Terrorismusbekämpfungsgesetz und Datenschutz

Marion Albers

Frühlingstr. 9
D-76131 Karlsruhe
Marion.Albers@web.de

Abstract: Das Terrorismusbekämpfungsgesetz hat die Kompetenzen der Sicherheitsbehörden zur Erhebung und Verarbeitung von Informationen und Daten erheblich erweitert. Grenzen müssen mit Hilfe eines prozeduralen Konzepts im jeweiligen Sach- und Regelungsbereich entwickelt werden. Die rechtliche Realisierung des Datenschutzes erfordert insgesamt eine im Ansatz bereichsspezifische Integration. Abstrakte, übergreifend geltende Vorgaben müssen ergänzend und systembildend hinzutreten.

1 Einleitung

Deutschland hat wie andere Länder auf den Anschlag des 11. September 2001 mit einer Diskussion um die äußere und innere Sicherheit reagiert. Das Phänomen des internationalen Terrorismus stellt eine besondere Herausforderung für die Handlungsmöglichkeiten des (National)Staates dar. Auf innenpolitischer Ebene ist erstens umgehend das Instrument der Rasterfahndung in einer Form und einem Umfang eingesetzt worden, die über den Einsatz zu Zeiten des 70er-Jahre Terrorismus hinausgehen. Mittlerweile gibt es mehrere Gerichtsentscheidungen, die das Vorliegen einer gegenwärtigen oder unmittelbar bevorstehenden Gefahrenlage verneint und den Einsatz in der vorgesehenen Form für rechtswidrig erklärt haben. Zweitens sind in aller Eile zwei Anti-Terror-Pakete verabschiedet worden. Deren wesentlicher Bestandteil ist das Gesetz zur Bekämpfung des internationalen Terrorismus mit einer Palette verschiedener Novellierungen.

Für die rechtliche Beurteilung dieser Maßnahmen spielt der Datenschutz eine zentrale Rolle. Von der einen Seite kommt das Schlagwort, er dürfe nicht zum Tatenschutz werden. Die andere Seite sieht in ihm ein wichtiges Instrument, Unbeteiligte vor staatlichen Zugriffen zu schützen. Der internationale Terrorismus verschärft diese Kontroverse aufgrund seiner Charakteristika und der daraus resultierenden Probleme für eine effektive und rechtsstaatliche Prävention.

Die folgenden Ausführungen befassen sich problemorientiert mit den wesentlichen Regelungen des Terrorismusbekämpfungsgesetzes. Es wird sich zeigen, dass ein sachgerechter Datenschutz differenzierte Regelungen in einem übergreifenden Regelungskonzept erfordert. Das ist nur im Wege einer bereichsspezifischen Integration zu leisten. Dieses Ergebnis ist zugleich ein Beitrag zur Diskussion um die Modernisierung des Datenschutzes.

2 Die Novellierungen des Terrorismusbekämpfungsgesetzes

2.1 Ziele der neuen Regelungen

Die neuen Regelungen verfolgen das Ziel, der Bedrohung durch den internationalen, insbesondere durch den fundamentalistischen Terrorismus entgegenzuwirken. Die Akzeptanz, die der Anschlag des 11. September Verschärfungen des Sicherheitsrechts verschafft hat, ist freilich zunächst genutzt worden, anderweitige und bislang nicht durchgesetzte Forderungen zu stellen. Dazu gehören der Ausbau des Bundeskriminalamtes bis hin zum Aufbau einer umfassenden Bundespolizei (Stichwort: deutsches FBI), die Beteiligung verdeckter Ermittler an Straftaten, die Ausweitung der Ermittlungsbefugnisse der Nachrichtendienste im Bereich der Beobachtung von Bestrebungen gegen die freiheitliche demokratische Grundordnung, nicht zuletzt sogar die Möglichkeit des Einsatzes der Bundeswehr im Innern. Einige dieser Forderungen sind in die ersten Gesetzesentwürfe eingeflossen. Wegen der Kritik der Öffentlichkeit sind sie im verabschiedeten Terrorismusbekämpfungsgesetz jedoch nicht realisiert worden. Das Gesetz nimmt in Anspruch, auf den internationalen Terrorismus zu reagieren und auf die damit verbundenen Anforderungen zugeschnitten zu sein.

2.2 Anforderungen aufgrund der Charakteristika des Terrorismus

Bereits seit Anfang der neunziger Jahre hat man mit neuartigen Formen des Terrorismus zu tun. Dessen Funktionen sind mehrdimensional: Anschläge sollen zum einen gegenüber dem konstruierten „Feind“ mit Schockeffekten Macht demonstrieren. Zum anderen sollen sie bei der Gruppe, die als die eigene betrachtet wird, Unterstützungsbereitschaft für das eigene Anliegen herstellen. Terrorismus ist insofern, ohne dass das verharmlosend gemeint ist, „Kommunikationsstrategie“. Auch seine Strukturen unterscheiden ihn von „klassischer“ Kriminalität: Auf der Zielebene ist er durch übergreifend-langfristige Zielsetzungen und eine Planmäßigkeit des Vorgehens gekennzeichnet. Auf der Organisationsebene finden sich teilweise abgeschottete, hierarchisch organisierte Zellenkonstruktionen, teilweise netzwerkartige Organisationsformen. Hinzu treten eine ausgeprägte Logistik, internationale Verflechtungen und ein besonderes Wissens- oder Geheimhaltungs„management“. Auf der Verhaltensebene werden zunehmend legale und illegale Verhaltensweisen kombiniert. Unter diesen Umständen sind die Finanzressourcen anders abgesichert als im Falle einer Geldbeschaffung durch Banküberfälle. Zum Teil sind Staaten in terroristische Handlungen verwickelt oder unterstützen sie zumindest mit Sympathie. Auch die Opferstrukturen gestalten sich im Vergleich zum Terrorismus der siebziger Jahre anders: Es wird relativ beliebig, welche Personen als Opfer betroffen sind. Die Auswahl des Orts und der Zeit von Anschlägen wird daher vom symbolischen Wert und von den erhofften Effekten gesteuert.

Funktionen und Strukturen des Terrorismus machen die Herausforderung für eine rechtsstaatliche Entgegnung deutlich: Einerseits reichen die traditionellen rechtlichen Reaktionsmuster der Abwehr konkreter Gefahren oder der Straftatenverfolgung nicht

aus. Staatliches Wissen muss schon das Vorfeld erfassen, damit beabsichtigte Anschläge rechtzeitig erkannt und verhindert werden können. Es darf sich nicht nur auf Einzelereignisse beschränken, sondern muss sich auf die Erforschung von Strukturen erstrecken, also etwa auf den sachlichen Zusammenhang verschiedener Ereignisse oder auf die Netzwerke von Personen. Zugleich ist es aufgrund der Langfristigkeit terroristischer Ziele, der Kombination legaler und illegaler Verhaltensweisen oder des Geheimhaltungsmanagements schwer, überhaupt brauchbares Wissen zu erlangen. Andererseits wäre eine umfassende staatliche Überwachung, die zwingend zahlreiche Unbeteiligte erfasst, grundrechtswidrig. Sie wäre zudem - wie nicht zuletzt die Ergebnisse der Rasterfahndung belegen - wegen der Vielzahl irrelevanter Informationen schlicht ineffizient.

2.3 Inhalte und Funktionen der neuen Regelungen

Mit welchen Novellierungen reagiert nun das Terrorismusbekämpfungsgesetz ? Es erweitert vor allem die Aufgaben und Befugnisse der Nachrichtendienste, der Bundespolizeien und der Ausländerbehörden. Ihnen sind neue Kompetenzen im Bereich ihrer eigenen Aufgaben und neue Kompetenzen im Bereich der Zusammenarbeit zugewiesen worden. Übergreifend sind die in allen Fällen der Identifizierung relevanten Regelungen über Pass, Personalausweis und Aufenthaltsgenehmigung geändert worden: Zur Sicherung einer eindeutigen Identitätsfeststellung dürfen diese Dokumente künftig biometrische Merkmale von Fingern, Händen oder Gesicht des Inhabers enthalten.

2.3.1. Neue Ermittlungs-, Entscheidungs- und Handlungskompetenzen

Bei den Nachrichtendiensten hatten die Verfassungsschutzämter als Inlandsnachrichtendienste bisher unter anderem die Aufgabe, Informationen über Bestrebungen im Inland zu gewinnen, die durch Gewaltanwendung auswärtige Belange der Bundesrepublik gefährden, und darüber die Bundesregierung zu informieren. Das Terrorismusbekämpfungsgesetz dehnt dies auf inländische Bestrebungen aus, die gegen den Gedanken der Völkerverständigung, insbesondere gegen das friedliche Zusammenleben der Völker gerichtet sind. Ziel ist, Organisationen wie die der Taliban oder Hizb Allah, die Gewalt gegen politische Gegner im Ausland einsetzen, überwachen zu können. Die neue Regelung ist bedingt durch die internationalen Verflechtungen des Terrorismus und in ihrer Zielrichtung durchaus sinnvoll. Sie führt allerdings dazu, dass die klare Trennung zwischen Inlands- und Auslandsnachrichtendienst verwischt wird. Die aus Kompetenzgründen notwendige Rückkoppelung zur „inneren Sicherheit“ und die Vielfältigkeit der Bestrebungen, die auf politische Ziele und gegen politische Gegner im Ausland gerichtet sind, kosten den Preis hochgradig unbestimmter Formulierungen.

Die Ermittlungsbefugnisse sowohl des Bundesamtes für Verfassungsschutz als auch des Bundesnachrichtendienstes werden im Finanz-, Post- und Telekommunikationsbereich erheblich erweitert. Bei Banken oder Finanzdienstleistern dürfen Auskünfte über Konten, Kontoinhaber und sonstige Berechtigte eingeholt werden. Das ist eine Reaktion auf die neuartigen Formen terroristischer Finanzressourcen, bei denen mit der Kombination

von Legalität und Illegalität operiert wird. Postdienstleister müssen Auskünfte zu Namen, Anschriften und Umständen des Postverkehrs und Telekommunikations- oder Teledienstleister Auskünfte über Verbindungs- oder Nutzungsdaten erteilen. Weiter wird der Einsatz des IMSI-Catchers erlaubt. Diese Überwachungsmöglichkeiten nutzen die international verflochtenen netzwerkartigen Organisationsformen und den daraus resultierenden Kommunikationsbedarf.

Da viele Unbeteiligte von diesen Maßnahmen betroffen sein können, sind deren Voraussetzungen von besonderer Bedeutung. Auskunftsverlangen im Finanzbereich sind an die Voraussetzung geknüpft, dass die Daten zur Erfüllung der jeweiligen Aufgaben erforderlich sind und tatsächliche Anhaltspunkte für schwerwiegende Gefahren für das friedliche Zusammenleben der Völker oder für außen- und sicherheitspolitische Belange Deutschlands vorliegen. Auskunftsverlangen im Post- oder Telekommunikationsbereich setzen die Erforderlichkeit für die Aufgabenerfüllung und bei den Verfassungsschutzämtern zusätzlich tatsächliche Anhaltspunkte für den Verdacht bestimmter Straftaten voraus. Die Tatbestandsvoraussetzungen sind schwer zu konkretisieren. Das soll durch organisations- und verfahrensrechtliche Schutzvorkehrungen kompensiert werden. Die Auskunftsverlangen erfordern einen begründeten Antrag, über den das zuständige Bundesministerium zu entscheiden hat. In allen Bereichen sind die G-10-Kommission und das Parlamentarische Kontrollgremium als Kontrollinstitution eingeschaltet.

Bei den Bundespolizeien regelt das Terrorismusbekämpfungsgesetz den Einsatz des Bundesgrenzschutzes im Grenzgebiet und an Bord von Luftfahrzeugen. Auch die Kompetenzen des Bundeskriminalamtes werden erweitert: Es erhält eine originäre Zuständigkeit für die Strafverfolgung im Bereich der Computersabotage und eigenständige Befugnisse zur Datenerhebung im Rahmen seiner Zentralstellenfunktion.

Den Ausländerbehörden werden eine Reihe neuer Befugnisse eingeräumt, die der Sicherung der Identität von Ausländern dienen. Zum Beispiel werden die Daten spezifiziert, die in der Aufenthaltsgenehmigung oder im Ausweisersatz enthalten sind. Unter bestimmten Voraussetzungen wird eine Identitätssicherung durch Abdrucke aller zehn Finger vorgeschrieben. Außerdem werden bestimmte Entscheidungskompetenzen verschärft: Eine Aufenthaltsgenehmigung darf versagt werden, wenn die antragstellende Person die freiheitliche demokratische Grundordnung gefährdet oder wenn Tatsachen belegen, dass sie eine Vereinigung des internationalen Terrorismus mitträgt oder unterstützt. Hinzuweisen ist in diesem Zusammenhang auch auf die erhebliche Erweiterung der Möglichkeit, Ausländervereine zu verbieten.

2.3.2 Neue Regelungen der Zusammenarbeit

Die Zusammenarbeit der verschiedenen Behörden durch wechselseitige Information und Datenübermittlungen ist wegen der Differenzierung der Kompetenzen wichtig. Freilich bedeutet gerade diese Differenzierung auch, dass ein uneingeschränkter Informationsaustausch rechtlich unzulässig ist. Im Terrorismusbekämpfungsgesetz wird die Zusammenarbeit zwischen Nachrichtendiensten, Polizeien und Ausländerbehörden bereits durch die jeweils neuen Ermittlungsbefugnisse erweitert, soweit sich die vorhandenen

Übermittlungstatbestände entsprechend ausdehnen. Darüber hinaus werden einige neue Regelungen eingeführt.

Man kann einige Beispiele hervorheben: Das Bundesamt für die Anerkennung ausländischer Flüchtlinge oder Ausländerbehörden müssen nunmehr von sich aus den Verfassungsschutzbehörden Informationen über Bestrebungen oder Tätigkeiten mitteilen, die durch Gewaltanwendung auswärtige Belange der Bundesrepublik gefährden oder gegen das friedliche Zusammenleben der Völker gerichtet sind. Nach der Gesetzesbegründung zählt dazu in der Regel die Tatsache, dass eine Person einer islamistischen gewaltbereiten Organisation angehört. Die Probleme, zu denen dies führen kann, wenn etwa ein Asylantrag mit der Mitgliedschaft in einer regimekritischen gewaltbereiten Organisation begründet wird, versucht das Gesetz durch Beschränkungen der Übermittlungsbefugnisse des Verfassungsschutzes zu lösen. Des Weiteren darf der Bundesnachrichtendienst Daten aus der strategischen, also anlass- und verdachtslosen Fernmeldekontrolle an die Verfassungsschutzbehörden übermitteln, wenn die Daten für deren neue Aufgabe der Beobachtung von Bestrebungen gegen das friedliche Zusammenleben der Völker relevant sind. In erheblichem Umfang werden außerdem die Speicher- und Übermittlungstatbestände im Bereich des Ausländerzentralregisters ausgedehnt.

2.4 Folgerungen und Beurteilungen

Das Terrorismusbekämpfungsgesetz erweitert insbesondere die Möglichkeiten der Erhebung, Verarbeitung und Übermittlung von Informationen und Daten. Dabei sind die tatbestandlichen Voraussetzungen der gesetzlichen Regelungen teilweise äußerst unbestimmt. Allerdings stellt der internationale Terrorismus in besonderer Weise Anforderungen daran, dass Gefahren überhaupt erst erkannt und richtig analysiert werden. Maßnahmen werden jedoch in absehbarer Weise mit einer sehr hohen Streubreite verbunden sein, also eine hohe Zahl von im Ergebnis ganz unbeteiligten Personen treffen. Das gilt um so mehr, wenn man berücksichtigt, dass die eigentlichen „Adressaten“ konspirativ operieren und etwa im Bereich der Telekommunikation Verschlüsselungstechniken nutzen werden.

Das Problem besteht somit darin, einerseits den Gefahren des Terrorismus zu begegnen, andererseits so wenig wie möglich Freiheiten Unbeteiligter einzuschränken. Eine Lösung lässt sich hier nur entwickeln, wenn man die Aufmerksamkeit nicht allein auf die Ermittlungskompetenzen, sondern auf den gesamten Prozess der Informations- und Datenverarbeitung richtet. Auf dieser Grundlage ist ein prozedurales Konzept rechtlich immer neu ansetzender Bindungen zu erarbeiten. So muss eine weit gefasste Befugnis zur Erhebung von Daten zumindest durch enger gestaltete Speicherbefugnisse, durch Zugriffsbeschränkungen oder durch Kontroll- und Korrekturmechanismen im Verarbeitungsprozess kompensiert werden. Das Terrorismusbekämpfungsgesetz sieht zum Teil organisations- und verfahrensrechtliche Schutzvorkehrungen vor, zum Beispiel die Kontrolle durch die G-10-Kommission. Dadurch wirken immerhin verschiedene Stellen an der Entscheidung über Überwachungsmaßnahmen mit.

Ein Konzept rechtlicher Bindungen, die im Prozess des Umgangs mit Informationen und Daten zu sachgerechten Vorgaben und Grenzen führen, erfordert zum einen die adäquate Abstimmung der Regelungen der Informations- und Datenverarbeitung untereinander. Es erfordert aber auch eine präzise Abstimmung mit den sachlichen Aufgaben und Befugnissen der jeweiligen Behörde. Datenschutz kommt somit ohne eine bereichsspezifische Integration nicht aus.

3 Die Zukunft des Datenschutzes

Ein sinnvoller Datenschutz - oder genauer: ein sinnvolles Informationsrecht - ist insgesamt nur zu entwickeln, wenn man die Regelungen des Umgangs mit Informationen und Daten miteinander, aber vor allem auch angemessen mit den jeweiligen sachlichen Aufgaben und Befugnissen koordiniert. Sie müssen also jedenfalls im Ansatz in den Sachzusammenhang eingegliedert werden. Das schließt nicht aus, dass man allgemeinerbereichsübergreifend geltende Vorgaben abstrahieren kann. Dabei handelt es sich jedoch um einen prinzipiell nachgeordneten Schritt.

Die jüngeren Überlegungen zur Modernisierung des Datenschutzes setzen geradezu umgekehrt an: Man könne den Datenschutz mit einer Reihe übergreifender Grundsatzbestimmungen und wenigen bereichsbezogenen Modifikationen regeln. Damit wird jedoch der falsche Weg gewählt.

Der Datenschutz wird aus seiner zu bürokratischen Ausgestaltung erst gelöst, wenn man statt der Datenebene die Informationsebene und sodann deren enge Verknüpfung zur Ebene der sachlichen Entscheidungen oder Handlungen in den Mittelpunkt stellt. Nur mit Blick auf den jeweiligen Sach- und Regelungsbereich lassen sich die Schutzziele, die Schutzerfordernisse, der Regelungsbedarf und die angemessenen Regelungsformen klären. Darüber muss präzisiert werden, an welcher Stelle wirklich Regelungsprobleme liegen. Es kommt künftig darauf an, dass das Datenschutz- oder Informationsrecht nicht faktische Vorgänge nachzeichnet, sondern dem Schutzbedarf betroffener Personen in den Hinsichten Rechnung trägt, in denen er sich begründen lässt. Wegen der Reichweite der Aspekte, die mit der Kategorie „Information“ angesprochen sind, wird dies bei allem Bemühen um Vereinfachung vielschichtig bleiben. Die Zukunft des Datenschutzes erfordert ein mehrdimensionales und gleichwohl transparentes Konzept.