Bundeskriminalamt

Innenausschuss
16(4)460 G

Anhörung des Präsidenten des Bundeskriminalamtes

Jörg Ziercke

vor dem Innenausschuss des Bundestages

am 15. September 2008

zum Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt

(Drs. 16/9588)

Einleitung

Nach dem Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (BT-Drs. 16/9588) soll das Bundeskriminalamt (BKA) die Aufgabe der Abwehr von Gefahren des internationalen Terrorismus in Fällen wahrnehmen, in denen

- eine länderübergreifende Gefahr vorliegt,
- die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder
- die oberste Landesbehörde um eine Übernahme ersucht.

Zur effektiven Wahrnehmung dieser Aufgabe sollen dem Bundeskriminalamt erstmals auch die hierzu benötigten Befugnisse an die Hand gegeben werden.

BKA

Ausgangslage und Handlungsbedarf

Der internationale Terrorismus ist mit seinen aktuellen Ausprägungen und Dimensionen zu einer zentralen Bedrohung für Staat und Bevölkerung geworden. Nach allem, was wir wissen, ist die Entscheidung, Anschläge auch in Deutschland zu begehen, auf höchster Ebene der AL QAIDA und anderer terroristischer Gruppierungen gefallen.

Mit einer Entspannung der Lage können wir in Deutschland trotz der Tatsache, dass bisherige Anschlagsversuche vereitelt werden konnten oder teils zufallsbedingt nicht über das Versuchsstadium hinausgingen, nicht rechnen. Auch das gleichbleibend hohe Ermittlungsaufkommen im islamistisch-terroristischen Gefahrenbereich und die zahlreichen insbesondere über das Internet verbreiteten Drohbotschaften zeigen, dass Deutschland unverändert im unmittelbaren Zielspektrum des islamistischen Terrorismus liegt. Dies wird sich kurzfristig auch nicht ändern.

Informationen über eine Bedrohung für Deutschland fallen sehr häufig im Ausland an. Der zur Verhütung oder zur Verfolgung von Straftaten erforderliche Dienstverkehr der Polizeien des Bundes und der Länder mit den Polizei- und Justizbehörden sowie sonstigen insoweit zuständigen öffentlichen Stellen anderer Staaten obliegt grundsätzlich dem Bundeskriminalamt (§ 3 Abs. 2 BKAG). Als Nationales Zentralbüro von Interpol, nationale Verbindungsstelle von Europol, als nationale Eingangsstelle im Rahmen des Schengen-Verbundes und als Mitglied der Police Working Group on Terrorism ist das Bundeskriminalamt erste Anlaufstelle ausländischer Staaten.

Um zu entscheiden, ob in einer solchen Situation Gefahrenabwehrmaßnahmen notwendig sind, müssen diese aus dem Ausland übermittelten Informationen regelmäßig weiter angereichert, bewertet, mit ausländischen Stellen kontinuierlich rückgekoppelt und damit insgesamt in einem ständigen Prozess grenzüberschreitender polizeilicher Zusammenarbeit bearbeitet werden. Gegebenenfalls sind darauf sofortige Maßnahmen zur Gefahrenabwehr erforderlich.

Tatsächlich hat das Bundeskriminalamt derzeit jedoch nicht die rechtliche Möglichkeit, über eine Informationssteuerung hinaus selbst Maßnahmen zu ergreifen, um solche Hinweise aus dem Ausland abzuklären und eventuell erforderliche Abwehrmaßnahmen einzuleiten.

Es ist im Bereich der Gefahrenabwehr auf seine Zentralstellenbefugnisse beschränkt, die es ihm lediglich erlauben, Informationen mittels sogenannter "Büroabklärungen" zu erheben oder Daten entgegenzunehmen und auszuwerten, die ihm auf freiwilliger Basis angeboten werden. Es verfügt damit noch nicht einmal über die Kompetenzen, über die selbst der kleinste Polizeiposten in einem Bundesland verfügt. Vielmehr muss es sich an die Polizeien der Länder wenden und um Übernahme bitten, sofern in diesem frühen Stadium die örtliche Zuständigkeit einer Länderpolizei überhaupt erkennbar ist. Anschließend muss dann das jeweilige Land hinsichtlich der weiteren Informationsanreicherung aus dem Ausland wiederum auf das Bundeskriminalamt zurückgreifen.

Während im ersten Fall erst Abstimmungsmaßnahmen zwischen mehreren betroffenen Ländern erfolgen müssen, bevor die erforderlichen Maßnahmen ergriffen werden, ist im zweiten Fall eine Gefahrenabwehr mangels örtlicher Anknüpfungspunkte für die Zuständigkeit eines Landes überhaupt nicht gewährleistet.

In solchen Konstellationen muss das Bundeskriminalamt selbst Maßnahmen zur Aufklärung und Beseitigung von Gefahren, insbesondere zur Verhütung von Straftaten des internationalen Terrorismus ergreifen können.

Hierbei geht es vornehmlich um die Übernahme von Sachverhalten, in denen der Generalbundesanwalt – sobald ein strafprozessualer Anfangsverdacht bestünde – das Bundeskriminalamt mit den Ermittlungen beauftragen würde. Damit würde die Übertragung von Gefahrenabwehrbefugnissen auf das Bundeskriminalamt auch einem führungstaktischen polizeilichen Grundsatz Rechnung tragen, demzufolge Strafverfolgung und Gefahrenabwehr möglichst weitgehend in einer Hand liegen sollten. Der Wechsel von Zuständigkeiten und die damit verbundenen notwendigen Abstimmungen bedeuten nämlich zwangsläufig Zeitverluste, die zu verlängerten Reaktionszeiten führen und zudem die Gefahr von Informationsverlusten bergen.

Ermessensentscheidung

Dem Bundeskriminalamt soll nicht automatisch in allen Fällen, in denen ein länderübergreifender terroristischer Bezug festgestellt wird, eine Zuständigkeit übertragen werden. Vielmehr ist die Übernahme der Aufgabe der Gefahrenabwehr in das Ermessen des BKA gestellt.

Bewusst wurde auf eine starre Regelung etwa anhand von Regelbeispielen oder typisierten Fallgestaltungen verzichtet. Dies entspricht einem dringenden fachpraktischen Bedürfnis. Die Vielgestaltigkeit möglicher Sachverhalte gebietet es, hier einen gewissen Spielraum zuzulassen. Das Bundeskriminalamt kann im gegebenen Fall auf eine Aufgabenübernahme verzichten und die Gefahrenabwehr der Länderpolizei überlassen, wenn dies zum Beispiel wegen der örtlichen Gegebenheiten oder gewichtiger regionaler Bezüge geboten ist.

Zusammenarbeit mit den Ländern

Der Gefahr des internationalen Terrorismus zu begegnen, ist eine gesamtstaatliche Herausforderung, auf die Bund und Länder gemeinsam reagieren müssen, indem sie ihre jeweiligen Kräfte optimal zum Einsatz bringen. Der Gesetzesentwurf bietet die Grundlage für eine noch effektivere Zusammenarbeit. Er enthält Regelungen, die eine Klärung der jeweiligen Zuständigkeit und eine effektive Kooperation bei der Lagebewältigung gewährleisten.

Grundzuständigkeit der Länder bleibt gewahrt

Die Möglichkeit der Gefahrenabwehr durch das BKA in bestimmten Fällen des internationalen Terrorismus soll die bestehende Zuständigkeitsverteilung zwischen dem Bundeskriminalamt und den Länderpolizeien sinnvoll ergänzen: Die Neuregelung lässt die Zuständigkeiten der Länder grundsätzlich unberührt; Gefahrenermittlungen und Gefahrenabwehrmaßnahmen wären auch nach der geplanten Neuregelung vorrangig auf örtlicher Ebene verankert – insbesondere wegen der dort vorhandenen Kenntnisse der örtlichen Gegebenheiten. Auch in den Fällen, in denen das Bundeskriminalamt von seinem Selbsteintrittsrecht Gebrauch macht, bleibt es auf die Zusammenarbeit mit den Ländern angewiesen. Zudem haben die Länderpolizeien jederzeit die Möglichkeit, in eigener Verantwortung Maßnahmen über den BKA-Sachverhalt hinaus zu ergreifen.

Befugnisse

Um die Aufgabe der Gefahrenabwehr effektiv wahrnehmen zu können, benötigt das Bundeskriminalamt die Ermächtigungsgrundlagen, die in den Ländern seit Jahrzehnten praktizierter und bewährter Standard sind. Die polizeilichen Ermittlungsinstrumente müssen sich allerdings auch an der rasant voranschreitenden technologischen Entwicklung orientieren, von der die Täter profitieren - beispielsweise um Maßnahmen der Gefahrenabwehrbehörden zu unterlaufen.

Zur Notwendigkeit besonderer Befugnisse

1. Verdeckte Eingriffe in informationstechnische Systeme, § 20k BKAG-E (Online-Durchsuchung)

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 27. Februar 2008 (1 BvR 370/07, 1 BvR 595/07) zur so genannten Online-Durchsuchung ausgeführt:

> *„Die Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit der Bevölkerung vor Gefahren für Leib, Leben oder Freiheit sind Verfassungswerte, die mit anderen hochwertigen Gütern im gleichen Rang stehen. Der Staat kommt seinen verfassungsrechtlichen Aufgaben nach, indem er Gefahren durch terroristische und andere Bestrebungen entgegen tritt. Maßnahmen des Gesetzgebers, die informationstechnische Mittel für staatliche Ermittlungen erschließen, sind insbesondere vor dem Hintergrund der Verlagerung herkömmlicher Kommunikationsformen hin zum elektronischen Nachrichtenverkehr und der Möglichkeiten zur Verschlüsselung oder Verschleierung von Daten zu sehen. Der heimliche Zugriff auf informationstechnische Systeme ist geeignet, diesen Zielen zu dienen“ (BVerfG a.a.O. Nr. 220/221).*

Die rasante Entwicklung des Internets hat einen Strukturwandel weltweiter Kommunikation und Interaktion bewirkt.

Das Internet und die Nutzung des Computers als Speichermedium können herkömmliche Gefahrenabwehrmaßnahmen gänzlich ins Leere laufen lassen: Verschlüsselungstechniken verhindern den Zugriff auf gefährdungsrelevante Informationen auf der Festplatte eines Computers und damit eine zeitnahe Gefahrenabwehr. Verschlüsselung schafft Räume abgeschotteter Täterkommunikation. Ohne eine Anpassung der polizeilichen Instrumentarien wird eine wirksame Gefahrenabwehr zukünftig erheblich erschwert oder gar nicht möglich sein.

Terroristen haben ihre Kommunikation ins Internet verlagert. Dabei werden über das Internet sowohl Bombenbauanleitungen verbreitet, Anschlagspläne geschmiedet und Anschlagsziele gesucht als auch junge Menschen radikalisiert und als Suizidattentäter angeworben.

Die Attentäter der Anschläge vom 11.03.04 in Madrid haben die Pläne für den Bau ihrer Bomben nachweislich aus dem Internet heruntergeladen. Auf ihren PC fanden sich zudem Unterlagen, wie diese Bomben – gedacht für den Einsatz auf Märkten, gegen Autobusse, Busbahnhöfe oder Restaurants – vor einer vorzeitigen Entdeckung durch die Polizei geschützt werden können.

Auch die Täter der versuchten Anschläge auf die beiden Regionalzüge bei Dortmund und Koblenz im Juli 2006 luden sich die Anleitung zum Bau der später verwendeten Unkonventionellen Spreng- und Brandvorrichtung aus dem Internet herunter.

Die bisherigen Erkenntnisse im Zusammenhang mit der Festnahme von drei mutmaßlichen Mitgliedern der Islamischen Jihad Union (IJU) am 04.09.07 in Deutschland unterstreichen ebenfalls die fachliche Notwendigkeit von Online-Durchsuchungen. Das Vorgehen der Täter und des dahinter stehenden Netzwerks ist durch ein hohes Maß an Konspiration geprägt. Es ist bislang trotz eines enormen technischen und personellen Aufwandes sowie einer Vielzahl sukzessiv durchgeführter kriminalpolizeilicher Maßnahmen nicht gelungen, alle Tatverdächtige zu identifizieren, obgleich wir davon ausgehen müssen, dass sich diese modernern Kommunikationsmittel bedient haben und wir auf den PCs der Täter weitere Hinweise hätten finden können.

Das Bundeskriminalamt hat derzeit keine rechtliche Möglichkeit, verdeckt an auf den Festplatten der Tatverdächtigen gespeicherte Informationen, Passwörter und Schlüssel zu gelangen. Zur Aufdeckung solcher Netzwerke – und im Ergebnis zur Verhinderung von terroristischen Anschlägen – sind offene Datensicherungsverfahren (Durchsuchung, Sicherstellung des PC und anschließende Datenträgerauswertung) nicht zielführend: Zur Abwehr von Gefahren des Terrorismus ist die offene Wohnungsdurchsuchung in der Regel nur geeignet, wenn keine anderen Maßnahmen mehr möglich sind, da sonst das Netzwerk gewarnt würde, Mittäter nicht identifiziert werden und die Anschlagsplanungen weitergeführt werden können. Auch die klassischen Instrumente der verdeckten Informationserhebung wie die Telekommunikationsüberwachung reichen angesichts des veränderten Interaktions- und Kommunikationsverhaltens der Täter nicht mehr aus.

Ein weiterer Grund für die Notwendigkeit eines verdeckten Zugriffs auf IT-Syteme ist die Zunahme der Verschlüsselung (Kryptierung). Die Dekryptierung verschlüsselter Informationen auf den sichergestellten Datenträgern ist ohne Kenntnis des Passwortes nicht zeitnah oder gar nicht möglich. Zunehmend kommt es zudem vor, dass brisante Informationen gerade nicht auf der eigenen Festplatte gespeichert werden, sondern die Informationen – zudem auch noch kryptiert – ausgelagert auf irgendeinem Server versteckt werden. Der einzige Weg für die Sicherheitsbehörden an diese kryptierten oder im Netz abgelegten Informationen zu gelangen, besteht darin, im Wege einer Online-Durchsuchung auf die Informationen zuzugreifen, bevor diese kryptiert bzw. versteckt werden, nach der Dekryptierung (z.B. wenn der User "online" ist) oder durch Feststellung des Schlüssels bzw. des Passwortes. Die Online-Durchsuchung ist daher ein für die Verhinderung terroristischer Anschläge unverzichtbares Instrument.

In Ausnahmefällen - bei Gefahr im Verzug - muss gewährleistet sein, dass die Maßnahme im Eilfall auch durch den Präsidenten des Bundeskriminalamtes angeordnet werden darf. Denkbar ist beispielsweise die Fallkonstellation, dass die einzusetzende Software aus taktischen Gründen nur in einem bestimmten kurzen Zeitfenster auf den Zielrechner implementiert werden kann und das Abwarten einer richterlichen Entscheidung (etwa an Wochenenden oder zur Nachtzeit) den gesamten Erfolg der Maßnahme gefährden würde.

Es bedarf jedoch einer unverzüglichen nachträglichen Bestätigung durch das Gericht. Wie bei anderen Maßnahmen mit erheblicher Eingriffsintensität auch (z.B. Wohnraumüberwachung oder TKÜ) wird im BKAG-E eine solche Option der Eilfallregelung normiert. Eine solche wurde vom Bundesverfassungsgericht ausdrücklich für zulässig erachtet. Technisch realisierbar ist der unverzügliche Eingriff in das informationstechnische System dann, wenn durch andere vorausgegangene Maßnahmen (z.B. TKÜ, WRÜ, Observation) bereits wichtige Vorerkenntnisse für die Umsetzung der Online-Durchsuchung gewonnen wurden.

Auch der Kernbereich privater Lebensgestaltung wird durch die gesetzlichen Vorgaben gewahrt. Das BVerfG hat deutlich gemacht, dass bei Eingriffen in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme der Kernbereichsschutz nicht allein zum Zeitpunkt der Anordnung der Maßnahme sicherzustellen ist, sondern in einem zweistufigen Verfahren und damit auch im Stadium der Auswertung der gewonnenen Daten sichergestellt werden kann. Hierzu sieht das Gesetz in § 20k BKAG-E dezidierte Regelungen vor, die den verfassungsrechtlichen Vorgaben Rechnung tragen: Eine Prüfung der erhobenen Daten auf Kernbereichsrelevanz erfolgt zunächst im "4-Augen-Prinzip" durch Beamte des Bundeskriminalamtes. Ist die Kernbereichsrelevanz erkennbar, sind die Daten unverzüglich zu löschen. Im Zweifelsfall sieht § 20k BKAG-E eine richterliche Überprüfung und Entscheidung vor. Der Vorgang ist im Übrigen zu dokumentieren.

2. Notwendigkeit der Wohnraumüberwachung, § 20h BKAG-E

Die Vorschrift umfasst neben der *akustischen* auch die *visuelle* Überwachung, wie sie im Grundgesetz (Art. 13 Abs. 4 GG) und - mit einer Ausnahme - in allen Landespolizeigesetzen geregelt ist. Eine akustische WRÜ ist dann nicht ausreichend, wenn die Ermittler unter Umständen nicht alles mitbekommen können, was zur Einschätzung der Situation nötig ist und sich Probleme bei der Zuordnung von Äußerungen zu den einzelnen Zielpersonen ergeben.

Beispiel „EG Zeit“: In dem sog. „Sauerland-Fall“ waren die Beschuldigten gerade damit befasst, Sprengstoff herzustellen und haben auch darüber gesprochen. Das Bundeskriminalamt konnte zwar akustisch den Gesprächen der Tatverdächtigen folgen, hatte jedoch - mangels visueller Mitverfolgung - nicht die nötige Kenntnis vom tatsächlichen Geschehen. Daher kam es zu Problemen bei der Lagebeurteilung und beim einsatztaktischen Vorgehen. Dies hatte zur Folge, dass bei der anschließenden Festnahme einer der Tatverdächtigen fliehen konnte und es - nach derzeitigem Ermittlungsstand - zu einem Mordversuch gegenüber einem der eingesetzten Polizeibeamten kam.

Die Erfahrungen auf Länderebene zeigen, dass die WRÜ in der Praxis auch im Bereich der Gefahrenabwehr maßvoll angewendet wird. Die Vorgaben des BVerfG zum Kernbereichsschutz werden auch für gefahrenabwehrrechtliche Maßnahmen der Wohnraumüberwachung berücksichtigt. Der BKAG-E sieht dementsprechend folgende Regelungen zum Kernbereichsschutz bei der WRÜ vor:

- Unzulässigkeit der Anordnung und Durchführung, wenn prognostisch kernbereichsrelevante Umstände erfasst werden
- Unverzügliche Unterbrechung, wenn kernbereichsrelevante Erkenntnisse erfasst werden
- Bestehen Zweifel, ob der Kernbereich betroffen ist, ist ein Live-Mithören untersagt, die - lediglich - automatisierte Aufzeichnung ist dann dem anordnenden Gericht zur Prüfung und Entscheidung vorzulegen (sog. "Richterband")
- Unverzügliche Löschungspflicht bei erkannten kernbereichsrelevanten Informationen
- Dokumentations-, Kennzeichnungs- und Benachrichtigungspflichten

3. Notwendigkeit der Telekommunikationsüberwachung / Quellen-TKÜ, § 20l BKAG-E

Dem Spektrum des internationalen Terrorismus zuzurechnende potentielle Gewalttäter kommunizieren aufgrund ihrer häufig länderübergreifenden Vernetzung und ihres konspirativen Vorgehens in der Regel auch über Mobilfunkgeräte und andere Kommunika-

tionswege, wie zum Beispiel Telefonie über das Internet. Dementsprechend haben notwendige Überwachungsmaßnahmen auch hier anzusetzen.

Besonders zu begrüßen ist die gesetzliche Klarstellung der Zulässigkeit der sog. *„Quellen – TKÜ“*. Nach § 20l Abs. 2 BKAG-E darf in vom Betroffenen genutzte informationstechnische Systeme dann eingegriffen werden, wenn durch technische Maßnahmen sichergestellt ist, dass hierbei *ausschließlich nur laufende Telekommunikation* überwacht wird und der Eingriff notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation *insbesondere auch in unverschlüsselter Form* zu ermöglichen. Damit zieht der Entwurf die Konsequenz aus der verfassungsgerichtlichen Feststellung (vgl. Urteil BVerfG vom 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07 – Nr. 190), dass Art. 10 GG der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer *„Quellen-Telekommunikationsüberwachung“* ist.

4. *Notwendigkeit der Rasterfahndung, § 20j BKAG-E*

Bei den in allen Ländern nach den Anschlägen vom 11. September 2001 durchgeführten präventiv-polizeilichen Rasterfahndungen hat sich gezeigt, dass die unterschiedlichen Regelungen in den Ländern sowie die uneinheitliche Rechtsprechung zu erheblichen Verzögerungen geführt haben. Mangels eigener Befugnis hierzu konnte das Bundeskriminalamt diese Aktion nur als Zentralstelle koordinierend und mit Maßnahmen des Datenabgleichs unterstützen.

Zu Unrecht wird oft von Kritikern der Erfolg der Rasterfahndung bezweifelt. Gerade bei der o. a. Aktion hat sich gezeigt, dass die Maßnahme zur Bekämpfung des Terrorismus erfolgreich eingesetzt werden kann. So hat sich ergeben, dass

- die Rasterfahndung das einzige geeignete Instrument der Polizeibehörden ist, um so genannte „Schläfer“ in einer anonymen Masse sich polizeilich unauffällig verhaltender Personen zu identifizieren
- durch die gewonnenen Informationen Ermittlungen initiiert bzw. gefördert werden konnten

- durch die Rasterfahndung „Gefährder"-Einstufungen verdichtet werden und
- im Zusammenhang mit weiteren Erkenntnissen aus dieser Maßnahme wesentliche Strukturen des internationalen Terrorismus aufgehellt und Gefährder erkannt werden konnten.

Das Bundesverfassungsgericht hat in seinem Beschluss vom 4. April 2006 – 1 BvR 518/02 (zur Rasterfahndung) – ausdrücklich festgestellt, dass für eine derartige Maßnahme eine *konkrete Gefahr*, etwa für die Vorbereitung oder Durchführung terroristischer Anschläge in Deutschland vorliegen müsse (vgl. hierzu: BVerfG aaO. Rdn. 147, Zitat: „*Der durch die Rasterfahndung bewirkte Eingriff in das Recht auf informationelle Selbstbestimmung setzt vielmehr das Vorliegen weiterer Tatsachen voraus, aus denen sich eine konkrete Gefahr ergibt, etwa weil tatsächliche Anhaltspunkte für die Vorbereitung terroristischer Anschläge oder dafür bestehen, dass sich in Deutschland Personen für Terroranschläge bereithalten, die in absehbarer Zeit in Deutschland selbst oder andernorts verübt werden sollen.*"). Diesen Anforderungen genügt der Entwurf. Er erklärt die Rasterfahndung für zulässig, soweit sie zur Abwehr einer (konkreten Gefahr) für

- den Bestand oder die Sicherheit des Bundes oder eines Landes oder
- für Leib, Leben oder Freiheit einer Person oder
- Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist, erforderlich ist.

Regelbeispielhaft und im Einklang mit der genannten Entscheidung des BVerfG geht der Entwurf von einer solchen Gefahr aus, wenn konkrete Vorbereitungshandlungen die Annahme rechtfertigen, dass eine Straftat nach § 4a Abs. 1 Satz 2 begangen werden soll.