

Antiterrordatei

Die Herausbildung des Gemeinsamen Terrorismusabwehrzentrums (GTAZ) und die Etablierung der Antiterrordatei weichen das Trennungsgebot auf und bewirken eine schleichende Verschmelzung von Polizei und Nachrichtendiensten.

Von Kai Rogusch

Seit dem 11. September 2001 orientiert sich die „westliche Wertegemeinschaft“ in ihren institutionellen Antworten auf den „globalen Terror“ am sicherheitspolitischen Paradigma der „globalen Risikogesellschaft“. Die Etablierung der neuen Sicherheitsarchitektur bewirkt dabei eine Relativierung demokratischer Tabus, die sich aus der föderalistischen Kompetenzordnung ergeben. Beispielhaft hierfür sind fortgesetzte Forderungen nach einem verstärkten Einsatz der Bundeswehr im Innern. Zugleich bilden sich als wichtige Bestandteile des neuen Sicherheitsparadigmas ein „Gemeinsames Terrorismusabwehrzentrum des Bundes und der Länder“ (GTAZ) und eine so genannte Antiterrordatei heraus. Der globalen Vernetzung des Terrors soll eine möglichst enge „Verzahnung“ der Polizeibehörden mit den Geheimdiensten entgegengesetzt werden, mit der man terroristischen Bestrebungen mittels einer möglichst schnellen Reaktionsfähigkeit bereits im Vorfeld begegnen will. Ziel ist, so früh wie möglich zu erkennen, ob jemandes Verhalten auf zukünftige terroristische Handlungen schließen lässt.

Hierbei zeichnet sich eine in der Geschichte der Bundesrepublik Deutschland beispiellose Relativierung eines weiteren Prinzips ab, das einst dazu gedacht war, Machtkonzentration undurchschaubarer Sicherheitsbehörden abzuwenden. Denn die mittels GTAZ und Antiterrordatei avisierte „Verzahnung“ sämtlicher deutscher Sicherheitsbehörden tastet nicht zuletzt das für freiheitliche Rechtsstaaten unerlässliche Trennungsgebot zwischen Nachrichtendiensten und Polizeibehörden an. Im GTAZ arbeiten Vertreter aller maßgeblichen Sicherheitsbehörden des Bundes und der Länder an einer „Optimierung“ des Informationsaustausches. Innerhalb des GTAZ bilden die Vertreter der Polizeibehörden und Strafverfolgungsorgane die „Polizeiliche Informations- und Analysestelle“ (PIAS) und die Vertreter der Nachrichtendienste die „Nachrichtendienstliche Informations- und Analysestelle“ (NIAS). In zahlreichen Kooperationsformen soll sich eine intensive und verstetigte Zusammenarbeit zum Zweck der Gefährdungsbewertung, des operativen Informationsaustausches, der

Fallauswertung, der Erstellung von Strukturanalysen und zur Aufklärung vor allem des islamistisch-terroristischen Personenpotenzials vollziehen.

Auch die Antiterrordatei dient der „Bündelung“ separater, auf den Terror bezogener Informationen. Die Antiterrordatei erfasst die Erkenntnisse von 37 verschiedenen Sicherheitsbehörden, die bisher traditionell in dieser Form nicht zusammenarbeiteten. Hieran beteiligen sich 16 Landeskriminalämter, 16 Landesämter für Verfassungsschutz, der Militärische Abschirmdienst, die Bundespolizei und das Bundeskriminalamt. Die Hardware für die Antiterrordatei wird beim Bundeskriminalamt in Wiesbaden angesiedelt.

Auf diese Datei sollen alle 37 Einrichtungen Zugriff haben. In der Praxis würde das so aussehen: Wenn etwa das hessische Landeskriminalamt in Wiesbaden einen Terrorverdächtigen im Visier hat, hätten ausgesuchte Beamte Zugang zur Antiterrordatei. Sie würden den Namen eingeben und bekämen bei positivem Bescheid einen Treffer. Sofort hätten sie ungehinderten Einblick in die so genannten „Grunddaten“ der Antiterrordatei, die Angaben über die Identität einer verdächtigen Person machen: Geheimdienstlich erlangte „Informationen“ über Namen, Aliaspersonalien, Geschlecht, Geburtsdatum und Geburtsort lägen dem LKA-Beamten genauso offen vor wie auch „Erkenntnisse“ über aktuelle und frühere Staatsangehörigkeiten, gegenwärtige und frühere Anschriften, besondere körperliche Merkmale, Sprachen, Dialekte und Lichtbilder. Unter bestimmten Voraussetzungen könnte der Beamte aber auch einen „vertieften“ Zugriff auf geheimdienstliche Verdachtsmomente in Form „erweiterter Grunddaten“ bekommen.

Problematisch hieran ist, dass die Polizei über die Antiterrordatei auch Zugang zu geheimdienstlich gewonnenen Daten erlangt, die sie so im Rahmen ihrer engeren Kompetenzen nicht bekommen hätte. Denn die Geheimdienste sind bei ihrer geheimen Informationsbeschaffung mit einem deutlich breiteren legalen Aktionsradius ausgestattet als die Polizeien: Ihnen sind Aufgabenfelder eröffnet, die weit vor der Entstehung konkreter Gefahren liegen können. Dazu zählen allgemeine Aufklärungsaufgaben unabhängig von Gefahrenszenarien, wie etwa die anlassunabhängige Überwachung des internationalen Telefonverkehrs durch den Bundesnachrichtendienst oder die fortgesetzte Beobachtung legaler Aktivitäten von Parteien und Religionsgemeinschaften durch die Landesämter und das Bundesamt für Verfassungsschutz. Der Aktionsradius der Geheimdienste erstreckt sich auf mögliche, aber im Vorhinein nicht absehbare Gefährdung für die „freiheitliche demokratische Grundordnung“. Neuerdings geraten auch „Bestrebungen“ ins Visier des Inlandsgeheimdienstes, die sich gegen den „Gedanken der Völkerverständigung“ richten.

Laut dem Verfassungsexperten Christoph Gusy begründet sich hierin das Trennungsgebot: Weil die Polizei, zumindest in der Theorie, nur über vergleichsweise enge Ermittlungsspielräume verfügt, darf sie sehr weitgehende Mittel einsetzen; weil die Nachrichtendienste sehr weitgehende Ermittlungsspielräume haben, sind ihnen polizeiliche Befugnisse versagt. Anders ausgedrückt: Die Polizei darf weniger wissen und daher ihr Wissen auch zu sehr einschneidenden Maßnahmen gegen die Bürger verwenden. Die Nachrichtendienste dürfen mehr wissen, dieses Wissen daher weniger zu Lasten der Bürger verwenden.

Mit der Herausbildung des GTAZ wie auch der Antiterrordatei wird dieser Grundsatz auf dem Feld der vorgeblichen Terrorbekämpfung aufgeweicht. Doch ist diese Entwicklung nicht ganz neu. Die Aufweichung des dem Trennungsgebot zugrunde liegenden Gedankens hat sich in den letzten Jahren schon auf Seiten der Polizei etabliert: Rasterfahndung, Lauschangriff, geheime Telekommunikationsüberwachung, verdeckte Ermittler im Polizei- wie auch Strafprozessrecht stehen für eine Polizei, die dem Bürger nicht mehr mit offenem Visier gegenübertritt.

Zwar hat das Bundesverfassungsgericht in seinen letzten Urteilen den Umfang der präventiven Telekommunikationsüberwachung ebenso eingeschränkt wie auch die Voraussetzungen der Rasterfahndung. In Zukunft müssen die Polizeibehörden die Bedrohungslage, die zum Einsatz dieser Methoden berechtigt, präziser spezifizieren. Und auch der „große Lauschangriff“ ist neuerdings starken Einschränkungen unterlegen und muss bei höchst intimen Sachverhalten abgestellt werden. Dennoch bleiben diese Mittel bestehen.

Hinzu kommt, dass auch der Zollfahndungsdienst verdeckte Ermittler einsetzt, die mit der Aufdeckung und Ermittlung unbekannter Steuerfälle betraut sind. Infolge des allgemeinen Aufgabenzuwachses für den Zoll durch eine Verschärfung der Außenwirtschaftsvorschriften hat sich auf diesem Gebiet die Bedeutung der Vorfeldermittlungen in den letzten Jahren erhöht. Dazu gehört etwa auch der Besuch von Märkten, auf denen üblicherweise auch unversteuerte Zigaretten verkauft werden. Hier liegt der Schwerpunkt der geheimpolizeilichen Tätigkeit auf Fällen, in denen mangels konkreter Anhaltspunkte noch offen ist, ob sie auf ein steuerverfahrensrechtliches oder strafverfahrensrechtliches Verfahren gegen einen bestimmten Steuerpflichtigen hinauslaufen werden.

Man wird wohl sagen können, dass sich die bereits vorhandenen Aufweichungen des Trennungsgebotes auf Seiten der Polizei mit den letzten sicherheitspolitischen Neuerungen in Form der Terrorismusbekämpfungsgesetze, die die Aufgaben und Informationsbeschaffungsbefugnisse der Geheimdienste erweitert haben, und dem Hinzutreten des GTAZ und der Antiterrordatei noch einmal vertieft haben.

Denn nun gelangen die Polizeibehörden an geheimdienstlich erlangte Informationen, die sie im Rahmen ihrer begrenzten rechtsstaatlichen Kompetenzen so nicht bekommen hätten. Im Ergebnis läuft dies auf eine Sprengung eng normierter polizeilicher Ermittlungsbefugnisse hinaus, und als Konsequenz ergibt sich die schleichende Herausbildung eines „geheimpolizeilichen“ Sicherheitsverbundes ohne wirkungsvolle demokratische Rechenschaftspflicht gegenüber dem Bürger.

So entsteht ein Antiterrornetz, in das sich ein zunehmendes Segment der Bevölkerung verstricken kann. So reicht es für die Aufnahme in die Antiterrordatei bereits aus, dass man bei den Sicherheitsbehörden den Verdacht erregt, „rechtswidrig Gewalt als Mittel zur Durchsetzung international ausgerichteter politischer oder religiöser Belange“ auch nur zu „befürworten“. Damit wird beispielsweise jeder gesellschaftliche Disput über völkerrechtlich zweifelhafte Angriffs- oder Verteidigungskriege zu einem sicherheitspolitischen Minenfeld.

Ab diesem Zeitpunkt greifen die herkömmlichen geheimdienstlichen Informationsbeschaffungsmaßnahmen über verdeckt ermittelnde Inlandsgeheimagenten, Observationen und dergleichen, und schon die völkerrechtlich umstrittene Äußerung wie auch die aus den nachfolgenden geheimdienstlichen Informationsbeschaffungsmaßnahmen sich ergebenden, möglicherweise auf den Terror bezogenen, „Erkenntnisse“ finden Eingang in die Antiterrordatei. Denn der Inlandsgeheimdienst kann auf Ersuchen ergänzende Informationen von anderen Behörden, etwa Schulbehörden, Universitätsbehörden, Einwohnermeldeämtern und Ausländerbehörden erlangen. Hier ergibt sich in der Antiterrordatei eine recht detaillierte Zusammenstellung geheimdienstlicher „Erkenntnisse“, zum einen über die auf die Identität einer verdächtigen Person bezogenen Grunddaten wie auch darüber hinausgehend über die so genannten „erweiterten Grunddaten“: Diese sollen eine „zuverlässige Gefährdungseinschätzung“ durch die Sicherheitsbehörden ermöglichen und Angaben machen über Telekommunikations- und Internetdaten, Bankverbindungen und Schließfächer, den persönlichen Bildungsweg, Arbeitsstelle, Familienstand, Volks- und Religionszugehörigkeit, Reisebewegungen und bekannte Aufenthalte an Orten mit terroristischem Hintergrund.

Auf diese geheimdienstlichen „Erkenntnisse“ hätten die Polizeibehörden bei einer Anfrage Zugriff, denn sie beziehen sich auf den vage formulierten polizeilichen Aufgabenbereich, die Begehung des sich auf das terroristische Vorfeld beziehenden strafrechtlichen Vereinigungsverbot der §§129 a und b STGB zu verhindern. Dies gilt jedenfalls ab dem Zeitpunkt, wo sich bei den Sicherheitsbehörden der Verdacht regt, hier schicke sich jemand an, Mitglied einer Vereinigung zu werden, deren *Zwecke* darauf *gerichtet* sind, terroristische Handlungen zu begehen.

Hier erstreckt sich der polizeiliche Zugang auch auf geheimdienstliche „Erkenntnisse“ intimer Daten – „Erkenntnisse“, deren geheimdienstliche Erlangung keiner wirkungsvollen demokratischen Kontrolle unterliegen kann. Auf diese Weise droht ein zunehmender Teil der Bevölkerung, der unter dubiosen und willkürlichen Terrorverdacht geraten kann, ins Visier von „geheim“ agierenden Sicherheitsbehörden zu geraten.

Dieser neue „Sicherheitsapparat“ kann intime Daten dieses nun unter Sonderbehandlung stehenden Segmentes der Bevölkerung speichern. Denn jetzt greifen die Befugnisse des geheimdienstlichen Apparates weiter aus: Das Bundesamt für Verfassungsschutz ist befugt, seine bereits erlangten Erkenntnisse über Telekommunikationsverbindungsdaten als auch über Anschriften, Postfächer und sonstigen Umständen des Postverkehrs dahingehend zu nutzen, auch den *Inhalt* der Telekommunikation aufzuzeichnen sowie die dem Post- und Briefgeheimnis unterliegenden Sendungen zu öffnen und einzusehen.

Sowohl das „Gemeinsame Terrorismusabwehrzentrum“ als auch die Antiterrordatei sollen als Kernbestand der „neuen Sicherheitsarchitektur“ die „Freiheit“ der so genannten westlichen Wertegemeinschaft sichern. Doch könnte sich der neue „Sicherheitsapparat“ seinerseits zu einer existenziellen Bedrohung der „freiheitlich-demokratischen Grundordnung“ entwickeln. Statt das „Sicherheitsgefühl“ der Bevölkerung zu stärken, scheint das neue sicherheitspolitische Paradigma den zunehmend verunsicherten Bürger einem verstärkt unberechenbaren und undurchschaubaren „Leviathan“ auszuliefern.

Kai Rogusch ist Redakteur des politischen Zweimonatsmagazins NOVO (www.novo-magazin.de) und lebt in Frankfurt/Main.