Innenausschuss
A-Drs 16(4)460 I

UNIVERSITÄT BAYREUTH

PROF. DR. MARKUS MÖSTL

LEHRSTUHL FÜR ÖFFENTLICHES RECHT II

Schriftliche Stellungnahme

zur öffentlichen Anhörung im Innenausschuss des Deutschen Bundestages am 15.9.2008

zum Gesetzentwurf der Fraktionen der CDU/CSU und SPD – Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt – BT-Drucks. 16/9588.

Meine Stellungnahme folgt der Gliederung nach Themenkomplexen, wie sie uns mitgeteilte Anhörungsstrukturierung vorsieht. Ich beschränke meine Ausführungen auf Fragen der verfassungsrechtlichen Bewertung, zu denen ich als Staatsrechtslehrer Substantielles beitragen kann. Die Antworten geben meine persönliche erste Einschätzung der Dinge wieder, wie sie sich mir nach Durchsicht des Gesetzentwurfs auf der Basis meiner Kenntnisse als Verfassungsrechtler und Polizeirechtlicher darstellen. Eine verlässliche gutachterliche Beantwortung der aufgeworfenen Rechtsfragen würde zum Teil eine vertiefte juristische Prüfung voraussetzen, wie sie im Rahmen der Vorbereitung auf eine Sachverständigenanhörung nur bedingt leistbar ist.

Themenkomplex I: Übergreifende Fragestellungen

- <u>Kernbereichsschutz</u>

(1) Sind Kernbereichsregelungen bei allen heimlichen Ermittlungsmaßnahmen geboten?

Hier sind zwei Fragenkreise auseinanderzuhalten: Im Ausgangspunkt kann nicht zweifelhaft sein, dass der durch Art. 1 Abs.1 GG gewährleistete Kernbereichsschutz – bereits verfassungsunmittelbar – gegenüber jeder wie auch immer gearteten staatlichen Ermittlungsmaßnahme gilt; staatliche Ermittlungsmaßnahmen, die sich den durch den Menschenwürdesatz als einem unmittelbar geltenden Grundrecht aufgerichteten Schranken entziehen, sind nicht vorstellbar. Art. 1 Abs.1 GG wirkt insoweit als eine immanente Schranke, die jeder Befugnisnorm unmittelbar entgegengehalten werden kann und ihre verfassungskonforme Reduktion verlangt. Eine hiervon zu unterscheidende Frage ist es sodann allerdings, ob der Gesetzgeber von Verfassungs wegen verpflichtet ist, auch ausdrückliche und besondere Vorkehrungen zum Kernbereichsschutz vorzu-

sehen, die den bereits kraft unmittelbar anwendbaren Verfassungsrechts geltenden materiellen Schutz nunmehr auch prozedural näher konkretisieren und ausgestalten; hier geht es um besondere gesetzliche Normierungspflichten, die sich nach den Grundsätzen der Wesentlichkeitstheorie sowie des Grundrechtsschutzes durch Organisation und Verfahren beantworten. Die Rechtsprechung des Bundesverfassungsgerichts gibt keinen Anhaltspunkt dafür, dass derartige besondere Schutzvorkehrungen gegenüber allen polizeilichen Ermittlungseingriffen notwendig wären. Vielmehr betrafen alle bisher entschiedenen Fälle Eingriffe in Grundrechte (Unverletzlichkeit der Wohnung, Fernmeldegeheimnis, Recht auf Vertraulichkeit informationstechnischer Systeme), deren Gewährleistungsgehalt eine besondere Nähe zum durch Art. 1 Abs.1 GG aufgerichteten Kernbereichsschutz aufweist und bei denen – wie das BVerfG selbst sagte (BVerfG vom 27.2.2008 – 1 BvR 370/07 u.a., Abs.-Nr. 274), infolgedessen eine „gesteigerte Gefahr“ besteht, dass Daten höchstpersönlichen Inhalts erhoben werden und es so zu Kernbereichsverletzungen kommt. Nur unter der Voraussetzung einer derartigen mit einem Ermittlungseingriff typischerweise einhergehenden „gesteigerten Gefahr“ von Kernbereichseingriffen und unter der zusätzlichen Voraussetzung der Heimlichkeit (BVerfG aaO Abs.-Nr. 275) greift die Pflicht, besondere prozedurale Schutzvorkehrungen zu statuieren. Im Übrigen, soweit Ermittlungseingriffe typischerweise nicht den unantastbaren Kernbereich tangieren (vgl. BVerfGE 112, 304/318), bedarf es dieser besonderen Schutzvorkehrungen nicht; vielmehr ist es völlig ausreichend, dass, sollte ausnahmsweise doch einmal der Kernbereich gefährdet sein, die bereits kraft unmittelbar anwendbaren Verfassungsrechts geltende Eingriffsschranke des Art. 1 Abs.1 GG eingreift. Dieser Konzeption folgen bislang – zu Recht – auch alle anderen Polizeigesetze sowie die StPO.

(2) (Zweistufiges) Schutzkonzept im Übrigen

Die Rechtsprechung des BVerfG zur genaueren prozeduralen Ausgestaltung des Kernbereichsschutzes (BVerfGE 109, 279/318 ff.; 113, 348/390 ff.; BVerfG vom 27.2.2008 – 1 BvR370/07 u.a., Abs.-Nr. 270 ff.) sind noch im Fluss und keineswegs in allen Einzelheiten so festgezurrt, dass dem Gesetzgeber – an den sich der Verfassungsauftrag zur Ausgestaltung des Kernbereichsschutzes zuallererst richtet – keine Spielräume mehr für eine eigenständige sachgerechte Ausgestaltung blieben. Das BVerfG hat sich von Beginn an bemüht, differenzierte Anforderungen für die jeweils betroffenen Grundrechte zu entwickeln, die deren besonderen Eigenarten gerecht werden (vgl. z.B. BVerfGE 113, 348/391 f.). Darüber hinaus können die Ausführungen zum „zweistufigen Schutzkonzept“ in der jüngeren Entscheidung zur Online-Durchsuchung (BVerfG vom

27.2.2008, Abs.-Nr. 280 ff.) durchaus als eine auch generelle Präzisierung früherer Aussagen (die zu Missverständnissen Anlass gegeben und praktische Umsetzungsschwierigkeiten mit sich gebracht hatten) gedeutet werden, die nunmehr eine gesteigerte Offenheit des BVerfG erkennen lassen, soweit ermittlungstechnisch sinnvoll nicht anders möglich, trotz eventueller teilweiser Kernbereichsrelevanz zunächst auch automatische Erfassungen zuzulassen, sofern zumindest auf einer zweiten Stufe (der Durchsicht) sichergestellt ist, dass der erforderliche Kernbereichsschutz verwirklicht wird. Auch bezüglich dieser zweiten Stufe hat sich das BVerfG mit detaillierten Anforderungen zurückgehalten und nur verlangt, dass für die Durchsicht auf kernbereichsrelevante Inhalte ein „geeignetes Verfahren vorzusehen ist, das den Belangen des Betroffenen hinreichend Rechnung trägt“ (BVerfG aaO, Abs.-Nr. 283). Vor diesem Hintergrund scheinen mir sie zum Kernbereichsschutz getroffenen Regelungen einwandfrei. Insbesondere die Regelungen zum sog. „Richterband“ (§§ 20 h Abs.5, 20 k Abs.7, 20 l Abs. 6) stellen aus meiner Sicht eine Einrichtung dar, die die durch die BVerfG-Rspr. zum zweistufigen Schutzkonzept eröffneten Spielräume in einer einleuchtenden, sachgerechten und Art. 1 Abs.1 GG gerecht werden Weise nutzt. Speziell zu Art. 20 k Abs.7 siehe unten Themenkomplex II.

- <u>Eilfallkompetenzen</u>

Zur tatsächlichen Erforderlichkeit von Eilfallregelungen in den verschiedenen Konstellationen kann ich nichts Sachverständiges beitragen. Soweit Eilfallregelungen tatsächlich erforderlich sind, ist nicht zweifelhaft, dass Ausnahmen vom prinzipiellen Richtervorbehalt verfassungsrechtlich zulässig sein können (vgl. BVerfG vom 27.2.2008, Abs.-Nr. 261).

- <u>Anforderungen an die richterliche Entscheidungsfindung und Begründung</u>

Die vorgesehenen Regelungen (z.B. §§ 20 h Abs.4, 20 k Abs.6) verlangen – mit Ausnahme des § 20 l Abs. 4 – durchgehend, dass die richterliche Anordnung auch die „wesentlichen Gründe“ anzugeben habe. Dieser unbestimmte Rechtsbegriff kann ohne weiteres so ausgelegt werden, dass damit den Anforderungen genügt wird, die das BVerfG aufgestellt hat (BVerfG vom 27.2.2008, Abs.-Nr. 259; BVerfGE 109, 279/359). Die Sätze des BVerfG im Einzelnen in das Gesetz zu übernehmen, würde die Regelung nur unnötig aufblähen und der ohnehin beklagenswerten Tendenz noch weiter Vorschub leisten, dass die Normen des polizeilichen Informationsrechts immer länger und unübersichtlicher werden. Dass der Bestimmtheitsgrundsatz durch eine Festlegung auf die

„wesentlichen Gründe“ nicht verletzt ist, wird auch daran deutlich, dass das BVerfG in E 109,279/359 sich sogar damit begnügt hat, dass nur überhaupt eine schriftliche Begründung vorgeschrieben war; darüber hinausgehender gesetzlicher Regelungen bedürfe es nicht.

- Evaluation und Befristung

Grundsätzliche Pflichten zu einem nur befristeten oder unter prozeduralen Evaluierungsvorbehalt gestellten Gesetzeserlass sind dem Grundgesetz fremd. Zwar können sich unter besonderen Umständen – z.B. bei unsicherem Wissensstand – aus dem materiellen Recht (z.B. aus dem Verhältnismäßigkeitsprinzip) Pflichten zur fortlaufenden Beobachtung und Überprüfung einmal getroffener gesetzgeberischer Entscheidungen ergeben (z.B. BVerfGE 110, 141/166); auch können Gesetze aus materiellen Gründen verfassungswidrig werden, wenn z.B. ihre Erforderlichkeit weggefallen ist. Ansonsten jedoch – in verfahrensrechtlicher Hinsicht – vertraut das Grundgesetz (im Stadium des Gesetzeserlasses) ganz der Richtigkeitsgewähr des parlamentarischen Gesetzgebungsverfahrens (Art. 76 ff. GG) sowie (später, bei der Anwendung des Gesetzes) den Kontroll-, Frage und Enquêterechten des Parlaments und gestattet deswegen prinzipiell auch eine unbefristete und nicht an besondere Evaluierungspflichten geknüpfte Gesetzesgeltung. Der einfachgesetzlichen Statuierung von Evaluationspflichten im Rahmen moderner Gesetzesfolgenabschätzung steht es zwar nicht entgegen, es verlangt solche Pflichten aber auch nicht. Fragen von Befristung und Evaluierung sind so gesehen grundsätzlich Fragen der politischen Opportunität, nicht jedoch der verfassungsrechtlichen Notwendigkeit. (Eine Ausnahme mag für inhaltlich freier gestellte, d.h. einer ggf. nur reduzierten materiellen Verfassungskontrolle unterliegende Experimentiergesetzgebung gelten; dies steht hier jedoch in keiner Weise zur Debatte). Besondere Gründe, die hier für Befristungen und Evaluierungsvorbehalte sprechen würden, sind nicht ersichtlich: Die Regelungen betreffen eine auf Dauer angelegte Aufgabe des BKA; gerade zu den besonders eingriffstiefen Befugnisnormen gibt es BVerfG-Rspr., die die prinzipielle Zulässigkeit, aber auch die wesentlichen verfassungsrechtlichen Grenzen geklärt hat; besondere Ungewissheitsfaktoren über Umstände und Folgen der Maßnahmen sind nicht ersichtlich.

Themenkomplex II: Online-Durchsuchung und Quellen-TKÜ

- Eingriffsvoraussetzungen

Die verfassungsrechtlichen Anforderungen an den Eingriffsanlass einer Online-Durchsuchung (Verdachtsgrad, Rechtsgüter) hat das BVerfG in seinem Leitsatz 2 der einschlägigen Entscheidung vom 27.2.2008 zusammengefasst: Hiernach ist die Online-Datenerhebung verfassungsrechtlich zulässig, „wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen“.

Gerade die Präzisierung des letzten Satzes ist von besonderer Bedeutung. Klargestellt ist aus meiner Sicht damit nämlich, dass nicht in jedem Fall bereits eine konkrete Gefahr für das überragend wichtige Rechtsgut eingetreten sein muss (vgl. auch Roggan, in: ders. (Hrsg.), Online-Durchsuchungen, 2008, S. 97/103 ff.). Zulässig sind mit anderen Worten auch Maßnahmen im Gefahrenvorfeld, soweit immerhin bereits bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen, d.h. ein konkreter personenbezogener Gefahrverdacht besteht (zu den Verdachtsgraden im Gefahrenvorfeld: Möstl, DVBl. 2007, 581/587 f.). Das BVerfG trägt damit dem Umstand Rechnung, dass der Einsatz der „Online-Durchsuchung“ häufig gerade in solchen Situationen nützlich und notwendig sein wird, in denen zwar bestimmte Tatsachen bereits den Schluss auf ein „seiner Art nach konkretisiertes und zeitlich absehbares Geschehen“ sowie auf einen bestimmten Täterkreis zulassen, in denen andererseits aber dennoch u.U. noch keine „konkrete Gefahr“ festgestellt werden kann, die bereits den für diesen Begriff geltenden Anforderungen an Absehbarkeit eines konkreten schadensträchtigen Kausalverlaufs und zeitliche Nähe des Umschlagens in einen Schaden genügt; vgl. BVerfG vom 27.2.2008, Abs.-Nr. 242, 251. Das so umrissene – freilich eng bemessene – Gefahrenvorfeld soll der Online-Datenerhebung also nicht grundsätzlich verschlossen sein. Dies zeigt sich auch darin, dass das BVerfG in dem zu entscheidenden Fall (der den Verfassungsschutz betraf) ausdrücklich auf den im Vorfeld konkreter Gefahren einsetzenden Aufklärungsauftrag

der Verfassungsschutzbehörden abhebt (BVerfG vom 27.2.2008, Abs.-Nr. 219). Die sich ergebende Eingreifschwelle soll gleichwohl nicht nur für den Verfassungsschutz, sondern ausdrücklich auch für den polizeilichen Bereich gültig sein (BVerfG vom 27.2.2008, Abs.-Nr. 254 ff). Nur ein „noch weitergehend in das Vorfeld“ einer konkreten Gefahr verlegtes Eingreifen, in dem das Vorfeldstadium nur „durch relativ diffuse Anhaltspunkte für mögliche Gefahren“ gekennzeichnet ist (abstrakter Gefahrverdacht), soll ausgeschlossen sein (BVerfG vom 27.2.2008, Abs.-Nr. 252 f.). Darin, dass das BVerfG das Vorfeldstadium für Online-Datenerhebungen keineswegs vollständig verschließt, trägt es der nach meiner Ansicht wichtigen Überlegung Rechung, dass Informationseingriffe ihrer typischen Zielrichtung nach nicht an das Vorliegen einer Gefahr gebunden sein, sondern seit jeher auch der Gefahrermittlung und -aufklärung im Gefahrenvorfeld dienen können. Gefahrbeseitigungseingriffe (d.h. die polizeiliche Unterbrechung des schadensträchtigen Kausalverlaufs) sind stets erst ab der Schwelle der konkreten Gefahr, also einer hinreichenden Wahrscheinlichkeit, zulässig; Informationseingriffe zur Gefahraufklärung im Gefahrenvorfeld sind dagegen nichts an sich ungewöhnliches (dass sie freilich der rechtsstaatlichen Eingrenzung durch vorfeldadäquate Verdachtsgrade bedürfen, ist unstrittig und steht auf einem anderen Blatt; vgl. dazu Möstl, DVBl. 2008, 581/584 ff.).

Legt man diese Maßstäbe zugrunde, ist die Regelung der Voraussetzungen eines verdeckten Eingriffs in informationstechnische Systeme in § 20 k Abs. 1 einwandfrei. Die Formulierungen lehnen sich eng an die Wortwahl des BVerfG an. Dies gilt auch für § 20k Abs.1 S.2, der nach hier vertretener Ansicht – wie dargelegt – jedenfalls eine geringfügige Vorverlagerung ins Gefahrenvorfeld gestatten würde. Andererseits scheint der Gesetzentwurf (vgl. Entwurfsbegründung S. 71 f.) davon auszugehen, dass auch insoweit die Grenzen der konkreten Gefahr noch gewahrt sind, d.h. eine Gefahrenabwehr- und keine Vorfeldbefugnis gegeben ist (vgl. auch § 20 k Abs.4, der hinsichtlich des Adressaten an die Störereigenschaft anknüpft, d.h. ganz offensichtlich eine Gefahr voraussetzt, denn ohne Gefahr gibt es auch keinen Störer; vgl. überdies den Zusammenhang mit § 20 a Abs.1, auf den auch die Entwurfsbegründung abhebt). Zuzugeben ist, dass die genaue Grenze zwischen konkreter Gefahr und unmittelbarem Gefahrenvorfeld schwer zu ziehen ist und nicht als gesichert gelten kann (vgl. auch Roggan aaO S. 103). Sollte die Norm als eine Gefahrenabwehrbefugnis auszulegen sein, die stets (auch im Fall des § 20 k Abs.1 S.2) eine konkrete Gefahr voraussetzt, dann schöpft sie – nach hiesigem Verständnis – die durch das BVerfG eröffneten Spielräume hinsichtlich zulässiger Vorverlagerung noch nicht einmal vollständig aus.

- Kernbereichsschutz

Vgl. hierzu allgemein bereits die Ausführungen zu Themenkomplex 1. Hinsichtlich der Ausgestaltung der zweiten Verfahrensstufe (Durchsicht auf kernbereichsrelevante Inhalte) verlangt das BVerfG, wie bereits ausgeführt, ohne nähere Festlegung allein, dass ein „geeignetes Verfahren vorzusehen ist, das den Belangen des Betroffenen hinreichend Rechnung trägt“. Das in § 20 k Abs.7 geregelte Verfahren, das eine Durchsicht zunächst durch zwei BKA-Beamte, von denen einer die Befähigung zum Richteramt hat, und in allen Zweifelsfällen die Vorlage an den Richter vorsieht, scheint mir diesen Anforderungen gerecht zu werden.

- Betretensregelung

Eine Betretensregelung zur Vorbereitung der Online-Durchsuchung enthält § 20 k BKAG-E – anders als Art. 34 e BayPAG (notwendige Begleitmaßnahmen) – nicht. Art. 20 t BKAG dürfte nicht weiterhelfen, da dieser wohl nur offene Eingriffe in Art. 13 GG betrifft, während ein Betreten zur Vorbereitung der verdeckten Online-Durchsuchung naturgemäß nur als seinerseits verdeckte Maßnahme Sinn macht. Ein Betreten der Wohnung zur Vorbereitung eines verdeckten Eingriffs in ein informationstechnisches System dürfte einen – zum Eingriff in das Recht auf Vertraulichkeit informationstechnischer Systeme hinzutretenden – eigenständigen Eingriff auch in das Grundrecht des Art. 13 GG darstellen, der einer gesonderten Befugnisgrundlage bedarf, d.h. nicht bereits implizit in der Befugnis zur Online-Durchsuchung enthalten ist (die ja keineswegs stets einen Eingriff in Art. 13 GG voraussetzt). Eine Befugnis zum vorbereitenden Betreten von Wohnungen enthält der BKAG-E mit anderen Worten nicht. Die Wirksamkeit der Online-Durchsuchung wird dadurch erschwert. Ihr deswegen – aufgrund Fehlens einer flankierenden Betretensregelung – bereits die nötige Eignung abzusprechen, dürfte umgekehrt jedoch zu weit gehen; auch das BVerfG hat diesbezüglich in seiner Entscheidung keine Zweifel geäußert und die Eignung auch einer Infiltration mittels Zugriffssoftware ausdrücklich bejaht (vgl. Abs.-Nr. 222: „Die gesetzgeberische Prognose, dass Zugriffe der geregelten Art im Einzelfall Erfolg haben können, ist zumindest nicht offensichtlich fehlsam“). Die Statuierung einer Betretensregelung müsste sich vor Art. 13 GG rechtfertigen, d.h. sich insbesondere unter eine der dort vorgesehenen Schranken subsumieren lassen. Hier ist noch einiges unsicher; dennoch wäre eine Rechtfertigung nach hier vertretener Ansicht – auch ohne Änderung des Art. 13 GG –

möglich. In der Anhörung des Bayerischen Landtags zu Online-Durchsuchung nach dem BayPAG am 27.5.2008 habe ich hierzu schriftlich ausgeführt:

Das ggf. notwendige Betreten und Durchsuchen der Wohnung zur Vorbereitung einer verdeckten Online-Datenerhebung stellt im Verhältnis zur (am Grundrecht der Integrität informationstechnischer Systeme zu messenden) späteren „Online-Durchsuchung" einen eigenständigen, an Art. 13 GG zu messenden Grundrechtseingriff dar, der gesondert gerechtfertigt werden muss.

> *Anders liegt es, wenn bereits die Hauptmaßnahme in Art. 13 GG eingreift, d.h. insbesondere bei verdeckten Abhörmaßnahmen nach Art. 13 Abs. 3 und 4 GG: Hier decken die Schranken des Art. 13 Abs.3 und 4 GG vorbereitende Maßnahmen wie das Betreten der Wohnung, die mit dem Abhören notwendig verbunden sind, ohne weiteres mit ab; vgl. Jarass/Pieroth Art. 13, Rn. 22. Auch hier liegt es freilich in der Gestaltungsfreiheit des Gesetzgebers, für das Betreten der Wohnung eine eigenständige Anordnung vorzuschreiben, die freilich nicht anders als die Hauptmaßnahme durch Art. 13 Abs.3 und 4 GG gerechtfertigt ist (und folglich auch an keine anderen Voraussetzungen geknüpft sein kann). Nichts anderes hat der Gesetzentwurf in Art- 34 e PAG-Ä-E getan, soweit dieser auch Begleitmaßnahmen für Eingriffe in Art. 13 GG erfasst.*

Das Verhältnis des neuen Grundrechts des Schutzes der Integrität informationstechnischer Systeme zu den möglicherweise auch betroffenen Art. 10 und 13 GG kommt in der Entscheidung des BVerfG nicht ganz eindeutig zum Ausdruck.

> *BVerfG vom 27.2.2008, Abs.-Nr. 181 ff.*

Einerseits scheint das neue Grundrecht Auffangfunktion zu haben, soweit Art. 10 und 13 GG nicht bereits ohnehin adäquaten Schutz bieten (was für eine eigenständige Prüfung an Art. 13 GG spräche). Andererseits scheint es im Verhältnis zu Art. 10 GG letztlich so, dass das neue – umfassendere – Grundrecht aus Art. 2 Abs.1 iVm 1 Abs.1 GG teilweise an die Stelle des Art. 10 GG tritt, der nur noch gelten soll, wenn sich die Überwachung allein auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt, ansonsten (bei weitergehenden Maßnahmen) aber vom neuen Grundrecht konsumiert wird. Auf Art. 13 GG dürfte sich diese (zur teilweisen Verdrängung des älteren und ausdrücklich geschriebenen Grundrechts führende) Linie nicht übertragen lassen. Entscheidend hierfür ist, dass sich im Verhältnis zu Art. 13 GG (anders als bei Art. 10 GG) die Maßnahmen zeitlich in verschiedene Einzelschritte zerlegen lässt: Die die Wohnung auf den Computer hin durchsuchende Polizei greift erst in Art. 13 GG ein, um sodann eine Online-Datenerhebung zu starten, die ihrerseits Art. 2 Abs.1 iVm Art. 1 Abs.1 GG beeinträchtigt. Die Situation ähnelt damit der Konstellation, dass nach einer Durchsuchung ein Computer beschlagnahmt wird, um dann ausgewertet zu werden: Auch hier wird von einem Nacheinander eines Eingriffs in Art. 13 GG und das Recht auf informationelle Selbstbestimmung ausgegangen.

> *BVerfGE 113, 29/45*

Einen eigenständigen Gehalt hat der Eingriff in Art. 13 GG außerdem schon deswegen, weil durchaus Online-Datenerhebungen denkbar sind, die ohne einen solchen Eingriff (d.h. ohne physische Manipulation eines Computers in einer Wohnung) auskommen. Ganz in diesem Sinne hat das BVerfG ausdrücklich ausgeführt, das Eindringen in eine Wohnung zum Zwecke der nachfolgenden „Online-Durchsuchung" sei ein Eingriff in Art. 13 GG (der die Zugriffsmodalitäten betrifft). Die nachfolgende Datenerhebung berührt dann (selbst soweit sich der Computer in einer Wohnung befindet, was freilich keineswegs zwingend ist) allein das Grundrecht auf Integrität informationstechnischer Systeme, das einen von den Zugriffsmodalitäten unabhängigen Schutz gewährt.

> *BVerfG vom 27.2.2008, Abs.- Nr. 193 f.*

In diesem Sinne ist es jedenfalls im Verhältnis zur Online-Datenerhebung nicht nur nicht angreifbar, sondern folgerichtig, wenn die Gesetzentwürfe eine eigenständige Regelung zu den Art. 13 GG berührenden Begleitmaßnahmen sowie zu ihrer Anordnung treffen (Art. 34 e PAG-Ä-E und Art. 6 g VSG-Ä-E).

Eine andere Frage ist es, welche Schranke innerhalb des Art. 13 GG für diese Begleitmaßnahme einschlägig sein soll, insbesondere ob sie auf Art. 13 Abs.2 GG (Durchsuchung) oder auf Art. 13 Abs.7 GG (sonstige Beschränkung) zu stützen ist. Die Schrankensystematik des Art. 13

GG und insbesondere das Verhältnis zwischen Abs.2 und 7 wird häufig als missglückt angesehen und ist nicht ins letzte geklärt. Im Streit steht insbesondere, ob für Art. 13 Abs.2 GG ein enger oder weiter Durchsuchungsbegriff anzulegen ist.

Hermes, in: Dreier, Art. 13, Rn. 30; Gornig, in v.Mangoldt/Klein/Starck, Art. 13, Rn. 57.

Diese Unsicherheit belastet auch die hiesige Fallgestaltung.

Im Ergebnis ist es im hiesigen Fall durchwegs präventiver Eingriffszwecke egal, ob die Begleitmaßnahme nach Art. 13 Abs.2 oder nach Abs.7 gerechtfertigt wird, denn beide Male ist eine Rechtfertigung möglich und genügt die vorgesehene gesetzliche Ausgestaltung den verfassungsrechtlichen Anforderungen.

Anders läge es, soweit es um die Vorbereitung strafprozessualer Online-Datenerhebungen ginge. Hier nämlich könnte die präventive Ausrichtung des Art. 13 Abs.7 GG Probleme bereiten.

Art. 13 Abs. 2 GG stellt zusätzlich zur richterlichen Anordnung keine weiteren materiellen Anforderungen; freilich gilt der begrenzende Grundsatz der Verhältnismäßigkeit. Es ist kein Grund ersichtlich, warum die vorbereitende Begleitmaßnahme der Wohnungsdurchsuchung unter Verhältnismäßigkeitsgesichtspunkten an strengere Voraussetzungen geknüpft sein sollte als die Hauptmaßnahme des verdeckten Online-Zugriffs auf das informationstechnische System. Insofern ist es einwandfrei, wenn der Gesetzgeber die Begleitmaßnahme an die gleichen Voraussetzungen knüpfen will wie die Hauptmaßnahme.

Sollte sich die Maßnahme dagegen nach Art. 13 Abs. 7 GG richten, ist zwar nicht unbedingt eine richterliche Anordnung nötig (was den Gesetzgeber freilich nicht daran hindert, eine solche vorzuschreiben), andererseits ist die Rechtfertigung der Maßnahme an die Voraussetzung geknüpft, dass sie „zur Verhütung dringender Gefahren“ erfolgt. Diesbezüglich ist anerkannt, dass noch keine konkrete Gefahr eingetreten sein muss, sondern auch eine vorgelagerte präventive Verhütung der Gefahr möglich ist, d.h. eine bloß „abstrakte“ Gefahr ausreicht.

Papier, in Maunz/Dürig, Art. 13, Rn. 128; BVerfGE 17, 232/251 f.

Auch wenn man hinzu nimmt, dass „dringende Gefahren“ eine gesteigerte Bedeutung des zu schützenden Rechtsguts voraussetzen, liegen die Anforderungen also nicht allzu hoch; sie sind durch Art. 34 e PAG-Ä-E und Art. 6 g VSG-Ä-E jedenfalls unproblematisch erfüllt.

Die Gesetzentwürfe gehen schon aufgrund ihrer Formulierung „betreten und durchsuchen“, aber auch indem ein Richtervorbehalt angeordnet wird, offenbar davon aus, dass die Begleitmaßnahme des vorbereitenden Eindringens in die Wohnung als Durchsuchung iSv. Art. 13 Abs.2 GG zu qualifizieren ist. Unter einer Durchsuchung wird regelmäßig verstanden: „das ziel- und zweckgerichtete Suchen staatlicher Organe nach Personen oder Sachen oder zur Ermittlung eines Sachverhalts, um etwas aufzuspüren, was der Inhaber der Wohnung von sich aus nicht offen legen oder herausgeben will.“

BVerwGE 47, 31/37; Gornig, in v. Mangoldt/Klein/Starck, Art. 13, Rn. 59

Legt man dies zugrunde, so kann das Eindringen in eine Wohnung, um dort z.B. einen Computer aufzuspüren, der dann manipuliert werden kann, mit guten Gründen als Durchsuchung begriffen werden. Insbesondere geht es um mehr als ein bloßes Betreten. Da regelmäßig nicht bekannt sein wird, wo genau der Computer sich befindet, ist vielmehr durchaus ein Element des gezielten Suchens feststellbar. Hierbei würde es auch nichts schaden, wenn der Computer sichtbar postiert ist; denn auch die Suche nach sichtbar Aufbewahrtem ist eine Durchsuchung.

Gornig, in v. Mangoldt/Klein/Starck, Art. 13, Rn. 61.

Noch viel mehr handelt es sich freilich um eine Durchsuchung, wenn etwa ein tragbarer Computer erst in Schränken/Schüben/Taschen aufgespürt werden muss; hier wird das Moment des Ausforschens eines privaten Lebensbereichs, um das es bei der Durchsuchung notwendig geht, besonders deutlich. Soweit der genaue Standort des Geräts nicht bekannt ist, kann jedenfalls nicht bestritten werden, dass der Suche ein eigenständiger Informationswert zukommt und auch insofern – wenn man voraussetzt, dass die Gewinnung von Informationen einen notwendigen Teil des Durchsuchungsbegriffs darstellt – eine Durchsuchung gegeben sein kann.

Hermes, in Dreier, Art. 13, Rn. 47.

Problematisch könnte allerdings sein, dass unter Durchsuchung im Allgemeinen eine prinzipiell offene staatliche Maßnahme verstanden wird,

Gornig, in v. Mangoldt/Klein/Starck, Art. 13, Rn. 65 f.

das Eindringen in die Wohnung als Vorbereitungsmaßnahme eines verdeckten Zugriffs auf informationstechnische Systeme allerdings seinerseits verdeckt wird stattfinden müssen. Z.B. verdeckte Abhörmaßnahmen konnten deswegen nach hM nicht auf Art. 13 Abs.2 GG gestützt werden, vielmehr mussten dafür die Schrankenregelungen der Art. 13 Abs.3 und 4 GG geschaffen werden. Zu bedenken ist im hiesigen Fall allerdings, dass es sich bei dem Eingriff in Art. 13 GG um eine bloße Vorbereitungsmaßnahme für eine ihrerseits verdeckte Hauptmaßnahme, den verdeckten Zugriff auf informationstechnische Systeme handelt. Der besondere Aspekt, dass die Gesamtmaßnahme heimlich abläuft, wird bereits dadurch „abgearbeitet", dass das gerade auch deswegen neu entwickelte Grundrecht der Integrität informationstechnischer Systeme für derartige heimliche Eingriffe hohe sachliche Hürden aufstellt. In dem Maße aber, wie der besondere Aspekt der Heimlichkeit bereits von dem Grundrecht auf Integrität informationstechnischer Systeme erfasst und sachlich abgearbeitet wird, scheint es vertretbar, für die nur vorbereitende Wohnungsdurchsuchung (die wegen ihrer Bezogenheit auf die heimliche Hauptmaßnahme natürlich nicht anders als heimlich ablaufen kann) den Aspekt der Heimlichkeit nicht besonders ins Gewicht fallen zu lassen – mit der Folge, dass Art. 13 Abs.2 GG jedenfalls für solche Vorbereitungsmaßnahmen, die sich auf Hauptmaßnahmen beziehen, deren Heimlichkeit noch gesondert gerechtfertigt werden muss, als geeignete Eingriffsgrundlage angesehen werden kann.

Dafür, im Zweifel von einer Durchsuchung und nicht von einer bloßen sonstigen Beschränkung auszugehen, spricht auch, dass es sich bei der Durchsuchung um den typischerweise tieferen Eingriff handelt, bzgl. derer mit dem Richtervorbehalt auch eine weitergehende prozedurale Eingriffsvoraussetzung statuiert wird.

Selbst wenn man nicht der von einer Mindermeinung vertretenen Ansicht folgt, dass alle richterlich angeordneten Wohnungsbeeinträchtigungen bereits per se eine „Durchsuchung" darstellen (weiter Durchsuchungsbegriff),

Dazu Hermes, in Dreier, Art. 13, Rn. 30

erscheint es nach alledem zumindest gut vertretbar, wenn der Gesetzgeber in der schwierigen Abgrenzungsfrage von Art. 13 Abs.2 und Abs.7 GG im Zweifel von einer Durchsuchung ausgeht.

Themenkomplex III: Zu einzelnen weiteren Befugnissen

- Telekommunikationsüberwachung

§ 20 l BKAG-E ist an den Bestimmtheits- und Verhältnismäßigkeitsanforderungen zu messen, die das BVerfG v.a. in E 113, 348 (zuvor auch E 110, 33) für die präventivpolizeiliche Telekommunikationsüberwachung aufgestellt hat. Er hält diesen Anforderungen stand.

Der näheren Prüfung wert kann insoweit bereits von vornherein allenfalls die Eingriffsvoraussetzung des § 20 l Abs.1 S.1 Nr. 2 erscheinen, die – anders als die vorangehende Nr. 1 – nicht ausdrücklich auf das Gegebensein einer Gefahr abstellt und insofern als eine bereits im Gefahrenvorfeld greifende Eingriffsbefugnis der Straftatenverhütung angesehen werden könnte. Die vom BVerfG in E 113, 348 entwickelten restriktiven Anforderungen betreffen nämlich ausschließlich die Zulässigkeit von Telekommunikationsüberwachungen im Vorfeldbereich; dass Telekommunikationsüberwachung in Situationen klassischer Gefahrenabwehr erlaubt werden kann, setzt diese Entscheidung als selbstverständlich voraus (vgl. E 113, 348/377).

Ob § 20 l Abs. 1 S.1 Nr.2 wirklich als eine Befugnis zu einer bereits im Gefahrenvorfeld greifenden Straftatenverhütung gedacht ist (so wie z.B. § 20 b Abs.2, vgl. dazu Entwurfsbegründung S. 55) oder aber allein als eine straftatenbezogene Konkretisierung der bereits in Nr. 1 beschriebenen Gefahrenlage anzusehen ist, die wie diese eine konkrete Gefahr voraussetzt, die hier nur näher umschrieben wird (so z.B. für das Verhältnis von Art. 34 a Abs.1 S.1 Nr. 1 und Nr. 2 BayPAG: Käß, BayVBl. 2008, 225/229 f.), lässt die Entwurfsbegründung (S. 78) nicht erkennen.

Vergleicht man den Wortlaut des § 20 l Abs.1 S. 1 Nr. 1, wonach „bestimmte Tatsachen die Annahme rechtfertigen“, dass die Person „Straftaten gemäß § 4a Abs.1 Satz 2 vorbereitet“ mit einer in anderem Kontext gebrauchten Formulierung des Gesetzentwurfs, die dieser noch recht eindeutig als Bestandteil der Gefahrenabwehr ansieht und gerade nicht dem Gefahrenvorfeld zurechnet – die Formulierungen des § 20 h Abs.1 Nr. 1 b) und des § 20 j Abs.1 S.1 2. Hs., wonach jeweils „konkrete Vorbereitungshandlungen“ die Annahme rechtfertigen, dass die Person eine „Straftat gemäß § 4 a Abs.1 Satz 2 begehen wird“ bzw. dass eine solche Straftat „begangen werden soll“ – so dürfte § 20 l Abs. 1 S.1 Nr. 1, der eben noch nicht eine (erwiesene) konkrete Vorbereitungshandlung verlangt (die dann Basis der Prognose der Straftatenbegehung ist), sondern nur die auf bestimmte Tatsachen gestützte Annahme einer Straftatenvorbereitung, an Strenge etwas hinter diesen anderen Eingriffsschwellen zurückbleiben. Es ist demnach

zumindest nicht ausgeschlossen, dass § 20 Abs.1 S.1 Nr. 1 als leicht ins Gefahrenvorfeld vorgelagerte Befugnis der Straftatenverhütung verstanden werden könnte.

Hieraus folgt freilich nicht, dass eine derartige Befugnis per se als verfassungsrechtlich bedenklich angesehen werden müsste. Das BVerfG hat in E 110, 33; 113, 348 Telekommunikationsüberwachungen im Gefahrenvorfeld keineswegs als solche verboten, sondern nur an bestimmte Voraussetzungen geknüpft. Auch die Entscheidung zur Online-Durchsuchung hat, wie bereits ausgeführt, deutlich gemacht, dass zumindest leichte Vorverlagerungen in das Gefahrenvorfeld selbst bei schwerwiegendsten Eingriffen in Betracht kommen können. Zu Recht: Denn dass Ermittlungsbefugnisse bereits im Gefahrenvorfeld ansetzen, ist keineswegs etwas Ungewöhnliches oder an sich besonders Rechtfertigungsbedürftiges. Der Gefahrbegriff setzt, indem er für Gefahrbeseitigungseingriffe (d.h. für die polizeiliche Unterbrechung des schadenträchtigen Kausalverlaufs) eine auf belastbare Erkenntnisse gestützte Wahrscheinlichkeitsprognose verlangt, Informationseingriffe im Gefahrenvorfeld, die der Erlangung der für die Gefahrprognose nötigen Erkenntnisse dienen, geradezu voraus. Gerade im Bereich der Terrorismusabwehr wird es, soll die Gefahr noch rechtzeitig abwendbar sein, häufig unumgänglich sein, nicht einfach abzuwarten, sondern bereits im Gefahrenvorfeld Informationen zu erheben (Möstl, DVBl. 2007, 581/584). Dass auch im Anwendungsbereich von Art. 10 GG Vorfeldbefugnisse zulässig sein können, kann demnach nicht prinzipiell zweifelhaft sein.

Eine andere Frage ist es, an welche rechtsstaatlichen Eingriffsvoraussetzungen dergleichen Vorfeldbefugnisse geknüpft werden müssen. Zur Klärung dieser Frage ist es vor allem wichtig, danach zu unterscheiden, um welche Art Vorfeldbefugnis es sich handeln soll. Das Gefahrenvorfeld ist ein weites Feld, das von rein lagebezogenen abstrakten Vermutungen bis hin zu bereits sehr konkreten personenbezogenen Verdachtslagen reichen kann, die hinter einer konkreten Gefahr nur wenig zurückbleiben. Für das Verständnis der Entscheidung zum NdsSOG (E 113, 348) ist ausschlaggebend, dass es sich dort um eine sehr weit in das Gefahrenvorfeld gezogene Ermittlungsbefugnis handelte; es genügte – wie das BVerfG formulierte (E 113, 348/378) bereits „die auf Tatsachen gegründete, nicht näher konkretisierte Möglichkeit, dass jemand irgendwann in Zukunft Straftaten von erheblicher Bedeutung begehen wird“. Vor allem, dass sich die damals streitgegenständliche Norm völlig von einem konkreten, in der Entwicklung begriffenen Vorgang oder zumindest dessen Planung oder Vorbereitung löste, wurde mehrfach bemängelt (BVerfGE 113, 348/378, 386). Nur für so weit vorgelagerte Ermittlungen, die in keiner Weise mehr an konkrete Planungs- oder Vorbereitungshandlungen

anknüpfen, besteht das in der Entscheidung beschriebene besondere Risiko falscher Prognosen, welches daraus resultiert, dass letztlich auf der Basis von nur diffusen Anhaltspunkten entschieden wird (BVerfGE 113, 348/377), und welches deswegen zwingend durch besonders strenge Maßgaben hinsichtlich Bestimmtheit und Verhältnismäßigkeit eingrenzender Tatbestandsmerkmale kompensiert werden muss, wie sie die Entscheidung sodann beschreibt.

Von einer solch starken Vorverlagerung ist § 20 l Abs.1 S.1 Nr. 2, falls er überhaupt eine Vorfeldbefugnis darstellt (s.o.), jedenfalls weit entfernt. Insbesondere genügt es ihm gerade nicht, dass bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person nur überhaupt irgendwann bestimmte Straftaten begehen wird (ungenau insofern die Entwurfsbegründung auf S. 78); vielmehr wird durch das Wort „vorbereitet" verlangt, dass sich der auf bestimmte Tatsachen gestützte Verdacht auf eine bereits im Gange befindliche Vorbereitung von Straftaten bezieht. Von einem konkreten, in der Entwicklung begriffenen Vorgang oder zumindest seiner Vorbereitung und Planung löst sich die Norm so gesehen gerade nicht; das in BVerfGE 113, 348/378 formulierte Hauptmonitum ist für die hiesige Befugnisnorm deswegen nicht relevant. § 20 l Abs.1 S.1 Nr. 2 stellt, falls er überhaupt eine Vorfeldbefugnis ist, jedenfalls nicht eine Vorverlagerung des Eingriffs in eine solche (frühe) Phase (vgl. BVerfGE 113, 348/377) dar, für die die vom BVerfG formulierten Bedenken und besonderen rechtsstaatlichen Anforderungen greifen. Aus BVerfG 113, 348 lassen sich deswegen im Ergebnis keine Einwände gegen die Befugnis herleiten.

- <u>Wohraumüberwachung</u>

Vgl. bereits die allgemeinen Ausführungen zu Themenkomplex 1.

- <u>Rasterfahndung</u>

Die in § 20 j Abs.1 formulierten Voraussetzungen genügen den in BVerfGE 115, 320 aufgestellten Anforderungen, insbesondere hinsichtlich des nötigen Vorliegens einer konkreten Gefahr für hochrangige Rechtsgüter. Dies gilt auch für die im zweiten Halbsatz des Satzes 1 aufgestellte Regelvermutung, dass von einer Gefahr in der Regel auch dann auszugehen ist, „wenn konkrete Vorbereitungshandlungen die Annahme rechtfertigen, dass eine Straftat nach § 4a Abs.1 Satz begangen werden soll". Vergleichbare, auf konkrete Vorbereitungshandlungen abstellende Formulierungen werden auch anderwärts als Verdeutlichungen der Schwelle der konkreten Gefahr, d.h. gerade nicht als eine Vorverlagerung ins Gefahrenvorfeld begriffen (vgl. z.B. für Art. 34 a Abs.1

S.1 Nr. 2 BayPAG: Käß, BayVBl. 2008, 225/229 f.; oder für Art. 34 Abs.1 S.1 Nr. 2 BayPAG: Schmidbauer/Steiner, PAG, Rn. 15, 53). Dies ist auch richtig, denn durch das Abstellen auf konkrete Vorbereitungshandlungen ist jener Bezug zu einem konkreten, bereits in Gang gesetzten Geschehensablauf hergestellt, der für die konkrete (im Gegensatz zur abstrakten) Gefahr kennzeichnend ist; das Merkmal „die Annahme rechtfertigen“ verlangt sodann einen Wahrscheinlichkeitsgrad, der dem der konkreten Gefahr entspricht.

Nur zusätzlich sei außerdem bemerkt, dass auch bereits im Gefahrenvorfeld ansetzende Rasterfahndungen nach hier vertretener Ansicht keineswegs als per se verfassungswidrig anzusehen wären. Die Festlegung des BVerfG, präventive Rasterfahndungen an die Gefahrenschwelle zu binden, muss als fragwürdig und im Lichte neuerer Rechtsprechung auch überprüfungsbedürftig erscheinen. Sie verkennt, dass polizeiliche Informationseingriffe – wie bereits mehrfach bemerkt – geradezu typischerweise, und ohne dass dies etwas an sich besonders Rechtfertigungsbedürftiges wäre, im Gefahrenvorfeld ansetzen müssen; die Gefahrenschwelle ist die rechtsstaatliche Regelvoraussetzung allein für kausalverlaufsrelevante Gefahrbeseitigungseingriffe, nicht aber für (nur vorbereitende) Informationseingriffe (Möstl, DVBl. 2007, 581 ff.). Gerade in Bezug auf die Rasterfahndung ist es sehr problematisch, eine Eingriffsschwelle (die konkrete Gefahr) zu fordern, die in einem Moment, in dem eine aufwändige Rasterfahndung noch Sinn macht, typischerweise noch gar nicht gegeben sein kann (Möstl, aaO, 588). Zu bedenken ist schließlich die in der Entscheidung zur Online-Durchsuchung (BVerfG vom 27.2.2007; siehe oben Themenkomplex 2) vollzogene Kehrtwende: Wenn dort selbst für den (im Vergleich zur Rasterfahndung weitaus belastenderen) verdeckten Eingriff in informationstechnische Systeme eine gewisse Verlagerung ins Gefahrenvorfeld gestattet wurde (siehe oben), ist es wenig verständlich, warum dies für die Rasterfahndung nicht gelten und diese weiter strikt an die Gefahrenschwelle gebunden sein soll.

- <u>Informationsübermittlung</u>

Zu Abs.5: Die „sonstigen öffentlichen Stellen“ werden durch die sodann aufgeführten zulässigen Übermittlungszwecke, die einen Rückschluss auf die Zuständigkeit und Eigenart der in Betracht kommenden Übermittlungsadressaten zulassen, m.E. hinreichend eingegrenzt.

Bayreuth, den 3.9.2008