Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)806 E

Gutachterliche Stellungnahme

zur Öffentlichen Anhörung des Gesetzentwurfs der Fraktionen der CDU/CSU und der SPD zur Neustrukturierung des Bundeskriminalamtgesetzes

BT-Drucksache 18/11163

im Innenausschuss des Deutschen Bundestages
am 20. März 2017

von

Dr. iur. Ulf Buermeyer, LL.M. (Columbia)

Richter am Landgericht Berlin
Vorsitzender der Gesellschaft für Freiheitsrechte e.V. (GFF)

ulf@buermeyer.de

Berlin, den 16. März 2017

Wesentliche Ergebnisse

1. Der Gesetzentwurf auf BT-Drucksache 18/11163 (im Folgenden: der Gesetzentwurf) bezweckt eine Systematisierung der Rechtsgrundlage der Arbeit insbesondere des Bundeskriminalamts und eine Umsetzung der Entscheidung des BVerfG zum BKA-Gesetz[1]. Dieses Anliegen ist im Grundsatz begrüßenswert.

2. Dies gilt aus systematischer Perspektive auch für den Ansatz, die Rechtsgrundlagen der Datenverarbeitung durch das BKA „vor die Klammer zu ziehen“[2]. Gleichwohl gibt das konkrete Regelungskonzept[3] zu verfassungsrechtlichen Bedenken Anlass[4], da wesentliche Grundsätze des Datenschutzrechts – namentlich die Gebote der Datensparsamkeit und der Zweckbindung – mit der Idee eines umfassenden BKA-Datenpools in ihr Gegenteil verkehrt werden, ohne die Vorgaben der Verfassung hinreichend in Rechnung zu stellen. Dieser Paradigmenwechsel soll hier indes nicht vertieft werden, da er Gegenstand der Stellungnahme des Sachverständigen Prof. Dr. Matthias Bäcker ist.

3. Der Gesetzentwurf setzt in Abschnitt 5 des BKAG-E (§§ 38 ff., „Terrorismusteil“) vielfach wortgetreu die Entscheidung des BVerfG zum BKA-Gesetz um. Die Übernahme von Formulierungen und ganzen Passagen aus dem Urteil in den Gesetzesentwurf erweckt auf den ersten Blick den Eindruck einer sehr akribischen Umsetzung der verfassungsgerichtlichen Vorgaben. In Gesetzesform gegossene Urteilsgründe führen jedoch oft zu Auslegungsschwierigkeiten, weil sich Gesetzestechnik und Urteilsbegründungstechnik grundlegend unterscheiden. Zudem würde der Gesetzgeber durch diese „Copy & Paste“ – Technik seine Aufgabe verfehlen, einen Ausgleich zwischen kollidierenden Gütern von Verfassungsrang zu schaffen: Das BKAG in der Fassung des Entwurfs markiert infolge der Orientierung an den vom BVerfG gezogenen äußersten Grenzen das Maximum an Grundrechtseingriffen zur Gefahrenabwehr, das noch verfassungsgemäß sein mag, in Details geht es über diese Grenzen sogar noch hinaus.

---

[1] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09.
[2] Abschnitt 2 des BKAG-E, §§ 9 ff.
[3] Insbesondere §§ 12, 16, 18, 19 BKAG-E.
[4] Vgl. insoweit nur die Stellungnahme des Bundesrats auf BR-Drucks. 109/1/17, Seite 2.

Damit würde der Gesetzgeber aber gerade keine Balance zwischen „Freiheit und Sicherheit“ schaffen, sondern Interessen der Sicherheitsbehörden umfassend den Vorrang geben. Bildhaft gesprochen würde sich der Gesetzgeber nicht in der Mitte der ihm von Verfassungs wegen vorgegebenen „Fahrspur“ möglicher Grundrechtseingriffe zum Zwecke der Gefahrenabwehr durch das Bundeskriminalamt bewegen, sondern konsequent an der rechten Leitplanke entlangschrammen – und an einigen Stellen gar von der Fahrbahn abkommen.

4. Daraus folgt zugleich eine wesentliche Konsequenz für die Landesgesetzgeber: Es wäre verfehlt, den „Terrorismusteil“[5] als Muster-Polizeigesetz anzusehen. Die hier vorgesehenen Eingriffe mögen angesichts der spezifischen Gefahr besonders schwerer Rechtsgutsbeeinträchtigungen, wie sie der internationale Terrorismus mit sich bringen kann[6], im Wesentlichen zu rechtfertigen sein[7]. Bei der Abwehr „normaler“ Gefahren, wie sie sich im Alltag der Polizeibehörden überwiegend stellen, fällt die anzustellender Güterabwägung hingegen anders aus. Die Aufgabeneröffnung des § 5 Abs. 1 BKAG-E muss in sämtliche Befugnisnormen des Terrorismusteils mit hineingelesen werden; allein im Rahmen dieser Aufgabe können die Befugnisse nach Maßgabe des BKAG-Urteils gerechtfertigt werden.

5. Die gravierendsten Bedenken im Hinblick auf die Befugnisse des „Terrorismusteils“ bestehen gegen die Ausgestaltung der Ermächtigung zum Einsatz von Staatstrojanern: § 49 BKAG-E stellt in keiner Weise verfahrensrechtlich sicher, dass die vom BKA einzusetzende Überwachungs-Software Mindestanforderungen an die Datensicherheit erfüllen. Hier fehlen Regelungen sowohl über die an Staatstrojaner zu stellenden technischen Anforderungen, die wenigstens im Verordnungswege erlassen werden sollten, als auch über eine obligatorische unabhängige Prüfung, dass ein Staatstrojaner diese Anforderungen auch erfüllt.

---

[5] § 38 ff. BKAG-E.

[6] Vgl. die Aufgabenzuweisung in § 5 Abs. 1 BKAG-E.

[7] Vgl. aber die unten zu übende Kritik.

6. Zudem schafft § 49 BKAG-E in seiner derzeitigen Form ein erhebliches Interesse für Sicherheitsbehörden, die Cyber-Sicherheit weltweit zu schwächen (!), um Systeme von Zielpersonen gegebenenfalls „hacken“ zu können. Diese Fehlanreize sollten durch ein Verbot der Ausnutzung von Sicherheitslücken verhindert werden, die auch den Herstellern noch unbekannt sind.

7. Schließlich enthält der Gesetzentwurf in § 41 Abs. 3 und § 62 Abs. 1 und 2 BKAG-E unzureichende Regelungen zum Schutz bestimmter Gruppen von Berufsgeheimnisträgern, insbesondere von Ärzten, Psychologischen Psychotherapeuten und Journalisten. Denn er schließt Eingriffe ihnen gegenüber nicht zuverlässig aus, sondern überlässt solche Maßnahmen einer im Einzelfall nicht zu prognostizierenden Abwägungsentscheidung.

Einzelaspekte des Gesetzentwurfs

Eine erschöpfende Stellungnahme zu einem 131 Seiten umfassenden, inhaltlich sehr komplexen Gesetzentwurf würde deutlich mehr Zeit erfordern, als den Sachverständigen zur Verfügung stand. Meine Stellungnahme konzentriert sich daher auf die Befugnisnormen des „Terrorismusteils“[8].

Hingewiesen werden kann aber auch insoweit angesichts des Umfangs des Vorhabens und der Kürze der Vorbereitungszeit nur auf ausgewählte rechtlich bedenkliche Vorschläge oder sonst änderungsbedürftige Aspekte des Entwurfs. Ist eine Regelung in dieser Stellungnahme nicht ausdrücklich erwähnt, so ist dies nicht dahingehend zu verstehen, dass sie als unbedenklich anzusehen wäre.

1.) Erhebung personenbezogener Daten, § 39 BKAG-E

Die Norm definiert, über welche Personen zur Erfüllung der Aufgabe der Abwehr des internationalen Terrorismus Daten erhoben werden dürfen, sofern die besonderen Erhebungsbefugnisse des Terrorismusteils nichts Abweichendes regeln. Bedenken begegnet die beabsichtigte Regelung im Hinblick auf die Befugnis zur Datenerhebung über die derzeit noch so genannten Kontakt- und Begleitpersonen (§ 20b Abs. 2 Nr. 2 lit. c BKAG). Nach der alten wie der neuen Fassung soll eine Datenerhebung auch über eine selbst in keiner Weise verantwortliche Person möglich sein, wenn *„die Person mit einer [terrorverdächtigen Person] nicht nur flüchtig oder in zufälligem Kontakt in Verbindung steht und die [terrorverdächtige Person] sich ihrer zur Begehung der Straftat bedienen könnte“* (§ 39 Abs. 2 Nr. 2 lit. c BKAG-E). Dies umfasst erkennbar einen potentiell weiten Kreis von gutgläubigen Umfeldpersonen, gegen die selbst keinerlei Verdachtsmomente vorliegen. Das BVerfG hat die inhaltsgleiche derzeitige Regelung nur im Zuge einer verfassungskonformen Reduktion hingenommen[9], indem es nämlich verlangt: *„Freilich dürfen die Merkmale von Verfassungs wegen nicht entgrenzend weit verstanden werden.“* Diesen Hinweis nimmt der Gesetzentwurf jedoch nicht auf, indem er keinerlei Versuch

[8] Abschnitt 5, §§ 38 ff. BKAG-E.
[9] BVerfG, BKAG-Urteil (oben Fn. 1), Rn. 169.

unternimmt, einer „entgrenzenden“ Interpretation durch entsprechend engere Formulierung der Eingriffsermächtigung vorzubeugen. Auch der bereits vom BVerfG monierten Gefahr einer zirkelschlüssigen Anwendung der Norm begegnet der Gesetzentwurf derzeit nicht: Das BVerfG hat ausdrücklich verlangt, dass bei der Anwendung der Vorschrift die Voraussetzungen des § 20b Abs. 2 Nr. 2 BKAG – nunmehr: § 39 Abs. 2 Nr. 2 BKAG-E – nicht ihrerseits aus dem bloßen Kontakt oder der bloßen persönlichen Nähe des Betreffenden zur Zielperson hergeleitet werden[10]. § 39 BKAG-E lässt dies derzeit gleichwohl zu.

Durch die Schaffung eines neuen polizeilichen Informationsverbundes, in dem alle Daten in einem „großen Topf“ für eine etwaige spätere Nutzung gespeichert werden[11], wird die Intensität des mit der Datenerhebung verbundenen Grundrechtseingriffs für Kontakt- und Begleitpersonen, die weitgehend unbeteiligte Dritte sein können, noch weiter intensiviert. Dabei ist auch zu berücksichtigen, dass das BVerfG diese erhebliche Vertiefung der sich an eine Datenerhebung knüpfenden Folgen für die informationelle Selbstbestimmung noch nicht in Rechnung stellen konnte, sodass die Abwägung insoweit heute durchaus anders ausfallen könnte.

2.) Schutz von Berufsgeheimnisträgern, § 41 Abs. 3 und § 62 BKAG-E

§ 62 beschränkt Maßnahmen aus dem Terrorismusteil des BKAG in der Fassung des Gesetzentwurfs, sofern sie sich gegen Berufsgeheimnisträger richten würden bzw. gegen Dritte richten, aber dabei Erkenntnisse von Berufsgeheimnisträgern erlangt würden, über die sie das Zeugnis verweigern dürften. Der Entwurf folgt weitgehend der Vorgängernorm des § 20u BKAG und übernimmt insbesondere die Zweiteilung in umfassend (§ 62 Abs. 1 BKAG-E) und lediglich relativ (§ 62 Abs. 2 BKAG-E) geschützte Berufsgeheimnisträger.

Absolut geschützt sind nach der Konzeption des Entwurfs Seelsorger (§ 53 Abs. 1 Satz 1 Nr. 1 StPO), Verteidiger (§ 53 Abs. 1 Satz 1 Nr. 2 StPO), Rechtsanwälte und

[10] BVerfG a.a.O, Rn. 168 a.E.
[11] Vgl. insbesondere §§ 12, 16 BKAG-E.

Kammerrechtsbeistände (§ 53 Abs. 1 Satz 1 Nr. 3 StPO) sowie Parlamentarier (§ 53 Abs. 1 Satz 1 Nr. 4). Insoweit sind Maßnahmen unzulässig, sofern die Berufsgeheimnisträger nicht selbst für die Gefahr verantwortlich sind.

Lediglich relativ geschützt sind hingegen weitere in § 53 Abs. 1 Satz 1 Nr. 3 StPO geschützte Berufsgruppen, insbesondere Ärzte, Zahnärzte und Psychologische Psychotherapeuten, sowie Journalisten (§ 53 Abs. 1 Satz 1 Nr. 5 StPO): Hier ist lediglich die Tatsache, dass Berufsgeheimnisträger betroffen wären und Informationen erlangt würden, die einem Schweigerecht unterliegen, *„im Rahmen der Prüfung der Verhältnismäßigkeit unter Würdigung des öffentlichen Interesses an den von dieser Person wahrgenommenen Aufgaben und des Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen."*

Zwar hat das BVerfG diesen Schutz-Dualismus grundsätzlich als verfassungsgemäß akzeptiert[12] und auch die konkrete Zuordnung einzelner Berufsgruppen zu dem einen oder anderen Schutzniveau als im Rahmen des *„erheblichen Einschätzungsspielraums"* des Gesetzgebers liegend noch hingenommen[13]. Die vom BVerfG monierte Differenzierung zwischen Verteidigern einerseits und anderen Rechtsanwälten andererseits[14] enthält § 62 Abs. 1 BKAG-E nicht mehr.

Indes hat das BVerfG ausdrücklich darauf verwiesen, dass sich Einschränkungen bei Maßnahmen gegenüber nur relativ geschützten Berufsgeheimnisträgern aus Art. 12 GG sowie unter dem Gesichtspunkt des Schutzes des unantastbaren Kernbereichs der privaten Lebensgestaltung ergeben können. Auf diese wesentlichen, die Prüfung der Verhältnismäßigkeit von Verfassungs wegen leitenden Gesichtspunkte sollte der Tatbestand des § 62 BKAG-E ausdrücklich verweisen.

Dass die Unterscheidung zwischen absolut und nur relativ geschützten Berufsgeheimnisträgern nicht zwingend gegen das Grundgesetz verstößt, besagt im

[12] BVerfG a.a.O., Rn. 256.
[13] BVerfG a.a.O., Rn. 258.
[14] BVerfG a.a.O., Rn. 257.

Übrigen für sich noch nicht, dass sie auch sachlich gerechtfertigt wäre. In der Tat erscheint die Binnendifferenzierung zwischen den Berufsgeheimnisträgern nach § 53 Abs. 1 Satz 1 Nr. 3 StPO wenig überzeugend: Es ist kein hinreichender Grund erkennbar, warum etwa gegenüber Psychologischen Psychotherapeuten oder Ärzten, die regelmäßig intimste Kenntnisse über ihre Patienten erlangen, die Eingriffsbefugnisse des 5. Abschnitts des BKAG-E grundsätzlich eingesetzt werden können, gegenüber Strafverteidigern – etwa wegen eines vergleichsweise banalen Verkehrsdelikts – hingegen nicht. Gerade im Lichte der oben bereits zitierten und vom BVerfG in diesem Kontext ins Feld geführten Kernbereichs-Rechtsprechung liegen im Falle der in § 53 Abs. 1 Satz 1 Nr. 3 StPO genannten Berufsgeheimnisträger insgesamt Erhebungs- und Verwertungsverbote sehr nahe. Indem die derzeitige Fassung des BKAG-E in Konstellationen (scheinbar) eine Abwägung erlaubt, in denen in aller Regel das Ermessen auf null reduziert sein wird, leistet sie der Gefahr von Fehlentscheidungen Vorschub. Auf die Differenzierung des Entwurfs sollte daher im Interesse der Rechtsklarheit und eines effektiven Schutzes des Kernbereichs der privaten Lebensgestaltung verzichtet werden. § 62 Abs. 1 Satz 7 und Abs. 2 Satz 3 BKAG-E sollten dementsprechend ersatzlos entfallen.

Ebenso wenig überzeugend ist die Benachteiligung von Journalistinnen und Journalisten[15]. In Bezug auf diese Berufsgruppe berücksichtigt der Gesetzentwurf nicht hinreichend, dass für die – nach der ständigen Rechtsprechung des BVerfG von Art. 5 Abs. 1 GG geschützte[16] – journalistische Recherche ein *absolutes* Vertrauen in den Informantenschutz erforderlich ist. Ein Schutz von Informantinnen und Informanten allein nach Maßgabe einer im Einzelfall nicht zu prognostizierenden Abwägung (vgl. § 62 Abs. 2 Satz 2 BKAG-E) kommt aus der Sicht eines potentiellen Informanten einem insgesamt fehlenden Schutz gleich, weil er sich nicht darauf verlassen kann, dass seine Kommunikation mit einer Journalistin nicht ausgespäht werden darf. Dies wiegt im Bereich der journalistischen Recherche umso schwerer, als potentielle Informanten –

[15] § 62 Abs. 1 und 2 BKAG-E i.V.m. § 53 Abs. 1 Satz 1 Nr. 5 StPO.

[16] Geschützt sind namentlich die Geheimhaltung der Informationsquellen und das Vertrauensverhältnis zwischen Presse und Informanten (vgl. BVerfGE 100, 313 <365> m.w.N.). „Dieser Schutz ist unentbehrlich, weil die Presse auf private Mitteilungen nicht verzichten kann, diese Informationsquelle aber nur dann ergiebig fließt, wenn sich der Informant grundsätzlich auf die Wahrung des Redaktionsgeheimnisses verlassen kann." (BVerfGE 117, 244 <259>, vgl. bereits BVerfGE 20, 162 <176, 187>; 36, 193 <204>).

anders als etwa Menschen, die medizinische Behandlung benötigen – auf den Kontakt zur Presse im Zweifel verzichten werden.

Dabei ist auch in Rechnung zu stellen, dass Informanten brisante Informationen auch vergleichsweise risikolos ins Netz stellen können, wobei die Kollateralschäden für die von Leaks betroffenen Personen typischerweise erheblich höher sind als bei verantwortlichem „Durchstechen" von Informationen an die Presse, die Persönlichkeitsrechte zu schützen versucht. Daraus folgt ein erhebliches öffentliches Interesse daran, dass Leaks an verantwortungsbewusste Journalistinnen und Journalisten und nicht etwa an Plattformen wie Wikileaks erfolgen. Gerade angesichts dessen erscheint der nur relative – und damit im Ergebnis nicht hinreichend belastbare– Schutz der Presse nach dem Gesetzentwurf anachronistisch. Berufsgeheimnisträger gem. § 53 Abs. 1 Satz 1 Nr. 5 StPO sollten daher ebenfalls in den Katalog des § 62 Abs. 1 BKAG-E aufgenommen werden.

3.) Besondere Mittel der Datenerhebung, § 45 BKAG-E

§ 45 BKAG-E regelt den Einsatz „besonderer Mittel" der Datenerhebung, nämlich Observationen (Abs. 2 Nr. 1), auch unter Einsatz von technischen Mitteln wie etwa Kameras und Richtmikrofonen (Nr. 2) oder GPS-Sendern (Nr. 3), Vertrauenspersonen (Nr. 4) und Verdeckten Ermittlern (Nr. 5). Bedenken ergeben sich hier zunächst wieder aus der Verweisung des Abs. 1 Nr. 4 auf die Kontakt- und Begleitpersonen (§ 39 Abs. 2 Nr. 2 BKAG-E)[17]. Vor allem aber dürfte die Umsetzung des vom BVerfG angemahnten Richtervorbehalts misslungen sein[18]: Gemäß § 45 Abs. 3 Nr. 5 soll ein Richtervorbehalt vor Einsatz einer Vertrauensperson oder eines Verdeckten Ermittlers nicht schlechthin, sondern nur bei Maßnahmen erforderlich sein, die sich *„gegen eine bestimmte Person richten oder bei denen die Vertrauensperson oder der Verdeckte Ermittler eine Wohnung betritt, die nicht allgemein zugänglich ist*".

[17] Vgl. oben Seite 4 zu § 39 BKAG-E.

[18] Im Ergebnis ebenso die Stellungnahme des Bundesrats, BR-Drucks. 109/1/17, Seite 10.

Das BVerfG[19] verlangt hingegen *„eine unabhängige Kontrolle ..., wenn Observationen ... längerfristig - zumal unter Anfertigung von Bildaufzeichnungen oder unter Nutzung besonderer technischer Mittel wie Peilsender - durchgeführt werden, wenn nichtöffentliche Gespräche erfasst oder Vertrauenspersonen eingesetzt werden. Diese Maßnahmen dringen unter Umständen so tief in die Privatsphäre ein, dass deren Anordnung einer unabhängigen Instanz, etwa einem Gericht, vorbehalten bleiben muss. Insoweit reicht es nicht, die Anordnung der Maßnahmen zunächst der Sicherheitsbehörde selbst zu überlassen und die disziplinierende Wirkung wegen des Erfordernisses einer richterlichen Entscheidung erst für deren Verlängerung - möglicherweise auf der Grundlage der so gewonnenen Erkenntnisse - vorzusehen. Soweit für diese Maßnahmen eine erstmalige Anordnung ohne richterliche Entscheidung vorgesehen ist, genügt [dies] einer verhältnismäßigen verfahrensrechtlichen Ausgestaltung nicht."*

Im Lichte dieser eindeutigen Aussage ist die Beschränkung des Richtervorbehalts auf ausgewählte Fälle des Einsatzes von VP / VE nicht haltbar.

4.) Staatstrojaner, § 49 BKAG-E

Aus verfassungsrechtlicher wie rechtspolitischer Perspektive besonders bedenklich erscheint § 49 BKAG in der Fassung des Entwurfs. Die Regelung weist zwei Defizite auf, die miteinander verzahnt sind: Sie überlässt es dem Bundeskriminalamt und dem Gericht, die technischen Anforderungen an Software zu definieren, die in informationstechnische Systeme eingreift („Staatstrojaner"), obwohl von ihnen – ebenso wie von den verfahrensrechtlichen Vorkehrungen, um ihre Einhaltung sicherzustellen – das Gewicht des Grundrechtseingriffs maßgeblich bestimmt wird. Dies ist mit dem Gebot des Grundrechtsschutzes durch Verfahrensgestaltung ebenso wie mit dem Wesentlichkeitsgrundsatz unvereinbar. Außerdem lässt die Norm dem BKA und dem Gericht Raum für den Missbrauch von Sicherheitslücken in informationstechnischen Systemen (sog. *Zero Day Exploits* oder kurz *0days*[20]) zum Zwecke der Infiltration. Dies schafft fatale Fehlanreize, weil deutsche Behörden damit ein Interesse daran haben

[19] BVerfG, BKAG-Urteil (a.a.O.), Rn.
[20] Gesprochen: Oh-Days.

könnten, Sicherheitslücken in informationstechnischen Systemen nicht an die Hersteller zu melden, sodass sie geschlossen werden können, sondern sie vielmehr zu horten.

a) Mangelhafte verfahrensrechtliche Sicherung

Die Eingriffsbefugnis enthält in § 49 Abs. 2 BKAG-E zwar bestimmte an der Rechtsprechung des BVerfG orientierte Begrenzungen des „Eingreifens“, etwa eine Beschränkung von Veränderungen auf das Notwendige oder einen Schutz von Zugriffen durch Dritte. Diese begrüßenswerten Regelungen finden indes keinerlei verfahrensrechtliche Absicherung. In der Aufzählung des § 49 Abs. 5 BKAG-E zum notwendigen Inhalt eines Antrags ist das technische Mittel, dessen Einsatz beabsichtigt ist, nicht einmal zu benennen, geschweige denn in seinen technischen Spezifikationen näher zu bezeichnen. Dies ermöglicht nach dem Wortlaut des Gesetzes den Einsatz beliebiger Staatstrojaner nach Gutdünken des Bundeskriminalamts, sofern ein Beschluss über eine Maßnahme einmal erlangt werden kann.

Die Verantwortung für die Prüfung der technischen Beschaffenheit des einzusetzenden Staatstrojaners kann auch nicht auf den Vorbehaltsrichter abgewälzt werden. Zum einen müsste er über den gesetzlich vorgegebenen Inhalt des Antrags (§ 49 Abs. 5 BKAG-E) hinaus Rückfragen stellen, um überhaupt zu erfahren, welches technische Mittel eingesetzt werden soll. Zum anderen kann vom zuständigen Richter des Amtsgerichts Wiesbaden nicht ernsthaft verlangt werden, eine EDV-technische Überprüfung des beabsichtigten Staatstrojaners selbst vorzunehmen. Eine externe Prüfung wiederum dürfte angesichts der hierfür notwenigen Zeit – wenigstens Tage, wohl eher Wochen –in vielen Fällen den Zweck der Maßnahme gefährden. Die Verantwortung hierfür wird in „Terror-Fällen“ kaum ein Richter auf sich nehmen wollen, sodass er sich im Zweifel auf Beteuerungen der antragstellenden Behörde verlassen wird, mit dem Staatstrojaner habe schon alles seine Ordnung. Im Ergebnis ist daher zu besorgen, dass die Einhaltung der in § 49 Abs. 2 BKAG-E genannten, aber auch weiterer aus der Perspektive der Informationssicherheit gebotener technischer Anforderungen an Staatstrojaner allenfalls vom BKA geprüft werden wird.

Aus der Perspektive des Schutzes der Integrität und Vertraulichkeit informationstechnischer Systeme (Art. 1 Abs. 1, Art. 2 Abs. 1 GG) ist ein derart blindes Vertrauen in die vom Bundeskriminalamt einzusetzenden Staatstrojaner ohne einen rechtsstaatlich gebotenen ausreichenden Überprüfungsmechanismus nicht hinnehmbar. Dies gilt insbesondere angesichts des Umstands, dass die Software nach dem Wortlaut des Gesetzes durchaus von einem externen Anbieter stammen kann, sodass das Bundeskriminalamt mitunter selbst nicht mit Sicherheit einzuschätzen vermöchte, welche Funktionen die einzusetzende Software ausführt. Ausdrücklich zu begrüßen ist in diesem Kontext, dass sich das BKA nach Presseberichten um die Eigenprogrammierung einer Überwachungssoftware bemüht; für den Bereich der sogenannten Quellen-Telekommunikationsüberwachung soll diese einsatzbereit sein[21]. Der vorliegende Gesetzentwurf schließt aber gerade nicht aus, dass auch – oder gar ausschließlich – Staatstrojaner zum Einsatz kommen, die weder vom BKA selbst programmiert noch extern und unabhängig geprüft sind.

Zwar mögen die technischen Details eines Staatstrojaners nicht unbedingt durch formelles Gesetz zu regeln sein. Zumindest aber muss das Gesetz im Lichte des Wesentlichkeitsgrundsatzes eine unabhängige technische Überprüfung der einzusetzenden Staatstrojaner vorschreiben. Die durch einen Staatstrojaner zu erfüllenden Spezifikationen könnten etwa im Verordnungswege durch das Bundesamt für Sicherheit in der Informationstechnik vorgegeben werden. Der Gesetzentwurf sollte hierzu um eine entsprechende Verordnungsermächtigung ergänzt werden. Zudem sollte ausschließlich der Einsatz erfolgreich geprüfter Staatstrojaner zulässig sein. Dies darzulegen sollte in den Katalog der obligatorischen Inhalte des Antrags (§ 49 Abs. 5 BKAG-E) aufgenommen werden.

b) Fehlanreize, die die Datensicherheit insgesamt schwächen

Zumindest ebenso schwer wie die geschilderten rechtlichen Bedenken gegen die fehlende Prüfung der Staatstrojaner wiegen indes die fatalen Fehlanreize, die die Norm für die Arbeit der Bundesbehörden – namentlich die im Aufbau befindliche „ZITIS“

[21] https://www.heise.de/newsticker/meldung/Quellen-Telekommunikationsueberwachung-Neuer-Bundestrojaner-steht-kurz-vor-Einsatzgenehmigung-3113444.html

(Zentrale Stelle für Informationstechnik im Sicherheitsbereich) – mit sich bringt. Nach § 49 Abs. 1 BKAG-E soll das BKA in informationstechnische Systeme „eingreifen“ dürfen, um aus ihnen Daten zu erheben. Hierzu ist denklogisch ein „Fuß in der Tür“ erforderlich, also das Aufbringen einer hoheitlichen Software, die Daten ausliest und an das BKA übermittelt. Solche Software-Lösungen werden allgemein als Staatstrojaner bezeichnet.

Der Entwurf definiert indes nicht weiter, wie der Staatstrojaner auf das Zielsystem aufgebracht werden darf. Denkbar sind insbesondere folgende Wege[22]:

- Aufspielen durch Hoheitsträger, etwa bei einer Grenzkontrolle
- Aufspielen durch Hoheitsträger durch heimliches Betreten der Räumlichkeiten, in denen sich das System befindet
- Ausnutzen der Unaufmerksamkeit des berechtigten Nutzers, etwa indem man ihm einen EMail-Anhang mit einem (getarnten) Infektions-Programm in der Hoffnung zuspielt, dass er ihn ausführen werde
- Aufspielen durch Ausnutzen von Sicherheitslücken des genutzten Systems, etwa indem der berechtigte Nutzer zum Aufruf einer speziell präparierten WWW-Seite animiert wird, deren bloße Ansicht aufgrund von Sicherheitslücken zur Infektion des Zielsystems führt (sogenannte *drive by downloads*)

Es erschließt sich unmittelbar, dass die rechtliche Bewertung der Zugriffe völlig unterschiedlich ausfällt: Das Betreten von Räumlichkeiten zur Infektion von Systemen ist im Lichte von Artikel 13 Abs. 1 des Grundgesetzes ohne eine (bisher fehlende) spezifische Ermächtigungsgrundlage hierzu schlechthin rechtswidrig. Das Aufspielen etwa bei einer Grenzkontrolle ist hingegen als solches unbedenklich, ebenso das Zusenden eine E-Mail mit einem getarnten Staatstrojaner (kriminalistische List), soweit dieser E-Mail-Anhang keine Sicherheitslücken ausnutzt.

Die Infektion des Zielsystems durch Ausnutzen von Sicherheitslücken – wiewohl vom Wortlaut des § 49 Abs. 1 BKAG-E gedeckt – führt hingegen zu gravierenden Fehlanreizen: Wenn Bundesbehörden solche Lücken ausnutzen dürfen, so haben sie ein

[22] Vertiefend zu den technischen Grundlagen *Buermeyer* HRRS 2007, S. 154 ff.

als solches durchaus nachvollziehbares Interesse daran, ein „Arsenal“ von Sicherheitslücken aufzubauen, um im Falle eines Falles eine Zielperson angreifen zu können. Dieses Interesse wird sie jedoch davon abhalten, gefundene oder gar auf dem Schwarzmarkt angekaufte Sicherheitslücke den jeweiligen Herstellern der IT-Systeme mitzuteilen, damit die Lücken geschlossen werden können. So entstehen Anreize für Bundesbehörden, ihnen bekannte Sicherheitslücken gerade nicht schließen zu lassen, sondern sie lieber zu horten.

Solange aber die Lücken nicht von den Herstellern der Systeme geschlossen werden können, weil sie von ihnen keine Kenntnis erlangen, können natürlich nicht nur Bundesbehörden diese Lücken für den Einsatz von Staatstrojanern ausnutzen. Vielmehr kann jeder, der sie findet oder seinerseits auf dem Schwarzmarkt für *0days* kauft, die Lücken zur Infiltration informationstechnischer Systeme missbrauchen – insbesondere auch Cyber-Kriminelle, die es beispielsweise darauf anlegen könnten, die betroffenen Systeme zum Teil eines Botnetzes zu machen oder Zahlungsdaten für Online-Überweisungen abzugreifen. Im Ergebnis würden Bundesbehörden mitunter viele Millionen Nutzerinnen und Nutzer von IT-Systeme weltweit, die von der jeweiligen Lücke betroffen sind, einem fortbestehenden Risiko von Cyber-Angriffen aussetzen, um Sicherheitslücken im Einzelfall selbst für Maßnahmen nach § 49 BKAG-E ausnutzen zu können.

Eine solche aus der Sicht einer Gefahrenabwehrbehörde noch nachvollziehbare Güterabwägung verbietet sich indes aus der Perspektive des Gesetzgebers, der das Wohl der Allgemeinheit in den Blick zu nehmen hat. Nicht zuletzt hat sich die Bundesregierung politisch zur Förderung der IT-Sicherheit bekannt[23]. Damit sind Anreize für Bundesbehörden, die Cyber-Sicherheit in Deutschland und weltweit im Interesse einer möglicherweise einmal erforderlichen Gefahrenabwehr zu schwächen, schlechthin unvereinbar.

[23] Vgl. die sog. Cyber-Sicherheitsstrategie für Deutschland 2016, abzurufen auf http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyber-Sicherheitsstrategie/cyber-sicherheitsstrategie_node.html

§ 49 BKAG-E sollte daher um ein explizites Verbot des Einsatzes von dem Hersteller eines informationstechnischen Systems bisher unbekannten Sicherheitslücken (sog. *0days*) ergänzt werden, um sicherzustellen, dass sich alle Bundesbehörden darum bemühen, ihnen bekannte Sicherheitslücken durch die Hersteller der Systeme so schnell wie möglich schließen zu lassen.

5.) Datenerhebungsermächtigung in § 64 Abs. 1 Nr. 1 BKAG-E

Insoweit wird auf die Erörterungen zu § 45 BKAG-E verwiesen.

6.) Benachrichtigungen, § 74 BKAG-E

Die Benachrichtigungsregelungen begegnen im Lichte des BKAG-Urteils ebenfalls Bedenken[24], sofern sie ein endgültiges Absehen von der Benachrichtigung nach fünf Jahren vorsehen, dabei aber die seitens des BVerfG vorgenommene verfassungskonforme Auslegung der Norm nicht aufgreifen[25]: Das endgültige Absehen ist als solches zwar verfassungsrechtlich zulässig, setzt aber *„voraus, dass eine weitere Verwendung der Daten gegen den Betroffenen ausgeschlossen ist und die Daten gelöscht werden"*. Dies ist durch § 74 Abs. 3 BKAG-E bisher nicht sichergestellt.

Nach dem Neuerlass einer Norm in zur Umsetzung einer hierzu ergangenen Entscheidung des BVerfG, aber ohne Berücksichtigung einzelner Monita des Gerichts würde sich indes eine (neuerliche) verfassungskonforme Auslegung verbieten: Der Verzicht auf eine Umsetzung würde insoweit auf einen entgegenstehenden Willen des Gesetzgebers hindeuten. § 74 Abs. 3 Satz 5 BKAG-E wäre also insoweit verfassungswidrig, als nicht sichergestellt ist, dass eine weitere Verwendung der Daten gegen den Betroffenen ausgeschlossen ist und die Daten gelöscht wurden[26].

---

[24] Vgl. auch die Stellungnahme des Bundesrats (a.a.O.), Seite 14.
[25] BVerfG a.a.O., Rn. 262.
[26] Vgl. auch die Stellungnahme des Bundesrats (a.a.O).

Schlussbemerkung

Angesichts des Änderungsbedarfs in dem in dieser Stellungnahme erörterten Teilen des Entwurfs, vor allem aber aufgrund der grundsätzlichen Bedenken gegen die Konzeption der Datenverarbeitung durch das BKA[27] sollte der Gesetzentwurf überarbeitet werden. Dies gilt insbesondere, führt man sich vor Augen, dass die Stellungnahmen der Sachverständigen schon aus Zeitgründen nur einen Abriss der verfassungsrechtlichen, aber auch rechtspolitischen Probleme des vorliegenden Entwurfs wiedergeben können.

Die seitens des BVerfG im Urteil zum BKA-Gesetz gesetzte Umsetzungsfrist (30. Juni 2018) lässt auch unter Berücksichtigung der Diskontinuität eine rechtzeitige Beschlussfassung durch den 19. Deutschen Bundestag durchaus zu, während sich die Schwächen des Entwurfs in dieser Legislaturperiode kaum rechtzeitig dürften beheben lassen. Insofern sollte von der Novelle einstweilen abgesehen werden.

Berlin, den 16. März 2016

Dr. Ulf Buermeyer, LL.M. (Columbia)[28]

[27] Vgl. §§ 12 ff. BKAG-E.

[28] Für wertvolle Hinweise dankt der Verfasser Herrn Univ.-Prof. Dr. Matthias Bäcker (Mainz) sowie Herrn Rechtsanwalt Dr. Nikolaos Gazeas (Köln).