnet werden)?

Insoweit hat die Landesbeauftragte für den Datenschutz bereits gegenüber dem Innenministerium des Landes Nordrhein-Westfalen datenschutzrechtliche Bedenken gegen die in § 10 Abs. 3 VSG NRW des Gesetzentwurfs der Landesregierung vorgesehene Verlängerung der Speicherfristen für personenbezogene Daten über Bestrebungen nach § 3 Abs. 1 Nr. 3 und 4 VSG NRW von 10 auf 15 Jahren erhoben. Die für die Verlängerung der Speicherfristen gegebene Begründung überzeugt nicht. Darauf abgestellt wird unter Hinweis auf die Anschläge vom 11.September 2001, dass sich Personen in diesen Beobachtungsfeldern bewusst so konspirativ verhalten, dass u. U. erst nach einem 10-Jahreszeitraum weitere Erkenntnisse anfallen. Inwiefern eine Information nach einem derart langen Zeitraum nach der letzten Datenspeicherung über terroristische und vor allem gegen den Gedanken der Völkerverständigung gerichtete Bestrebungen für die Terrorismusbekämpfung allerdings tatsächlich noch relevant sein kann, lässt sich aus dieser Begründung nicht erschließen. Soweit derartige Bestrebungen zugleich auch Erkenntnisse über sicherheitsgefährdende Tätigkeiten im Sinne des § 3 Abs. 1 Nr. 2 VSG NRW beinhalten, gilt für diese ohnehin nicht die Befristungsdauer für eine Aufbewahrung nach § 10 Abs. 3 des Gesetzentwurfs. Zudem konnte schon bisher die Höchstspeicherfrist im Einzelfall verlängert werden.

5. (Frage 9):

Gemäß § 6 des Informationsfreiheitsgesetzes ist ein Informationszugang abzulehnen, soweit u.a. die Tätigkeit des Verfassungsschutzes beeinträchtigt würde. Sehen Sie eine Möglichkeit, im Verfassungsschutzgesetz ein uneingeschränktes, z.B. nur auszugsweises Akteneinsichtsrecht zu verankern?

Es ist zu unterscheiden zwischen den Möglichkeiten der betroffenen Personen, etwas über zur eigenen Person gespeicherte Informationen beim Verfassungsschutz zu erfahren und einem allgemeinen Informationszugangsrecht nach dem Informationsfreiheitsgesetz. Das Verfassungsschutzgesetz Nordrhein-Westfalen räumt betroffenen Personen bisher gerade kein

Akteneinsichtsrecht, sondern nur ein Auskunftsrecht ein, das bei Vorliegen der Voraussetzungen des § 14 Abs. 2 VSG NRW sogar noch ausgeschlossen werden kann. Um die Rechte der betroffenen Personen zu stärken, sollte auch ein Einsichtsrecht eingeführt werden. Ebenso wie vor einer Auskunft durch den Verfassungsschutz das Recht der betroffenen Person auf informationelle Selbstbestimmung mit dem staatlichen Geheimhaltungsanspruch abgewogen wird, lässt sich dies auch vor Gewährung einer Akteneinsicht vornehmen, die mit den Aufgaben des Verfassungsschutzes keineswegs von vornherein unvereinbar ist.

Demgegenüber geht das Informationsfreiheitsgesetz davon aus, dass den Wünschen der Informationssuchenden in der Regel zu entsprechen ist. Sie können nämlich grundsätzlich selber darüber bestimmen, ob sie eine Information im Wege der Einsichtnahme oder der Auskunftserteilung erlangen wollen. Da der Verfassungsschutz völlig zu Recht nicht generell von einem Informationszugang nach dem Informationsfreiheitsgesetz ausgenommen worden ist, können diejenigen Personen, die nicht nach den über sich selbst gespeicherten Daten fragen, von ihrem grundsätzlichen Wahlrecht zwischen Einsicht und Auskunft Gebrauch machen.

Denjenigen, die wissen möchten, welche Daten der Verfassungsschutz zu ihrer eigenen Person gespeichert hat, sollte ein solches Wahlrecht ebenfalls eingeräumt werden. § 14 VSG NRW sollte entsprechend geändert werden.

6. (Frage 10):
Ist es mit dem Recht auf informationelle Selbstbestimmung vereinbar, wenn Auskunftsverpflichtungen von Behörden, insbesondere von Ausländerämtern, eingeführt werden?

Die in § 16 Abs. 1 Satz 2 VSG NRW des Gesetzentwurfs der Landesregierung vorgesehene Bestimmung verpflichtet die Ausländerbehörden zur Übermittlung von näher bestimmten Erkenntnissen und Informationen an die Verfassungsschutzbehörde. Voraussetzung ist allerdings das Vorliegen tatsächlicher Anhaltspunkte dafür, dass diese Informationen für die Aufgabenerfüllung des Verfassungsschutzes erforderlich sind. Die Ausländerbehörden werden damit dazu angehalten, ihnen vorliegende Informationen zu übermitteln, die sie mangels Fachwissen regelmäßig gar nicht daraufhin überprüfen können, ob sie für die Aufgaben des Verfassungsschutzes erforderlich sind oder nicht. Somit besteht die Gefahr,

dass Datenübermittlungen im Übermaß und ohne rechtliche Grundlage stattfinden könnten. Überdies ist bisher nicht belegt, dass eine Übermittlungsverpflichtung insoweit erforderlich ist. Danach muss zumindest daran gezweifelt werden, ob die vorgesehene Übermittlungsverpflichtung der Ausländerbehörden noch mit dem Recht auf informationelle Selbstbestimmung vereinbar ist. Mindestens wäre eine Präzisierung der Vorschrift in dem Sinne erforderlich, wie er sich aus der Gesetzesbegründung ergibt.

7. (Frage 11):

§ 17 Abs. 3 Satz 4 des Entwurfs stellt fest, dass eine Übermittlung der Daten, die von einer ausländischen Stelle empfangen wurden, nur dann erfolgen darf, wenn dies völkerrechtlich geboten ist. Welche konkreten Bedingungen müssen danach erfüllt sein?

Die beabsichtigte Ergänzung der Vorschrift hat folgenden Wortlaut:

> *„Die Übermittlung der von einer Ausländerbehörde empfangenen Daten unterbleibt, es sei denn, die Übermittlung ist völkerrechtlich geboten."*

Da zu befürchten ist, dass die Ausländerbehörden aufgrund ihrer Auskunftsverpflichtung nach dem geplanten § 16 Abs. 1 Satz 2 VSG NRW eher mehr als weniger Informationen an die Verfassungsschutzbehörde übermitteln werden, ist es zu begrüßen, dass diese Informationen wenigstens dem Grundsatz nach vom Verfassungsschutz nicht noch weiter an ausländische, über- oder zwischenstaatliche Stellen übermittelt werden dürfen. Welche konkreten Voraussetzungen erfüllt sein müssen, damit die ausnahmsweise vorgesehene Übermittlung im Falle einer völkerrechtlichen Gebotenheit zulässig ist, kann von hier nicht verläßlich beantwortet werden. Aufgrund der zu knappen personellen Ressourcen sind keine völkerrechtlichen Spezialkenntnisse bei der Landesbeauftragten für den Datenschutz vorhanden. Die Arbeitsüberlastung erlaubt den Mitarbeiterinnen und Mitarbeitern auch keine Einarbeitung in diese Thematik, die im Arbeitsalltag bisher keine Rolle gespielt hat. Zudem ist hier nicht bekannt, ob überhaupt die Arbeit der Nachrichtendienste betreffende völkerrechtliche Verträge existieren.

8. (Frage 12):

In § 25 Abs. 3 wird als Verweigerungsgrund der Unterrichtung der „Kernbereich exekutiver Eigenverantwortung" genannt. Unter welchen Voraussetzungen sehen Sie diesen Kernbereich als tangiert an?

Regierung und Verwaltung – also der Exekutive – sind im Grundgesetz einige Aufgaben zwingend zugewiesen. Dies betrifft beispielsweise die Bestimmung der Richtlinien der Politik durch den Bundeskanzler nach Art. 65 S. 1 GG, den Erlaß von Rechtsverordnungen nach Art. 80 Abs. 1 S. 1 GG und weitere im Grundgesetz ausdrücklich benannte Kompetenzen, die der Exekutive nicht durch einfaches Gesetz durch das Parlament entzogen werden können. Ob über die im Grundgesetz und in den Landesverfassungen vorgesehenen Beschränkungen des parlamentarischen Zugriffs hinaus ein „Kernbereich exekutiver Eigenverantwortung" existiert, ist in der juristischen Literatur nach wie vor nicht gänzlich unumstritten. Darunter verstanden wird die Begrenzung des Zugriffsrechts des Parlaments auf das Regierungs- und Verwaltungshandeln – sei es in Form gesetzgeberischer oder kontrollierender Tätigkeit. Der Wortlaut von Art. 20 Abs. 3 GG, nach dem die vollziehende Gewalt an Gesetz und Recht gebunden ist, spricht so zunächst einmal auch eher gegen ein derartiges Postulat. Gleichwohl hat das Bundesverfassungsgericht einen „Kernbereich exekutiver Eigenveranwortung" anerkannt, ihn aber zugleich auf einen engen Initiativ-, Beratungs- und Handlungsbereich begrenzt. Als Beispiel dafür sei hier etwa der Willensbildungsprozeß der Regierung genannt – „sowohl hinsichtlich der Erörterungen im Kabinett als auch bei der Vorbereitung von Kabinetts- und Ressortentscheidungen, die sich vornehmlich in ressortübergreifenden und – internen Abstimmungsprozessen vollzieht" (BverfGE 67, 100/139).

Da der „Kernbereich exekutiver Eigenverantwortung" demnach nur sehr eng zu fassen ist, dürften Maßnahmen der Verfassungsschutzbehörde regelmäßig nicht darunter fallen. Möglicherweise könnte der Hintergrund der Einschränkungen der Unterrichtungspflicht des Kontrollgremiums durch die Landesregierung vielmehr sein, die Funktionsfähigkeit des Verfassungsschutzes dadurch zu gewährleisten, dass entsprechende Informationen gar nicht erst an außenstehende Dritte geraten und dadurch die Aufgabendurchführung gefährden. Im Hinblick auf die Verschwiegenheitsverpflichtung der Mitglieder des Kontrollgremiums ebenso wie der Angehörigen der Verfassungsschutzes sind derartige Gefährdungen jedoch nicht zu besorgen.

9. (Frage 13):
Halten Sie die Frist für eine Evaluierung der Erfahrungen nach dem neuen Gesetz für sachgerecht und nach welchen Kriterien sollte aus Ihrer Sicht eine solche Evaluierung erfolgen?

Die in Art. 3 Abs. 1 des Gesetzentwurfs der Landesregierung vorgesehene Fünfjahresfrist, vor deren Ablauf die Neuregelungen zu evaluieren sind, entspricht der in Art. 22 Abs. 1 des Terrorismusbekämpfungsgesetzes vorgesehenen Frist und erscheint gerade noch hinnehmbar. In Abs. 2 des vorliegenden Gesetzentwurfs ist allerdings unzutreffend auf Abs. 1 Satz 2 der Vorschrift verwiesen. Gemeint sein müßten die Regelungen in Abs. 1 Satz 3.

Die Evaluierung soll ermöglichen, Wirksamkeit und Verhältnismäßigkeit der mit erheblichen Grundrechtseinschränkungen verbundenen neuen Eingriffsbefugnisse zu beurteilen. Dafür bedarf es zunächst einer Ist-Analyse der derzeitigen Praxis und der Wirksamkeit der bisherigen Maßnahmen, um die Erforderlichkeit der neuen Eingriffsbefugnisse zu begründen. Die auf die neuen Eingriffsbefugnisse gestützten Maßnahmen sind dann im Einzelfall daraufhin zu untersuchen, welche Wirksamkeit sie allein im Hinblick auf die Terrorismusbekämpfung haben und wieviele unbeteiligte Personen in welcher Weise von den Maßnahmen betroffen sind oder waren. Aussagen müssen unter anderem mindestens zu folgenden Punkten getroffen werden: auskunftgebende Stelle, Anlaß der Maßnahme, Anordnungsgrund, Umfang und Dauer, Kosten, Ergebnis, Wirksamkeit bezogen auf die Terrorismusbekämpfung, Anzahl der unbeteiligten Personen, Benachrichtigung der Betroffenen, Übermittlungen an andere Stellen, Löschung von Daten und der gleichen mehr.

Seit dem 01.01.02
zugleich Beauftragte
für das Recht auf Information

Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen

Postanschrift: Landesbeauftragte für den Datenschutz NRW
Postfach 20 04 44, 40102 Düsseldorf

Reichsstraße 43, 40217 Düsseldorf
E-Mail: datenschutz@lfd.nrw.de
Bearbeitung: Herr Schiemann
Durchwahl: (0211) 38 424 – 36
Aktenzeichen:
- 23.1.1 -
(bitte immer angeben)

02. Mai 2002

Innenministerium
des Landes Nordrhein-Westfalen
Haroldstraße 5

40190 Düsseldorf

Entwurf des Gesetzes zur Stärkung des Verfassungsschutzes und seiner Kontrollorgane
Ihr Schreiben vom 23.04.2002 - 615/1-0020-4839-301/02 -

Zu dem mit Ihrem Schreiben vom 23.04.2002 übersandten Entwurf eines Gesetzes zur Stärkung des Verfassungsschutzes nehme ich aus datenschutzrechtlicher Sicht wie folgt Stellung.

Mit dem vorliegenden **Gesetzentwurf zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen (VSG NW)** sollen die in Artikel 1 des Terrorismusbekämpfungsgesetzes vom 09.01.2002 enthaltenen Datenerhebungsbefugnisse des Bundesamtes für Verfassungsschutz in Landesrecht übernommen werden. Zum Entwurf eines Terrorismusbekämpfungsgesetzes des Bundes haben die Datenschutzbeauftragten des Bundes und der Länder bereits in Ihrer Entschließung vom 24./26.10.2001 darauf hingewiesen, dass sich alle neu erwogenen Maßnahmen daran messen lassen müssen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Grundsatz der Verhältnismäßigkeit einhalten. Die Datenschutzbeauftragten haben sich insbesondere gegen eine Ausdehnung von Auskunftspflichten und Ermittlungskompetenzen gewandt. Die an den Bundesregelungen geäußerte Kritik wird nach wie vor aufrechterhalten. Um Wiederholungen zu vermeiden, wird insoweit auf den Beitrag von Dr. Susanne Rublack in der DUD 2002, S. 202 verwiesen, der beigefügt ist. Soweit der Entwurf des Landesgesetzes die Bundesregelungen ins Landesrecht „übersetzt", gilt die Kritik entsprechend. Der Gesetzentwurf

stößt insgesamt und in jedem einzelnen Punkt auf erhebliche datenschutzrechtliche Bedenken. Dies wird hier exemplarisch an drei Punkten erläutert:

1. zu § 5 a VSG NW (E):

Ebenso wie die Gesetzesbegründung zu § 8 BVerfSchG lassen auch die Begründungen zu § 5 a des vorliegenden Gesetzentwurfs eine Erforderlichkeit für die weitreichenden Datenerhebungsbefugnisse der Verfassungsschutzbehörde bei den genannten Stellen nicht erkennen. Die nunmehr auch landesgesetzlich vorgesehene erhebliche Kompetenzausweitung der Verfassungsschutzbehörde trägt insgesamt dem Gebot einer Trennung der Aufgaben des Verfassungsschutzes von den Aufgaben der Polizei nicht ausreichend Rechnung. Die zwangsläufig eintretenden Grenzverschiebungen der Aufgaben und Befugnisse dieser Bereiche der Exekutive ist zudem deshalb problematisch, weil sie zu möglicherweise kontraproduktiven Mehrfacherhebungen von Daten führen kann.

2. zu § 7 Abs. 4 VSG NW (E):

Nach dieser Vorschrift sollen künftig unter besonderen Voraussetzungen auch technische Mittel zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes und zur Ermittlung der Geräte- und Kartennummern eingesetzt werden dürfen. Als technische Mittel sind derzeit sogenannte "IMSI-" bzw. "IMEI-Catcher" im Gespräch und zum Teil bereits auf dem Markt.

Gegen den Einsatz dieser Mobilfunk-Ortungsgeräte bestehen schwerwiegende Bedenken, weil die technischen Rahmenbedingungen nicht hinreichend diskutiert sind und ihre Verwendung zu erheblichen Eingriffen in die Kommunikationsrechte Dritter führt. Bei ihrer Verwendung können sämtliche Mobiltelefone in der Reichweite des zu ortenden Mobiltelefons lokalisiert werden. Der Mobilfunkverkehr für die entsprechende Funkzelle während des Einsatzes eines IMSI-Catchers wird massiv gestört. Im übrigen ermöglichen diese Ortungsgeräte im Gegensatz zu dem durch den Gesetzestext erweckten Anschein keineswegs ohne weiteres die Feststellung des Standorts eines Mobiltelefons. Eine präzise Lokalisierungsinformation ist vielmehr Voraussetzung für die Nutzung des IMSI-Catchers. Die Zuordnung der IMSI zu einer Anschlussnummer ist nur für diejenigen Karten möglich, die von zur Auskunft verpflichteten (d.h. deutschen) Telekommunikationsunternehmen ausgegeben worden sind. Für die naheliegende Nutzung der Karten ausländischer Provider ist der Einsatz des IMSI-Catchers wir-

kungslos.[1] Im übrigen dürfte absehbar sein, dass hierdurch auch die Anzahl staatlicher Telekommunikationsüberwachungen weiter steigen wird.

3. zu § 10 Abs. 3 VSG NW (E):

Datenschutzrechtlichen Bedenken begegnet ferner die in dieser Vorschrift vorgesehene Ausweitung der Löschungsfrist für gespeicherte personenbezogene Daten über Bestrebungen nach § 3 Abs. 1 Nrn. 3 und 4 von 10 auf 15 Jahren. Die hierfür gegebene Begründung lässt sich nicht nachvollziehen. Darauf abgestellt wird unter Hinweis auf die Anschläge vom 11.September 2001, dass sich Personen in diesen Beobachtungsfeldern bewusst so konspirativ verhalten, dass u. U. erst nach einem 10-Jahreszeitraum weitere Erkenntnisse anfallen. Inwiefern eine Information nach einem derart langen Zeitraum nach der letzten Datenspeicherung über terroristische und vor allem gegen den Gedanken der Völkerverständigung gerichtete Bestrebungen für die Terrorismusbekämpfung allerdings tatsächlich noch relevant sein kann, lässt sich aus dieser Begründung nicht erschließen. Soweit derartige Bestrebungen zugleich auch Erkenntnisse über sicherheitsgefährdende Tätigkeiten im Sinne des § 3 Abs. 1 Nr. 2 VSG NW beinhalten, gilt für diese ohnehin nicht die Befristungsdauer für eine Aufbewahrung nach § 10 Abs. 3 des Gesetzentwurfs. Zudem konnte schon bisher die Höchstspeicherfrist im Einzelfall verlängert werden.

Im Auftrag

(Schiemann)

---

[1] Einzelheiten hierzu s. "Materialien zum Datenschutz" des Berliner Beauftragten für Datenschutz und Informationsfreiheit (Jahresbericht 2001 - Anlagenband) – abrufbar unter http://www.datenschutz-berlin.de/jahresbe/01anl/11d9.htm ;
s.a. Rublack, DuD 2002, S. 202 ff., 204 und Fox, ebenda, S. 212 ff., 214 f.

DuD
Datenschutz und Datensicherheit

Terrorismusbekämpfungsgesetz: Neue Befugnisse für die Sicherheitsbehörden

Susanne Rublack

Auf die Ereignisse des 11. September 2001 hat der Bundesgesetzgeber mit wesentlichen Erweiterungen der Befugnisse der Geheimdienste und des Bundeskriminalamtes reagiert, die Susanne Rublack im folgenden darstellt und kritisch kommentiert.[1] Die ausländerrechtlichen Regelungen sowie die durch die Einführung neuer später biometrischer Merkmale aufgeworfenen Fragen werden Gegenstand gesonderter Artikel in den nächsten Ausgaben von DuD sein.

Dr.
Susanne Rublack

Referentin beim Unabhängigen Landeszentrum für Datenschutz Schleswig Holstein

E-Mail: ld5@datenschutzzentrum.de

1 Kritik am Gesetzgebungsverfahren

Das zweite Sicherheitspaket von Bundesinnenminister Otto Schily wurde in rekordverdächtigem Tempo als Terrorismusbekämpfungsgesetz am 14. Dezember 2001 vom Bundestag und bereits sechs Tage (!) am 20. Dezember 2001 vom Bundesrat verabschiedet.

Die Fülle der in diesem Artikelgesetz enthaltenen Regelungen einerseits und die teilweise innerhalb weniger Tage aufeinander folgenden geänderten Fassungen andererseits erschwerten es den Parlamentariern zur Kenntnis zu nehmen, worüber sie inhaltlich zu entscheiden hatten.[2] Insgesamt bewegte sich der Ablauf des Gesetzgebungsverfahrens im Hinblick auf die Tragweite der Regelungsinhalte an der Grenze des demokratisch Verantwortbaren. Vor diesem Hintergrund ist die am 1. Januar 2002 auf der Homepage der Bundesregierung verbreitete Pressemitteilung, das Terrorismusbekämpfungsgesetz sei am nämlichen Tage in Kraft getreten, von geradezu symbolischer Bedeutung für das gesamte Gesetzgebungsverfahren. Denn zu diesem Zeitpunkt prüfte noch der Bundespräsident und fertigte das Gesetz, dessen Art. 22 bestimmt, es trete am 1. Januar 2002 in Kraft, erst am 9. Januar 2002 aus. In Kraft getreten ist es am Tage seiner Verkündung im Bundesgesetzblatt am 11. Januar 2002.[3] Eine echte Rückwirkung seiner Regelungen auf den vor diesem Zeitpunkt liegenden Zeitraum dürfte aus verfassungsrechtlichen Gründen ausscheiden.

Am deutlichsten werden durch das Gesetzespaket Ausländer in ihren Grundrechten betroffen: Die neuen Datenerhebungs-, -übermittlungs- und –speicherungsbefugnisse im Ausländerrecht sind so weitreichend, dass man von einer datenschutzrechtlichen Zwei-Klassen-Gesellschaft sprechen kann. Deutlich wird dies etwa an der Einführung neuer biometrischer Merkmale in Ausweisdokumenten, die bei Deutschen aus gutem Grund unter dem Vorbehalt eines Ausführungsgesetzes stehen[4], während die entsprechende Erhebungs- und Verarbeitungsbefugnis für Ausländerausweisdokumente unmittelbar von der Verwaltung umgesetzt werden kann.[5] Einen sachlichen Grund für diese Differenzierung gibt es nicht, denn wesentliche, an den Gesetzgeber zu richtende Fragen über die Auswahl des biometrischen Verfahrens, seiner Realisierbarkeit sowie der Begrenzung von Sekundärnutzungen betreffen sowohl Deutsche als auch Ausländer gleichermaßen.

2 Erweiterter Beobachtungsauftrag

Der Gesetzgeber hat den Beobachtungsauftrag des *Bundesamtes für Verfassungsschutz* sowie des *Militärischen Abschirmdienstes* auf Bestrebungen erweitert, die gegen den Gedanken der Völkerverständigung, insbesondere gegen das friedliche Zusammenleben der Völker, gerichtet sind.[6]

Für das Bundesamt für Verfassungsschutz müssen diese Bestrebungen, anders

[1] Grundlage dieses Beitrages ist das Positionspapier des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein vom 7.12.2001 zum damaligen Entwurf des Terrorismusbekämpfungsgesetzes.

[2] Süddeutsche Zeitung v. 12.12.01, S. 6; Stellungnahmen, Entwürfe und Beschlüsse zum Terrorismusbekämpfungsgesetz unter www.cilip.de/terror/

[3] BGBl. 2002 I S. 361

[4] § 4 Abs. 4 Passgesetz, § 1 Abs. 5 Personalausweisgesetz.

[5] §§ 5 Abs. 4, 39 Abs. 1, 56a, 69 Abs. 2 Ausländergesetz, § 63 Asylverfahrensgesetz.

[6] Art. 1 Nr. 1 und Art. 2 Nr. 1 Terrorismusbekämpfungsgesetz (TerrBkG) – § 3 Abs. 1 Nr. 4 Bundesverfassungsschutzgesetz (BVerfSchG) und § 1 Abs. 1 S. 2 MAD-Gesetz.

als für den MAD, im Inland bestehen. Schon bislang bestand der Auftrag des Verfassungsschutzes in der Beobachtung des gewaltgeneigten Extremismus, so dass die Beobachtung der seit den Terroranschlägen interessierenden islamisch-fundamentalistischen Strukturen offensichtlich bereits hinreichend gesetzlich abgesichert war. Nach der Begründung des Gesetzentwurfs der Bundesregierung[7] soll die Tätigkeit des Bundesamtes künftig jedoch bereits weit im Vorfeld terroristischer Bestrebungen ansetzen, nämlich bei Bestrebungen, die „den Nährboden für die Entstehung extremistischer Auffassungen bilden" können. Bezweckt ist nach der Begründung allerdings vor allem die Lockerung des bislang vorausgesetzten Inlandsbezuges der geplanten oder durchgeführten Gewaltanwendung extremistischer Gruppierungen. Über dieses durchaus nachvollziehbare Anliegen, dem durch eine Erweiterung der Ziff. 2 und 3 des §3 Abs. 1 Bundesverfassungsschutzgesetz (BVerfSchG) auf Schutzgüter im Ausland hätte Rechnung getragen werden können, geht die nun verabschiedete Befugnis jedoch weit hinaus. Als Folge sind ausufernde Datensammlungen der Bundesverfassungsschutzbehörde zu befürchten, die gerade keine Konzentration geheimdienstlicher Aufklärung auf den eindeutig gewaltorientierten islamischen Extremismus mit sich bringen. Das Gleiche gilt für die Informationssammlung durch den MAD.

3 Auskunftspflicht der Unternehmen

Das *Bundesamt für Verfassungsschutz* hat umfangreiche Auskunftsbefugnisse u.a. gegenüber Banken, Post-, Telekommunikations-, Flug- und Teledienste- sowie Luftfahrtunternehmen erhalten.[8] Im einzelnen sind dies Auskünfte über

- Konten, Kontenbewegungen und -inhaber sowie sonstige Berechtigte, über am Zahlungsverkehr Beteiligte und über Geldbewegungen und -anlagen bei Banken und sonstigen Finanzunternehmen,
- Namen, Anschriften, Postfächer und sonstige Umstände des Postverkehrs bei Postunternehmen,
- Namen, Anschriften und Daten über Transportleistungen und „sonstige Umstände des Flugverkehrs" bei Luftfahrtunternehmen,
- TK-Verbindungsdaten und Teledienstenutzungsdaten, auch in Bezug auf künftige Kommunikation bzw. Nutzung, bei Telekommunikations- und Teledienstebetreibern. Diese Daten sind im Gesetz näher definiert.

Zwar sind die tatbestandlichen Voraussetzungen für solche Auskunftsersuchen gegenüber dem ursprünglichen Entwurf deutlich angehoben worden, indem tatsächliche Anhaltspunkte für qualifizierte Gefahren verlangt werden bzw. im Bereich der Kommunikation auf die Voraussetzungen des § 3 Abs. 1 des G 10 verwiesen wird. Dennoch bewegen sich die geplanten Befugnisse in einem typischerweise polizeilichen Bereich konkreter Ermittlungen zu individuellen Verhaltensweisen und weniger im Bereich der geheimdienstlichen Strukturinformationen. Die verfassungsrechtlich gebotene Trennung von Polizei und Geheimdiensten wird hierdurch wie bereits bei den individualbezogenen Abhörbefugnissen des Bundesnachrichtendienst (BND) angesichts der Übermittlungsmöglichkeiten an die Polizei weiter aufgeweicht.

Außerdem sind parallele Ermittlungen und in diesem Zuge doppelte Grundrechtseingriffe durch Polizei und Verfassungsschutz zu befürchten. Zu berücksichtigen sind auch faktisch diskriminierende Auswirkungen für die Betroffenen insbesondere, wenn sich ein Geheimdienst bei Kreditunternehmen über Konten und Transaktionen einer Person erkundigt, ohne dass ein strafrechtlicher Anfangsverdacht vorliegen muss.

Eine der aus rechtsstaatlicher Sicht wesentlichen Nachbesserungen des Regierungsentwurfs noch in spätem Stadium sorgte dafür, dass die formalen Anforderungen an die Anordnung der Auskünfte, deren Kontrolle durch die G 10-Kommission und durch das Parlamentarische Kontrollgremium an diejenigen des G 10-Gesetzes angeglichen wurden.[9]

Dennoch bleibt es ein Systembruch, dass die neuen kommunikationsbezogenen Auskunftsbefugnisse außerhalb des G 10 angesiedelt wurden. Nach der Rechtsprechung des Bundesverfassungsgerichts unterliegen auch die näheren Umstände der Kommunikation dem Fernmeldegeheimnis. Alle Eingriffsbefugnisse der Geheimdienste in Bezug auf Art. 10 GG sollten daher innerhalb des G 10 und nicht in den Spezialgesetzen geregelt sein, um ein einheitliches System der materiellen Voraussetzungen, des Anordnungsverfahrens, der Datenverarbeitungsbefugnisse und ihrer Kontrolle zu Gewähr leisten. Auch in diesem Rahmen wären sachgerechte Abstufungen der materiellen wie auch der formellen Anforderungen in Bezug auf Inhalts- und Verbindungsdaten möglich.

Aufgrund der Änderungsanträge der Regierungsfraktionen[10] wurden die Auskunftsbefugnisse des Bundesamtes für Verfassungsschutz auch den Verfassungsschutzbehörden des Landes zugestanden, stehen dort jedoch unter dem Vorbehalt einer gleichwertigen Regelung der Verfahrensanforderungen und Kontrollmöglichkeiten.[11] Zudem bestehen alle Auskunftsrechte nur für den Einzelfall, dürfen also nicht zur Übermittlung gesamter Datenbestände genutzt werden.

Dem MAD und dem BND wurden entsprechende telekommunikations-/teledienstebezogene Auskunftsbefugnisse eingeräumt; der BND hat darüber hinaus entsprechende Auskunftsrechte gegenüber Banken und Finanzunternehmen.[12]

4 Kleiner Lauschangriff

Noch in spätem Stadium wurde eine Art. 13 Abs. 5 GG umsetzende Befugnis des *Bundesamtes für Verfassungsschutz* zum Einsatz verdeckter technischer Mittel zur Eigensicherung der bei einem Einsatz in Wohnungen tätigen Personen (bemannte Wanze, sog. „kleiner Lauschangriff") in das Sicherheitspaket eingefügt.[13] Eine terrorismusspezifische Begründung sucht man vergeblich; vielmehr war nach dem 11. September stets die Rede davon, dass ein Einschleusen von Personen in die Strukturen des islamisch-fundamentalistischen Terrors kaum möglich sei. Die Regelung über die Verwendung der erlauschten Informationen schöpft die grundgesetzliche Ermächtigung (zu Zwecken der Gefahrenabwehr) für den Aufgabenbereich des Bundesamtes vollständig aus.[14]

[7] BT-Dr. 14/7386, S. 38

[8] § 8 Abs. 5 bis 12 BVerfSchG (Art. 1 Nr. 3 TerrBkG).

[9] § 8 Abs. 9 bis 11 BVerfSchG.

[10] (soweit ersichtlich, keine Drs.-Nr.).

[11] § 8 Abs. 11 BVerfSchG.

[12] Art. 2 Nr. 4 TerrBkG (§ 10 Abs. 3 MAD-Gesetz) und Art. 3 Nr. 1 u. 2 TerrBkG (§§ 2 Abs. 1a, 8 Abs. 3a BND-Gesetz).

[13] Art. 1 Nr. 4 TerrBkG (§ 9 Abs. 2 S. 8 – 12 BVerfSchG).

[14] § 9 Abs. 2 S. 10 BVerfSchG.

5 IMSI-Catcher

Die bislang rechtlich umstrittene Zulässigkeit des Einsatzes des sog. IMSI-Catchers ist nun, auch bei bloßem Stand-by-Betrieb von Mobilfunkendgeräten, für das *Bundesamt für Verfassungsschutz* gesetzlich geregelt worden.[15] Sie soll die Ermittlung des Standortes einer Person und der von ihr verwendeten Geräte- und Kartennummer ermöglichen.

Gegen den Einsatz des IMSI-Catchers bestehen gravierende datenschutzrechtliche Bedenken. Technisch bedingt greift dieses Gerät besonders intensiv in die Kommunikationsrechte Dritter ein, die während der Zeit seines Einsatzes im Sendebereich des IMSI-Catchers keine Gespräche führen können und deren Daten zunächst ebenfalls mit abgefangen werden. Mit der Legitimierung des staatlichen Einsatzes von IMSI-Catchern wird eine Technik gefördert und „salonfähig" gemacht, die etwa im Bereich der Wirtschaftskriminalität von hohem Interesse ist, da es mit ihr nach dem gegenwärtigen technischen Standard auch möglich ist, die Verschlüsselung von Gesprächen auszuschalten und Inhalte abzuhören. Die technische Option des Abhörmodus würde im Übrigen, sofern der IMSI-Catcher auch von der Polizei eingesetzt würde – wie in zunehmendem Maße bereits jetzt ohne gesetzliche Grundlage –, auch absehbar zu einer weiteren Steigerung der Zahl staatlicher TK-Überwachungen führen.

Nach der Begründung des Regierungsentwurfs[16] sollen mit dem IMSI-Catcher lediglich die Anschlussnummern für Maßnahmen der Telefonüberwachung nach dem G 10 ermittelt und damit die Voraussetzung für deren Anordnung geschaffen werden. Auch diese Befugnis ist jedoch nicht im G 10, sondern außerhalb dieses Regelungszusammenhangs in § 9 BVerfSchG eingefügt worden. Nach ihrem Wortlaut soll der IMSI-Catcher zur Ermittlung des Standorts einer überwachten Person über die Vorbereitung von G 10-Anordnungen hinaus allgemein zur Erfüllung der Aufgaben des Bundesamtes für Verfassungsschutz (mit Ausnahme des § 3 Abs. 1 Nr. 1 BVerfSchG) eingesetzt werden. Damit wird jedoch die Regelungsintention weit überschritten. Die Befugnis unterliegt einer Subsidiaritätsklausel, den tatbestandlichen Voraussetzungen des § 3 Abs. 1 G 10 sowie der Datenverarbeitungsregelung in § 4 G 10.

Angesichts des hohen Ausstattungsgrades der Bevölkerung mit Mobiltelefonen ist zu befürchten, dass die Erstellung und Auswertung von Bewegungsbildern von Personen mit aktiv geschaltetem Handy zu einer Standardermittlungsmethode der Sicherheitsbehörden wird, soweit sie ihnen gesetzlich zugestanden ist. Wie entsprechende Anträge im Bundesrat bereits gezeigt haben[17], steht die Befugnis zum Einsatz eines IMSI-Catchers für die Strafverfolgungsbehörden bereits auf der politischen Tagesordnung. Dann ergäbe sich insgesamt eine neue Qualität der immer vollständigeren staatlichen Überwachbarkeit des Aufenthaltsortes von Personen, die durch Aktivschaltung ihres Mobiltelefons erreichbar sein möchten. Betrachtet man die Generation der heute Jugendlichen, dann wird deutlich, welches Ausmaß diese aus Sicht der Betroffenen unerwünschte „Nebenwirkung" der Teilnahme an der Informationsgesellschaft bereits in wenigen Jahren erreichen könnte.

6 Verlängerung der Löschfristen

Schwer nachvollziehbar ist, dass in § 12 Abs. 3 Satz 2 BVerfSchG die Löschfrist für Speicherungen über terroristische und vor allem über gegen die Völkerverständigung gerichtete Bestrebungen von zehn auf fünfzehn Jahre seit dem Zeitpunkt der letzten gespeicherten relevanten Information verlängert worden ist.

Es muss bezweifelt werden, dass eine Information nach einer so langen Zeit ohne weitere hinzugekommene Erkenntnisse noch von Aktualität und Bedeutung für die Terrorismusbekämpfung sein kann. Die Bundesregierung hat ihren Entwurf insoweit mit der konspirativen Verhaltensweise relevanter Personen begründet.[18] Die Anwendung einer Fünfzehn-Jahres-Frist auf die in das Extremismusvorfeld hineinreichenden Bestrebungen gegen die Völkerverständigung (s.o. 2.) erscheint besonders problematisch.

7 Sicherheitsüberprüfungen

Bislang regelte das Sicherheitsüberprüfungsgesetz des Bundes (SÜG), so wie die entsprechenden Gesetze der Bundesländer, lediglich den personellen Geheimschutz, d.h. den Schutz von Verschlusssachen. Das Terrorismusbekämpfungsgesetz hat nun Regelungen in das SÜG des Bundes eingefügt, nach denen einfache Sicherheitsüberprüfungen (sog. Ü 1) im Zuständigkeitsbereich des Bundes auch zu Zwecken des personellen Sabotageschutzes durchgeführt werden dürfen.[19]

Einer solchen Überprüfung werden künftig Personen unterzogen, die an einer sicherheitsempfindlichen Stelle innerhalb einer lebens- oder verteidigungswichtigen Einrichtung oder innerhalb einer besonders sicherheitsempfindlichen Stelle des Bundesverteidigungsministeriums beschäftigt sind oder noch werden sollen.[20] Mit solchen Stellen sind nach der Gesetzesbegründung vor allem Teile von Versorgungseinrichtungen in den Bereichen Energie, Wasser, chemisch-pharmazeutische Industrie, Bankwesen, Telekommunikation und Transport gemeint, ferner Stellen, deren Zerstörung in besonderem Maße eine Gesundheits- oder Lebensgefährdung großer Teile der Bevölkerung zur Folge haben könnte.[21] Diese Bereiche sollen gem. § 34 SÜG durch Rechtsverordnung der Bundesregierung im Einzelnen festgelegt werden.

Die Ergänzung des SÜG erscheint grundsätzlich nachvollziehbar und im Verhältnis zu den Gefahren des extremistischen Terrorismus, die sich am 11. September 2001 manifestiert haben, angemessen, zumal lediglich die am wenigsten eingreifende Form der Sicherheitsüberprüfung gewählt wurde. Allerdings sollte in der Praxis der Gefahr einer im Volumen ausufernden Überprüfung von Beschäftigten im gesamten Versorgungsbereich widerstanden werden und eine Konzentration auf wirklich für Sabotagezwecke kritische Bereiche erfolgen.

---

[15] § 9 Abs. 4 BVerfSchG; Zum IMSI-Catcher Fox DuD 1997, 539.

[16] BT-Dr. 14/7386, S. 40.

[17] Vgl. Art. 2 des Antrages Bayerns und Thüringens im Bundesrat, BR-Drs. 1014/01 v. 27.11.2001.

[18] BT-Dr. 14/7386, S. 41.

[19] Art. 5 TerrBkG.

[20] § 1 Abs. 4 SÜG.

[21] BT-Dr. 14/7386, S. 43.

8 Erweiterte Ermittlungsbefugnis des BKA

Zu den Hauptkritikpunkten am ersten Entwurf des zweiten Schily'schen Sicherheitspaketes gehörte eine sog. „Initiativermittlungsbefugnis" des BKA, d.h. die Befugnis, ohne Vorliegen eines strafrechtlichen Anfangsverdachtes oder einer polizeirechtlichen Gefahr Ermittlungen gegen bestimmte Personen aufzunehmen. Diese Befugnis sollte in Form eines § 7a Bundeskriminalamtgesetz (BKAG) eingefügt werden, dessen vorgeschlagener Wortlaut an dieser Stelle dokumentiert werden soll:

„§ 7 a – Feststellung zureichender tatsächlicher Anhaltspunkte für eine Straftat:

Das BKA kann zur Feststellung, ob zureichende tatsächliche Anhaltspunkte für eine Straftat vorliegen, in den Fällen, in denen es für die Strafverfolgung nach § 4 Abs. 1 [BKAG] zuständig ist, personenbezogene Daten erheben sowie weitere Maßnahmen durchführen. Die Vorschriften der StPO über besondere Maßnahmen der Datenerhebung bleiben unberührt.[22]„

Zulässig sollten also nur „einfache Maßnahmen" sein, dies jedoch außerhalb der Sachleitungsbefugnis der Justiz und vor allem ohne Einhaltung der rechtsstaatlich wesentlichen Schwelle für polizeiliches Tätigwerden, des Anfangsverdachts nach der Strafprozessordnung. Dieses Regelungsvorhaben, das wohl wie viele andere aus diesem Gesetzespaket lange bis zur passenden Gelegenheit in den Schubladen der Sicherheitsbehörden gelegen hatte, überstieg jedoch selbst unter dem noch recht frischen Eindruck des 11. September 2001 die Schmerzgrenze der öffentlichen Meinung wie auch der Justizressorts und wurde alsbald fallen gelassen.

Geblieben ist dennoch eine Erweiterung der Ermittlungsbefugnisse des BKA, ein Stück Autonomie gegenüber den nach dem Grundgesetz primär für die Strafverfolgung und Gefahrenabwehr zuständigen Länderpolizeien, wenn auch in anderer Form und von geringerer Tragweite: Nach dem neu gefassten § 7 Abs. 2 S. BKAG wird die Funktion des BKA als Zentralstelle erweitert, indem es unabhängig von den Länderpolizeien und den dort möglicherweise bereits vorhandenen Daten bei sämtlichen öffentlichen oder nichtöffentlichen Stellen Informationen originär erheben darf, um vorhandene Sachverhalte zu ergänzen oder sonst zu „Auswertungszwecken". Die Erhebung wird im Gesetz auch nicht mehr als Ersuchen bezeichnet, wodurch auf Seiten der angesprochenen Stelle der Eindruck einer Verpflichtung zur Datenübermittlung erweckt wird, ohne dass dies allerdings ausdrücklich gesetzlich vorgesehen wäre.

Durch die Neufassung des § 7 Abs. 2 BKAG wird die Rolle des BKA in einer Weise gestärkt, die der grundgesetzlichen Kompetenzverteilung auf dem Gebiet des Polizeirechts kaum mehr entspricht. Dem BKA wird eine Grauzone präventiver Ermittlungen eröffnet, in der eine Koordination mit den originär zuständigen Länderpolizeien bei der Datenerhebung nicht mehr in jedem Falle stattfinden muss. Dies geht weit über das bisherige Verständnis der Zentralstellenfunktion des BKA hinaus und wird zwangsläufig Doppelerhebungen personenbezogener Daten von Bund und Ländern an Stelle der notwendigen Bündelung und Koordinierung polizeilicher Informationssammlungen zur Folge haben.

Um die Betroffenen so schonend wie möglich zu belasten, müssten demgegenüber innerhalb der Polizei bereits vorhandene Daten auf Grundlage der hierfür vorhandenen Übermittlungsbefugnisse des BKAG und der Landespolizeigesetze genutzt werden, bevor Anfragen an dritte Stellen getätigt werden. Zudem wird das BKA häufig nicht erkennen können, ob in einem Land bereits Strafermittlungsverfahren gegen die sie interessierende Person laufen, sodass auch die justizielle Aufsicht über Datenerhebungen gem. § 7 Abs. 2 S. 3 BKAG leer laufen kann.

Die gegenwärtige Praxis der Beiziehung von Abgleichsdateien durch das BKA im Rahmen der Rasterfahndung zur Aufspürung von islamisch-fundamentalistischen „Schläfern" zeigt bereits, wie großzügig das BKA seine Rechtsgrundlagen für „ergänzende Datenerhebungen" auslegt und dies bereits vor Schaffung des Terrorismusbekämpfungsgesetzes getan hat[23].

9 Sozialdaten für Rasterfahndung

Etwas versteckt, nämlich in Art. 18 des Terrorismusbekämpfungsgesetzes, findet sich eine weitere Schwächung des Sozialdatenschutzes ausgerechnet für den mit ausholenden Netzen durchgeführten Fischzug der Rasterfahndung. Gegenüber Maßnahmen der Rasterfahndung wird der Schutz von Sozialdaten eines bestimmten Kataloges (Pesonalgrunddaten, Staats- und Religionszugehörigkeit, Anschriften des Betroffenen sowie seiner Arbeitgeber, Geldleistungen) nach dem nun eingeführten § 68 Abs. 3 Sozialgesetzbuch (SGB X) durchbrochen. Ursprünglich sollte die Übermittlung sämtlicher Sozialdaten zu Zwecken einer Rasterfahndung für zulässig erklärt werden.[24]

Sozialdaten gehören zu den sensibelsten Daten in staatlicher Verfügungsgewalt und reichen insbesondere im medizinischen Bereich (der nun nach der Endfassung nicht tangiert ist) weit in die Persönlichkeitssphäre des Einzelnen hinein. Es erscheint völlig unangemessen, diese dem besonderen Schutz des Staates anvertrauten Daten über die bisherigen, genau abgestuften Möglichkeiten polizeilicher Einzelfallermittlungen hinaus in eine Maßnahme wie die Rasterfahndung einzubeziehen, die vom Ansatz her notwendigerweise zu einem überwiegenden Anteil rechtstreue Bürger erfasst. Bei der Übermittlung von Sozialdaten an Sicherheitsbehörden müssen Einzelfallerwägungen immer eine Rolle spielen können.

Es konterkariert die verfassungsrechtliche Aufgabe des Sozialstaates, wenn Bürger dadurch in eine u.U. für sie folgenschwere Maßnahme wie die Rasterfahndung mit den sich anschließenden Maßnahmen polizeilicher Ermittlungen geraten können, dass sie staatliche Sozialvorsorge in Anspruch nehmen. Sofern Sozialdaten, zumindest die Tatsache der Inanspruchnahme von Sozialleistungen, eine wesentliche Rolle bei der Ermittlung einer (potenziellen) Tätergruppe spielen, wäre es allenfalls angemessen, sie erforderlichenfalls nach der Phase des maschinellen Abgleiches der Rasterfahndungsdaten in konventioneller Weise auszuwerten und hierfür die einzelfallbezogenen Übermittlungsgrundlagen des SGB X heranzuziehen.

[22] Referentenentwurf des Bundesinnenministeriums für ein Terrorismusbekämpfungsgesetz, Stand: 12.10.01, unveröffentlicht.

[23] News-Mitteilung im Virtuellen Datenschutzbüro www.datenschutz.de v. 08.11.2001.

[24] Vgl. Art. 18 i.d.F.d. Regierungsentwurfs, BT-Dr. 14/7386. S. 17.

10 Evaluierung

Politik und Gesetzgeber waren nach den Terroranschlägen des 11. September, die bislang Undenkbares real werden ließen und damit sicherlich auch neue gedankliche Horizonte der Rechtspolitik eröffneten, zu einer schwierigen Suche nach angemessenen Reaktionen zum Schutze der Bevölkerung aufgerufen. Was in die Form des Terrorismusbekämpfungsgesetzes gegossen wurde, hat vielfach – wenngleich nicht durchweg – mit dem Phänomen des islamisch-fundamentalistischen Terrorismus wenig zu tun, wurde oft als lang gehegter Wunsch aus den Schubladen der Bürokraten geholt und schießt weit über das Ziel einer gezielten Terrorismusbekämpfung hinaus.

Schlechte Gesetze werden dadurch nicht besser, immerhin aber ein Stück erträglicher, dass sie befristet sind und, unterstützt durch eine wissenschaftliche Auswertung der Rechtspraxis, dem Gesetzgeber noch einmal zur Entscheidung vorgelegt werden müssen. Durch Art. 22 Abs. 2 und 3 des Terrorismusbekämpfungsgesetzes sind die neuen Befugnisse der Geheimdienste und des BKA in deren Fachgesetzen – nicht jedoch in anderen Gesetzen wie dem Sozialgesetzbuch oder im Ausländerrecht – bis zum 11. Januar 2007 befristet und eine Evaluierung vor Ablauf der Frist verbindlich vorgeschrieben worden.