Prof. Dr. Martin Kutscha
Professor für Staats- und Verwaltungsrecht
an der FHVR Berlin, Fb. 1
Alt-Friedrichsfelde 60
D-10315 Berlin

25. 8. 2008

Innenausschuss
A-Drs. 16(4)460D

Stellungnahme zum Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (BT-Drs. 16/9588)

Die folgende Stellungnahme enthält keine umfassende Würdigung des oben genannten Gesetzentwurfs, sondern muss sich auf einige als wesentlich erscheinende Gesichtspunkte beschränken.

1) Veränderung des Kompetenzgefüges zwischen Bund und Ländern

Indem der Gesetzentwurf dem BKA zahlreiche neue Befugnisse zur Gefahrenabwehr zuweist, die sich im Übrigen keineswegs nur auf den internationalen Terrorismus beziehen, verändert er das Kompetenzgefüge zwischen Bund und Ländern bei der Inneren Sicherheit nachhaltig: Nach dem Grundgesetz ist die polizeiliche Gefahrenabwehr durch Behörden der Länder der Regelfall und nur zur Erfüllung bestimmter Zentralstellenfunktionen ausnahmsweise einigen Behörden des Bundes überantwortet (vgl. Art. 30 u. 87 I GG)[1]. Dem entsprechend hat das BVerfG 1998 im Hinblick auf den damaligen Bundesgrenzschutz zu Recht festgestellt, dass dieser „nicht zu einer allgemeinen, mit den Landespolizeien konkurrierenden Bundespolizei ausgebaut werden und damit sein Gepräge als Polizei mit begrenzten Aufgaben verlieren“ darf[2]. Damit im Einklang weist § 2 I BKAG dem BKA als „Zentralstelle“ auch nur eine unterstützende Funktion für die anderen Polizeibehörden zu. Im Gegensatz dazu wird das BKA durch die Zuweisung zahlreicher neuer Eingriffsbefugnisse durch den hier zu beurteilenden Gesetzentwurf zu einer Art deutschem FBI umgewandelt, das in Konkurrenz zu den Polizeien der Länder auch weit im Vorfeld von Rechtsgutverletzungen agieren kann[3]. Problematische Parallelzuständigkeiten werden insbesondere durch die neuen Befugnisregelungen

[1] Vgl. im Einzelnen Lisken/Denninger, in: Dies. (Hrsg.), Handbuch des Polizeirechts, 4. Aufl. München 2007, Rdnr. C 146; Kutscha, in: Roggan/Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Aufl. Berlin 2006, S. 78 ff.
[2] BVerfGE 97, 198 (Leits. 2).
[3] Vgl. Hilbrans, DANA 2008, 60; v. Denkowski, Kriminalistik 2007, 292.

zur Platzverweisung (§ 20 o)[4], zum Gewahrsam (§ 20 p), zur Durchsuchung von Personen (§ 20 q), zur Sicherstellung (§ 20 s) sowie zum Betreten und Durchsuchungen von Wohnungen (§ 20 t) geschaffen, die nicht nur terrorismusbezogene Tatbestandsvoraussetzungen enthalten, sondern darüber hinaus auch allgemeine Gefahrenbegriffe als Eingriffsvoraussetzung, wie sie sich ebenso in den entsprechenden Befugnisregelungen für die Polizeien der Länder befinden. Mit solchen an eine allgemeine Gefahr anknüpfenden Eingriffsermächtigungen überschreitet der Gesetzentwurf die nur auf die Abwehr von Gefahren des internationalen Terrorismus begrenzte Gesetzgebungskompetenz des Bundes nach dem neuen Art. 73 I Nr. 9 a GG; er ist insoweit verfassungswidrig.

2) Einhaltung der verfassungsmäßigen Vorgaben für die Rasterfahndung

In seiner Grundsatzentscheidung vom 4. 4. 2006 hat das BVerfG festgestellt, dass die präventive Rasterfahndung mit dem Grundrecht auf informationelle Selbstbestimmung nur dann vereinbar ist, wenn eine „konkrete Gefahr für hochrangige Rechtsgüter“ besteht; im „Vorfeld der Gefahrenabwehr“ scheide eine solche Rasterfahndung hingegen aus[5].
Nach § 20 j I des hier zu beurteilenden Gesetzentwurfs soll eine solche Rasterfahndung hingegen zulässig sein, „soweit dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist, erforderlich ist“. Damit ist nach dem Gesetzentwurf bereits eine abstrakte Gefahr für die genannten Rechtsgüter für die Durchführung der Rasterfahndung ausreichend. Dies ändert sich auch nicht durch den folgenden Satz: „eine solche Gefahr liegt in der Regel auch dann vor, wenn konkrete Vorbereitungshandlungen die Annahme rechtfertigen, dass eine Straftat nach § 4 a Abs. 1 Satz 2 begangen werden soll“. „Auch dann“ bedeutet schließlich, dass neben der aufgeführten Tatbestandsvoraussetzung auch andere gegeben sein können, um die Rechtsfolge auszulösen. Die im Sinne des BVerfG eingrenzende Wirkung könnte der gesetzliche Tatbestand nur dann erfüllen, wenn er den Begriff der Gefahr ausdrücklich auf das

[4] Einzige Tatbestandsvoraussetzung ist hier „ zur Abwehr einer Gefahr“. Diese findet sich wortgleich in den entsprechenden polizeigesetzlichen Ermächtigungen fast aller Bundesländer; vgl. Rachor, in: Lisken/Denninger a. a. O. (Fn. 1), Rdnr. F 489.
[5] BVerfGE 115, 320 (Leits. 1).

Vorliegen konkreter Vorbereitungshandlungen für eine solche Straftat beschränken würde.
Im Übrigen ist recht fraglich, ob das Instrument der Rasterfahndung überhaupt zur Abwehr der Gefahr von Terroranschlägen geeignet ist und damit dem Gebot der Verhältnismäßigkeit von Eingriffsmaßnahmen entspricht. Wie auch das BVerfG in der genannten Entscheidung feststellte, haben die nach den Anschlägen am 11. September 2001 in ganz Deutschland durchgeführten Rasterfahndungen nach „Schläfern“ zu keinem einzigen „Treffer“ geführt[6] - wohl aber zu Eingriffen in die Grundrechte zahlreicher Bürger, und zwar nicht nur durch die Datenabgleiche, sondern auch durch die sich daran anschließenden intensiven Ermittlungsmaßnahmen der Polizei.

3) Einhaltung der verfassungsmäßigen Vorgaben für die „Online-Durchsuchung“

§ 20 k des Gesetzentwurfs gestattet den verdeckten Eingriff in vom Betroffenen genutzte informationstechnische Systeme und die Erhebung von Daten daraus (sog. „Online-Durchsuchung“), wenn bestimmte Tatsachen die Annahme rechtfertigen, „dass eine Gefahr vorliegt für 1. Leib, Leben oder Freiheit einer Person oder 2. solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt“.
Tatsächlich sind diese Tatbestandsvoraussetzungen wörtlich aus dem Urteil des BVerfG vom 27. 2. 2008 zur „Online-Durchsuchung“ abgeschrieben worden[7]. Die entsprechenden Aussagen des BVerfG sind aber keineswegs so zu verstehen, dass sich das Gericht damit an die Stelle des Gesetzgebers setzen wollte, der diese Vorgaben lediglich „1:1“ zu übernehmen bräuchte[8]. Vielmehr markieren sie nur die äußerste verfassungsrechtliche Grenzlinie, die der Gesetzgeber einzuhalten hat. Die möglicherweise durch eine „Online-Durchsuchung“ zu schützenden „Güter der Allgemeinheit“ sind deshalb vom Gericht auch nur vage umschrieben worden. Der Gesetzgeber jedoch darf es nicht bei einer solchen vagen Umschreibung belassen, sondern muss diese wegen des verfassungsrechtlichen Gebots der Tatbestandsbestimmtheit[9] präzise definieren.

---

[6] BVerfGE 115, 320 ff.
[7] BVerfG, NJW 2008, 822 (Leits. 2).
[8] Vgl. Hilbrans, DANA 2008, 60 (62).
[9] Dazu BVerfGE 110, 33 (53 f.); Kutscha a. a. O. (Fn. 1), S. 69 ff.

Auf welche Weise verhindert werden kann, dass der heimliche Zugriff wirklich den Computer einer Person trifft, von der eine terroristische Gefahr ausgeht, und nicht statt dessen hochsensible Daten völlig Unbeteiligter ausgeforscht werden, lässt sich dem Gesetzentwurf nicht entnehmen. Die Wahrscheinlichkeit einer Infiltration der Computer von Unbeteiligten ist aber schon deshalb besonders hoch, weil dynamisch mit dem Internet verbundene Rechner in der Regel nicht über eine konstante IP-Adresse verfügen und sich deshalb nicht hinreichend sicher eindeutig adressieren lassen[10].

Zu Recht geht das BVerfG davon aus, dass eine staatliche Datenerhebung aus komplexen informationstechnischen Systemen „ein beträchtliches Potential für die Ausforschung der Persönlichkeit des Betroffenen“ aufweist[11]. Es verlangt deshalb besondere Vorkehrungen des Gesetzgebers, um den Kernbereich privater Lebensgestaltung zu schützen und damit der Menschenwürdegarantie des Art. 1 I GG Genüge zu tun. Dem soll offenbar durch die Bestimmungen in § 20 k VII des Gesetzentwurfs Rechnung getragen werden. Dessen erster Satz lautet: „Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig“. Die Intention des BVerfG wird damit aber geradezu auf den Kopf gestellt, weil die Erfüllung dieser Tatbestandsvoraussetzung völlig unrealistisch ist und deshalb diese Schutzregelung in der Praxis wohl nie zur Anwendung gelangen dürfte[12]: Es ist schwer vorstellbar, dass auf einem Computer *allein* Daten gespeichert sind, die dem Kernbereich zuzurechnen sind. Auch z. B. bei einem Gespräch zwischen einem Liebespaar innerhalb einer Wohnung, das heimlich belauscht werden soll („Lauschangriff“), weiß man vorab nie, ob nicht doch neben intimen Details auch Pläne für Straftaten zur Sprache kommen werden[13]. In allen solchen Fällen die Überwachungsmaßnahme zuzulassen, würde den vom BVerfG postulierten Schutz des Kernbereichs privater Lebensgestaltung zu völliger Bedeutungslosigkeit verurteilen.

[10] So die Informatiker Hansen/Pfitzmann, in: Roggan (Hrsg.), Online-Durchsuchungen, Berlin 2008, S. 131 (139).
[11] BVerfG, NJW 2008, 822 (829).
[12] Vgl. Baum/Schantz, ZRP 2008, 137 (138); Hilbrans, DANA 2008, 60 (62).
[13] Für die Unzulässigkeit des Abhörens eines „Mischgesprächs“ z. B. OLG Düsseldorf, StV 2008, 181.

Angesichts der Fülle von zum Teil hochsensiblen persönlichen Daten, die heute auf zahlreichen Personalcomputern gespeichert sind, ist der Eingriff in den genannten Kernbereich bei der Durchführung einer heimlichen „Online-Durchsuchung“ nahezu zwangsläufig[14]. Warum diese Maßnahme zur Abwehr von Terrorgefahren wirklich „unverzichtbar“ sein soll, ist bisher nicht überzeugend begründet worden[15]. Die zur Wahrung der Menschenwürdegarantie in Art 1 I GG konsequenteste Lösung wäre deshalb der Verzicht auf diese Überwachungsmethode[16].

4) Datenübermittlung im internationalen Bereich

In den letzten Jahren haben Fälle von Personen u. a. mit deutscher Staatsangehörigkeit, die als Terroristen verdächtigt und deshalb in anderen Ländern festgehalten und vermutlich der Folter unterzogen wurden, nicht zuletzt auch die Problematik der Übermittlung personenbezogener Daten an Sicherheitsbehörden anderer Staaten verdeutlicht. Die Novellierung des BKAG hätte deshalb den Anlass geboten, auch die entsprechenden Bestimmungen über Datenübermittlungen zu präzisieren. Immerhin lässt § 14 I Nr. 1 BKAG diese Übermittlung an ausländische Sicherheitsbehörden sowie an zwischen- und überstaatliche Stellen bereits dann zu, wenn dies zur Erfüllung einer dem BKA obliegenden Aufgabe erforderlich ist. Diese Tatbestandsvoraussetzung könnte kaum unspezifischer formuliert sein. Im Hinblick auf die zahlreichen neuen Eingriffsbefugnisse nach dem Gesetzentwurf sowie auf das verfassungsrechtliche Gebot der Tatbestandsbestimmtheit wäre der Gesetzgeber gut beraten, auch die Voraussetzungen für die Übermittlung der dadurch gewonnenen personenbezogenen Daten zu präzisieren.

[14] Vgl. dazu BVerfG, NJW 2008, 822 (834); Kutscha, NJW 2008, 1042 (1044); Warntjen, in: Roggan a. a. O. (Fn. 10), S. 57 ff.
[15] Ebenso Hoffmann-Riem, „Süddeutsche Zeitung“ v. 12./13. 4. 2008.
[16] Ebenso z. B. die Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. Oktober 2007 sowie Sachs/Krings, JuS 2008, 481 (485 f.).