Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
16(4)460C

Univ.-Prof. Dr. jur. Dirk Heckmann
Mitglied des Bayerischen Verfassungsgerichtshofs
Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht
Universität Passau
www.mein-jura.de heckmann@uni-passau.de

Gutachterliche Stellungnahme[*]

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

Vorbemerkung

Anlässlich der Sachverständigenanhörung vor dem Innenausschuss des Deutschen Bundestages am 15. September 2008 wurde ich gebeten, vorab eine schriftliche Stellungnahme einzureichen. Dem komme ich hiermit gerne nach. Ich möchte aber darauf hinweisen, dass die Erstellung eines umfassenden wissenschaftlichen Rechtsgutachtens zu allen Facetten des Gesetzentwurfes nicht möglich war. Im Wesentlichen beschränkt sich die Stellungnahme deshalb auf die nach der Arbeitsgruppe Inneres noch zu klärenden Fragestellungen.

Die Ausführungen beziehen sich ausschließlich auf die Beurteilung des verfassungsrechtlichen Gestaltungsrahmens für den Gesetzgeber, insbesondere in Folge der jüngsten Rechtsprechung des *BVerfG*. Auf eine rechtspolitische Bewertung wurde weitgehend verzichtet; vereinzelte Anmerkungen in dieser Hinsicht sind gekennzeichnet.

Passau, den 5. August 2008

[*] Unter Mitarbeit von *Dr. Frank Braun*, Geschäftsführer der Forschungsstelle für Rechtsfragen der Hochschul- und Verwaltungsmodernisierung an der Universität Passau (ReH..Mo).

Zusammenfassung der wesentlichen Ergebnisse

Die Eingriffsbefugnisse zur „Online-Durchsuchung“, Telekommunikationsüberwachung und zum Einsatz technischer Mittel in oder aus Wohnungen sind verfassungskonform ausgestaltet.

Der Entwurf berücksichtigt die Vorgaben der Rechtsprechung des Bundesverfassungsgerichts. Die geforderten hohen **Eingriffsschwellen** wurden gesetzt. Insbesondere ist es nicht erforderlich, beim verdeckten Eingriff in informationstechnische Systeme ebenso wie beim sog. Lauscheingriff eine dringende Gefahr festzuschreiben. Bedenken bestehen allenfalls bei der Maßnahme zur sog. Rasterfahndung. Das Regelbeispiel in § 20j Abs. 1 Satz 1, 2. Halbsatz BKAG-E bildet nach hier vertretener Ansicht die vom Bundesverfassungsgericht geforderte „konkrete Gefahr“ nicht in ausreichendem Maße ab. Im Übrigen ist es den Entwurfsverfassern gelungen, zur Gewährleistung der Inneren Sicherheit Maßnahmen zu regeln, die – trotz deren unbestrittener Eingriffsintensität – den verfassungsrechtlichen Anforderungen der Verhältnismäßigkeit und Normenbestimmtheit umfassend Rechnung tragen. Den gesetzestechnisch alles andere als einfach umzusetzenden Handlungsanweisungen des Bundesverfassungsgerichts an den Gesetzgeber wurde umfassend nachgekommen. In besonderem Maße anerkennenswert ist, dass die Entwurfsverfasser dabei eine Regelungslandschaft zu schaffen versucht haben, die - trotz der genannten Schwierigkeiten in der Umsetzung – eingängig und verständlich bleibt; dass dies im vorliegenden Kontext keine Selbstverständlichkeit ist, zeigt ein Blick auf die Landesgesetzgebung.

Der Kreis der **Eingriffsadressaten** ist bei Maßnahmen zur Online-Durchsuchung aber nicht in jeder Hinsicht zustimmungswürdig gefasst. So begegnet die Einbeziehung des Zustandsstörers (i.S.d. § 18 BundesPolG) in den Kreis der Maßnahmeadressaten verfassungsrechtlichen Bedenken. Soweit dagegen verfassungsrechtliche Einwände gegen die Einbeziehung sog. „Kontakt- und Begleitpersonen“ (im Rahmen von Maßnahmen nach § 20g BKAG-E) bzw. von „Nachrichtenmittlern“ (Maßnahmen nach § 20l BKAG-E) vorgebracht werden, greifen diese nach hier vertretener Auffassung nicht.

Der **Schutz des Kernbereichs privater Lebensgestaltung** wird in ausreichendem Maße gewährleistet, wobei bestimmte Formulierungen dabei quasi aus den Entscheidungen des Bundesverfassungsgerichts „abgeschrieben“ wurden (was legitim ist). Nach hier vertretener Ansicht ist ein „allgemeiner Kernbereichsschutz“ bei allen heimlichen Maßnahmen nicht erforderlich. Außerhalb des Schutzbereichs der Unverletzlichkeit der Wohnung, der Telekommunikationsfreiheit und der Vertraulichkeit und Integrität informationstechnischer Systeme, besteht keine derartige Vertraulichkeitserwartung in höchstpersönliche Handlungen und Äußerungen, die das Erfordernis gesetzlicher Schutzvorkehrungen vorzeichnen würden. Der Entwurf berücksichtigt bei der Online-Durchsuchung und der Telekommunikationsüberwachung das Erfordernis, den Kernbereichsschutz in zwei Stufen zu regeln (Erhebungsphase und Auswertungsphase). Der Kernbereichsschutz der ersten Stufe ist dabei insoweit nicht optimal ausgestaltet, als ein Erhebungsverbot nur dann besteht, wenn durch die Maßnahme *allein* Er-

kenntnisse aus dem Kernbereich gewonnen würden. Praktische Bedeutung haben die so formulierten Regelungen (wie ihr „Vorbild“ § 100a Abs. 4 StPO) kaum. Der Schutz zeugnisverweigerungsberechtigter Personen (wiederum in Anlehnung an Regelungen der StPO, hier § 160a StPO) ist dagegen eindeutig verfassungskonform ausgestaltet.

Der Entwurf enthält zudem durchgehend angemessene Regelungen zum gebotenen **Grundrechtsschutz durch Verfahren**. Soweit hierbei Einwände gegen die Eilfallkompetenzen oder die Ausgestaltung des Richtervorbehalts (Unbestimmtheit des Begriffs der Angabe der „wesentlichen Gründe“ bei der Anordnung von Maßnahmen nach § 20h und § 20k BKAG-E) vorgebracht werden, können diese nach hier vertretener Ansicht zerstreut werden. Was den Umfang der richterlichen Begründung der Maßnahmen betrifft, könnte allerdings (in Anbetracht mehrfacher kritischer Äußerungen des Bundesverfassungsgerichts zur mangelhaften richterlichen Kontrolle bei heimlichen Maßnahmen) „vorsorglich“ eine Präzisierung (nach dem Vorbild des § 100d Abs. 3 StPO) in Betracht gezogen werden. Vorbildlich ist der – insbesondere für die Zukunft an Bedeutung gewinnende – Grundrechtsschutz durch technische Verfahren in § 20k BKAG-E geregelt. Die Regelungen zur Verwendung und Übermittlung der Daten nach § 20v BKAG-E konnten im Rahmen der vorliegenden Stellungnahme nur kursorisch untersucht werden. Dabei erscheinen die Regelungen überarbeitungsbedürftig. Bei der gestatteten Datenübermittlung und Zweckänderung erscheint das Prinzip der „Rechtmäßigkeit des hypothetischen Ersatzeingriffes“ nicht durchgehend beachtet worden zu sein. Zudem wird eine explizite bereichsspezifische Regelung zur Datenübermittlung an ausländische Stellen für erforderlich gehalten. Ein Rückgriff auf die allgemeine Vorschrift des § 14 BKAG erscheint dagegen fragwürdig. Die ausdifferenzierten Regelungen zur Benachrichtigung Betroffener nach § 20k BKAG-E wurde nicht untersucht.

A. Eingriffsschwellen und Maßnahmerichtung

I. Eingriffsschwellen

1. Online-Durchsuchung

Die sog. Online-Durchsuchung, d.h. der Zugriff auf informationstechnische Systeme und die in ihnen gespeicherten Daten, soll dem Bundeskriminalamt ein Instrument zur Abwehr erheblicher Gefahren für hochrangige Rechtsgüter geben. Das in den letzten Jahren gestiegene Bedrohungspotenzial (insbesondere terroristische Bedrohungen) ist offenkundig. Die Wirksamkeit alternativer Maßnahmen zur Gefahrenabwehr (etwa die körperliche Inbesitznahme betreffender Rechner bzw. Speichermedien zur Auswertung der gespeicherten Daten) ist nicht in der Weise erwiesen, dass der verfassungsrechtliche Gestaltungsspielraum des Gesetzgebers die Online-Durchsuchung a priori ausschließen würde. Unter rein verfassungsrechtlichen Erwägungen (rechtspolitische oder staatsphilosophische Überlegungen bleiben außer Betracht) bestehen nur wenige Bedenken gegen den Gesetzentwurf.

Was die Online-Durchsuchung betrifft, ist diese in § 20k BKAG-E **verfassungskonform** umgesetzt. Soweit im Einzelfall Bedenken bestehen, wird im Folgenden explizit darauf hingewiesen. Der Entwurf berücksichtigt im Wesentlichen die Vorgaben des Bundesverfassungsgerichts. Heimliche Zugriffe auf IT-Systeme stellen erhebliche Grundrechtseingriffe dar, nämlich in das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“. Dieses Grundrecht ist aber - wie das Bundesverfassungsgericht betont - nicht schrankenlos gewährleistet, sondern unter bestimmten Eingriffsvoraussetzungen und Verfahrensvorkehrungen einschränkbar. Es ist die Aufgabe des Gesetzgebers, zur Erfüllung wesentlicher Aufgaben, wie eben die Gewährleistung der inneren Sicherheit, Maßnahmen zu regeln, die den besagten Grundrechtseingriff verfassungskonform ausgestalten. Um solche Maßnahmen handelt es sich bei § 20k BKAG-E.

Die mit der Online-Durchsuchung einhergehenden **Grundrechtseingriffe** lassen sich **verfassungsrechtlich rechtfertigen.** Die geforderten **hohen Eingriffsschwellen** wurden gesetzt. Die verfassungsrechtlichen Anforderungen an den Eingriffsanlass hat das *BVerfG* wie folgt zusammengefasst[1]: 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“.

[1] BVerfG ,Urt. v. 27.02.2008 - 1 BvR 370/07 LS 2 sowie Absatz-Nr. 242, 251.

Gerade die Präzisierung des letzten Satzes ist von besonderer Bedeutung. Klargestellt ist dadurch, dass nicht in jedem Fall eine konkrete Gefahr für ein überragend wichtiges Rechtsgut bestehen muss. Zulässig sind auch Maßnahmen im „Gefahrenvorfeld", soweit 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). Das *BVerfG* trägt damit dem Umstand Rechnung, dass der Einsatz einer Online-Durchsuchung häufig in Situationen 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, dass andererseits aber dennoch 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[2].

Legt man diese verfassungsrechtlichen Maßstäbe zugrunde, ist § 20k BKAG-E verfassungsrechtlich unbedenklich gefasst. Die Norm greift wortwörtlich (was legitim ist) die Formulierungen des Gerichts auf und schöpft damit die von der Verfassung vorgegebenen Spielräume aus (siehe § 20k Abs. 1 Satz 2 BKAG-E). Kritik hieran mag rechtspolitisch legitim sein (was vorliegend ausgeblendet wird), rechtsdogmatisch wäre sie nicht berechtigt. Der Gesetzgeber ist nicht angehalten – auch nicht bei intensivsten Grundrechtseingriffen – seine rechtssetzerischen Möglichkeiten nicht voll auszuschöpfen (und quasi einen „Sicherheitsabstand" zu halten).[3]

Soweit gefordert wird, die Gefahrenschwelle (vermeintlich) höher zu justieren und bei der Befugnis zum verdeckten Eingriff in informationstechnische Systeme ebenso wie beim sog. „Lauscheingriff" eine **dringende Gefahr** festzuschreiben, wird dies vorliegend für nicht erforderlich erachtet. Einerseits sind höhere Gefahrenschwellen – wie festgestellt - verfassungsrechtlich nicht geboten, andererseits entsprechen sich nach hier vertretener Auffassung die in Art. 13 Abs. 4 GG umschriebene „dringende Gefahr" und die vom *BVerfG* in seiner Entscheidung zur Online-Durchsuchung herausgearbeitete Gefahrenlage:

Art. 13 Abs. 4 GG verlangt als Eingriffsvoraussetzung eine „dringende Gefahr" für die öffentliche Sicherheit. Was unter einer dringenden Gefahr i.S.d. Art. 13 Abs. 4 GG genau zu verstehen ist, ist noch nicht bis ins letzte Detail geklärt[4]. Nach h.M. bezieht sich das Erfordernis der *„Dringlichkeit der Gefahr"* aber weniger auf die Wahrscheinlichkeit der Schadenskonkretisierung als auf den Schadensumfang[5]. Dies ergibt sich aus einem Vergleich mit der in Art. 13

[2] BVerfG ,Urt. v. 27.02.2008 - 1 BvR 370/07 Absatz-Nr. 242, 251.

[3] Einen anderen Weg wählte der bayerische Gesetzgeber, der mit der Regelung des Art. 34 d Abs. 1 Nr. 1 PAG-E eine „konkrete Gefahr" fordert und damit der hergebrachten Dogmatik des klassischen Polizeirechts verhaftet bleibt.

[4] BVerfGE 17, 232 (251 f.); *Papier*, in Maunz/Dürig, GG, Art. 13 Rn. 96, 129 ff.; *Gornig*, in: v. Mangoldt/Klein/Starck, GG, Art. 13 Rn. 124; *Hermes*, in: Dreier, GG, Art. 13 Rn. 78.

[5] *Braun*, NVwZ 2000, 375 (376 f. m.w.N.).

Abs. 4 Satz 1 GG ausdrücklich angeführten gemeinen Gefahr und der Lebensgefahr, anhand derer ein Wertungsgleichklang mit der als Oberbegriff genannten dringenden Gefahr für die öffentliche Sicherheit herzustellen ist[6]. Dies ist auch wegen der Weite des Begriffs „öffentliche Sicherheit" geboten und fordert der in dem Ausdruck „dringend" intendierte Verhältnismäßigkeitsgrundsatz[7]. Ein solches Verständnis legte auch der Gesetzgeber bei der Neufassung des Art. 13 Abs. 4 GG zu Grunde[8], so dass es sich um Gefahren handeln muss, aus denen Schäden für wichtige Rechtsgüter oder Schäden in besonders großem Ausmaß zu erwachsen drohen[9]. In zeitlicher Hinsicht bedeutet die Dringlichkeit der Gefahr nach „polizeirechtlicher Lesart" so viel wie unmittelbar bevorstehend. An diesem temporären Aspekt - also die Anforderungen an die Wahrscheinlichkeit des Schadenseintrittes - werden wegen der besonders hochrangigen geschützten Rechtsgüter aber regelmäßig **geringe Anforderungen** zu stellen sein[10]. Denn bei jeder anderen Interpretation wäre die Regelung in Art. 13 Abs. 4 GG sinnlos: Der Einsatz von Überwachungsmaßnahmen durch die Polizei etwa zur Abwehr unmittelbarer Lebensgefahren wäre i.d.R. ein völlig ungeeignetes Instrument[11]. Der Polizei wird vielmehr daran gelegen sein, die bei einer Maßnahme nach Art. 13 Abs. 4 GG gewonnenen Daten zur Verhinderung bevorstehender Verbrechen zu nutzen. Nach dieser praktischen Intention ist auch die „dringende Gefahr" in Art. 13 Abs. 4 GG auszulegen. Der verfassungsrechtliche Begriff der dringenden Gefahr ist insoweit nicht mit dem polizeirechtlichen Begriff der konkreten Gefahr gleichzusetzen[12]. Die Eigenständigkeit und grundsätzlich nicht fachrechtliche Determinierung verfassungsrechtlicher Begriffsverwendungen ist insoweit zu beachten[13]. Legt man diese Auffassung zu Grunde, besteht zwischen den Eingriffsschwellen in § 20h (Einsatz technischer Mittel in/aus Wohnungen) und § 20k („Online-Durchsuchung") bereits ein Gleichklang. Beide Maßnahmen sind nur zum Schutze höchstrangiger Rechtsgüter wie Leib, Leben oder Freiheit einer Person zulässig und dürfen nur ergriffen werden, wenn eine durch bestimmte Tatsachen erhärtete Prognose (zumindest eines personenbezogenen Gefahrenverdachts) auf eine Gefährdung dieser Rechtsgüter schließen lässt.

---

[6] *Braun*, NVwZ 2000, 375 (376 f.); *Herdegen*, in: BK, Art. 13 GG Rdnr. 42.

[7] *Götz*, JZ 1996, 669 (670); *Knemeyer/Keller,* SächsVBl 1996, 197 (201).

[8] BT-Dr 13/8650, S. 5.

[9] *BVerfGE* 17, 232 (252); *VGH München,* NVwZ 1991, 680 (690).

[10] So auch die Rspr., z.B. BVerwGE 62, 36 (39); anders aber SächsVerfGH, JZ 1996, 957 (968).

[11] *Benfer,* NVwZ 1999, 237, der in solchen Fällen ein Betreten oder Durchsuchen der betreffenden Wohnungen für wirkungsvoller hält.

[12] Anders aber SächsVerfGH, JZ 1996, 957 (968) sowie SächsVerfGH, JZ 1996, 957 (968).

[13] So *Möstl*, , LT-Drs. 15/10345 S. 79; schriftliche Stellungnahme zum bayerischen Polizeiaufgabengesetz – Online-Datenerhebung v. 27.05.2008.

2. Rasterfahndung

Das *BVerfG* sieht die präventive Rasterfahndung wegen ihrer besonderen Grundrechtsrelevanz an bestimmte Vorgaben gebunden. Der Gesetzgeber muss die mit der Rasterfahndung verbundenen Eingriffe beschränken. Auch bei der „Verfolgung fundamentaler Staatszwecke der Sicherheit und des Schutzes der Bevölkerung" ist der Staat an rechtsstaatliche Grundsätze gebunden[14]. Für die präventive Rasterfahndung als verdachtslosen Eingriff bedeut dies, dass der Gesetzgeber sie nicht ohne jedwede Einschränkungen der Polizei gestatten darf. Eine Möglichkeit, wie der Gesetzgeber diese Begrenzung herstellen kann, ist für das *BVerfG* das Tatbestandsmerkmal „Gefahr". Nur wenn eine konkrete Gefahr für hochrangige Rechtsgüter vorliegt, genügt eine präventive Rasterfahndung rechtstaatlichen Grundsätzen. Allerdings bedarf es zur Feststellung einer solchen konkreten Gefahr einer Wahrscheinlichkeitsprognose, die sich auf Tatsachen beziehen muss. „Vage Anhaltspunkte oder bloße Vermutungen ohne greifbaren, auf den Einzelfall bezogenen Anlass" reichen nicht aus[15]. Die Wahrscheinlichkeitsprognose darf sich also nicht nur auf die allgemeine außen- und sicherheitspolitische Lage und auf abstrakte Gefährdungsszenarien beziehen, sondern es sind vielmehr „hinreichend fundierte konkrete Tatsachen" für das Vorliegen einer Gefahr erforderlich. Demnach ist eine Rasterfahndung zur Gefahrenabwehr nur dann zulässig, wenn hinreichend fundierte konkrete Tatsachen das Bestehen einer konkreten Gefahr belegen.

Diesen Anforderungen wird die Regelung des § 20j Abs. 1 BKAG-E grundsätzlich gerecht. Allerdings ist **§ 20j Abs. 1 Satz 1, 2. HS BKAG-E nicht unproblematisch** gefasst. Dort wird der Fall einer konkreten Gefahr für hochrangige Rechtsgüter (§ 20j Abs. 1 Satz 1, 1. HS BKAG-E) mit der Konstellation gleichgestellt, dass „*konkrete Vorbereitungshandlungen die Annahme rechtfertigen, dass eine Straftat nach § 4a Abs. 1 Satz 2 begangen werden soll*." Nach hier vertretener Ansicht ist fraglich, ob diese Anwendungsalternative der Rasterfahndung den verfassungsgerichtlichen Vorgaben entspricht. Zwar bestehen hinsichtlich des Ranges der geschützten Rechtsgüter (hier die in § 4a BKAG-E i.V.m. § 129a StGB genannten) keine Bedenken. Allerdings kann bezweifelt werden, ob die Schwelle zu einer „konkreten Gefahr" überschritten wird.

Einerseits ist die Regelungsstruktur von einer typischen polizeilichen Gefahrenlage losgelöst. Es ist die Prognose der künftigen Begehung einer qualifizierten Straftat erforderlich (hier § 129a StGB), was – wie das *BVerfG* in seiner Entscheidung zur präventiven Telekommunikationswachung zutreffend festgestellt hat[16] – im präventiv-polizeilichen Bereich wegen der Schwierigkeit der Prognose der Begehung künftiger Straftaten nicht unproblematisch ist. Allerdings werden vorliegend immerhin konkrete Vorbereitungshandlungen für die vermeintliche Begehung der Straftat gefordert. Insoweit ist die Regelung nur scheinbar vom herkömmli-

[14] BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02 = NJW 2006, 1939 (1945).
[15] BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02 = NJW 2006, 1939 (1947).
[16] BVerfG, Urt. v. 27.07.2005 - 1 BvR 668/04 = BVerfGE 113, 348.

chen Gefahrenbegriff losgelöst. Inhaltlich besagt sie nichts anderes, als dass eine Rasterfahndung erfolgen kann, wenn aufgrund konkreter Vorbereitungshandlungen einer Straftat nach § 4a BKAG-E ein Schaden für die von dieser Norm geschützten hochrangigen Rechtsgüter zu erwarten ist. Diesbezüglich läge eine konkrete Gefahr vor. Richtet man allerdings den Blick auf die in § 4a BKAG-E verwiesene Norm des § 129a StGB, ist wohl eine andere Beurteilung angezeigt. Diese Regelung stellt die Bildung terroristischer Vereinigungen unter Strafe. Hierfür muss (verkürzt) eine Vereinigung gegründet werden, deren Tätigkeit auf die Begehung bestimmter schwerster Straftaten gerichtet ist. Dadurch wird eine „Unschärfe" erreicht, die die (einer konkreten Gefahr immanente) erforderliche Wahrscheinlichkeitsprognose eines möglichen Schadenseintrittes nicht mehr in hinreichendem Maße gestattet. Es müssen konkrete Vorbereitungshandlungen die Annahme rechtfertigen, dass jemand eine terroristische Vereinigung bildet bzw. sich als Mitglied beteiligt usw., deren Zweck die Begehung schwerster Straftaten ist, wobei die einzelnen Tatbestandsvoraussetzungen der Strafnormen nur als vage bezeichnet werden können[17]. Eine Prognose erscheint mit hinreichender Wahrscheinlichkeit kaum möglich (sollte sich die Prognose allein auf die Begehung der in § 129a StGB genannten Straftaten beziehen, läge indes eine konkrete Gefahr vor). Auch wenn das *BVerfG* in seiner Entscheidung zur Rasterfahndung klargestellt hat (worauf die Gesetzesbegründung verweist[18]), dass eine konkrete Gefahr auch eine Dauergefahr sein kann, bei der die hinreichende Wahrscheinlichkeit des Schadenseintritts über einen längeren Zeitraum hinweg zu jedem Zeitpunkt besteht[19], kann diese Aussage nicht als Rechtfertigung herangezogen werden. Denn das Gericht hat klargestellt, dass eine derartige Dauergefahr beispielsweise nur vorläge, „wenn tatsächliche Anhaltspunkte für die Vorbereitung terroristischer Anschläge oder dafür bestehen, dass sich in Deutschland Personen für Terroranschläge bereithalten, die in absehbarer Zeit in Deutschland selbst oder andernorts verübt werden sollen"[20]. Eine vergleichbare Konstellation ist vorliegend nicht gegeben, wenn lediglich tatsächliche Vorbereitungshandlungen auf eine Straftat nach § 129a StGB schließen lassen. Eine Streichung von § 20j Abs. 1 Satz 1, 2. HS BKAG-E sollte in Betracht gezogen werden.

---

[17] Treffend *Miebach/Schäfer*, in: Joecks/Miebach, Münchener Kommentar zum StGB, Bd. 2/2, 2005, § 129a Rn. 18: „Die Norm ist insgesamt fraglos noch komplexer, differenzierter und durch die Einfügung zahlreicher nur schwer eindeutig bestimmbarer Rechtsbegriffe vor allem in Abs. 2 sicherlich in der Praxis nicht einfacher handhabbar geworden. Daneben erreicht die Tatbestandsgestaltung des Abs. 2 n.F. und dabei insb. die auffällige Häufung jeweils für sich genommen bereits nur mühevoll eingrenzbarer unbestimmter Rechtsbegriffe den **Grenzbereich des hinsichtlich des verfassungsrechtlichen Bestimmtheitsgebots noch Zulässigen.** Dieser Umstand fällt umso stärker ins Gewicht, als die Norm Anknüpfungspunkt zahlreicher Ermittlungsmaßnahmen mit teilw. erheblicher Eingriffsintensität ist." [Hervorhebung im Original]; zur gebotenen einschränkenden Auslegung des Tatbestandes der Unterstützung einer terroristischen Vereinigung in der neueren Rechtsprechung des BGH, *Bader*, NStZ 2007, 618.

[18] BT-Drs. 16/9588 S. 69 [elektronische Vorabfassung].

[19] BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02 Absatz-Nr. 144 ff.

[20] BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02 Absatz-Nr. 144 ff.

II. Maßnahmerichtung

1. Online-Durchsuchung

§ 20k Abs. 4 BKAG erstreckt die Eingriffsbefugnis zur Online-Durchsuchung neben dem „Handlungsstörer“ (nach § 17 BundesPolG) auch auf den **Zustandsstörer** (Verweis auf § 18 BundesPolG). Dies ist **verfassungsrechtlich bedenklich**.

Das *BVerfG* geht davon aus, dass der Gefahrverdacht bereits auf einen bestimmten Kreis von Tatbeteiligten eingeengt sein muss, auf den sich die Überwachungsmaßnahme gezielt beziehen und auch weitgehend beschränken kann[21]. Insoweit hat der Zugriff auf den Handlungsstörer erste Priorität. Über die Frage, inwieweit sich heimliche Informationseingriffe auch gegen Nicht-*Tat*verdächtige richten dürfen, herrscht im Allgemeinen noch beträchtliche Unsicherheit[22]. Die Einbeziehung des Zustandsstörers als Maßnahmeadressat (in allgemeiner polizeirechtlicher Diktion) im Rahmen der Online-Durchsuchung erscheint indes kaum vertretbar; ein Verstoß gegen das verfassungsrechtliche Bestimmtheitsgebot liegt nahe. Denn wer ist Zustandsstörer im Rahmen einer Online-Durchsuchung? Die Gesetzesbegründung sagt dazu, „*dass die abzuwehrende Gefahr von der Sache, dem informationstechnischen System selbst, ausgehen muss*“. Nur: Welche Fallkonstellationen sind davon erfasst? Sind damit die Fälle gemeint, in denen gefährliche Informationen (etwa Bombenbaupläne) auf informationstechnischen Systemen Dritter – etwa Providern – (i.d.R. ohne deren Wissen) abgelegt sind? Dann geht aber die Gefahr nicht von dem informationstechnischem System (der Provider), sondern von deren Inhalt aus und es läge lediglich eine „Drittbetroffenheit“[23] bzw. eine Inanspruchnahme eines Nichtsstörers vor. Oder sind nur diejenigen Fälle gemeint, in denen die Gefahr tatsächlich nur von dem System selbst ausgeht, was (bei der Terrorismusbekämpfung) nur in seltenen Konstellationen – wie etwa der Bot-Netz-Kriminalität – der Fall sein kann? Jedenfalls ist durch die – wenig sinnvolle – Inbezugnahme der Zustandsstörerschaft nach § 18 BundesPolG das erforderliche Maß an Normenklarheit und Bestimmtheit nicht erreicht. Potentielle Eingriffsadressaten können einen möglichen (unverschuldeten) schweren Eingriff in ihre Grundrechte nicht vorhersehen. Eine gesetzliche Klarstellung ist erforderlich.

Dabei sei erwähnt, dass sich nach hier vertretener Auffassung Eingriffe im Rahmen einer Online-Durchsuchung nicht ausschließlich auf den (Handlungs-)Störer beschränken müssen. Eine allgemeine Regel, dass Informationseingriffe nur gegenüber dem Störer (dem Gefahrverursacher) zulässig sind, existiert nicht. Andererseits ist zu beachten, dass jede Drittbetroffenheit die Eingriffsintensität erhöht und dass die Maßnahme auch dem nicht selbst Tatverdächtigen gegenüber als zumutbar erscheinen muss. Den (hier freilich nicht verwendeten) Begriff der Kontakt- und Begleitperson hat das *BVerfG* für schwerwiegende Grundrechtsein-

[21] BVerfG, Urt. v. 27.02.2008 - Absatz-Nr. 251.
[22] Hierzu *Möstl*, DVBl. 2007, 581 (583).
[23] So *Baum/Schantz*, ZRP 2008, 137 (139).

griffe als zu unbestimmt verworfen und näher eingrenzende Tatbestandsmerkmale gefordert[24]. Unter der Voraussetzung einer hinreichenden Präzisierung wären aber entsprechende Regelungen denkbar.

2. „Kontakt- und Begleitpersonen" sowie „Nachrichtenmittler"

a) Im Rahmen des § 20g Abs. 1 Nr. 3 BKAG-E (besondere Mittel der Datenerhebung)

Im Rahmen des § 20g Abs. 1 Nr. 3 BKAG-E (Besondere Mittel der Datenerhebung) können auch sog. „Kontakt- oder Begleitpersonen" in Anspruch genommen werden. Der Begriff der Kontakt- und Begleitpersonen ist wiederum in § 20b Abs. 2 Nr. 2 BKAG-E legaldefiniert.

Vor dem Hintergrund der Entscheidung des *BVerfG*[25] zur Telekommunikationsüberwachung nach dem niedersächsischen Polizeigesetz werden teils Einwände gegen die Inanspruchnahme sog. Kontakt- und Begleitpersonen vorgebracht[26]. Das Gericht stellte fest, dass - soweit von der Überwachungsmaßnahme Dritte betroffen sind - *hinreichend sichere tatsächliche Anhaltspunkte für deren Beziehung zu dem Tatverdächtigen bestehen müssen*; allerdings seien (im Gegensatz zum repressiven Bereich) die praktischen Möglichkeiten, solche Anhaltspunkte zu ermitteln, im Hinblick auf *künftig lediglich erwartete Straftaten grundsätzlich schwächer*[27]. In Anbetracht dessen hielt das Gericht sodann eine Inanspruchnahme sog. *Kontakt und Begleitpersonen* nach dem niedersächsischen Polizeigesetz für verfassungswidrig. Der Begriff der „Kontakt und Begleitpersonen" sei nicht ausreichend bestimmt.

Diese Aussagen der Rechtsprechung des *BVerfG* sind nach hier vertretener Auffassung nicht auf die vorliegende Konstellation übertragbar. Zwar ist ebenfalls die schwierige Prognose zukünftiger Straftaten (i.S.d. § 4a Abs. 1 Satz 2 BKAG-E, vgl. § 20b Abs. 2 Nr. 1, 2 BKAG-E) zu treffen. Jedoch ist hier der Begriff der „Kontakt- und Begleitpersonen" in § 20b Abs. 2 Nr. 2 BKAG-E **wesentlich enger gefasst** als nach dem niedersächsischen Polizeigesetz. Während nach der niedersächsischen Regelung Personen umfasst waren, „die mit einer anderen Person, von der Tatsachen die Annahme rechtfertigen, dass diese eine Straftat von erheblicher Bedeutung begehen wird, in einer Weise in Verbindung stehen, die erwarten lässt, dass durch diese Hinweise über die angenommene Straftat gewonnen werden können" werden nach § 20b Abs. 2 Nr. 2 BKAG-E nur Personen betroffen, die von der Vorbereitung einer Straftat nach § 4a Abs. 1 Satz 2 BKAG-E Kenntnis haben, aus der Verwertung der Tat Vorteile ziehen oder deren sich der Gefahrverursacher zur Begehung einer Straftat bedienen könnte. Aufgrund dieser wesentlichen Einschränkungen ist die Inanspruchnahme der sog. Kontakt- oder Begleitpersonen im Rahmen des § 20b BKAG-E ausreichend bestimmt gefasst.

---

[24] BVerfG, Urt. v. 27.07.2005 - 1 BvR 668/04 = BVerfGE 113, 348 (380 f.).

[25] BVerfG, Urt. v. 27.07.2005 - 1 BvR 668/04.

[26] Vgl. „Auflistung der noch zu klärenden Fragestellungen" der Arbeitsgruppe Inneres v. 11.06.2008 in Bezugnahme auf *Baldus*, S. 1

[27] BVerfG, Urt. v. 27.07.2005 - 1 BvR 668/04 Absatz-Nr. 147.

b) Im Rahmen des § 20l Abs. 1 Nr. 3 und 4 BKAG-E (Telekommunikationsüberwachung)

Eine ähnliche Konstellation besteht im Rahmen der Telekommunikationsüberwachung nach § 20l Abs. 1 Nr. 3 und 4 BKAG-E. Dort wird hinsichtlich der genannten Maßnahmeadressaten nicht auf die allgemeine Vorschrift des § 20b Abs. 2 Nr. 2 BKAG-E abgestellt. Nach § 20l Abs. 1 Nr. 3 und 4 BKAG-E können sich Maßnahmen vielmehr auch gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Störer nach Abs. 1 Nr. 1 bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Störer ihren Telekommunikationsanschluss oder ihr Endgerät benutzt.

Diese Umschreibung der Eingriffsadressaten orientiert sich an den v.a. im Zusammenhang mit strafprozessualen Maßnahmen herkömmlich als **„Nachrichtenmittler“** bezeichneten Personenkreis, wie er in § 100a StPO definiert ist. Die Inanspruchnahme eines derartigen „Nachrichtenmittlers“ im Rahmen der (repressiven) Telekommunikationsüberwachung ist allgemein anerkannt und wurde vom *BVerfG* in mehreren Entscheidungen jedenfalls nicht beanstandet. Das Gericht hat dabei die Prognosevoraussetzungen („bestimmte Tatsachen“) geschärft; mit dem betroffenen Personenkreis hat es sich nicht näher auseinandergesetzt (bis auf die Berufsgruppe der Journalisten[28]). Zuletzt hat das *BVerfG* im „El Masri-Beschluss zur Person des Nachrichtenmittlers Stellung genommen.[29] Insoweit wird mit der Anlehnung an den Begriff des Nachrichtenmittlers an eine Definition angeknüpft, die in der Rechtsprechung bereits (wenn auch in einem anderen Kontext) beleuchtet wurde. Die Regelung in § 20l Abs. 1 Nr. 3 und 4 BKAG-E ist insoweit ausreichend bestimmbar. Es kann zumindest auf die Ausfüllung der Rechtsprechung und Literatur zum bisher vorwiegend strafprozessual geprägten Begriff des Nachrichtenmittlers zurückgegriffen werden, wenn auch einzugestehen ist, dass dieser bislang nur wenig greifbare Konturen erfahren hat[30].

Verfassungsrechtliche Bedenken müssten im Hinblick auf die Entscheidung des *BVerfG*[31] zum niedersächsischen Polizeigesetz nur dann erhoben werden, wenn vom Anwendungsbe-

---

[28] BVerfG, Urt. v. 12.03.2003 - 1 BvR 330/96 Absatz-Nr. 122. „Die Einordnung der Beschwerdeführer als Nachrichtenmittler steht mit Art. 5 Abs. 1 Satz 2 GG nicht im Widerspruch. Nicht ausreichend wäre insoweit allerdings allein der Umstand, dass die Betroffenen als Journalisten über die Beschuldigten recherchierten. Die journalistische Tätigkeit darf nicht zum Anlass genommen werden, Journalisten einem höheren Risiko auszusetzen als andere Grundrechtsträger, Objekt der Erhebung von Verbindungsdaten für Zwecke der Strafverfolgung Dritter zu werden. Insbesondere darf die Inanspruchnahme von Journalisten nicht allein auf den Erfahrungssatz gestützt werden, dass Journalisten auf Grund ihrer Recherchen häufig mehr über gesuchte Straftäter wissen als andere Bürger. Die Annahme eines Handelns als Nachrichtenmittler muss vielmehr auf konkrete Tatsachen gegründet sein, die den jeweiligen Fall betreffen. Über allgemeine Erfahrungssätze hinaus müssen bestimmte tatsächliche Anhaltspunkte der Kontaktaufnahme des betreffenden Journalisten zu den gesuchten Straftätern bestehen, die auch ausreichen würden, um entsprechende Maßnahmen gegen andere Personen anzuordnen …“

[29] BVerfG Urt. v. 30.04.2007 - 2 BvR 2151/06 Absatz-Nr. 19 f.

[30] Im Ergebnis bestehen so gut wie keine allgemein anerkannten Eingrenzungen auf einen bestimmten Personenkreis, vgl. umfassend *Sankol*, MMR 2008, 154 (155 f.).

[31] BVerfG, Urt. v. 27.07.2005 - 1 BvR 668/04 Absatz-Nr. 147.

reich der Norm auch Nachrichtenmittler der in § 20l Abs. 1 Nr. 2 genannten Personen erfasst würden. Denn in diesem Falle wäre die Regelung aufgrund der Anknüpfung an künftig lediglich zu erwartende Straftaten als zu unbestimmt zu bewerten. Dies haben die Entwurfsverfasser erkannt und eine Inanspruchnahme des sog. Nachrichtenmittlers auf die Beziehung zum Störer nach § 20l Abs. 1 Nr. 1 BKAG-E beschränkt. Diese begegnet dann keinen verfassungsrechtlichen Bedenken. Mit der Anforderung einer „dringenden Gefahr“ für hochrangige Rechtsgüter ist die anzustellende polizeiliche Prognose in ausreichendem Maße determiniert.

B. Kernbereichsschutz

I. Allgemeine Fragen zum Kernbereichsschutz

1. Reichweite des Kernbereichsschutzes im präventiven Bereich?

Wie der **Schutzbereich** des absolut geschützten Kernbereichs privater Lebensgestaltung zu gewährleisten ist, lässt sich nach den Ausführungen des *BVerfG* nur grob umreißen. Der absolut zu schützende Kernbereich privater Lebensgestaltung wird im Wesentlichen durch den jeweiligen **Gesprächsinhalt** bestimmt, der prognostisch[32] zu ermitteln ist. Als Indikatoren für einen möglichen Kernbereichsbezug sollen bei der erforderlichen Wahrscheinlichkeitsprüfung in typisierender Weise teils der Ort des Gesprächs (Privatwohnung oder Geschäftsraum)[33] und insbesondere die potentiellen Gesprächspartner (Familienangehörige oder sonstige engste Vertraute) nutzbar gemacht werden. Allerdings besteht **kein Schutz**, soweit Gespräche betroffen sind, die Angaben über begangene Straftaten enthalten[34]. Dieser „Ausnahmetatbestand" ist im Anwendungsbereich von Art. 13 Abs. 4 GG dahingehend zu erweitern, als dass es sich um Gespräche handeln muss, die Angaben über dringende Gefahren für die öffentliche Sicherheit i.S.d. Art. 13 Abs. 4 GG enthalten. Im präventiv-polizeilichen Bereich erscheint es allgemein **geboten, dass auch Gespräche mit Kernbereichsbezug abgehört werden dürfen, wenn zu erwarten ist, dass Informationen zur Abwehr von Gefahren für Würde und Leben Dritter gewonnen werden können**. Das bedeutet prinzipiell, dass auch dann abgehört werden darf, wenn nach typisierender Betrachtungsweise ein Kernbereichsbezug besteht, jedoch aufgrund *konkreter* Anhaltspunkte (also strenge Anforderungen im Rahmen der vorgängigen Prognose) zu vermuten ist, dass in dem betreffenden Gespräch Angaben über Gefährdungen von Würde und Leben Dritter gemacht werden[35].

Diese Auslegung erhält in der Literatur zunehmend Konturen[36]. Dezidiert anderer Auffassung bleibt aber ein Teil des Schrifttums - insbesondere *Kutscha* und *Roggan* – auch in Illustration prekärer Fälle, wie der Entführung Jakob von Metzlers[37]. Nach deren Ansicht hätte die Wohnung des der Entführung Verdächtigen, in der er sich gewöhnlich mit seiner Freundin aufhielt,

---

[32] „Der Schutz des Kernbereichs privater Lebensgestaltung fordert, dass vor Maßnahmen akustischer Wohnraumüberwachung tatsächliche Anhaltspunkte gegeben sind, aus denen zumindest in typisierender Weise geschlossen werden kann, dass das Gespräch nicht den Bereich des Höchstpersönlichen betrifft. Die Ermittlungsmaßnahme muss dort unterbleiben, wo das Abhören des nichtöffentlich gesprochenen Wortes in Wohnungen mit Wahrscheinlichkeit zu einer Kernbereichsverletzung führen wird", BVerfG, Urt. v. 03.03.2004 - 1 BvR 2378/98 = NJW 2004, 999 (1004); vgl. *Kötter*, DÖV 2005, 225, (227, 229).

[33] BVerfG, Urt. v. 03.03.2004 - 1 BvR 2378/98 = NJW 2004, 999 (1004).

[34] BVerfG, Urt. v. 03.03.2004 - 1 BvR 2378/98 = NJW 2004, 999 (1003).

[35] Vgl. *Zippelius/Würtenberger*, Deutsches Staatsrecht, § 28 II 2c, bb mit Hinweis auf die dann gebotenen Lösungspflichten und Verwertungsgebote.

[36] Seit jeher *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, 6. Aufl. 2005, Rn. 622 ff. und zuletzt mit ausholender und überzeugender Argumentation *Baldus*, JZ 2008, 218 (255 ff.).

[37] *Kutscha/Roggan,* Große Lauschangriffe im Polizeirecht, in: Roggan (Hrsg.), Lauschen im Rechtsstaat GS Lisken, 2004, S. 32 ff.

nicht überwacht werden dürfen, obwohl die Polizei davon ausgehen musste, dass das Kind an einem unbekannten Ort festgehalten wurde und in Lebensgefahr schwebte.

Generell müssen Überwachungsmaßnahmen in Situationen von vornherein unterbleiben, in denen Anhaltspunkte bestehen, dass die Menschenwürde durch die Maßnahme verletzt wird[38]. Dieser Forderung kann nur mittels einer entsprechenden gesetzlichen Absicherung im Tatbestand der eingriffseröffnenden Norm nachgekommen werden. Wie sich aus den geschilderten Anforderungen des *BVerfG* ergibt, kann dies mittels einer typisierten Prognose eines möglichen Kernbereichsbezugs bewerkstelligt werden. Dass auch bei rechtmäßiger Anwendung derart ausgestalteter Eingriffsbefugnisse Kernbereichsverletzungen möglich sind (etwa bei unvorhersehbar unzutreffender Prognose des Rechtsanwenders), liegt in der Natur der Sache. Hier kann gebotener Schutz nur nachträglich erfolgen, nämlich durch **Abbruch der Aufzeichnungen**, deren **Löschung** bzw. einem obligatorischen **Verwendungsverbot**[39]. Dies muss mittels flankierender gesetzlicher Regelungen gewährleistet werden.

2. Sind kernbereichsschützende Regelungen bei allen heimlichen Maßnahmen erforderlich?

In der Literatur wird teils für alle heimlichen Überwachungsmaßnahmen eine „kernbereichsschützende Generalklausel" gefordert[40]. Dem ist etwa der brandenburgische Gesetzgeber nachgekommen, der – unabhängig von der Überwachungsmaßnahme – eine Datenerhebung für unzulässig erklärt, wenn dadurch in den Kernbereich privater Lebensgestaltung eingegriffen wird (§ 29 Abs. 6 BbgPolG).

Nach hier vertretener Ansicht sind entsprechende ausdrückliche gesetzliche Schutzvorkehrungen verfassungsrechtlich nicht geboten; eine entsprechende Einschränkung des § 20g BKAG-E ist nicht erforderlich. Denn es kommt weniger auf die Art der Datenerhebung (Heimlichkeit) an, ob der Kernbereich privater Lebensgestaltung berührt wird, sondern auf die typischerweise zu erwartenden Informationen und die Sphäre aus der diese erhoben werden. Dass im Rahmen einer Online-Durchsuchung, einer Wohnraumüberwachung und einer Telekommunikationsüberwachung typischerweise auch kernbereichsrelevante Inhalte erhoben werden können, liegt auf der Hand. Hier hat der betroffene Bürger eine **Vertraulichkeitserwartung** (aufgrund der Räumlichkeit, in der er sich befindet bzw. aufgrund des spezifischen Kommunikationsmittels), die das Erfordernis gesetzlicher Schutzvorkehrungen vorzeichnet. Dass das *BVerfG* dieser „Vertraulichkeitserwartung" entscheidendes Gewicht beimisst, zeigt seine Entscheidung zur präventiven Telekommunikationsüberwachung. Hier hat das Gericht (im Vergleich zur Wohnraumüberwachung) geringere Maststäbe an den zu gewährleistenden

[38] BVerfG, Urt. v. 03.03.2004 - 1 BvR 2378/98 = NJW 2004, 999 (1003).

[39] BVerfG, Urt. v. 03.03.2004 - 1 BvR 2378/98 = NJW 2004, 999 (1003); *Kötter*, DÖV 2005, 225 (230); *Zippelius/Würtenberger*, Deutsches Staatsrecht, § 29 II 2c, bb.

[40] So zuletzt *Baldus*, JZ 2008, 218 (221); *Denninger* ZRP 2004, 101 (104); *Roggan*, NJ 2007, 199.

Kernbereichsschutz angelegt, da ein Telefonkontakt wegen der Entfernung der Kommunizierenden voneinander und der Einbindung der Diensteanbieter als Kommunikationsmittler keinen mit der Wohnung als „letzten Rückzugsbereich“ vergleichbaren Rahmen für den Austausch höchstpersönlicher Informationen bietet[41]. Greift nun aber eine Überwachung regelmäßig Informationen auf, die der **„Sozialsphäre“** zuzurechnen sind (wie etwa bei einer Observation), sind gesetzliche Schutzvorkehrungen nicht erforderlich. Es besteht keine schützenswerte Vertrauensposition. Freilich können Situationen des „höchstpersönlichen Erlebens“ vereinzelt auch im Rahmen von Überwachungsmaßnahmen nach § 20g BKAG-E den ermittelnden Polizeibeamten zur Kenntnis gelangen (etwa beim Abhören des gesprochenen Wortes in Fahrzeugen). Allerdings sind bei diesen Maßnahmen Informationen mit Kernbereichsbezug nicht typischer Weise zu erwarten. Aus der Tatsache, dass gesetzliche Schutzvorkehrungen nicht erforderlich sind, folgt auch nicht, dass kein Kernbereichsschutz besteht. Ein solcher kommt vielmehr in angemessener Form zur Geltung, wenn es um die Verwertung kernbereichsrelevanter Informationen im Strafprozess geht. Für diese Fälle können nach der Rechtsprechung des *BVerfG* und des *BGH* auch unmittelbare Beweisverwertungsverbote aus Art. 1 Abs. 1 GG gefolgert werden[42]. Spezifische einfachgesetzliche Schutzvorkehrungen werden in der Rechtsprechung indes nicht gefordert.

II. Kernbereichsschutz bei Online-Durchsuchung (und Telekommunikationsüberwachung)

1. Zwei-stufiges Schutzkonzept

In seiner Entscheidung zur **Online-Durchsuchung** hat das *BVerfG* ein zweistufiges Schutzkonzept zur Gewährleistung des absolut geschützten Kernbereichs privater Lebensgestaltung entwickelt.

Die gesetzliche Regelung hat darauf hinzuwirken, dass die Erhebung kernbereichsrelevanter Daten soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt; insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen[43]. Gibt es im Einzelfall konkrete Anhaltspunkte dafür, dass eine bestimmte Datenerhebung den Kernbereich privater Lebensgestaltung berühren wird, so hat sie grundsätzlich zu unterbleiben[44]. Anders liegt es, wenn zum Beispiel konkrete Anhaltspunkte dafür bestehen, dass kernbereichsbezogene Kommunikationsinhalte mit Inhalten verknüpft werden, die dem Ermittlungsziel unterfallen, um eine Überwachung zu verhindern[45] (**1. Stufe**).

---

[41] BVerfG, Urt. v. 27.07.2005 – 1 BvR 668/04 Absatz-Nr. 164 ff.

[42] Siehe BVerfGE 35, 202 (220); 34, 238 (245); BGHSt 19, 325 (329); 31, 296 (299); BGHZ 73, 120 (122 ff.).

[43] BVerfG, Urt. v. 27.02.2008 - 1 BvR 370/07 Absatz-Nr. 281, sowie zur Telekommunikationsüberwachung BVerfGE 113, 348 (391 f.); zur akustischen Wohnraumüberwachung BVerfGE 109, 279,(318, 324).

[44] BVerfG, Urt. v. 27.02.2008 - 1 BvR 370/07 Absatz-Nr. 281.

[45] BVerfG, Urt. v. 27.02.2008 - 1 BvR 370/07 Absatz-Nr. 281.

Ist es praktisch unvermeidbar, Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann, muss das Gesetz für hinreichenden Schutz in der Auswertungsphase sorgen[46]. Ergibt die Durchsicht, dass kernbereichsrelevante Daten erhoben wurden, sind diese unverzüglich zu löschen[47]. Eine Weitergabe oder Verwertung ist auszuschließen[48] (**2. Stufe**).

Im Ergebnis die gleichen Anforderungen gelten bei Maßnahmen zur **Telekommunikationsüberwachung**. Auch hier hat das *BVerfG* einen gesetzlichen Schutz des Kernbereichs der privaten Lebensgestaltung in erster Linie für die sog. Auswertungsphase für erforderlich gehalten[49].

a) 1. Stufe

Der Kernbereichsschutz der **„1. Stufe“** ist nach hier vertretener Ansicht (sowohl bei der sog. Online-Durchsuchung, § 20k Abs. 7 Satz 1 BKAG-E als auch im Rahmen der Telekommunikationsüberwachung, § 20l Abs. 6 Satz 1 BKAG-E) **nicht optimal ausgestaltet**. Nach diesen Regelungen – die sich offensichtlich an strafprozessualen Regelungen wie § 100a Abs. 4 StPO orientieren – besteht ein Erhebungsverbot, wenn durch die Maßnahme *allein* Erkenntnisse aus dem Kernbereich gewonnen würden. Praktische Bedeutung hat die so formulierte Regelung nicht. Im Rahmen einer Telekommunikationsüberwachung (und schon gar nicht bei einer Online-Durchsuchung) sind kaum jemals Fallgestaltungen denkbar, in denen schon zum Zeitpunkt der Anordnung der Maßnahme feststeht, dass ausschließlich und von vornherein nur (nicht verwertbare) Erkenntnisse aus dem Kernbereich privater Lebensgestaltung zu erwarten sind. Zwar könnte man eine derartige Situation bei absolut geschützten Gesprächen mit bestimmten Berufsgeheimnisträgern (z.B. den Ermittlungsbehörden ist bekannt, dass der Verdächtige ein Gespräch mit seinem Verteidiger führen wird) annehmen und – in extensiver Interpretation – im Rahmen der Online-Durchsuchung, wenn auf einen beruflich genutzten Rechner eines entsprechenden Berufsgeheimnisträger zugegriffen werden soll. Allerdings wäre auf diese Situationen die Regelung des § 20k Abs. 7 Satz 1 BKAG-E bzw. § 20l Abs. 6 Satz 1 BKAG-E schon nicht anwendbar. Hier würde vielmehr der (absolute) Schutz des § 20u Abs. 1 BKAG-E greifen. Die Regelungen haben keinen eigenständigen Anwendungsbereich. Allenfalls für § 20l Abs. 6 Satz 1 BKAG-E ließe sich nach der Gesetzesbegründung der „Schwestervorschrift“ in § 100a Abs. 4 StPO ein Anwendungsbeispiel konstruieren[50]: Kommunikation mit der Telefonseelsorge, die nicht von Geistlichen i.S.d. § 53 Abs. 1 Nr. 1 StPO, sondern von besonders geschulten Mitarbeitern im Auftrag der Kirchen durchgeführt wird.

[46] BVerfG, Urt. v. 27.02.2008 - 1 BvR 370/07 Absatz-Nr. 282.
[47] BVerfG, Urt. v. 27.02.2008 - 1 BvR 370/07 Absatz-Nr. 283.
[48] Diesbezüglich genauer BVerfG 109, 279 (324) [Lauschangriff] und BVerfG 113, 348 (392) [Niedersachsen PolG].
[49] BVerfGE 113, 348 (391 f.).
[50] BT-Drs. 16/5846 S. 45.

Praktische Bedeutung hat diese Konstellation freilich keine. Die Regelungen sind weitestgehend untauglich[51], eine Änderung wird empfohlen.

Hierbei könnte man sich – die Online-Durchsuchung betreffend – am Wortlaut der Entscheidung vom 27.02.2008 orientieren[52]. Hinsichtlich der Telekommunikationsüberwachung hält *Gusy* mit überzeugender Argumentation einen spezifischen Kernbereichsschutz der „1. Stufe" gar für entbehrlich[53].

b) 2. Stufe (Auswertungsphase)

Auch den Schutzanforderungen der 2. Stufe wird entsprochen. Zur Gewährleistung eines hinreichenden Kernbereichsschutzes in der **Auswertungsphase** müssen nach der Rechtsprechung des *BVerfG* kernbereichsrelevante Daten unverzüglich gelöscht werden; eine Weitergabe oder Verwertung der Daten ist gesetzlich auszuschließen[54]. Regelungen, die dies sicherstellen, finden sich in § 20k und § 20l BKAG-E in ausreichendem Maße.

Soweit im Rahmen der Online-Durchsuchung die Auswertung der erhobenen Daten ausschließlich von zwei Beamten des Bundeskriminalamts auf kernbereichsrelevante Inhalte untersucht wird (§ 20k Abs. 7 Satz 3 BKAG-E), wird dagegen vereinzelt der Einwand entgegengebracht, die Einbindung weisungsgebundener Beamter gewährleiste nicht ausreichend die Interessen des Betroffenen; vielmehr müsse die Überprüfung von einer unabhängigen Instanz (Richter) durchgeführt werden[55]. Tatsächlich sprechen aus rechtspolitischer Sicht gute Gründe für eine Einbeziehung einer „unabhängigen" Instanz. Verfassungsrechtlich zwingend ist dies allerdings nach hier vertretener Ansicht nicht. Denn einerseits besteht nach § 20k Abs. 7 Satz 4 BKAG-E ohnehin eine Vorlagepflicht an das zuständige Gericht, soweit die auswertenden Beamten Zweifel daran haben, ob Daten dem Kernbereich privater Lebensgestaltung zuzuordnen sind oder nicht. Dass insoweit ein gewisser Beurteilungsspielraum zugunsten der auswertenden Beamten besteht („wann bestehen Zweifel, wann nicht?"), schadet indes nicht. Für eine vergleichbare Regelung im Bereich der repressiven Wohnraumüberwachung (§ 100a Abs. 6 StPO) hat das *BVerfG* festgestellt, dass es nicht zu beanstanden ist, wenn der Staatsanwaltschaft ein Beurteilungsspielraum dahingehend eingeräumt wird, ob ein Verwertungs-

[51] Vgl. auch die Kritik von *Nöding*, StraFo 2007, 456 (458) und *Puschke/Singelnstein*, NJW 2008, 113 (114) jeweils zu § 100a Abs. 4 StPO.

[52] So etwa der bayerische Gesetzgeber in Art. 34d Abs. 1 Satz 5 und 6 PAG: „Soweit dies informationstechnisch und ermittlungstechnisch möglich ist, hat die Polizei durch geeignete Vorkehrungen sicherzustellen, dass die Erhebung von Daten unterbleibt, die dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind. Wird erkennbar, dass solche Daten betroffen sind und bestehen keine Anhaltspunkte dafür, dass diese Daten dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen, ist die Maßnahme insoweit unzulässig."

[53] *Gusy*, NdsVBl. 2006, 65 (69).

[54] BVerfG Urt. v. 27.02.2008 - 1 BvR 370/07 Absatz-Nr. 284..

[55] Vgl. „Auflistung der noch zu klärenden Fragestellungen" der Arbeitsgruppe Inneres v. 11.06.2008 in Bezugnahme auf *Wiefelspütz* und *Giesler*, S. 7.

verbot in Betracht kommt[56]: Der Staatsanwaltschaft könne es aufgrund eigener Kompetenz anvertraut werden, selbst zu entscheiden, ob ein Verwertungsverbot überhaupt in Betracht kommt. Allein die Möglichkeit, dass die Staatsanwaltschaft die Grenze ihres Beurteilungsspielraums überschreiten könnte, führt nicht zur Verfassungswidrigkeit der Vorschrift (des § 100d Abs. 6 StPO). Der Gesetzgeber dürfe jedenfalls davon ausgehen, dass die Staatsanwaltschaft gerade auch mit Blick auf den Grundrechtsschutz in verantwortungsvoller Weise mit ihrem Beurteilungsspielraum umgehen wird.

Nachdem keinerlei vernünftige Gründe ersichtlich sind, warum Beamte des Bundeskriminalamts (mit Befähigung zum Richteramt) weniger vertrauenswürdig und verantwortungsvoll sein sollten als Exekutivbeamte der Staatsanwaltschaft, bestehen nach hier vertretener Ansicht keine verfassungsrechtlichen Bedenken gegen die Regelung in § 20k Abs. 7 Satz 1 BKAG-E.

2. Schutz zeugnisverweigerungsberechtigter Personen, § 20u BKAG-E

a) Allgemeines zur Regelung

Die Vorschrift des § 20u BKAG-E enthält nach dem Vorbild des § 160a StPO ein harmonisiertes System zur Berücksichtigung der Interessen der zeugnisverweigerungsberechtigten Berufsgeheimnisträger nach §§ 53 f. StPO und trägt dem obligatorischen Kernbereichsschutz nach der Rechtsprechung des *BVerfG* ausreichend Rechnung. Die Vorschrift des § 20u BKAG-E soll übergreifend für alle Überwachungsmaßnahmen des Unterabschnittes 3a des BKA-Gesetzes gelten. Insoweit finden die „allgemeinen" Vorschriften zum Schutz des Kernbereichs privater Lebensgestaltung (etwa in § 20k Abs. 7 oder § 20l Abs. 6 BKAG-E) keine Anwendung, wenn ein besonders geschütztes Vertrauensverhältnis i.S.d. §§ 53 f. StPO betroffen ist.

b) Differenzierender Schutz von Berufsgeheimnisträgern nach § 20u Abs. 1 und 2 BKAG-E

Was das erforderliche Schutzniveau betrifft, differenziert die Regelung zwischen den in § 53 Abs. 1 Nr. 1, 2 und 4 StPO (Geistliche, Verteidiger und Abgeordnete) genannten Berufsgeheimnisträgern und den sonstigen zeugnisverweigerungsberechtigten Personen nach § 53 Abs. 1 Satz 1 Nr. 3 bis 3b und 5 StPO (insbesondere Rechtsanwälte und Presseangehörige). Für erstere gewährt die Regelung einen **absoluten Schutz** (unter dem Vorbehalt der Gefahrenverursachung nach Abs. 4 der Regelung). Die Vertraulichkeit der Kommunikation mit Geistlichen, dem Verteidiger und Abgeordneten ist umfassend geschützt; es besteht ein absolutes Erhebungs- und Verwertungsverbot. Den in § 20u Abs. 2 BKAG genannten Personen kommt hingegen nur ein **relativer Schutz** zu. Das Schutzniveau wird von Verhältnismäßigkeitserwägungen im Einzelfall abhängig gemacht.

[56] BVerfG, Beschl. v. 11.05.2007 – 2 BvR 543/06 = NJW 2007, 2753 (2757) [Neuregelung der akustischen Wohnraumüberwachung].

Die Regelung des § 20u BKAG-E ist verfassungskonform ausgestaltet. Die Differenzierung zwischen einzelnen Berufsgeheimnisträgern ist nicht zu beanstanden. Aus Sicht des erforderlichen Kernbereichsschutzes hält die Regelung den Anforderungen des *BVerfG* stand. Der Kreis der nach der Rechtsprechung des *BVerfG* besonders geschützten Vertrauenspersonen deckt sich nur teilweise mit den in §§ 52 und 53 StPO genannten Zeugnisverweigerungsberechtigten. Die aus dem Kernbereich privater Lebensgestaltung folgenden Abhörverbote sind nicht identisch mit den strafprozessualen Zeugnisverweigerungsrechten[57]. Als vom Schutzbereich des Art. 1 Abs. 1 GG erfasst, sieht das *BVerfG* aber seelsorgerische Gespräche mit Geistlichen sowie Gespräche mit dem Strafverteidiger und Arztgespräche an[58]: „So gehört der Schutz der Beichte oder der Gespräche mit Beichtcharakter zum verfassungsrechtlichen Menschenwürdegehalt der Religionsausübung im Sinne des Art. 4 Abs. 1 und 2 GG. Auch dem Gespräch mit dem Strafverteidiger kommt die zur Wahrung der Menschenwürde wichtige Funktion zu, darauf hinwirken zu können, dass der Beschuldigte nicht zum bloßen Objekt im Strafverfahren wird. Arztgespräche können im Einzelfall ebenso dem unantastbaren Kernbereich privater Lebensgestaltung zuzuordnen sein“[59]. Diesem Schutzauftrag wird die Regelung allenthalben gerecht.

c) Verstrickungsregelung des § 20u Abs. 4 BKAG-E

Die Verstrickungsregelung in § 20u Abs. 4 BKAG-E, wonach der Schutz der Abs. 1 bis 3 suspendiert wird, wenn eine zeugnisverweigerungsberechtigte Person für die Gefahr verantwortlich ist, begegnet keinen verfassungsrechtlichen Bedenken. In diesen Fällen besteht kein verfassungsrechtlicher Schutz[60]. Es sei aber darauf hingewiesen, dass die Vorschrift nur so gelesen werden kann, dass die Anhaltspunkte für eine Störerschaft schon vor Ergreifen der Überwachungsmaßnahme bestehen müssen. Es darf nicht in den Kernbereich privater Lebensgestaltung eingegriffen werden, um erst festzustellen, ob die Informationserhebung diesen Bereich betrifft[61]. Sollte dies geschehen, bestünde nach der Rechtsprechung des *BVerfG* ein absolutes Verwertungsverbot[62].

d) Exkurs zu § 20c BKAG-E (allgemeine Befragung und Auskunftspflicht)

In § 20c BKAG-E ist die Befragung durch das Bundeskriminalamt nach dem Muster der allgemeinen Polizeigesetze der Länder geregelt. Danach besteht (über die Verpflichtung, die Personalien anzugeben, hinaus) eine weitergehende Auskunftspflicht (Angaben in der Sache) bei den in §§ 17 und 18 bzw. § 20 Abs. 1 Bundespolizeigesetz genannten Personen (Störer und Notstandspflichtiger) sowie im Falle des Bestehens gesetzlicher Handlungspflichten. Nach § 20c Abs. 3 BKAG-E sind allerdings unter den Voraussetzungen der §§ 52 bis 55 StPO

[57] BVerfG, Urt. v. 03.03.2004 - 1 BvR 2378/98 = NJW 2004, 999 (1004).
[58] BVerfG, Urt. v. 03.03.2004 - 1 BvR 2378/98 = NJW 2004, 999 (1004).
[59] Vgl. dazu auch BVerfGE 32, 373 (379).
[60] Vgl. oben B.I.1.
[61] BVerfG, Urt. v. 03.03.2004 - 1 BvR 2378/98 = NJW 2004, 999 (1004).
[62] BVerfG, Urt. v. 03.03.2004 - 1 BvR 2378/98 = NJW 2004, 999 (1007).

die Betroffenen zur Auskunftsverweigerung berechtigt. Dies gilt jedoch nicht, „*wenn die Auskunft zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person erforderlich ist*“. Diese Regelung ist nach hier vertretener Auffassung verfassungsrechtlich nicht unbedenklich und für die Praxis auch wenig zielführend. Dem Fragerecht der Polizei entspricht grundsätzlich nur eine Anhörungspflicht des Bürgers. Entfernt er sich verfrüht, darf er angehalten werden (notfalls mittels unmittelbaren Zwang). Soweit dann eine Antwortpflicht besteht, also in den Fällen des § 20b Abs. 2 BKAG-E, ist eine zwangsweise Durchsetzung kaum möglich. Unmittelbarer Zwang zur Abgabe einer Erklärung scheidet stets aus[63]. Ob eine Auskunft mittels eines Zwangsgeldes erzwungen werden darf, ist dagegen umstritten[64]. Schon angesichts dieser beschränkten Möglichkeiten zur Durchsetzung der Verpflichtung, erscheint die Einschränkung der Zeugnisverweigerungsrechte in § 20c Abs. 3 BKAG-E als verfehlt. Alles in allem beruht die gesetzliche Regelung der Sachauskunft ohnehin auf der vielfach bestätigten Erwartung einer weitgehend freiwilligen Mitwirkung des Bürgers. Dies ist sinnvoll, da der Ertrag erzwungener Aussagen ohnehin gering zu veranschlagen ist. Eine Streichung des betreffenden Passus in § 20c Abs. 3 BKAG-E sollte insoweit in Erwägung gezogen werden.

[63] *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, 6. Aufl. 2005 Rn. 584 m.w.N.

[64] Dafür etwa *Heckmann*, VBl.BW 1992, 164 (171) sowie *Drews/Wacke/Vogel/Martens*, Gefahrenabwehr, 9. Aufl. 1987, S. 194 Fn. 70 wonach das Gebot des fair trial nur körperliche Gewalt, aber nicht ein Zwangsgeld zur Herbeiführung der Aussage ausschließt.

C. Grundrechtsschutz durch Verfahren

I. Effektiver Richtervorbehalt: Anforderungen an die Begründung der Anordnung von „Lauscheingriff“ und Online-Durchsuchung

In seiner Entscheidung zur Online-Durchsuchung hat das *BVerfG* noch einmal betont, dass der Richter die Rechtmäßigkeit der vorgesehenen Maßnahme eingehend prüfen und die Gründe schriftlich festhalten müsse.[65] Hinsichtlich der konkreten Anforderungen an die richterliche Anordnung verwies das Gericht auf seine Entscheidung zur akustischen Wohnraumüberwachung.[66] Danach muss das Gericht durch die Begründung der Anordnung u.a. dafür Sorge tragen, dass die Interessen der Betroffenen gewahrt werden und eine angemessene Begrenzung der Maßnahme sichergestellt ist. Aus Gründen effektiven Rechtsschutzes muss sich die Begründung auf sämtliche materiellen und prozessualen Voraussetzungen beziehen. Aus ihr muss sich die konkrete Gefahrenlage ergeben und es muss erkennbar werden, dass eine Abwägung auf Grund der im Einzelfall relevanten Umstände stattgefunden hat[67]. Diese Anforderungen an die richterliche Begründung werden in den Regelungen der § 20h Abs. 4 Nr. 3 und § 20k Abs. 6 Nr. 4 BKAG-E zumindest nicht explizit abgebildet. Es wird lediglich gefordert, dass in der schriftlichen Anordnung die „*wesentlichen Gründe*“ anzugeben sind. Was unter diesen wesentlichen Gründen zu verstehen ist, wird in der Gesetzesbegründung nicht näher ausgeführt.

Nach hier vertretener Auffassung begegnet dies allerdings **keinen verfassungsrechtlichen Bedenken**. Die Entwurfsregelungen sind den verfassungsrechtlichen Anforderungen entsprechend auszulegen und anzuwenden. Dass dies möglich ist, hat das *BVerfG* in seiner Entscheidung zum sog. „großen Lauschangriff“ bestätigt: Aus § 34 i.V.m. § 100d Abs. 6 Satz 1 StPO a.F. folgte, dass die Anordnung einer akustischen Wohnraumüberwachung schriftlich zu begründen war. Darüber hinausgehender gesetzlicher Präzisierungen bedurfte es nach Ansicht des Gerichts nicht[68]. Das Gericht betonte aber, dass es Aufgabe und Pflicht des anordnenden Gerichts sei, den Inhalt und Umfang der Begründung an den oben beschriebenen Maßstäben auszurichten[69]. Angesichts der klaren Hinweise des Gerichts bestehen keine Bedenken, dass der unbestimmte Rechtsbegriff der „wesentlichen Gründe“ in dem eben beschriebenen Sinne interpretiert wird.

Dennoch sollte **vorsorglich eine Präzisierung in Betracht gezogen werden** (wie sie der Bundesgesetzgeber mittlerweile in § 100d Abs. 3 StPO vorbildlich umgesetzt hat). Es sei darauf hingewiesen, dass das *BVerfG* bereits mehrfach Kritik an der Praxis der Ausübung des

[65] BVerfG, Urt. v. 27.02.2008 - 1 BvR 370/07 Absatz-Nr. 259.
[66] BVerfGE 109, 279 (358 ff.).
[67] BVerfGE 109, 279 (358); wegen der ultima ratio-Klausel sind dabei auch die Umstände anzugeben, die belegen, dass der Subsidiaritätsgrundsatz beachtet worden ist.
[68] BVerfG, Urt. v. 03.03.2004 - 1 BvR 2378/98 Absatz-Nr. 276 ff.
[69] BVerfG, Urt. v. 03.03.2004 - 1 BvR 2378/98 Absatz-Nr. 276 ff.

Richtervorbehalts geäußert hat[70]. Insbesondere hat es zu Recht die Neigung zu exzessiver und zum Teil missbräuchlicher Anwendung der Eilkompetenz durch die Strafverfolgungsbehörden, insbesondere durch die Polizei beklagt und die Mangelhaftigkeit der richterlichen Kontrolle beanstandet.

II. Eilfallkompetenzen

Teilweise wird vertreten, dass eine Eilkompetenz des Präsidenten des Bundeskriminalamts im Falle des § 20h Abs. 3 (Lauscheingriff), § 20j Abs. 4 (Rasterfahndung) und § 20k Abs. 5 BKAG-E (Online-Durchsuchung) nicht erforderlich sei[71]. Verfassungsrechtlich relevant ist diese Position nicht, rechtspolitisch hat sie aber – jedenfalls was Maßnahmen zur sog. Online-Durchsuchung betrifft – durchaus Gewicht. Angesichts der technisch aufwändigen und langwierigen Vorbereitungszeit zur Durchführung entsprechender Maßnahmen dürfte ein Fall der „Gefahr in Verzug", in dem die Anordnungskompetenz auf den Präsidenten des Bundeskriminalamts übergeht, kaum jemals relevant werden. Dies bedeutet aber nicht, dass entsprechende Eilfälle nicht denkbar wären und der Beurteilungsspielraum des Gesetzgebers diesbezüglich eingeschränkt wäre. Es steht ihm – auch hinsichtlich der abzuwehrenden dringenden Gefahren – frei, Vorsorge für den Eil- und Notfall zu treffen. Dass ein derartiger „Eilfall" nur in ganz besonderen Ausnahmefällen eintreten wird, liegt dagegen in der Natur der Sache.

Freilich muss der Gesetzgeber einer missbräuchlichen Anwendung der Eilfallkompetenz entgegenwirken[72]. Vorliegend entsprechen die Ausnahmen für Eilfälle den Vorgaben des *BVerfG*; eine unverzügliche anschließende richterliche Überprüfung ist sichergestellt.[73] Die Anknüpfung an die Fälle einer „*Gefahr im Verzug*" entspricht ebenso den gängigen Regelungsmodellen. Für die tatsächlichen und rechtlichen Voraussetzungen der Annahme eines Eilfalls bestehen wiederum verfassungsrechtliche Vorgaben.[74] Eine diesbezüglich explizite gesetzliche Regelung ist nicht erforderlich.

---

[70] BVerfGE 103, 142 (152 m.w.N.) [Wohnungsdurchsuchung].

[71] *Baum/Schantz*, ZRP 2008, 137 (139); *Hofmann* und *Benneter* in „Auflistung der noch zu klärenden Fragestellungen" der Arbeitsgruppe Inneres v. 11.06.2008.

[72] Siehe BVerfGE 103, 142 (152).

[73] BVerfGE 109, 279 (358 ff.).

[74] Hierzu BVerfG 103, 142 (153 ff.): Eine wirksame gerichtliche Nachprüfung einer nichtrichterlichen Durchsuchungsanordnung wegen Gefahr im Verzug setzt voraus, dass der handelnde Beamte vor oder jedenfalls unmittelbar nach der Durchsuchung seine für den Eingriff bedeutsamen Erkenntnisse und Annahmen in den Ermittlungsakten dokumentiert. Insbesondere muss er, unter Bezeichnung des Tatverdachts und der gesuchten Beweismittel, die Umstände darlegen, auf die er die Gefahr des Beweismittelverlusts stützt. Allgemeine Formulierungen, die etwa bloß die juristische Definition von „Gefahr im Verzug" wiedergeben, reichen nicht aus. Das Gericht muss über die konkrete Sachlage zum Zeitpunkt der Entscheidung des handelnden Beamten informiert sein. Insbesondere muss erkennbar sein, ob der Beamte den Versuch unternommen hat, den Ermittlungsrichter zu erreichen. Eine verspätete Dokumentation des zeitlichen Ablaufs birgt die Gefahr von Ungenauigkeiten oder gar Umgehungen mit der Folge, dass eine Behauptung der Strafverfolgungsbehörden, die Herbeiführung einer richterlichen Entscheidung erfolglos versucht zu haben, nicht mehr nachzuprüfen ist. Zudem führt die Pflicht zur

Allerdings sollte eine explizite Regelung in Betracht gezogen werden, dass – im Falle einer Anordnung durch den Präsidenten des Bundeskriminalamts bei Gefahr im Verzug, die gerichtlich nicht bestätigt wird – die bis dahin gewonnenen Daten zu löschen sind und einem Verwertungsverbot unterliegen[75].

III. Verwendung und Übermittlung der Daten § 20v BKAG-E

1. Die Vorschriften des § 20v Abs. 4 und 5 BKAG-E erscheinen überarbeitungsbedürftig. Die potentiellen schweren Grundrechtseingriffe, die eine Übermittlung (und Zweckänderung) insbesondere nach §§ 20h, k oder l BKAG-E erhobener Daten impliziert, scheinen nicht hinreichend berücksichtigt worden zu sein. Die Gesetzesbegründung problematisiert dies jedenfalls nicht. Angesichts der schwierigen rechtlichen Fragestellungen – im Einzelnen besteht hier noch wesentliche Unklarheit – die bei der Ermittlung der rechtlichen Grenzen einer Datenübermittlung an andere öffentliche Stellen und die weitere Verwendung dieser Daten in einem neuen Kontext relevant werden, erscheint eine intensivere Auseinandersetzung im Gesetzgebungsprozess erforderlich, falls man an der vorgeschlagenen ausdifferenzierten Regelungssystematik festhalten will. Alternativ käme eine klare, restriktive Regelung in Betracht, die sich (auch bei der Frage der Datenübermittlung) ausschließlich am Prinzip der Rechtmäßigkeit des hypothetischen Ersatzeingriffes orientiert.

Soweit die Regelung in § 20v Abs. 5 BKAG-E eine Regelung zur Zweckänderung der nach § 20h, k oder l BKAG-E erhobenen Daten enthält, ist diese teils verfassungsrechtlich nicht unproblematisch (insbesondere was eine Übermittlung an die „Dienste“ betrifft). Die Zweckänderung von Daten bedeutet für den Betroffenen einen erneuten Grundrechtseingriff. Denn der Betroffene hat das Recht, selbst zu bestimmen, zu welchem Zweck seine Daten verarbeitet werden. Der Gesetzgeber muss daher nicht nur die Verarbeitung, sondern auch die Zweckänderung von Daten bereichsspezifisch und präzise regeln[76]. Dazu gehört, dass die Zweckänderung durch Allgemeinbelange gerechtfertigt ist, die die grundrechtlich geschützten Interessen überwiegen. Der neue Verwendungszweck muss sich auf die Aufgaben und Befugnisse der Behörde beziehen, der die Daten übermittelt werden und hinreichend klar geregelt sein. Schließlich dürfen der Verwendungszweck, zu dem die Erhebung erfolgt ist, und der veränderte Verwendungszweck nicht miteinander unvereinbar sein[77]. Eine solche Unvereinbarkeit

---

Dokumentation vor oder jedenfalls unmittelbar nach dem Eingriff dazu, dass sich der anordnende Beamte in besonderem Maße der Rechtmäßigkeit seines Handelns vergewissert und dass er überdies im Falle der Nachprüfung dieses Handelns auf dokumentierte Tatsachen wird verweisen können, die sein Handeln erklären […]. Auf der Grundlage dieser Dokumentation haben die Strafverfolgungsbehörden ihre Durchsuchungsanordnung in einem späteren gerichtlichen Verfahren zu begründen […]. Außerdem müssen sie darlegen, warum eine richterliche Anordnung zu spät gekommen wäre, und gegebenenfalls, warum von dem Versuch abgesehen wurde, eine richterliche Entscheidung zu erlangen.

[75] So überzeugend *Baum/Schanz*, ZRP 2008, 137 (139).

[76] BVerfGE 65, 1 (46); 100, 313 (389); *Schenke*, JZ 2001, 997 (998).

[77] BVerfGE 100, 313 (369).

läge vor, wenn mit der Zweckänderung grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Erhebungsmethoden umgangen würden, die Informationen also für den geänderten Zweck nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen[78].

Im Falle divergierender Eingriffsschwellen ist eine Zweckänderung solcher Daten, die unterhalb der höheren Eingriffsschwelle verwendet werden sollen, unzulässig[79]. Diese besondere Form der Konkretisierung des Verhältnismäßigkeitsprinzips ist z.B. in § 100d Abs. 6 Nr. 2, 3, § 161 Abs. 2 und § 477 StPO näher geregelt („**Prinzip der Rechtmäßigkeit eines hypothetischen Ersatzeingriffes**"). Vor diesem Hintergrund ist jedenfalls eine Übermittlung und Verwendung von Daten, die im Rahmen einer Online-Durchsuchung gewonnen wurden, fragwürdig, da eine entsprechende Maßnahme etwa nach der StPO nicht möglich ist. Gleiches gilt für eine Übermittlung von Maßnahmen einer optischen Wohnraumüberwachung (die StPO sieht lediglich Maßnahmen zur akustischen Wohnraumüberwachung vor).

2. Eine Datenübermittlung an ausländische Stellen ist in § 20v BKAG-E nicht geregelt. Insoweit ist Rückgriff auf die allgemeine Vorschrift des § 14 BKAG zu nehmen. Dies ist nach hier vertretener Auffassung nicht unproblematisch. Angesichts der Eingriffsintensität und der Grundrechtsrelevanz der nach dem Unterabschnitt 3a des BKAG-E erhobenen Daten wird eine bereichsspezifische Regelung zur Übermittlung der aus diesen Maßnahmen gewonnenen Daten an ausländische Stellen für erforderlich gehalten.

IV. Benachrichtigung, § 20w BKAG-E

Eine Bewertung der ausdifferenzierten Regelungen zur Benachrichtigung Betroffener nach § 20w BKAG-E war im Rahmen des vorliegenden Gutachtens nicht möglich.

[78] BVerfGE 100, 313 (389 f).

[79] Vgl. BVerfGE 100, 313 LS 6 sowie BVerfG, Urt. v. 03.03.2004 - 1 BvR 2378/98 = NJW 2004, 999 (1016 f.).

D. Sonderfragen

I. Begleitmaßnahme heimliches Betreten und Durchsuchen von Wohnungen?

„Begleitmaßnahmen“ in Form eines Betretens und Durchsuchens einer Wohnung zur Vorbereitung einer „Online-Durchsuchung“ (insbesondere zur Installation von Überwachungssoftware) sind nach der Rechtsprechung des *BVerfG* am Wohnungsgrundrecht zu messen: Art. 13 GG kommt zur Anwendung, „wenn und soweit Mitarbeiter der Ermittlungsbehörde in eine als Wohnung geschützte Räumlichkeit eindringen, um ein dort befindliches informationstechnisches System physisch zu manipulieren“[80].

Ein weiterer Anwendungsfall des Art. 13 Abs. 1 GG ist die Infiltration eines informationstechnischen Systems, das sich in einer Wohnung befindet, um mit Hilfe dessen bestimmte Vorgänge innerhalb der Wohnung zu überwachen, etwa indem die an das System angeschlossenen Peripheriegeräte wie ein Mikrofon oder eine Kamera dazu genutzt werden[81].

1. Die Schranke des Art. 13 Abs. 2 GG

Nachdem es sich bei der diskutierten Begleitmaßnahme begrifflich um eine „Durchsuchung“ handelt[82], ist die Schranke des Art. 13 Abs. 2 GG einschlägig, ein Rückgriff auf Art. 13 Abs. 7 GG scheidet dann aus („Sperrwirkung des Art. 13 Abs. 2 GG).

Allerdings wären die gegenständlichen Begleitmaßnahmen nicht von der Schranke des Art. 13 Abs. 2 GG gedeckt. Denn wesentliches Charakteristikum einer Durchsuchung im Sinne von Art. 13 Abs. 2 GG ist nach herrschender Auffassung das ungeschriebene Merkmal der **Offenheit** der Maßnahme[83]. Kennzeichen einer Durchsuchung soll gerade die Erkennbarkeit staatlichen Handelns sein. Wegen der Schwere des Eingriffs in das Wohnungsgrundrecht muss eine Durchsuchung für den Betroffenen offen und erkennbar sein, damit dieser ausreichenden Rechtsschutz erlangen kann. Auch die Grundgesetzänderung aus dem Jahre 1998 gibt mittelbar Aufschluss darüber, dass eine Durchsuchung offen zu erfolgen hat. Die Einführung des „Großen Lauschangriffs“ war erforderlich um eine technische Wohnraumüberwachung zu ermöglichen, wie das Bundesverfassungsgericht einleitend in seinem Urteil ausführte[84]. Durch die diesbezügliche Anpassung des Grundgesetzes wurde klargestellt, dass technische Überwachungsmaßnahmen nicht – wie nach teilweise vertretener Ansicht in der Literatur[85] – als Durchsuchung im Sinne von Art. 13 Abs. 2 GG angesehen werden können.

---

[80] BVerfG, Urt. v. 27.02.2008 - 1 BvR 370/07 - Absatz-Nr. 193.

[81] BVerfG, Urt. v. 27.02.2008 - 1 BvR 370/07 - Absatz-Nr. 193.

[82] Also um ein ziel- und zweckgerichtetes 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, siehe BVerfGE 28, 235 (287 ff.); 47, 31 (36f.); 76, 83 (89).

[83] *Kutscha*, DuR 1992, 247 ff. *Gornig*, in: von Mangoldt/Klein/Starck, GG, Art. 13 Rn. 65; *Kühne*, in: Sachs, GG, Art. 13 Rn. 25: „Lausch- und Späheingriffe durch Heimlichkeit, d.h. Unmerklichkeit gegenüber dem Betroffenen, gehen typischerweise über die Qualität des klassischen Eingriffs in Art. 13 Abs. 2 und Abs. 7 GG hinaus. D.h. der klassische Eingriff im Rahmen des Art. 13 Abs. 2 GG hat offen zu erfolgen“.

[84] BVerfG, Urt. v. 03.03.2004 - 1 BvR 2378/98 = NJW 2004, 999.

[85] Z.B. *Guttenberg*, NJW 1993, 567 ff.

2. Heimliches Betreten und Durchsuchen einer Wohnung nach Art. 13 Abs. 3 und 4 GG

Ein heimliches Betreten und Durchsuchen von Wohnungen kann von den Schranken des Art. 13 Abs. 3 bzw. 4 GG gedeckt sein, soweit die Durchsuchung zur Einleitung von einer Wohnraumüberwachung nach diesen Vorschriften erforderlich ist. Bei der technischen Wohnraumüberwachung ist die Begleitmaßnahme der Installation der Abhörtechnik derselben Schrankenregelung wie die Hauptmaßnahme unterworfen[86]. Es kann angenommen werden, dass der Gesetzgeber stillschweigend auch zu notwendigen Begleitmaßnahmen ermächtigt hat, als er die (Primär-)Eingriffsbefugnis zur heimlichen akustischen Wohnraumüberwachung schuf[87]. Außerdem würde eine Ermächtigung zur akustischen Wohnraumüberwachung, sei es nun im repressiven oder im präventiven Bereich, ins Leere laufen, wenn nicht zugleich mit der Maßnahme einhergehende unerlässliche Vorbereitungs- bzw. Begleithandlungen zulässig wären[88].

3. Wertungswiderspruch und Lösung durch „Schrankenübertragung"

Ungeachtet der Tatsache, dass ein Betreten und Durchsuchen von Wohnungen aufgrund der gewachsenen Systematik und der herkömmlichen Auslegung von Art. 13 GG wohl grundsätzlich offen erfolgen müssen, sind zweifellos entsprechende heimliche Eingriffe als „notwendige Begleitmaßnahmen" im Rahmen von Art. 13 Abs. 3 und 4 GG statthaft. Dies zu Grunde gelegt, führt – betrachtet man die vom *BVerfG* in seiner Entscheidung zur Online-Durchsuchung formulierten Beispielsfälle zur Abgrenzung von Art 13 und dem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme – zu denkwürdigen und im Ergebnis widersprüchlichen Ergebnissen:

> **Beispiel 1**: Mitarbeiter der Ermittlungsbehörde dringen heimlich in eine als Wohnung geschützte Räumlichkeit ein, um ein dort befindliches informationstechnisches System physisch zu manipulieren, um eine „herkömmliche" Online-Durchsuchung zu veranlassen **->** Für die „Begleitmaßnahme" ist Art. 13 GG einschlägig, also heimliches Betreten und Durchsuchen nicht erlaubt (die Online-Durchsuchung selbst wäre am Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme zu messen)
>
> **Beispiel 2**: Mitarbeiter der Ermittlungsbehörde dringen heimlich in eine als Wohnung geschützte Räumlichkeit ein, um ein dort befindliches informationstechnisches System physisch zu manipulieren, um mit der Infiltration des Systems **ausschließlich Vorgänge innerhalb der Wohnung zu überwachen**, etwa indem die an das System angeschlossenen Peripheriegeräte wie ein Mikrofon oder eine Kamera dazu genutzt werden. **->** In diesem Fall richtet sich die Überwachung selbst ausschließlich nach Art. 13 Abs. 4 GG; ein heimliches Eindringen in die Wohnung ist als Begleitmaßnahme von Art. 13 Abs. 4 GG gedeckt und damit unter gesetzlicher Beachtung der dortigen Anforderungen zulässig.

---

[86] *Stern*, Handbuch des Staatsrechts, Bd. 4/1, 2006, S. 283 f. *Papier*, in: Maunz/Dürig, GG, Art. 13 Rn. 47, 79, 89, *Meyer/Hetzer*, NJW 1998, 1017 (1026).

[87] BGH, JR 1998, 163.

[88] *Heger*, JR 1998, 164.

Beispiel 3 (auf die Spitze getrieben): Mitarbeiter der Ermittlungsbehörde dringen heimlich in eine als Wohnung geschützte Räumlichkeit ein, um ein dort befindliches informationstechnisches System physisch zu manipulieren, um mit der Infiltration des Systems Vorgänge innerhalb der Wohnung zu überwachen **und zugleich** auch auf andere Daten zuzugreifen (also „herkömmliche" Onlinedurchsuchung) **->** Muss man jetzt diese „einheitliche" Maßnahme trennen? Wäre das Eindringen zugleich zulässig (soweit Art. 13 Abs. 4 GG einschlägig) als auch unzulässig, da das Eindringen auch zu anderen Zwecken mit veranlasst ist? – Wohl kaum. Vielmehr müsste man für diesen (theoretischen Fall) davon ausgehen, dass das sich als einheitlicher Lebenssachverhalt darstellende Verhalten jedenfalls von Art. 13 Abs. 4 GG gedeckt und als solches rechtskonform ist - insbesondere weil sich eine Online-Durchsuchung insoweit als die „mildere" Maßnahme darstellt. Soll also in der Praxis (unter den Voraussetzungen des Art. 13 Abs. 4 GG) immer auch ein Zugriff auf Peripheriegeräte „vorgeschoben" werden, um ohne Grundgesetzänderung eine Wohnung als „Begeleitmaßnahme" für eine Onlinedurchsuchung heimlich betreten zu können? – Wohl kaum.

Die aufgeführten Beispielsfälle zeigen einen erheblichen Wertungswiderspruch auf. Faktisch werden identische Eingriffe, die in Auswirkung und Folgen sich für den potentiell Betroffenen kaum unterscheiden, einer (bis auf einen dogmatischen Grundansatz) nicht zu rechtfertigenden Differenzierung unterworfen. Eine Auflösung dieser Problematik kann nicht nur durch eine Grundgesetzänderung erfolgen. Als dogmatischer Ansatzpunkt zur Rechtfertigung der betreffenden Begleitmaßnahmen für eine Online-Durchsuchung kommt vielmehr auch eine **Übertragung der Schranken des Art. 13 Abs. 4 GG in Betracht**. Dies schon deshalb, weil sich die typischen Begleitmaßnahmen von Online-Durchsuchung und Lauschangriff in Art, Schwere und Zielrichtung entsprechen. Zudem fordert die dann anzulegende Schranke des Art. 13 Abs. 4 GG durchwegs strenge Eingriffsvoraussetzungen, die diejenigen einer Online-Durchsuchung übertreffen können. Anders als beim gescheiterte Versuch einer Schrankenübertragung (Art. 13 Abs. 2 bzw. Abs. 3 a.F., jetzt Abs. 7) zur Rechtfertigung eines Lauscheingriffes, wird vorliegend (wie die angeführten Beispiele verdeutlichen) nicht der gekünstelte Versuch unternommen, wesensfremde Eingriffe durch Kunstbegriffe in einem bestehendes System zu verorten, sondern es werden im Ergebnis entsprechende Lebenssachverhalte einer einheitlichen und (aufgrund der hohen Anforderungen des Art. 13 Abs. 4 GG) die Bürgerrechte ausreichend berücksichtigenden Lösung zugeführt. Insoweit ließe sich nach hier vertretener Ansicht eine Schrankenübertragung gut rechtfertigen. Unter Beachtung der Eingriffsschwellen des Art. 13 Abs. 4 GG erscheint eine Begleitmaßnahme für eine Online-Durchsuchung jedenfalls als zulässig. Freilich unter der Voraussetzung einer klaren gesetzlichen Regelung der „Begleitmaßnahme" unter entsprechenden Eingriffsschwellen[89].

[89] Vgl. die Regelung in Art. 34e PAG.

Zu einem ähnlichen Ergebnis gelangt *Möstl*[90]. Dieser hält eine Rechtfertigung nach Art. 13 Abs. 2 GG für möglich. Der besondere Aspekt der Heimlichkeit der Begleitmaßnahme werde bereits durch die hohen sachlichen Hürden des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme „abgearbeitet", mit der Folge, dass Art. 13 Abs. 2 GG jedenfalls für solche Vorbereitungsmaßnahmen, die sich auf Hauptmaßnahmen beziehen, deren Heimlichkeit nicht gesondert gerechtfertigt werden muss, als geeignete Eingriffsgrundlage angesehen werden könne.

II. Grundrechtsschutz durch technische Verfahren

Der Gesetzentwurf implementiert in § 20k Abs. 2 und Abs. 7 Satz 2 BKAG-E (notwendige) automatisierte technische Schutzvorkehrungen, die (mit) sicherstellen sollen, dass Eingriffe in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme auf das erforderliche Maß minimiert werden. Einerseits ist (nach dem jeweiligen Stand von Forschung und Technik) sicherzustellen, dass Veränderungen des informationstechnischen Zielsystems auf das unerlässliche Maß beschränkt werden und diese Veränderungen bei Beendigung der Maßnahme automatisiert rückgängig gemacht werden (**Schutz der Integrität**, § 20k Abs. 2 BKAG-E). Andererseits ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, (möglichst) schon nicht erhoben werden (**Schutz der Vertraulichkeit**, § 20k Abs. 7 Sazu 2 BKAG-E).

Damit kommen die Entwurfsverfasser dem Auftrag nach, schützende Regelungen zu schaffen, die sich auf die eingesetzten Technologien beziehen (Schlagwort: „technikkonformes Recht – rechtskonforme Technik"). Aus diesem Bestreben heraus kann der Staat spezifische Gefährdungen, die aus dem Technikeinsatz hervorgehen, seinerseits mit Technikeinsatz begegnen. Es wird insoweit ein Paradigma aufgegriffen, das ich bereits vor vier Jahren mit der Formel **„Grundrechtsschutz durch technische Verfahren"** auf den Begriff gebracht habe[91]. Durch Systemdatenschutz und durch gezielte Steuerung der eingesetzten technischen Systeme kann (im Optimalfall) erreicht werden, dass Daten unbeteiligter Dritter zwar verarbeitet, aber nicht gespeichert werden, sodass im Rahmen polizeilicher Maßnahmen keine Grundrechtseingriffe geschehen. Für den Einsatz von Kennzeichenerkennungssystemen hat dies nun auch das *BVerfG* bestätigt, wenn es feststellt, dass kein Grundrechtseingriff vorliegt, wenn Daten unmittelbar nach ihrer Erfassung technisch wieder spurenlos, anonym und ohne Möglichkeit einen Personenbezug herzustellen, gelöscht werden[92]. Freilich kann Entsprechendes (noch) nicht bei technisch hochkomplexen Ermittlungsmaßnahmen wie einer Online-Durchsuchung gewährleistet werden. Das *BVerfG* hat dies bei der Frage nach der Möglichkeit eines „automatisierten Kernbereichsschutzes" auf den Punkt gebracht: „Technische Such- oder Aus-

[90] Expertenanhörung zur „Online-Datenerhebung", LT-Drs. 15/10345.
[91] *Heckmann*, IT-Einsatz und Gefahrenabwehr, in: KommunalpraxisSpezial 2/2005 S. 52 ff.
[92] BVerfG, Urt. v. 11.03.2008 – 1 BvR 2074/05 Absatz-Nr. 68.

schlussmechanismen zur Bestimmung der Kernbereichsrelevanz persönlicher Daten arbeiten nach einhelliger Auffassung der vom Senat angehörten sachkundigen Auskunftspersonen nicht so zuverlässig, dass mit ihrer Hilfe ein wirkungsvoller Kernbereichsschutz erreicht werden könnte.[93]“ Dies bedeutet allerdings nicht, dass entsprechende Schutzvorkehrungen nicht erforderlich wären. Denn nur zwei Absätze später stellt das Gericht in seiner Entscheidung fest: „Die gesetzliche Regelung hat darauf hinzuwirken, dass die Erhebung kernbereichsrelevanter Daten soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt. Insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen.“ Diesem Auftrag ist der Gesetzgeber vorliegend nachgekommen. Dennoch bleibt daran zu erinnern, dass der Staat die erforderlichen Mittel zur Verfügung stellen muss, um den Einsatz bislang nicht perfekter technischer Schutzvorkehrungen auf Grundlage der neuesten wissenschaftlichen Erkenntnisse weiter zu effektuieren. Ansonsten würden die gesetzlichen Schutzregelungen lediglich einen (praktisch belanglosen) Tribut an die Rechtsprechung des *BVerfG* darstellen. Das Bundeskriminalamt hat nicht nur – worauf die Gesetzesbegründung explizit hinweist[94] - dafür Sorge zu tragen, dass die eingesetzte Software nicht durch Dritte (Hacker) zweckentfremdet werden kann, sondern in gleichem Maße auch, dass durch die eingesetzte Software – im Sinne eines effektiven Grundrechtsschutzes durch technische Verfahren – Eingriffe in das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme sowie in den Kernbereich privater Lebensgestaltung minimiert werden.

[93] BVerfG, Urt. v. 27.02.2008 - 1 BvR 370/07 Absatz-Nr. 278.

[94] BT-Drs. 16/9588 S. 73 [elektronische Vorabfassung].