ANTITERRORDATEI

Schriftliche Stellungnahme des Chaos Computer Clubs (CCC) anläßlich der Anhörung am 6. November 2012

an das Bundesverfassungsgericht

1 BvR 1215/07

Berlin, 6. November 2012

Constanze Kurz, Frank Rieger, Beata Hubrig, Dirk Engling

Das Antiterrordateigesetz (ATDG) trat am 22. Dezember 2006 in Kraft. Anläßlich der Anhörung des Bundesverfassungsgerichts am 6. November nimmt der CCC schriftlich Stellung hinsichtlich der Eingriffe in Grundrechte sowie zu Zweck, Funktionsweise und Informationsgehalt der Antiterrordatei (ATD). Auch Fragen der Bestimmtheit, der Reichweite und der erfaßten Daten nach § 3 ATDG sowie der Verwendung der Daten nach §§ 5 und 6 ATDG werden berücksichtigt.

Datenkontrolle und Korrekturmöglichkeiten

Bevor die Frage, welche Menschen unter welchen Voraussetzungen in der Antiterrordatei gespeichert werden dürfen, untersucht wird, soll hervorgehoben werden, daß ein solcher Eintrag nachhaltige Folgen haben kann. Denn die Mechanismen der Datenkontrolle, die das Recht auf informationelle Selbstbestimmung jedem Menschen gibt, sind im ATDG ungenügend berücksichtigt (Betroffenenrechte). Falsche oder veraltete Daten aus der ATD können nahezu unbegrenzt gegen den Betroffenen weiterverwendet werden. Sollte er Kenntnis von einem Eintrag in der ATD erhalten, beispielsweise durch offenes Vorgehen der Polizei gegen ihn, und dann erfahren wollen, ob und was in der ATD über ihn gespeichert ist, wird er in der Regel an die ursprünglich erhebende Stelle verwiesen werden. Er wird sich also nicht nur rechtlich mit einer erhebenden Stelle auseinandersetzen müssen, sondern einer Vielzahl von Behörden gegenüberstehen.

Nur die Behörde, die den Eintrag vorgenommen hat, kann einmal vermerkte Daten selbst löschen oder berichtigen, hat aber keinen Einfluß mehr auf die Datensätze, welche bei weiteren Empfängern anderer Behörden verarbeitet werden. Das erweist sich als ganz praktisches Problem, wie im Rahmen der NSU-Untersuchung ans Tageslicht kam. Bundesverteidigungsminister Thomas de Maizière räumte ein, daß „zwischen dem Militärischen Abschirmdienst (MAD), dem Bundesamt für Verfassungsschutz und den Landesämtern nicht klar sei, wer welche Informationen habe und wer was wann löschen müsse."[1] Zudem ist ein weiteres praktisches Problem die fehlende Einflußnahmemöglichkeit der einstellenden Behörde, was die abrufende Behörde mit den erlangten Daten macht: So könnte beispielsweise eine Ordnungsbehörde mit Vorfelddaten gegen den Betroffenen vorgehen und damit eine Gesinnungsstrafbarkeit einführen oder der Betroffene nachrichtendienstlich in das Visier heimlicher Datenerhebung geraten.

Ganz praktisch heißt das: Wenn man einmal ins Visier der Nachrichtendienste geraten ist, kann man durch den Eintrag in die ATD zusätzlich bei allen mit nachrichtendienstlicher oder polizeilicher Arbeit befaßten Behörden stigmatisiert werden. Man kann so schnell zur Figur in einem kafkaesken Alptraumroman werden, nur daß dieser nicht zwischen zwei Buchdeckeln stattfindet, sondern im echten Leben, mit nicht abwendbaren Folgen im Alltag oder im Berufsleben. Die Regelung im Antiterrordateigesetz ist insofern eine Zumutung: „Die Auskunft

[1] Die Zeit vom 4. November 2012: http://www.zeit.de/politik/deutschland/2012-11/gedenken-nsu-mordserie

zu verdeckt gespeicherten Daten richtet sich nach den für die Behörde, die die Daten eingegeben hat, geltenden Rechtsvorschriften."

Die Betroffenen sollen im Fall eines Auskunftbegehrens einen Hinweis auf diese Regelung und eine Adressenliste aller beteiligten Stellen erhalten, um dort jeweils die Auskunft einzeln zu beantragen. Die Bürgerinnen und Bürger haben grundsätzlich keine leise Ahnung, welche der zur Zeit mehr als vierzig an der ATD beteiligten Stellen Daten über sie gespeichert haben. Sie sind also gezwungen, mehr als vierzig Anträge zu stellen, wenn sie ihr Auskunftsrecht wahrnehmen wollen. Im Zweifel sind ebenso viele Widerspruchs- und Klageverfahren „ins Blaue hinein" nötig, ohne die Erfolgsaussichten ansatzweise vorher abschätzen zu können. Dieses Auskunftsverfahren ist weder mit den Grundrechten noch mit der Rechtsweggarantie des Grundgesetzes zu vereinbaren.

Unbestimmtheit des Terrorbegriffes

Während Gesetze üblicherweise ihren Anwendungsbereich präzise definieren, schweigt sich das ATDG über seinen aus. Das verfassungsrechtliche Bestimmtheitsgebot verlangt aber vom Gesetzgeber, daß die betroffenen Personen grundsätzlich erkennen können, bei welchen Anlässen und unter welchen Voraussetzungen ein Verhalten mit dem Risiko der Überwachung verbunden ist. Trotz der Allgegenwart des Begriffes „Terrorismus" ist er legal nicht definiert: „Der Begriff des internationalen Terrorismus ist durch das internationalen und nationalen Normen zugrunde liegende Verständnis vorgeprägt, aber zugleich für künftige Entwicklungen offen."[2]

Nach welchen Kriterien bzw. nach welchem Verdachtsgrad zu beurteilen ist, ob eine Person im Sinne des § 2 ATDG einzustufen ist, sagt das Gesetz nicht. Es verlangt noch nicht einmal, daß Tatsachen – also beweiskräftige, objektive Fakten – vorliegen, aus denen unmittelbar auf bestimmte Sachverhalte geschlossen werden kann. Eine Differenzierung der Speicherung danach, zu welchem Zweck die Daten ursprünglich erhoben und gespeichert wurden, enthalten die Regelungen des ATDG nicht. Ob auch personenbezogene Daten von Strafunmündigen gespeichert werden, bleibt unklar.

Die Zahl der eingetragenen Betroffenen spricht eine deutliche Sprache: Über 18.000 gespeicherte potentielle Terroristen (laut Schriftsatz der Regierung) sind ein klares Indiz dafür, daß der Anwendungsbereich überdehnt wurde. Diese Zahl entsteht erst daraus, daß nirgends präzise definiert wird, um was für geplante Anschläge oder Angriffe es sich handeln soll, um einen Eintrag einer verdächtigen Person in der ATD zu begründen.

Der Kontext der Speicherung geht zudem bei der Anlage von Datensätzen als Verweis verloren. Die Maßgabe, die vorhandenen Informationen in den einzelnen Behörden müßten nach Terrorverdachtsfällen durchsucht werden und in die ATD Eingang finden, führt zu unter-

---

[2] BT-Drs. 16/813, S. 12.

schiedlich gewichteten Einträgen. Wo vielleicht im Bayerischen schon die Forderung nach Abhängen der Kreuze im Klassenraum Terrorverdacht begründen könnte, ist in Hamburg ein Bewohner der Hafenstraße noch Gemäßigter. Daß ohne Definition des Terror- und Gewaltbegriffs alle angeschlossenen Behörden ihre eigene Deutungshoheit haben, unterläuft die Bestimmtheit des Gesetzes.

Es ist zu betonen, daß es keinen wissenschaftlichen oder anderen Nachweis gibt, daß Antiterrorlisten, ob national oder international, überhaupt einen wesentlichen oder auch nur meßbaren Beitrag zur Terrorismusbekämpfung leisten.

Internationale Kooperationen der Dienste

Die Regierung schweigt sich zum Thema der internationalen Verflechtungen der Dienste und der Rolle der ATD hierin nahezu vollständig aus. Klar ist nur, daß die Mehrzahl der Einträge ausländische Menschen betrifft. Aus vergangenen bekanntgewordenen Fällen (beispielsweise die Entführung von Khaled al-Masri) ergab sich, daß in erheblichem Maße Informationen zwischen Geheimdiensten und Polizei über Ländergrenzen hinweg ausgetauscht werden. Allein die Tatsache einer Speicherung in der ATD, die einem ausländischen Dienst durch Kooperation bekanntwird, kann zu im Einzelfall gravierenden Konsequenzen für den Betroffenen führen, inklusive Einreiseverboten, Festnahmen oder Verhören außerhalb Deutschlands, unabhängig von der Substanz des Speichergrundes.

Designfehler der verdeckten Suche

Wie der NSU-Fall und eine Vielzahl von weiteren Vorfällen gezeigt haben, ist schon die Konstruktion der ATD, bei der Geheimdienste die Anfragen der Polizeien nach verdeckten Daten einseitig sehen können, ein struktureller Fehler. Dienste neigen nachgewiesenermaßen dazu, ihre V-Leute vor polizeilichen Maßnahmen bzw. auch nur bei polizeilichem Interesse zu warnen. Der Verfassungsschutz hatte im konkreten Fall seine V-Männer vor geplanten polizeilichen Festnahmen und Durchsuchungen gewarnt.[3] Die ATD ist dafür das perfekte Werkzeug. Es sollte daher strukturell vermieden werden, daß Geheimdienste diesen Informationsvorteil erlangen dürfen, um vorzubeugen, daß als Terroristen verdächtigte V-Männer auf freiem Fuß bleiben, weil die Dienste mit Hilfe der Antiterrordatei deren Festnahme verhindert haben.

Ein in der jetzigen Struktur der ATD mögliches Szenario wäre beispielsweise: Ein LKA fragt vorsichtshalber in der ATD an, ob gegen einen Verdächtigen X etwas vorliegt. Der in der ATD gespeicherte Betroffene ist ein V-Mann von Geheimdienst Z, also handelt es sich um einen

[3] Vgl. Der SPIEGEL, 45/12, S. 38–41.

verdeckten Eintrag. Dem Polizisten des LKA wird dieser Eintrag nicht angezeigt, allerdings ist nun Geheimdienst Z informiert und kann seinen V-Mann warnen.

Integration in Fahndungssoftware

Die Polizeibehörden und Dienste arbeiten mit einer weitgehend identischen, nur im Detail abweichenden Fahndungssoftware der Firma „rola Security Solutions GmbH“, die auf der Polizeiseite als „rsCase“ bekannt ist. Diese Software hat ausweislich der Eigenwerbung der Firma nicht nur Schnittstellen in alle relevanten Verbunddateien, sondern auch in die ATD. Der vordergründige Eindruck, die ATD wäre lediglich ein einfach nutzbares Instrument zur Kontakterleichterung an einer isolierten PC-Arbeitsstation zum Zwecke des Heraussuchens der zuständigen Behörde zu einem ATD-Eintrag, ist offensichtlich irreführend. Wenn Heinrich Wolff in seiner Stellungnahme behauptet, man könne „die Daten nur vom Bildschirm abschreiben“, dann verdeutlicht das lediglich seinen Versuch der Verharmlosung, denn die Schnittstellen in der Fahndungssoftware wären so nutzlos. Vielmehr muß davon ausgegangen werden, daß die Weiterverwendung von digitalen Kopien der erlangten Daten aus der ATD zum Normalfall werden wird. Soweit Wolff versucht, den Eindruck zu erwecken, der „Zugriff“ bedeute lediglich die „optische Wahrnehmbarkeit am Bildschirm“, so dürfte er ein gutes Stück neben der Realität liegen.[4] Er behauptet weiter, eine „Speicherung der Daten des Treffers im System der anfragenden Behörde ist technisch garnicht (sic) möglich.“ Man könne „die Daten nur vom Bildschirm abschreiben“.[5] Auch dies kann man getrost ins Reich der Märchen einordnen. Wolff selbst schreibt wenige Seiten später in seiner Stellungnahme ausdrücklich über das Speichern der erlangten Datensätze.[6]

Es geht im Gegenteil bei der ATD, wie auch bei den konzeptionell ähnlich gelagerten Verbunddateien darum, die Informationsbestände von Polizei und Diensten zu integrieren und zu vermaschen. Dies ist auch erklärtes Ziel der Datei. Durch den Einsatz von Software wie „rsCase“, die für die Verarbeitung großer Datenmengen, die Erstellung von Lebensprofilen Verdächtiger und die Entdeckung und Visualisierung von Beziehungsgeflechten optimiert ist, entsteht eine völlig neue Qualität des Grundrechtseingriffs aus den ATD-Daten. Selbst ein aus der ATD übermittelter reiner Grunddatensatz ermöglicht durch die Vielzahl von sonstigen Verbunddateien, die mit der Fahndungssoftware technisch gekoppelt sind, eine weitgehend automatische Ausforschung von Datenbeständen. Auch die Einspeisung von Daten aus der ATD aus algorithmisch gewonnenen Verdächtigungen ist aus „rsCase“ möglich.

---

[4] Stellungnahme Heinrich Wolff, S. 24f.

[5] A. a. O., S. 25.

[6] A. a. O., S. 31.

Additiver Grundrechtseingriff

Eine isolierte Betrachtung der ATD ist angesichts der umfangreichen und teils kaum überschaubaren Zahl von polizeilichen und nachrichtendienstlichen Zentral- und Verbunddateien nicht mehr möglich. Vielmehr muß der additive Effekt einer ATD-Speicherung zusätzlich zu weiteren polizeilichen Datenbanken, etwa den 33 bekannten Verbunddateien sowie den 44 Zentraldateien, gesehen werden.[7] Die logischerweise auf einen oder mehrere Treffer in der ATD folgende weitergehende Auflösung in anderen Datenbanken, die der suchenden Behörde zugänglich sind, führt zwangsläufig zu einer Verdichtung der Informationen und damit zu einer Verschärfung des Grundrechtseingriffs. In die Zukunft projiziert, ergibt sich das Bild einer zwar aus rechtlichen Gründen fragmentierten Dateienlandschaft, die jedoch effektiv am Abfrageplatz zusammengeführt werden kann, mit Hilfe einer einheitlichen Schnittstelle, wie etwa bei der beschriebenen Fahndungssoftware „rsCase". Die Schwere des Eingriffs kann also nicht aus der alleinigen Betrachtung einer einzelnen Datei wie der ATD abgeleitet werden, sondern muß in der Gesamtschau aller dem Bearbeiter zugänglichen Datenquellen gesehen werden.

Automatische Stigmatisierung

Die Anlage der ATD als universelles automatisches Auskunftsmittel für Menschen unter Terrorismusverdacht verschlimmert mit Blick auf die Zukunft die Folgen einer Speicherung für die Betroffenen kontinuierlich. Die geplante automatische Vernetzung des Prozesses der Visa-Beantragung mit der ATD ist nur ein erster Anwendungsfall, der zukünftig problemlos auf andere Felder erweitert werden könnte.[8]

Dazu gehören allgemein Personenüberprüfungsverfahren und Zuverlässigkeitsüberprüfungen, die in ihrer Anzahl zunehmende Tendenz haben. So hielt der schleswig-holsteinische Datenschutzbeauftragte fest: „Auch die Deutsche Bundesbank ist auf die Idee gekommen, außerhalb des Anwendungsbereichs des Sicherheitsüberprüfungsgesetzes ihr Fremdpersonal überprüfen zu lassen. Die Deutsche Bundesbank und das LKA Schleswig-Holstein haben eine Vereinbarung geschlossen, wonach das LKA kriminalpolizeiliche wie auch staatsschutzrelevante Erkenntnisse aus den Kriminalakten und den INPOL-Verbunddateien an die Deutsche Bundesbank zur Bewertung übermittelt."[9] Daß diese Überprüfungen bereits heute oder in Zukunft auch für Terrorverdächtige vorgenommen werden, scheint keineswegs ausgeschlossen.

---

[7] Vgl. BT-Drs. 16/2875, S. 10–18.

[8] Öffentliche Anhörung des Innenausschusses des Deutschen Bundestages am 24. Oktober 2011: http://www.bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung14/Protokoll.pdf

[9] Tätigkeitsbericht 2009 des ULD Schleswig-Holstein, S. 33.

Die Tatsache eines ATD-Eintrages, auch wenn er falsch, unberechtigt oder veraltet ist, führt zu einer Form unregulierter Stigmatisierung, gegen die der Betroffene de facto keine Abwehrmöglichkeiten hat. Es sind auch keine internen Mechanismen für den Fall vorgesehen, daß sich der Verdacht, es handele sich um einen Terroristen, nicht erhärtet.

Große Anzahl zugriffsberechtigter Behörden

Die Anzahl der tatsächlich zum direkten Zugriff auf die ATD berechtigten Behörden ist im Gesetz nicht beschränkt. Die schon heute als zugangsberechtigt bekannten Stellen dürften nur der Anfang sein: Bereits in der Anhörung im Deutschen Bundestag wurde mehrfach moniert, daß mehr als dreißig Behörden die Voraussetzungen nach § 1 Absatz 1 ATDG erfüllen. Das übersteigt die Zahl der Behörden, die in Deutschland tatsächlich mit Terrorabwehr befaßt sind. Dazu könnten viele weitere Behörden kommen, da entgegen des Grundsatzes der Normenklarheit im ATDG keine Eingrenzungen festgeschrieben worden sind. Dazu könnten sich nach § 1 Abs. 2 die Folgen eines ATD-Eintrages für Betroffene und deren Kontaktpersonen unabsehbar ausweiten.

Technische Risiken

Ein Risiko des großen und ausufernden Teilnehmerkreises ist die damit unweigerlich wachsende Gefahr eines technischen Angriffs. Für einen Angreifer ergeben sich mehrere attraktive Ziele, je nach Ausrichtung. Inländische und ausländische Dienste würden durch eine unbefugte Datensatzmodifikation ein erhebliches Machtmittel erhalten. Ausländische Dienste dürften ein großes Interesse an einem vollständigen Datenbankabzug haben. Angesichts der Kapitulation der IT-Sicherheit vor gezielten Angriffen mit von staatlichen Akteuren entwickelten Angriffswerkzeugen ist dies kein theoretisches Risiko mehr und kann nach heutigem Stand der Technik nicht ausgeschlossen werden. Die Berichte des Bundesamtes für Sicherheit in der Informationstechnik (BSI) über die fortwährenden Angriffe gegen deutsche Regierungsnetze durch ausländische Interessenten sprechen eine deutliche Sprache, was die tatsächlich zu gewährleistende technische Sicherheit solcher Systeme angeht. Innen- und Außentätern wird hier ein attraktives Angriffsziel mundgerecht zusammengeführt, das vorher mit Bedacht in separaten Domänen verteilt war.

Die technische Konzeption der ATD ist analog zu der der Rechtsextremismusdatei (RED) angelegt. Das heißt, daß ein zentraler Datenbankserver beim BKA alle gespeicherten Daten in einer Standard Oracle-Datenbank enthält, inklusive der verdeckt gespeicherten. Zugegriffen wird über mittels SINA-Box-VPN angebundene Computer, auf denen weitere Software installiert sein kann (beispielsweise „rsCase“). Im Alltag wird es sehr wahrscheinlich zu einer Bündelung der Softwareprodukte zum Zugriff auf die Verbunddateien auf entsprechend physisch

gesicherten Geräten kommen, auf denen praktischerweise auch gleich die Fahndungssoftware installiert sein dürfte.

Es stellt sich die Frage, durch welche Maßnahmen beispielsweise verhindert wird, daß die Administratoren des BKA nicht einfach an allen Protkollierungsmechanismen vorbei eine vollständige Kopie der Oracle-Datenbank speichern, in der sämtliche, auch die verdeckt gespeicherten Daten enthalten sind. Ohnehin wird aus Gründen der Datensicherung stets ein Duplikat der Datenbank erstellt.

Unzureichende Umsetzung des Zitiergebots

Ein Verstoß gegen das Zitiergebot betrifft den Wortlaut des Art. 19 Abs. 1 S. 2 GG, nach dem das Gesetz Einschränkungen von Grundrechten unter Angabe des Artikels zu nennen hat. Sinn und Zweck des Zitiergebotes ist es, daß der Gesetzgeber sich mit dem Grundrechtseingriff auseinandersetzt. Bezüglich des ATDG hat sich der Gesetzgeber offensichtlich nicht ausreichend mit dem Recht auf informationelle Selbstbestimmung befaßt, da § 13 ATDG dieses Grundrecht nicht zitiert.