Prof. Dr. Fredrik Roggan

Professor für Strafrecht

Dienstliche Erreichbarkeit:
FH der Polizei des Landes Brandenburg
Bernauer Str. 146
16515 Oranienburg

Tel.: 03301 / 850 - 2545
Fax: 03301 / 850 - 2509
E-Mail FredrikRoggan@gmx.de

www.fhpolbb.de

Berlin/Oranienburg, 17.06.2016

Prof. Dr. F. Roggan | Bernauer Str. 146 | 16515 Oranienburg

Deutscher Bundestag
- Innenausschuss –

11011 Berlin

Entwurf eines
Gesetzes zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus
- BT-Drucks. 18/8702 -

Sehr geehrter Herr Vorsitzender,
sehr geehrte Damen und Herren,

zu dem o.g. Gesetzentwurf nehme ich – soweit das von hier aus angezeigt erscheint und in dem vorgegebenen Zeitrahmen möglich war – wie folgt Stellung:

A. Informationelle Zusammenarbeit mit ausländischen Geheimdiensten

I. Bewältigung der Grundprobleme der Kooperation des BfV mit Partnerdiensten

1. Grundprobleme

Als gesetzgeberisch zu bewältigendes Grundproblem stellt sich, dass bereits die Einrichtung einer gemeinsam mit ausländischen Geheimdiensten geführten Datei,

namentlich die Einspeicherung von personenbezogenen Daten in eine solche, mit der Gefahr einer Relativierung von datenschutzmäßigen Standards verbunden ist. Was die Einspeicherung von Daten des BfV anbelangt, so stellt sich die Frage der Nutzbarkeit dieser Informationen im Ausland durch solche Geheimdienste, die einen anderen Kompetenzzuschnitt als Inlandsgeheimdienste besitzen, also etwa Zwangsbefugnisse einschließen. Im besonderen muss der Gesetzgeber gewährleisten, dass die Informationen nicht in den Dienst von Menschenrechtsverletzungen durch ausländische Partnerdienste (etwa anlässlich von Verhören in Geheimdienstgefängnissen) gestellt werden: Keinesfalls darf der Staat seine Hand zu Verletzungen der Menschenwürde reichen (zuletzt *BVerfG*, 1 BvR 966/09 u.a., Urt. v. 20. April 2016, Rdnr. 328).

Auch was den „gegenläufigen" Informationsfluss anbelangt, hat der Gesetzgeber dafür Sorge zu tragen, dass der inländische Geheimdienst nicht in den Besitz von personenbezogenen Daten gerät, die unter Verstoß gegen elementare rechtsstaatliche Grundsätze erhoben wurden (wiederum etwa durch Verhöre in ausländischen Geheimdienstgefängnissen), denn eine Entgegennahme und Verwertung von durch ausländische Behörden menschenrechtswidrig erlangte Daten ist gesetzgeberisich auszuschließen (*BVerfG*, 1 BvR 966/09 u.a., Urt. v. 20. April 2016, Rdnr. 327).

Bei der dateimäßigen Zusammenarbeit von in- und ausländischen Geheimdiensten ist insbesondere zu berücksichtigen, dass bereits das Einspeichern von personenbezogenen Daten in eine Verbunddatei, selbst wenn deren Nutzung ausschließlich der Datenübermittlungsanbahnung diente (vgl. aber § 22b Abs. 4 BVerfSchG-E) mit einer erheblichen Beeinträchtigung der informationellen Selbstbestimmung der Betroffenen verbunden ist, weil hierdurch ein Informationsaustausch zwischen einer großen Zahl von Geheimdiensten mit zum Teil deutlich unterschiedlichen Aufgaben und Befugnissen ermöglicht wird (vgl. dazu BVerfGE 133, 277 [323]). Für das BfV etwa gilt, dass es nach zutreffender Ansicht in der Literatur (vgl. *Poscher/Rusteberg*, KJ 2014, 57, 62 ff.; wohl auch *Gusy*, Polizei- und Ordnungsrecht, 9. Aufl. 2014, S. 20; a. A.. etwa *Schenke*, Polizei- und Ordnungsrecht, 9. Aufl. 2016, S. 271) sowie im Verständnis des *BVerfG nicht* als Sicherheitsbe-

hörde anzusehen ist (BVerfGE 133, 277 [326 f.]). Stattdessen ist seine Aufgabe darauf beschränkt, Informationen für die politische Führung anhand von Lagebildern oder –einschätzungen zu generieren, mithin *nicht* die Zielsetzung, seine Informationsbestände in Gefahrenabwehr– oder Strafverfolgungsmaßnahmen umzusetzen (vgl. etwa *Pieroth/Schlink/Kniesel*, Polizei- und Ordnungsrecht, 8. Aufl. 2014, S. 27).

2. Gewährleistung der Einhaltung rechtsstaatlicher Grundsätze

Vor diesem Hintergrund ist die geplante Neuregelung verfassungsrechtlich keineswegs unproblematisch. Dies gilt sowohl für die Bestimmung der teilnehmenden Staaten an den Dateien (a.) wie auch für ihre Nutzung (b.). Aus der verfassungsrechtlichen Judikatur lassen sich insoweit nur vage Anhaltspunkte für Grenzmarken herleiten: So soll der Umgang mit anderen Staaten auch dann, wenn deren Rechtsordnungen und –anschauungen *nicht vollständig* mit den deutschen innerstaatlichen Auffassungen übereinstimmen, möglich sein (*BVerfG*, 1 BvR 966/09 u.a., Urt. v. 20. April 2016, Rdnr. 325).

a) Unklarheit hinsichtlich teilnehmender Staaten

Das BfV darf gemeinsame Dateien nur mit solchen Staaten einrichten, in denen die Einhaltung grundlegender rechtsstaatlicher Prinzipien gewährleistet ist (§ 22b Abs. 1 Nr. 2 BVerfSchG-E). Eine nähere Bestimmung wird nicht vorgenommen.

Vor allem fehlt eine hinreichende Konturierung der „grundlegenden rechtsstaatlichen Prinzipien". So könnte die Vorschrift so zu verstehen sein, dass beispielsweise eine systematische Verfolgung von Journalisten in einem Staat aufgrund besonders restriktiver Anti-Terror-Gesetze eine gemeinsame Datei ausschließt. Auch eine nicht hinreichend klare Trennung von geheimdienstlicher und polizeilicher Aufgabenwahrnehmung käme als Ausschlusskriterium in Betracht. Beides wäre nach hier vertretener Ansicht durchaus begrüßenswert, dürfte aber kaum intendiert sein, denn dies würde auch Kooperationen mit einzelnen NATO-Partnerstaaten ausschließen.

Im Ergebnis birgt diese weitgehend offene Formulierung die Gefahr, dass nicht zuletzt politische Opportunitätserwägungen in die Beurteilung, ob ein Staat teilnahmefähig ist oder nicht, einfließen. Das ist schon deswegen nicht abwegig, weil eine informationelle Kooperation mit anderen Staaten auch darauf zielt, die zwischenstaatlichen Beziehungen im gegenseitigen Interesse wie auch die außenpolitische Handlungsfreiheit der Bundesregierung zu erhalten (vgl. *BVerfG*, 1 BvR 966/09 u.a., Urt. v. 20. April 2016, Rdnr. 325).

b) Schriftliche Festlegung der dateimäßigen Zusammenarbeit

Mittels schriftlicher Fixierung soll ein „angemessenes" Datenschutzniveau bestimmt und eine „unangemessene" Verwendung der Daten ausgeschlossen werden (§ 22b Abs. 5 BVerfSchG-E). Gegen diese Formulierungen wäre nichts zu erinnern, wenn namentlich mit dem Ausschluss einer unangemessenen Verwendung eine unverhältnismäßige bzw. unzumutbare Datennutzung gemeint wäre. Indessen bekennt sich die Gesetzesbegründung explizit dazu, dass ein mit der deutschen Rechtsordnung vergleichbarer Schutz der Daten nicht erforderlich ist (BT-Drucks. 18/8702, S. 22). Damit wären namentlich Verstöße gegen den Verhältnismäßigkeitsgrundsatz bis an die Grenze von Verstößen gegen elementare Anforderungen des menschenrechtlichen Schutzes personenbezogener Daten möglicher Gegenstand einer Zusammenarbeitsvereinbarung. Damit wäre ein jedenfalls partielles Unterlaufen der Grenzen der inländischen Datenerhebung und –verarbeitung durch die Regelung des § 22b Abs. 5 BVerfSchG nicht ausgeschlossen.

II. Gemeinsame Dateien zur Informationsanbahnung

Die mit ausländischen Geheimdiensten gemeinsam geführten Dateien sollen als Indexdateien errichtet werden, § 22b Abs. 3 BVerfSchG-E. Sie ist insoweit vergleichbar mit der Anti-Terror-Datei (ATD) sowie der Rechtsextremismus-Datei (RED). Allerdings wird im Falle eines Treffers lediglich derjenige ausländische Geheimdienst angezeigt, der die Daten eingegeben hat. Die Befugnis zur Dateneingabe ergibt sich aus § 22b Abs. 6 BVerfSchG-E. Die Regelung begegnet so-

wohl unter Bestimmtheits- wie auch (daraus folgend) Verhältnismäßigkeitsgesichtspunkten erheblichen Bedenken.

1. Bestimmtheitsgebot

Das Bestimmtheitsgebot soll sicherstellen, dass Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte eine wirksame Rechtskontrolle durchführen können. Ferner erlauben die Bestimmtheit und Klarheit der Norm, dass die betroffenen Bürgerinnen und Bürger sich auf mögliche belastende Maßnahmen einstellen können (st. Rspr., vgl. etwa BVerfGE 133, 277 [336]). Dabei sind die Bestimmtheitsanforderungen umso höher, je intensivere Grundrechtseingriffe durch die Regelung selber oder aufgrund ihrer erlaubt werden.

Im Falle der dateimäßigen Zusammenarbeit von verschiedenen Behörden müssen zwar die konkreten Behörden im Gesetz nicht ausdrücklich aufgeführt werden. Jedoch genügt die Umschreibung nach weiten und wertungsoffenen Kriterien nicht (BVerfGE 133, 277 [338]). Als an den gemeinsamen Dateien beteiligten Behörden werden in § 22b Abs. 1 BVerfSchG-E lediglich ausländische öffentliche Stellen, die mit nachrichtendienstlichen Aufgaben betraut sind, genannt. Damit wird beispielsweise nicht ausgeschlossen, dass auch solche ausländischen Stellen beteiligt werden können, die neben nachrichtendienstlichen auch sicherheitsbehördliche Aufgaben wahrnehmen, namentlich also auch Zwangsbefugnisse besitzen.

Unter Bestimmtheitsgesichtspunkten ist weiter zu bemängeln, dass die Zwecke der gemeinsamen Dateien nicht hinreichend präzise umschrieben werden. So sollen die Indexdateien sich auf bestimmte Ereignisse oder Personenkreise, deren Erforschung von erheblichem Sicherheitsinteresse für die Bundesrepublik und den jeweils teilnehmenden Staat ist, beziehen (§ 22b Abs. 1 Nr. 1 BVerfSchG-E). Eine Beschränkung etwa auf terroristische Gefahren, wie die Bezeichnung des Gesetzes suggerieren könnte, wird nicht vorgenommen. Damit werden gemeinsame Dateien letztlich zu allen sicherheitserheblichen Bestrebungen ermöglicht. Eine

derart offene Formulierung vermag eine hinreichende Begrenzungswirkung nicht zu erzielen.

Nicht mit dem Bestimmtheitsgrundsatz vereinbar ist auch die fehlende Festlegung auf diejenigen personenbezogenen Daten, die in die Datei eingespeichert werden dürfen. Der Entwurf beschränkt sich diesbezüglich auf einen Verweis auf die allgemeinen Vorschriften der §§ 10 und 11 BVerfSchG sowie die Vorraussetzung, dass diese Daten im Falle eines Treffers den teilnehmenden Geheimdiensten auch übermittelt werden dürfen, § 22b Abs. 6 BVerfSchG-E. Namentlich ist eine Festlegung des Personenkreises, die von einer Speicherung betroffen sein kann, dem Entwurf nicht zu entnehmen. Er unterscheidet sich insoweit erheblich von vergleichbaren Befugnissen zur Errichtung von Indexdateien (vgl. etwa § 2 ATDG).

2. Verhältnismäßigkeitsprinzip

Bei der Speicherung von personenbezogenen Daten in einer Datei, die der Informationsanbahnung zwischen in- und ausländischen Behörden dienen soll, handelt es sich um einen schwerwiegenden Eingriff in die informationelle Selbstbestimmung der betroffenen Individuen. Das liegt nicht nur daran, dass die Aufgabenzuschnitte der Geheimdienste in den Ländern sich durchaus unterscheiden. Vielmehr kann und soll sich ein durch die Indexdatei-Nutzung ermöglichter Datenaustausch ja gerade darin niederschlagen, dass sich hieran zumindest weitere Informationseingriffe anschließen. Im Falle von Ländern, in denen keine klare Trennung zwischen geheimdienstlichen und sicherheitsbehördlichen Stellen existiert, mögen als Folgeeingriffe gar operative Maßnahmen drohen.

Damit ist festzustellen, dass die Aufnahme in eine solche Datei für die Betreffenden erheblich belastende Wirkung haben kann. Wer einmal in der Datei erfasst ist, muss damit rechnen, aufgrund einer Abfrage dem Umkreis sicherheitsrelevanter Bestrebungen zugeordnet und – mittels weiterer, dadurch erleichterter Übermittlungsersuchen – hieran anknüpfenden belastenden Maßnahmen unterworfen zu werden. Die Konsequenzen einer solchen Zuordnung können beträchtlich sein und Einzelne in schwierige Lagen bringen, ohne dass sie um diese Einordnung

wissen und eine praktikable Möglichkeit haben, sich hiergegen zu wehren (vgl. BVerfGE 133, 277 [331]).

Vor diesem Hintergrund ermöglicht die beabsichtigte Neuregelung unverhältnismäßige Eingriffe beispielsweise in die Rechte derer, die nur am Rande von geheimdienstlich beobachteten Bestrebungen stehen (Kontakt- und Begleitpersonen etc.). Die Ursache hierfür liegt in der fehlenden Beschränkung auf solche Personen, die etwa für terroristische Gefahren verantwortlich gemacht werden („Foreign Terrorist Fighters", vgl. BT-Drucks. 18/8702, S. 20). Das gilt insbesondere auch vor dem Hintergrund, dass es sich um keine reine Indexdatei handelt, sondern unter im Folgenden zu erörternden Umständen auch einen umfänglich nutzbaren Datenpool.

III. Insbesondere: Erweiterte Dateinutzung zum Austausch und gemeinsamen Auswertung

Die in § 22b Abs. 4 BVerfSchG-E vorgesehene analytische Nutzung von gemeinsamen Dateien geht in Ausmaß und Qualität deutlich über die Nutzung als Übermittlungsanbahnungsinstrument hinaus. Wie auch die Gesetzesbegründung anerkennt, ist sie mit einer noch intensiveren Beeinträchtigung der informationellen Selbstbestimmung verbunden (BT-Drucks. 18/8702, S. 22). Dieser Umstand ist schon deswegen von besonderer Bedeutung, weil das *BVerfG* in seiner Entscheidung zur ATD mehrfach betonte, dass für seine Entscheidung, die Datei in ihren Grundstrukturen für verfassungsgemäß zu erklären, der Charakter der ATD als bloßes Übermittlungs- bzw. Informationsanbahnungsinstrument entscheidend war (BVerfGE 133, 277 ([320 f, 322 f, insbes. 329 ff, 339, 353 f, 356, 364 und 369]; vgl. auch *Hörauf*, NVwZ 2015, 181 [185]).

Als tatbestandliche Voraussetzung für diese analytische Nutzung werden besondere Sicherheitsinteressen verlangt, die ihrerseits in der Erforschung von Bestrebungen oder Tätigkeiten, die auf die Begehung von schwerwiegenden Straftaten gegen den Bestand oder die Sicherheit eines Staates oder einer internationalen Organisation gerichtet sind, bestehen.

Gleichzeitig soll bei einer solchen Datei der Umfang der in ihr gespeicherten, personenbezogenen Daten erweitert werden. Tatsächlich wird durch die Wendung, dass die Datei in solchen Fällen die „erforderlichen Daten" enthalten darf, die einspeicherbaren Informationen fast vollständig entgrenzt, denn bei dem nicht näher konkretisierten Austausch und der ebenso wenig näher konkretisierten Auswertung kann praktisch jede den Geheimdiensten bekannte „analysefähige" Information über wiederum nicht näher spezifizierte Personen von Bedeutung sein. Eine solch offene Formulierung ist mit dem Bestimmtheitsgrundsatz unvereinbar und birgt die konkrete Gefahr von unverhältnismäßigen Informationseingriffen in sich.

B. Einführung einer Befugnis zum Einsatz von Verdeckten Ermittlern (VE) im BPolG

I. Betreten von Wohnungen durch VE

Nach § 28 Abs. 6 Nr. 2 BPolG-E sollen VE das Recht zum Betreten von Wohnungen erhalten. Der durch ein solches Verhalten eines VE bewirkte Eingriff in das Wohnungsgrundrecht kann ebenso wenig gerechtfertigt werden, wie das bei der Vorbildvorschrift des § 110c S. 1 und 2 StPO (vgl. BT-Drucks. 18/8702, S. 25) der Fall ist.

1. Schutzbereich und Eingriff

Es soll an dieser Stelle keine nähere Begründung erfahren, dass das Betreten einer dem Schutzbereich unterfallenden Räumlichkeit durch Hoheitsträger untrennbar mit der Möglichkeit zur Kenntnisnahme von dortigen Vorgängen, der Anwesenheit von Personen einschließlich geführter Kommunikationen unter den Bedingungen der vermeintlichen, räumlichen Abschottung und den speziellen örtlichen Verhältnissen, namentlich der Einrichtung etc. verbunden ist.

Ein solcher Eingriff kann – wenn überhaupt – nur unter der Voraussetzung einer dem Verhältnismäßigkeitsgrundsatz genügenden, ausdrücklichen Ermächtigung zulässig sein. Die Gegenmeinung, die bereits einen hoheitlichen Grundrechtseingriff anlässlich der Informationserhebungen durch strafprozessuale VE in Wohnungen ablehnt, hat sich zu Recht nicht durchgesetzt (vgl. die Nachweise bei Meyer-Goßner/*Schmitt*, 59. Aufl. 2016, § 110c Rdnr. 1; HK-StPO/*Gercke*, 5. Aufl. 2012, § 110c Rdnr. 2; MünchKomm-StPO/*Günther*, § 110c Rdnr. 13; a. A. *Kühne*, Strafprozessrecht, 9. Aufl. 2015, S. 348). Für VE-Einsätze nach (Bundes-)Polizeirecht kann nichts anderes gelten. Darüber hinausgehend muss sich eine entsprechende Vorschrift im Rahmen der grundrechtlichen Schranken halten.

2. Mangelnde verfassungsrechtliche Rechtfertigung

Es existiert keine Grundrechtsschranke, die einen VE-Einsatz in Wohnungen erlauben würde. Zwar wird mitunter Art. 13 Abs. 2 GG in Erwägung gezogen (vgl. etwa *Jarass*, in: Jarass/Pieroth, GG, 14. Aufl. 2016, Art. 13 Rdnr. 23), diese Vorschrift betrifft nach ihrem eindeutigen Wortlaut jedoch die Wohnungsdurchsuchung, die ein VE-Einsatz offensichtlich nicht ist. Wesentliches Merkmal einer Durchsuchung ist, dass sie als offene staatliche Maßnahme durchzuführen ist (vgl. etwa §§ 105 Abs. 2, 106 StPO). Wesentliche weitere Voraussetzung ist, dass die Ergreifung des Verdächtigen bezweckt wird und/oder eine Vermutung des Auffindens von Beweismitteln besteht (§ 102 StPO). Keine dieser Merkmale werden beim Betreten einer Wohnung durch einen VE erfüllt oder bezweckt. Deshalb entspricht es einer verbreiteten Meinung in der strafprozessualen (Kommentar-)Literatur, dass die so verstandene Vorbildvorschrift (s. o.) des § 110c S. 1 StPO verfassungswidrig ist (näher LR-StPO/*Hauck*, 26. Aufl. 2014, § 110c Rn 11 ff.; vgl. auch SK-StPO/*Wolter/Jäger*, 5. Aufl. 2015, § 110c Rn 6;; SSW-StPO/*Eschelbach*, § 110c Rn 4; a. A. KK-StPO/*Bruns*, 7. Aufl. 2013, § 110c Rn 3). Nach hier vertretener Ansicht gilt dasselbe Verdikt – ohne dass der Streit an dieser Stelle im Einzelnen dargelegt werden könnte – für die geplante Regelung des § 28 Abs. 6 Nr. 2 BPolG-E.

Als nicht überzeugend ist aus Wortlautgründen demgegenüber das Modell einer „indirekten verfassungsrechtlichen Billigung" durch Art. 13 Abs. 5 GG anzusehen (so aber *Frister*, in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, Kap F Rn 332).

Folgt man der hier vertretenen Ansicht, so stellt sich die Frage einer Rechtfertigung von technischen Überwachungsmaßnahmen zur Eigensicherung ermittelnder Amtsträger in Wohnungen (dazu im Folgenden) bereits nicht. Anders als für das bloße Betreten von Wohnungen durch Amtsträger existiert für solche verdeckten Datenerhebungen jedoch eine Grundrechtsschranke in Art. 13 Abs. 5 GG, die ihrerseits freilich voraussetzt, dass der Einsatz von VE in Wohnungen auf einer (verfassungsgemäßen) gesetzlichen Grundlage basiert (*Jarass*, in: Jarass/Pieroth, GG, 14. Aufl. 2016, Art. 13 Rdnr. 23).

II. Einsatz von technischen Mitteln zur Eigensicherung

Nach § 28a Abs. 1 BPolG-E sollen technische Mittel zur akustischen und optischen Überwachung auch innerhalb von Wohnungen eingesetzt werden dürfen. Als Gelegenheit wird das Beisein oder ein unmittelbarer zeitlicher Zusammenhang mit einem VE-Einsatz genannt. Die Gesetzesbegründung spricht davon, dass hierdurch die Möglichkeit zu einer umgehenden Reaktion (Rettungszugriff) geschaffen werden solle (BT-Drucks. 18/8702, S. 27). Sie ist diesbezüglich § 16 Abs. 1 BKAG nachgebildet.

Soweit mit solchen Maßnahmen der Eigensicherung Eingriffe in Art. 13 Abs. 1 GG einhergehen, bildet Art. 13 Abs. 5 GG die Grundrechtsschranke. Dort ist die Rede davon, dass die Mittel zum Schutze der bei einem Einsatz in Wohnungen tätigen Personen vorgesehen werden kann. Der Wortlaut der Verfassungsnorm ist dabei so zu verstehen, dass die Eigensicherungsmaßnahmen in Wohnungen auf die *Anwesenheitsphasen* eines VE beschränkt sein müssen (*Kühne*, in: Sachs (Hrsg.), GG, 7. Aufl. 2014, Art. 13 Rdnr. 47).

Der Wortlaut des § 28a Abs. 1 BPolG-E geht über die Grundrechtsschranke insoweit hinaus, als dass die Überwachungsmaßnahmen auch im unmittelbaren zeitlichen Zusammenhang, also auch ohne das Beisein des VE in einer Wohnung, erlaubt. Richtigerweise wird man demgegenüber davon auszugehen haben, dass die Aktivierung einer Eigensicherungsmaßnahme zwei personelle Voraussetzungen besitzt, um sich im Rahmen der Grundrechtsschranke zu halten: Die Anwesenheit des VE und die des „Betroffenen", ohne dessen Wissen die Maßnahme zulässig ist. In der Abwesenheit einer der beiden können die Voraussetzungen der Maßnahme also nicht vorliegen (ähnlich *Graulich*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, § 16 BKAG Rdnr. 10, der die Verfassungsmäßigkeit der Parallelvorschrift im BKAG allerdings nicht anzweifelt). Daraus folgt, dass eine akustische wie optische Überwachung einer Wohnung erst mit dem Betreten der Wohnung durch den VE beginnen darf. Eine bereits – ggf. kurz – vorher einsetzende Überwachung kann ebenso wenig verfassungsrechtlich gerechtfertigt werden, wie das nach dem Verlassen einer Wohnung durch einen VE der Fall ist.

III. Verwendung von Daten zur Gefahrenabwehr

Nach § 28a Abs. 4 S. 3 BPolG-E sollen Daten, die aus Maßnahmen der Eigensicherung in Wohnungen stammen, nach einer Rechtmäßigkeitskontrolle allgemein zur Gefahrenabwehr verwendet werden können. Hierbei handelt es sich um eine Zweckänderung, die rechtfertigungsbedürftig ist. Zwar handelt es sich auch bei Maßnahmen der Eigensicherung um solche, die der Gefahrenabwehr zuzurechnen sind, aber speziell den Schutz des VE bezwecken. Die in der Vorschrift genannte „Gefahrenabwehr" geht über diesen Zweck aber weit hinaus und meint die Gefahrenabwehr in ihrem allgemeinen Sinn. (vgl. dazu auch *Graulich*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, § 16 BKAG Rdnr. 23). Eine anderweitige Verwendung der Daten ist als erneuter Eingriff in das Wohnungsgrundrecht zu betrachten und hat nicht nur den Anforderungen Art. 13 Abs. 5 S. 2 GG zu genügen, sondern muss darüber hinaus mit dem Verhältnismäßigkeitsprinzip vereinbar sein.

Nicht erst nach der jüngeren Rechtsprechung des *BVerfG* gilt, dass Informationen, die durch besonders eingriffsintensive Maßnahmen erlangt wurden, auch nur zu besonders gewichtigen Zwecken benutzt werden können (*BVerfG*, 1 BvR 966/09 u.a., Urt. v. 20. April 2016, Rdnr. 286 m.w.N.). Es kommt demnach darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben neu auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln erhoben werden dürften (hypothetische Datenneuerhebung). Nach diesen Maßstäben ist eine unterschiedslose Verwendbarkeit von den hier interessierenden Daten zu allgemein gefahrenabwehrenden Zwecken verfassungsrechtlich unzulässig. Vielmehr ist an eine solche Verwendungsregelung der Maßstab des Art. 13 Abs. 4 GG anzulegen. Zu verlangen wäre demgemäß die Erforderlichkeit der Datenverwendung zum Zwecke der Abwehr von dringenden Gefahren für die öffentliche Sicherheit. Dabei ist das Verständnis des BVerfG zugrunde zu legen, nach dem der Begriff der dringenden Gefahr nicht nur im Sinne des *qualifizierten* Rechtsgüterschutzes auf das Ausmaß, sondern auch auf die *Wahrscheinlichkeit* eines Schadens Bezug nimmt (zuletzt *BVerfG*, 1 BvR 966/09 u.a., Urt. v. 20. April 2016, Rdnr. 110).

Damit lässt sich feststellen, dass die beabsichtigte Regelung zu unverhältnismäßigen Grundrechtseingriffen ermächtigt. Dieser Umstand ist auch deswegen unverständlich, weil sie im Bereich der Verwendung zu Zwecken der Strafverfolgung (§ 28a Abs. 4 Satz 1 BPolG-E) das Prinzip des hypothetischen Ersatzeingriffs (§ 161 Abs. 2 StPO) explizit anerkennt.

IV. Schutz des Kernbereichs privater Lebensgestaltung

§ 28a Abs. 2 BPolG-E enthält zwar kernbereichsschützende Bestimmungen, beschränkt diese aber auf den Einsatz technischer Mittel zur Eigensicherung. Der Kernbereich privater Lebensgestaltung beansprucht aber gegenüber allen Überwachungsmaßnahmen Beachtung. Können sie typischerweise zur Erhebung kernbereichsrelevanter Daten führen, muss der Gesetzgeber Regelungen schaffen, die einen wirksamen Schutz normenklar gewährleisten (sog. verletzungsgeneigte Datenerhebungsbefugnisse, vgl. *BVerfG*, 1 BvR 966/09 u.a., Urt. v. 20. April 2016, Rdnr. 123).

Der Einsatz von VE ist seinem Sinn nach dazu bestimmt, das Vertrauen von Personen zu gewinnen, um auf diese Weise an Informationen zu gelangen, die ohne ein Vertrauensverhältnis nicht zu erlangen wären. Vor diesem Hintergrund sind dauerhafte VE-Einsätze als Maßnahmen zu verstehen, die geeignet sind, tief in das private Leben einer Person und ihr soziales Netz einzudringen (vgl. *Bergemann*, NVwZ 2015, 1705 [1707]; *Bäcker*, BT-Innenausschuss, A-Drs. 18(4)328 A, S. 10; *Roggan*, GA 2016, 393 [395]). Richtigerweise wird man sogar davon sprechen müssen, dass der Einsatz solcher Personen (nach den großen Lauschangriffen) die eingriffsintensivste Datenerhebungsmethode überhaupt ist, da er nicht nur das erfasst, was die Betroffenen „zufällig" äußern, sondern die VE auch aktiv fragen, die Kommunikation steuern oder in sonstiger Weise Einfluss nehmen können. Alleine die Angst davor, zur Zielperson eines solchen Einsatzes zu werden, kann nicht nur die persönliche Entfaltung hemmen, sondern auch tiefgreifende soziale Störungen hervorrufen (*Bergemann*, in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, Kap H Rn. 85). Es ist nicht einmal ausgeschlossen, dass sich im Zuge eines länger andauernden Einsatzes intime Kontakte zu Zielpersonen entwickeln. Das dürfte in bestimmten Szenen auch polizeilicherseits nicht einmal generell unerwünscht sein, weil sich in dann die Chancen auf Erlangung besonders werthaltiger Informationen erhöhen können.

Die Typik des VE-Einsatzes, die im Wesentlichen in dem Ausnutzen von Vertrauensbeziehungen besteht, lässt eine mögliche Verletzung des Kernbereichs privater Lebensgestaltung keineswegs abwegig erscheinen. Vielmehr sind solche Einsätze geradezu als Paradefall einer verletzungsgeneigten Informationserhebung anzusehen. Das Fehlen von kernbereichsschützenden Bestimmungen in der Befugnis des VE im BPolG-E unterwirft die gesamte Regelung dem Verdikt der Verfassungswidrigkeit (vgl. für § 20g BKAG *BVerfG*, 1 BvR 966/09 u.a., Urt. v. 20. April 2016, Rdnr. 175).

C. Änderung des Artikel 10–Gesetzes

Geplant ist eine Eilfall-Regelung, die zu einer Vorbehalts-Speicherung von TK-Daten berechtigen soll. Hiervon sollen Maßnahmen des BND betroffen sein sowie der Fall, dass bereits der Überwachung unterliegende Fernmeldeverkehrsbeziehungen nach zusätzlichen Telekommunikationsmerkmalen gefiltert werden sollen (BT-Drucks. 18/8702, S. 30). Jedenfalls diese Begründung spricht dafür, dass strategische Beschränkungen betroffen sein sollen.

I. Redaktionelles Versehen?

Die genannte Eilfall-Regelung soll als neuer Satz 3 in § 15 Abs. 6 G10 eingefügt werden. Sie stände sodann im inhaltlichen Zusammenhang mit der bereits bestehenden Eilfall-Regelung, die eine Ausnahme von der grundsätzlich vorherigen Befassung der G10-Kommission vor dem Vollzug einer G10-Maßnahme darstellt (näher dazu *Huber*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, § 15 Artikel 10-Gesetz, Rdnr. 52; *Roggan*, NK-G10, 2012, § 15 Rdnr. 17 f.) und würde Maßnahmen auch schon vor der Anordnung durch das Bundesministerium erlauben. Hiervon betroffen wären sämtliche G10-Maßnahmen, neben Beschränkungen nach §§ 5 und 8 G10 also auch solche nach § 3 G10. Indessen geht es in letztgenannten Konstellationen um Beschränkungen in Einzelfällen, mithin nicht um solche, in denen es um das Filtern von bereits der Überwachung unterliegenden Fernmeldeverkehrsbeziehungen nach zusätzlichen Telekommunikationsmerkmalen geht. Es spricht viel dafür, dass die neue Eilfallkompetenz nach § 15 Abs. 6 Satz 4 eingefügt werden und Maßnahmen nach § 8 G10 betreffen soll.

II. Zur Annahme eingriffsloser „Vorbehaltsspeicherung“

Die Gesetzesbegründung geht davon aus, dass die Speicherung von TK-Daten über einen Zeitraum von 24 Stunden nicht mit Eingriffen in das TK-Grundrecht der betroffenen TK-Nutzer verbunden ist, wenn diese Daten lediglich vorbehalt-

lich einer nachfolgenden Anordnung einer menschlichen Kenntnisnahme unterliegen („Vorbehaltsspeicherung", vgl. BT-Drucks. 18/8702, S. 30).

Nach der Rechtsprechung des *BVerfG* ist ein eingriffsbegründender „Gefährdungstatbestand" lediglich in solchen Fällen abzulehnen, in denen Daten unmittelbar nach ihrer Erfassung technisch wieder spurenlos, anonym und ohne die Möglichkeit, einen Personenbezug herzustellen, ausgesondert werden. Demgegenüber ist von einem Informationseingriff (hier: Eingriff in das TK-Geheimnis) auszugehen, wenn ein personenbezogenes oder personenbeziehbares Datum in einem Speicher festgehalten wird und gegebenenfalls Grundlage weiterer Maßnahmen werden kann (vgl. dazu BVerfGE 120, 378 [399]). Entsprechend verhält es sich bei den TK-Daten, die unter dem Vorbehalt der späteren Anordnung der Beschränkungsmaßnahme bis zu 24 Stunden gespeichert und danach nutzbar sein sollen. Während dieses mehrstündigen Zeitraums bestehen für die Daten sämtliche „Risiken", die typischerweise mit einer Datenspeicherung – bis hin zu rechtswidrigen Zugriffen – verbunden sind. Damit wird gleichsam die spezifische Persönlichkeitsgefährdung für Verhaltensfreiheit und (hier: telekommunikative) Privatheit ausgelöst, die das TK-Grundrecht schützen soll (vgl. zur informationellen Selbstbestimmung als allgemeinerer Gewährleistung BVerfGE 120, 378 [400]).

Als Konsequenz ergibt sich hieraus, dass es durch eine alleine geheimdienstliche Entscheidung zu einem Eingriff in das TK-Geheimnis kommen soll, bei dem ein vorgelagerter, verfahrensmäßiger Grundrechtsschutz nicht einmal durch die ministerielle Anordnung gewährleistet sein soll. Dies ist nach hier vertretener Ansicht mit der Bedeutung des TK-Grundrechts nicht vereinbar. Dies gilt sowohl im Fall des vermuteten redaktionellen Versehens (s. o.) wie auch bei einer Einfügung der Eilfallregelung nach Satz 4 von § 15 Abs. 6 G10.

Für Nachfragen stehe ich in der Anhörung gerne zur Verfügung.

gez.
Prof. Dr. Fredrik Roggan