Humanistische Union

Etikettenschwindel, Unschärfen und kreative Gesetzesanwendung

Eine kritische Lektüre des „Evaluationsberichts“ zum Terrorismusbekämpfungsergänzungsgesetz. Aus: Mitteilungen Nr. 214 (3/2011), S. 6-8

An der einseitigen Perspektive des „Evaluationsberichts“, den der Bundesminister des Innern (BMI) vorgelegt hat, kann es keine Zweifel geben: Aus der Sicht der Sicherheitsbehörden erscheinen alle neuen Befugnisse als nützlich, sinnvoll und in vielerlei Hinsicht ausbaufähig. Von einmal geschaffenen „Werkzeugen“ mag man sich nur schwer wieder trennen. Andererseits wird die Entwicklung der Gefährdungslage selbst kaum thematisiert [1]; pauschale Urteile über fortwährende terroristische Bedrohungen ersetzen eine substantielle Debatte über die Angemessenheit und Notwendigkeit der Sicherheitsgesetze nach 10 Jahren „war on terrorism“.

Dennoch soll hier der Versuch unternommen werden, aus dem Bericht – gewissermaßen zwischen den Zeilen – Anhaltspunkte für problematische Entwicklungen in der praktischen Anwendung der Anti-Terror-Gesetze und damit Aufgaben einer echten Evaluation herauszuarbeiten. Die folgenden Ausführungen sind eine erste Skizze, ohne Anspruch auf Vollständigkeit.

Etikettenschwindel „Terrorismusbekämpfung“

Eine erste Irritation befällt einen, wenn man verschiedene Verlautbarungen zum Sinn und Zweck der sog. Anti-Terror-Gesetze vergleicht: In den vom Innenministerium veröffentlichten Fragen und Antworten zum TBEG heißt es, „als betroffene Personen kommen hier insbesondere vermutliche Terroristen und deren Unterstützer in Betracht. Für andere Zwecke können die Auskunftsbefugnisse nicht genutzt werden“ (BMI 2011c: 1). Im Evaluationsbericht heißt es dagegen, die Befugnisse seien zwar nicht nur gegen terroristische Bestrebungen angewandt worden – dies stelle jedoch keine Zweckentfremdung dar, da der Gesetzgeber die Intention gehabt habe, „Instrumente zu schaffen, die auf alle Phänomenbereiche anwendbar sind“ (BMI 2011a: 36). Ein genauer Blick auf die Zahlen bestätigt diese universelle Anwendung der „Anti-Terror-Gesetzgebung“ – einige Beispiele: Anfragen zu Bestandsdaten von Postdienstleistern und Teledienstleistern (§ 8a Abs. 1 BVerfSchG) wurden vor allem im Zusammenhang mit dem nationalen Rechtsextremismus eingeholt; Ausschreibungen zur verdeckten Beobachtungen im Schengener Informationssystem (§ 17 Abs. 3 BVerfSchG) werden vor allem bei Verdacht auf Spionage und Proliferation eingesetzt.

Massenhafte Sicherheitsüberprüfungen werfen massenhaft Fragen auf

Die in quantitativer Hinsicht wohl bedeutsamsten Anti-Terror-Maßnahmen sind die sog. Sicherheitsüberprüfungen. Sie sollen dem Schutz lebens- und verteidigungswichtiger Einrichtungen vor Sabotageakten dienen, darunter fallen etwa Bundestag, Bundesbank, Dienstleister für behördliche Infrastrukturen, Teile von TK-Unternehmen, Verkehrsbetriebe, Energie- und Wasserversorger. Von den Sicherheitsüberprüfungen waren zwischen 2007 und 2009 über 64.000 Personen betroffen. Mögliche „Treffer“ in den abgefragten Datenbanken werden in einer dreistufigen Skala bewertet: als

„sicherheitserhebliche Erkenntnisse“, „Sicherheitshinweise“ oder „Sicherheitsrisiken“. In die letzte, risikostärkste Kategorie fielen dabei 628 Fälle (rd. 1 Prozent der Überprüften), bei fast 10 Prozent gab es „Auffälligkeit“ jedweder Art. Über die jeweiligen Konsequenzen für die Betroffenen, die sich aus ihrer Einstufung in eine der drei Risikogruppen ergibt, schweigt sich der Bericht weitgehend aus. Obwohl eine Risikoeinstufung genauso wie die verweigerte Überprüfung ernsthafte Konsequenzen nach sich zieht (etwa den Verlust des Arbeitsplatzes), stuft das BMI die Belastung der Betroffenen als „unerheblich“ ein, da die Untersuchung auf freiwilliger Basis erfolge (BMI 2011a: 32).

Mehr noch, die vom Ministerium selbst erkannte Unschärfe der Einstufung in Risikogruppen – Was sind sicherheitsrelevante Bereiche? Wer muss überprüft werden? Welche Tatsachen rechtfertigen ein starke Risikodiagnose? – werden zwar als Risiken der öffentlichen Sicherheit, nicht jedoch als Sicherheitsdefizit für die Überprüften erkannt: „Trotz Beratung in Veranstaltungen oder im Einzelfall stoßen die Vorschriften mit unbestimmten Rechtsbegriffen zum Teil auf erhebliche Anwendungsschwierigkeiten in den Unternehmen, etwa weil allgemeingültige branchenspezifische Kriterien zur Feststellung sicherheitsempfindlicher Stellen fehlen. Das hat zur Folge, dass sicherheitsempfindliche Stellen nicht oder in einer Branche unterschiedlich festgestellt werden, was wiederum Einfluss auf die Auswahl der zu überprüfenden Personen hat. Dies bedeutet, dass in sabotagegefährdeten lebenswichtigen Einrichtungen der gleichen Branche sowohl sicherheitsüberprüftes als auch nicht sicherheitsüberprüftes Personal eingesetzt wird. (…) Im Ergebnis gehen die von BfV und MAD aufgrund der durchgeführten Sicherheitsüberprüfungen festgestellten Sicherheitsrisiken im Schwerpunkt auf Zweifel an der Zuverlässigkeit der überprüften Personen zurück. Zweifel an der Zuverlässigkeit ergaben sich dabei in den meisten Fällen aus Straftaten, oftmals verbunden mit einer Alkohol- oder Drogenproblematik, und aus Fällen, in denen finanzielle Schwierigkeiten, insbesondere eine Überschuldung, eine Rolle spielten. Es handelte sich um Feststellungen, die die Zuverlässigkeit im Allgemeinen betreffen, aber nicht unbedingt auf terroristische oder zielgerichtete Sabotageabsichten schließen lassen. Im militärischen Bereich ergeben sich darüber hinaus sicherheitserhebliche Erkenntnisse oft auch aus der Herkunft von Soldaten und Beschäftigten aus Staaten mit besonderen Sicherheitsrisiken (Staaten im Sinne des § 13 Abs. 1 Satz 1 Nr. 17 SÜG) bzw. aus deren Kontakten oder verwandtschaftlichen Beziehungen dorthin“ (BMI 2011a: 29).

Diskriminierungsverbot oder Konspirationszwang?

Wie kreativ das Innenministerium mit den Rechtsschutzbedürfnissen überwachter BürgerInnen umgehen kann, zeigt das Beispiel der Kontodatenabfragen: In mehreren Fällen kam es infolge der Sicherheitsanfragen des BfV bei Kreditinstituten und Finanzdienstleistern zu Kontosperrungen und -kündigungen für die (unwissenden) Betroffenen. Die Banken begründen ihr Verhalten u.a. damit, dass das BfV die betreffenden Unternehmen nicht von Haftungsfragen freistelle. Sie verstießen damit zwar nicht direkt gegen das im Gesetz vorgeschriebene Gebot der Vertraulichkeit der Abfragen gegenüber ihren Kunden.

Dennoch sorgt sich das BMI darum, dass die Überwachten aus der Kündigung bzw. dem Nicht-Abschluss neuer Verträge einen Hinweis auf ihre Bespitzelung ziehen könnten. Daher fordert das BMI in seinem Bericht ein gesetzliches Diskriminierungsverbot, dessen Motiv jedoch weniger im Schutz der Betroffenen, sondern in der geräuschlosen Abwicklung weiterer Überwachungsmaßnahmen liegt. So schreibt das Ministerium, durch ein gesetzliches Benachteiligungsverbot aufgrund von Kontodatenabfragen des BfV „würde klargestellt, dass aus einer Fortsetzung der Geschäftsbeziehung trotz des Eingangs des Auskunftsersuchens keine zivil-, straf- oder öffentlich-rechtlichen Nachteile entstehen, weil die Fortsetzung der Geschäftsbeziehung dann einer gesetzlich normierten öffentlich-rechtlichen Verpflichtung entspricht. Eine solche Regelung würde den Betroffenen schützen, der nicht bereits auf Grund nur von tatsächlichen Anhaltspunkten in seiner wirtschaftlichen Bewegungsfreiheit beschränkt werden soll, ebenso wie die verpflichteten Unternehmen der Finanzbranche, die keine Verantwortlichkeit oder Haftung bei einer Fortsetzung der Geschäftsbeziehung befürchten müssten; zudem würde sie die Aufgabenerfüllung der Nachrichtendienste fördern, da ein vorzeitiger Abbruch der Geschäftsbeziehung die weitere Beobachtung

und damit die Erkenntnisgewinnung gefährden kann. Dass das Benachteiligungsverbot vom Betroffenen nicht effektiv zwangsweise durchsetzbar ist, solange er keine Kenntnis von dem Auskunftsersuchen und damit den Gründen der Benachteiligung hat, ändert nichts am Wert einer derartigen Regelung. Ihre Wirkung wird sie entfalten, indem gegenüber dem Auskunftspflichtigen gesetzlich klargestellt wird, dass die Aufrechterhaltung der Geschäftsbeziehung nicht rechtswidrig ist.“ (BMI 2011a: 74 f.).

IMSI-Catcher auch gegen Laptops

Ein Beispiel, wie sich geheimdienstliche Befugnisse unterhalb der gesetzlichen Ebene ausweiten lassen, bietet der Einsatz des IMSI-Catchers beim BfV: Sogenannte IMSI-Catcher erlauben es, wahlweise den Standort eines bekannten Mobilfunkendgerätes (sprich: Handys) zu ermitteln (Lokalisierung) oder aber bei einer observierten Zielperson (deren Standort bekannt ist) die Gerätenummer ihres Handys (IMEI) bzw. ihre Kartennummer (IMSI) zu bestimmen. Der IMSI-Catcher wird üblicherweise zur Vorbereitung einer Telefonüberwachung (TKÜ) eingesetzt, weil dafür Geräte- und Kartennummern benötigt werden.

Wie aus dem Evaluationsbericht hervorgeht, wurde die Befugnis zum IMSI-Catcher-Einsatz vom Bundesamt für Verfassungsschutz (§ 9 Abs. 4 BVerfSchG) auch genutzt, um mit einem WLAN-Catcher die Netzwerkanschlüsse von Computern zu ermitteln. Das Ministerium schreibt dazu: „Die Norm ... wurde konkret im Hinblick auf Mobiltelefone ausgestaltet, wobei unterstellt wurde, dass diese Telefone stets mit einer Geräte- oder Kartennummer ausgestattet sind. Im Laufe der Zeit, vor allem im Zusammenhang mit den nachrichtendienstlichen Erhebungen gegen die so genannte Sauerland-Gruppe, hat sich Bedarf an der Schaffung einer Regelung zum Einsatz so genannter WLAN-Catcher gezeigt. Bei einem WLAN-Catcher handelt es sich um ein Gerät, das Daten von aktiv geschalteten, funkbasierten Computernetzwerken anzeigt. Von Interesse für die Sicherheitsbehörden bei der Vorbereitung von G10-Maßnahmen sind dabei insbesondere die MAC-Adressen (eindeutige Gerätenummern) der von der betroffenen Person verwendeten Funk-Netzwerkschnittstellen. Rein begrifflich handelt es sich bei der MAC-Adresse eines zumindest mobil einsetzbaren, WLAN-basierten Endgeräts in einem Computernetz zwar um die Gerätenummer eines mobilen, funkbasierten Endgerätes, so dass der Einsatz eines WLAN-Catchers noch unter den Wortlaut des § 9 Abs. 4 BVerfSchG fallen dürfte.“ (BMI 2011a: 80 f.) Für die Zukunft fordert das BMI jedoch eine technikneutrale Formulierung der Vorschrift, mit der sich alle funkbasierten Geräte und Anwendungen überwachen lassen. Das würden den Rahmen der zu überwachenden Geräte stark erweitern – nicht nur alle Computer, Laptops und Tablets, sondern auch moderne Fernseher, Videorekorder, Kühlschränke oder Stromzähler dürften dann gecatcht werden.

Man kann die MAC-Adressen der Netzwerkschnittstellen von Computern oder Smartphones im weitesten Sinne als Gerätekennung verstehen, und die Datenübertragung per Wireless Lan stellt sicher auch eine Form der Mobilfunktechnik dar. Dennoch ist die freihändige Übertragung einer Überwachungsbefugnis, die für eine auf Providern aufbauende Mobilfunktechnik konzipiert war, in den Bereich der „privaten Funktechnik“ problematisch. Zum einen: Viele Nutzer vernetzen heutzutage ihre elektronischen Geräte innerhalb ihrer Wohnung mittels WLAN und ersparen sich dadurch das Verlegen von Kabeln. Handelt es sich dabei um Telekommunikation, wenn die Daten vom heimischen Arbeitsrechner zur Tablet-LeserIn auf dem Sofa übertragen werden (und die Wohnung eigentlich gar nicht verlassen sollen)? Und außerdem: Wofür kann das BfV die mittels WLAN-Catcher ermittelten Netzwerkkennungen eigentlich nutzen? Eine Überwachung der computergestützten Telekommunikation setzt üblicherweise beim Mail-/Internet-Provider an, dafür werden keine MAC-Adressen benötigt. Online-Durchsuchung, ich hör Dir trapsen ...

Gesetzliche Mitteilungspflicht – anders verstanden

Damit sich Betroffene gegen ihre Überwachung überhaupt mit rechtsstaatlichen Mitteln wehren können, müssten sie zumindest nachträglich darüber informiert werden. Die bestehende gesetzliche Mitteilungspflicht wird meist mit Verweis auf eine drohende „Offenlegung der Arbeitsweise oder konkreter Beobachtungsfelder“ der Geheimdienste übergangen. So hat das BfV bei Ausschreibungen zur verdeckten Beobachtungen im Schengen-Informations-System im Jahr 2009 keinen einzigen Betroffenen (wie vom Gesetz vorgesehen) über diese Fahndung informiert. Insgesamt – so der Bericht des BMI – wurden nur etwa 50% der Betroffenen über die gegen sie eingeleiteten Überwachungsmaßnahmen informiert, und das mit einer Verzögerung von bis zu 10 Jahren. Viel besorgniserregender, als die damit faktisch verbundene Aussetzung aller Rechtsschutzmöglichkeiten, findet das BMI jedoch, dass bei fehlender Benachrichtigung die Verfahren bei den Sicherheitsbehörden nicht abgeschlossen werden könnten, solange keine Mitteilung an die Betroffenen erfolgte. Als wenn die offenen Akten das zentrale Problem der Mitteilungspflicht wären, fordert das BMI deshalb die Möglichkeit, von der Mitteilungspflicht endgültig absehen zu können.

Stefan Apell und Sven Lüders

[1] Zur Diskussion um die Gefahrenlage: Von 249 im Jahr 2010 in Europa begangenen Straftaten, die von Europol als „terroristisch“ eingestuft werden, hatten lediglich drei einen islamistischen Hintergrund (vgl. Europol: EU Terrorism and Trend Report 2011 (TE-SAT 2011), S. 15 ff., https://www.europol.europa.eu/sites/default/files/publications/te-sat2011.pdf).

[2] Der grüne Netzpolitiker Malte Spitz hat für eine Demonstration der Datenmengen die bei seinem Provider gespeicherten Verbindungsdaten für den Zeitraum eines halben Jahres abgerufen und diese Daten in anonymisierter Form veröffentlicht – die Liste umfasste für sechs Monate 35.831 Einträge (s. http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten).

Bundesministerium des Inneren (BMI) 2011a: Bericht zum Ergebnis der Evaluierung nach Artikel 11 des Terrorismusbekämpfungsergänzungsgesetzes vom 5. Januar 2007 (BGBI. I S. 2), ÖS II 1 -611 120-5/0. Entwurf vom 14.03.2011.

Bundesministerium des Inneren (BMI) 2011b: Eckpunkte zu den Anti-Terror-Gesetzen. http://www.bmi.bund.de/SharedDocs/Downloads/DE/ Kurzmeldungen/antiterrorgesetze.pdf

Bundesministerium des Inneren (BMI) 2011c: Antiterrorgesetze FAQ. In: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Kurzmeldungen/antiterrorgesetze_faq.pdf

Bundesministerium der Justiz (BMJ) 2011: Stellungnahme zur Evaluierung des Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes (Terrorismusbekämpfungsergänzungsgesetz – TBEG), Berlin.
