HUMANISTISCHE UNION e.V. – Haus der Demokratie und Menschenrechte
Greifswalder Straße 4, 10405 Berlin

Tel.: 030 / 20 45 02 –56
Fax: 030 / 20 45 02 –57
info@humanistische-union.de
www.humanistische-union.de

Humanistische Union

An die Mitglieder des
Innenausschuss des Thüringer Landtags
Jürgen-Fuchs-Straße 1

99096 Erfurt

Berlin, 9.9.2013

Stellungnahme der Humanistischen Union

zum Gesetzentwurf der Landesregierung „Thüringer Gesetz zur Änderung des Polizeiaufgabengesetzes und des Ordnungsbehördengesetzes“
Drs. 5/6118 vom 21.5.2013

Die Humanistische Union bedankt sich für die Einladung, zu dem o.g. Gesetzentwurf Stellung zu nehmen. Aufgrund der umfangreichen Vorlage und der urlaubsbedingten Verhinderung zahlreicher ExpertInnen unseres Vereins können wir nur zu ausgewählten Aspekten des Vorhabens Stellung nehmen.

Übersicht:

I. Vorbemerkungen

Ein unabweisbarer Novellierungsbedarf ergibt sich aus der Entscheidung des Thüringer Verfassungsgerichtshofes[1] zu zahlreichen verfassungswidrigen Bestimmungen des bisherigen Gesetzes. Daneben sollten bei einer Neuregelung jedoch weitere sicherheitspolitische Debatten und Entwicklungen berücksichtigt werden, deren Auswirkungen auf die präventive Polizeiarbeit nicht minder wichtig sind.
Das betrifft zum einen die bisherigen Ergebnisse der Untersuchungen zum Versagen zahlreicher Behörden bei der Verhinderung / Aufklärung der NSU-Mordserie. Angesichts der herausragenden Stellung thüringischer Sicherheitsbehörden ist es angezeigt, dass sich der thüringische Landesgesetzgeber dieser Aufgabe stellt. Dazu findet sich im vorliegenden Gesetzentwurf leider keinerlei Ansatzpunkt. Auch wenn es für viele Fragen noch verfrüht erscheint, das polizeiliche wie geheimdienstliche Handeln im NSU-Kontext abschließend zu bewerten, so benennen die bisher vorliegenden Untersuchungen[2] übereinstimmend gravierende Defizite bei Anwerbung, Einsatz und Führung von V-Leuten und der fehlenden Prüfung bzw. (Nicht-)Auswertung der von ihnen gelieferten Informationen. Den von Sicherheitsbehörden immer wieder beschworenen Informations- und damit Sicherheitslücken, die bei einem Verzicht auf V-Leute entstünden widersprechen die jetzt vorliegenden Untersuchungen. Demnach seien die von V-Leuten gelieferten Informationen oft wenig aussagekräftig, bisweilen belanglos.
Die Humanistische Union spricht sich seit langem für einen Verzicht auf das rechtspolitisch äußerst fragwürdige Instrument der V-Leute aus.[3] Doch selbst, wenn man weiter an diesem Instrument festhalten will, ist es aufgrund der gesetzgeberischen Verantwortung geboten, bis zu einer gesetzlichen Regelung, die den jetzt erkannten Schwachstellen des Einsatzes von „Vertrauenspersonen“ Einhalt gebietet, auf dieses Instrument (vorerst) zu verzichten. Der weitere Einsatz solcher V-Leute ohne eine explizite gesetzliche Regelung ihres Einsatzes ist – gerade im Vergleich mit der Regelungsdichte der technischen Ermittlungsinstrumente, die weniger Tendenzen zu Missbrauch und „Verselbständigung“ aufweisen – unter rechtsstaatlichen Gesichtspunkten unverantwortlich.

Empfehlung: Die Humanistische Union empfiehlt, zumindest bis zum Erlass einer umfassenden gesetzlichen Regelung auf den Einsatz sog. V-Leute komplett zu verzichten. § 34 Abs. 2 Nr. 5 PAG-E sowie alle darauf verweisenden Regelungen sind zu streichen.

Die Notwendigkeit zu einer weiteren Neubewertung heimlicher Ermittlungsmaßnahmen ergibt sich auch aus den in den letzten Monaten bekannt gewordenen Überwachungsmaßnahmen us-amerikanischer Sicherheitsbehörden. Der Umfang und die Reichweite dieser Überwachung werfen zahlreiche Fragen auf, etwa: Inwiefern deutsche Sicherheitsbehörden gewährleisten können, dass die auf ihre Anordnung oder von ihnen erhobenen Daten nicht auch von Dritten genutzt werden? Vor allem aber beweist die Konzentration der amerikanischen Behörden auf die Auswertung sog. Kommunikations-Metadaten (Verbindungsdaten), dass deren inhaltliche „Aussagekraft“ (und damit auch deren grundrecht-

[1] TH-VerfGH 19/09 vom 21.11.2012.
[2] Zwischenbericht des Thüringer Untersuchungsausschusses 5/1 vom 7.3.2013, LT-Drs. 5/5810, S. 533 ff.; Beschlussempfehlung und Bericht des 2. Untersuchungsausschusses nach Artikel 44 GG [NSU-Untersuchungsausschuss] vom 22.8.2013, BT-Drs. 17/14600, S. 856 f.; BMI / Ständige Konferenz der Innenminister und -senatoren der Länder, Abschlussbericht der Bund-Länder-Kommission Rechtsterrorismus vom 30. April 2013 - Zusammenfassung der Empfehlungen, S. 8 ff.
[3] Humanistische Union: Memorandum zum Under Cover Agent. Auf dem Wege zu einer halbkriminellen Geheimpolizei. München 1984.

liche Sensitivität) weitaus höher als bisher angenommen ist. Ein amerikanischer IT-Experte kam jüngst zu dem Urteil: "In some cases, telephony metadata can reveal information that is even more sensitive than the contents of the communication."[4] Dies stützt sich vor allem auf folgende Umstände:[5]

- die Möglichkeit der automatisierten Auswertung von Metadaten im großem Maßstab,
- die Möglichkeit, Beziehungen zwischen den Beteiligten der Kommunikation aus den äußeren Umstanden ihrer Kommunikation zu rekonstruieren
- die Aggregation großer Bestände an Metadaten kann mehr Informationen über eine Person enthalten, als die Auswertung ihrer Kommunikationsinhalte.

II. Querschnittsfragen

Zunehmende Ermittlungen im Gefahrenvorfeld

Mit ihrem Gesetzentwurf befördert die Landesregierung eine Entwicklung, die die Humanistische Union seit Jahren mit Sorge betrachtet: Staatliche Eingriffsbefugnisse werden kontinuierlich ins Gefahrenvorfeld verlagert, in dem (noch) keine konkreten Bedrohungen für Rechtsgüter auszumachen sind. Mit zunehmender Verlagerung ins Gefahrenvorfeld verschwimmt die Unterscheidbarkeit zwischen legalem und strafbaren Handeln; ob das beobachtbare Verhalten irgendwann in strafbare Handlungen mündet, können in diesem Stadium selbst die besten Ermittler kaum erkennen. Die zunehmende Überwachung von – im Nachhinein erwiesenermaßen – legalem Handeln beschädigt nicht nur die Freiheitsgarantien unserer Verfassung, sondern gefährdet auch unsere Rechtsordnung. Erhard Denninger hat darauf hingewiesen, dass die ‚Versicherheitlichung an der Substanz normativer Errungenschaften' des Rechtsstaates zehre.[6] Diese Entwicklung gilt es zu stoppen. In einem Rechtsstaat müssen unbescholtene Bürger von der Staatsgewalt in Ruhe gelassen werden. Für Grundrechtseingriffe fern jeglicher Wahrscheinlichkeit eines Schadenseintritts besteht keine Notwendigkeit.

Im Gesetzentwurf schlägt sich diese Tendenz in der Festlegung der materiellen Eingriffsschranken für die verschiedenen Ermittlungsmaßnahmen nieder: Für fast alle Formen der heimlichen Datenerhebung (alleinige Ausnahmen: § 34d Abs. 1 Unterbrechung der TK; § 35 Abs. 1 Wohnraumüberwachung) werden mehr oder weniger gewichtige Rechtsgüter benannt, deren Gefährdung den Einsatz der jeweiligen Maßnahmen rechtfertigen soll. Allerdings geht aus dem Gesetz nicht hervor, in welcher Art und Weise diese Rechtsgüter gefährdet sein müssen oder welcher Grad der Gefährdung vorliegen muss, um die Voraussetzungen für eine Anwendung der Norm zu erfüllen. Die Vorschrift genügt deshalb nicht den verfassungsrechtlichen Anforderungen an die Bestimmtheit. Es läge im Ermessen der Polizeibehörden, beispielsweise eine Telekommunikationsüberwachung (TKÜ, § 34a Abs. 1) bereits bei einer abstrakten Gefährdung einzusetzen, bei der noch gar nicht erkennbar ist, ob sich eine konkrete Gefahrenlage hinsichtlich der benannten Rechtsgüter überhaupt ergeben wird. Das wäre offenkundig verfassungswidrig, zumal die Anwendung nicht auf

[4] Zu den technischen Hintergründen s. Prof. Edward W. Felten, Declaration to the United States District Court – Southern District of New York, Case No. 13 cv - 03994 (WHP) ECF CASE, S. 15. Abrufbar unter http://ia601803.us.archive.org/22/items/gov.uscourts.nysd.413072/gov.uscourts.nysd.413072.27.0.pdf (Abruf: 9.9.2013).
[5] A.a.O.
[6] Denninger in Koch (Hrsg.), Terrorismus – Rechtsfragen der äußeren und inneren Sicherheit, Baden-Baden 2002, S. 90.

die Verantwortlichen der mutmaßlich entstehenden Gefahrenlage begrenzt ist. **Eine Begrenzung auf die konkrete Gefährdung der genannten Rechtsgüter ist unumgänglich.** Hinzu kommt, dass nahezu alle heimlichen Ermittlungsmaßnahmen (Ausnahme: Unterbrechung der TK, § 34d Abs. 2 S. 2) quasi unbefristet fortgeführt werden können. Zwar sind die Einzelanordnungen befristet (z.B. TKÜ: 3 Monate), jedoch ist eine beliebige Verlängerung möglich. Mit zunehmender Dauer der Überwachung wird nicht nur der damit verbundene Grundrechtseingriff verstärkt, es stellt sich auch verstärkt die Frage nach der Validität der Gefahrenprognose, wenn sich die Gefährdung auch nach u.U. jahrelanger Beobachtung nicht einstellt. Deshalb sollte (ungeachtet der weiteren Änderungsvorschläge) für alle Eingriffsschwellen nicht nur eine konkrete, sondern auch eine gegenwärtige Gefahr vorgeschrieben werden, bei der auf Grund von Tatsachen anzunehmen ist, dass die abzuwendende Gefahr mit großer Wahrscheinlichkeit in absehbarer Zeit eintreten könnte.

Empfehlung: In den §§ 34 Abs. 1 S. 1, 34a Abs. 1 S. 1, 34b Abs. 1 S. 1, 34c Abs. 1 S. 1 und 34e Abs. 1 S. 1 wird jeweils das Wort Gefahr durch „gegenwärtige, konkrete Gefahr" ersetzt.

Schutz des Kernbereichs privater Lebensgestaltung (§ 34 Abs. 1 S. 2, § 34 a Abs. 1 S. 3)

Der Entwurf besagt sowohl für die verdeckten Datenerhebungen generell als auch für die Telekommunikationsüberwachung, dass jene dann unzulässig seien, „*wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch die Maßnahme* allein *Kenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden.*"
Diese Regelung wiederholt entsprechende Vorgaben zum Kernbereichsschutz aus der Strafprozessordnung (§ 100a Abs. 4 S. 1 StPO), die vom Bundesverfassungsgericht im Wege der Rechtsauslegung zwar als verfassungskonform erklärt wurden, nichtsdestotrotz aber sehr missverständlich bleiben und im Sinne der Normklarheit korrigiert werden sollten. Die Formulierung „*allein*" suggeriert, dass Ermittlungsmaßnahmen von vornherein nur dann unzulässig seinen (und deshalb unterlassen werden müssen), wenn sie *ausschließlich* intime Informationen zutage fördern. Eine solche Situation ist kaum vorstellbar, denn es wird kaum ein Gespräch geben, in dem sich die Beteiligten nicht auch über öffentliche oder belanglose Dinge austauschen. Ein so naheliegendes Verständnis dieser Vorschrift aber führt den verfassungsrechtlich gebotenen Schutz des Kernbereichs ad absurdum, er würde faktisch nie wirksam.
Dagegen hat das BVerfG in seiner Entscheidung zur o.g. Vorschrift des Kernbereichsschutzes bei der strafprozessualen TKÜ bekräftigt, dass die Norm nicht in dieser Weise ausgelegt werden dürfe: „*Bestehen im Einzelfall konkrete Anhaltspunkte dafür, dass eine bestimmte Datenerhebung den Kernbereich privater Lebensgestaltung berühren wird, hat sie grundsätzlich zu unterbleiben …*"[7] Lediglich für den Fall, das kernbereichsrelevante Inhalte gezielt (d.h. vorsätzlich) mit jenen Informationen verknüpft werden, auf die sich die Ermittlungen richten, könne die Ermittlungsmaßnahme im Sinne einer effektiven Strafverfolgung (hier dann: Gefahrenabwehr) nicht von vornherein ausgeschlossen werden (ebd.). Dafür müssen jedoch konkrete Tatsachen vorliegen, die eine solche Annahme rechtfertigen.

Empfehlung: Das Wort „allein" wird an beiden Stellen ersatzlos gestrichen.

[7] BVerfG, 2 BvR 236/08 vom 12.10.2011, Rn. 210.

Im Übrigen ist nicht ersichtlich, warum der Schutz des Kernbereichs privater Lebensgestaltung bei den verschiedenen Ermittlungsmaßnahmen unterschiedlich konsequent verfolgt wird. Der Schutzanspruch ergibt sich aus Art. 1 Abs. 1 GG, dem Schutz der menschlichen Würde, und ist als solches nicht abwägbar. Zwar ist es richtig, dass verschiedene Ermittlungsmethoden grundsätzlich eine unterschiedliche Nähe zum Kernbereich aufweisen. Wie in der Einleitung (anhand der TK-Verbindungsdaten) jedoch ausgeführt, ist diese Kernbereichs-Relevanz keine feststehende Größe, sondern kann sich durch eine zunehmende Ausbreitung der überwachten Technik Alltag sowie durch neue Methoden der Datenauswertung ohne Weiteres und innerhalb kurzer Zeiträume steigern. Um derartigen Entwicklungen vorzubeugen und die Polizeibehörden für einen aktiven Schutz des Kernbereichs bei allen heimlichen Datenerhebungen zu sensibilisieren, sollte der Kernbereichsschutz einheitlich, auf einem hohen Niveau analog den Bestimmungen bei der akustischen Wohnraumüberwachung (§ 35 Abs. 6) umgesetzt werden.

Überwachung der Nachrichtenmittler (§ 34 Abs. 1 Ziff. 2)

Der Entwurf sieht vor, dass sämtliche Maßnahmen der verdeckten Datenerhebung auch auf sog. Nachrichtenmittler angewandt werden dürfen. Dabei handelt es sich um Personen, die selbst überhaupt keinen (nicht einmal einen unwissentlichen) Beitrag zu den prognostizierten Gefahren leisten müssen, sondern lediglich Mitteilungen von den Gefahrverantwortlichen entgegennehmen bzw. an diese weitergeben.

Dieser Vorschlag ist in mehrfacher Hinsicht zu unbestimmt:
a) Weder aus dem Gesetzestext noch aus der Begründung geht hervor, um welche Art von Mitteilungen es sich dabei handeln soll, ob diese überhaupt einen Bezug zum gefahrvorbereitenden Handeln aufweisen müssen oder nicht. Nach dem Wortlaut des Gesetzes könnte auch der Zeitungsverkäufer im Laden an der Ecke, bei dem der Verdächtige seine Zeitung erwirbt, überwacht werden.
b) Der Einsatz der verdeckten Ermittlungsmaßnahmen gegenüber den Nachrichtenmittlern beschränkt sich nicht auf die Überwachung der maßgeblichen Kommunikationsmittel. Allein die Tatsache, dass er/sie Mitteilungen entgegen nimmt bzw. weiterleitet soll demnach auch längerfristige Observationen, Lauschangriffe oder Standortbestimmungen rechtfertigen. Dies ist nicht zuletzt aufgrund der unter a) aufgeführten unbestimmten Beteiligung der Nachrichtenmittler am Gefahrenhandeln absolut unverhältnismäßig.

Einheitliche Subsidiaritätsklausel für alle verdeckten Datenerhebungen

Mit sog. Subsidiaritätsklauseln wird üblicherweise der Vorrang offener Ermittlungs- bzw. Gefahrenabwehrmethoden gegenüber verdeckten Maßnahmen festgeschrieben. Damit setzt der Gesetzgeber das Übermaßverbot um. Jenes verlangt vom Gesetzgeber als auch von der ausführenden Polizeibehörde, bei einer möglichen Wahl zwischen verschiedenen polizeilichen Sanktionen jeweils das mildeste Mittel auszuwählen, bei dessen Einsatz der Grundrechtseingriff für die betroffenen Bürgerinnen und Bürger minimal gehalten werden kann. Verdeckte polizeiliche Datenerhebungen greifen – im Gegensatz zur offenen Erhebung der gleichen Daten – tiefer in die grundrechtlichen Schutzbereiche ein; allein schon wegen der fehlenden Erkennbarkeit des polizeilichen Handelns und der mangelnden Möglichkeiten eines nachträglichen Rechtsschutzes.

Leider präsentiert der Gesetzentwurf keinen konsistenten Ansatz zur Umsetzung der Subsidiaritätsprüfung. Für immerhin fünf verdeckte Ermittlungsinstrumente wird keinerlei Prüfung auf weniger belastende Maßnahmen vorgeschrieben. Für die verbleibenden Maß-

nahmen kann auch die hierarchische Ausprägung der Subsidiaritätsklauseln nicht überzeugen:

- keine Subsidiarität & keine Erforderlichkeitsprüfung:
  (§ 34 Abs. 2, 4 und 5 verdeckte Ermittler, verdeckt ermittelnde Beamte, V-Leute)
- keine Subsidiarität: „soweit dies zur Abwehr einer Gefahr erforderlich ist“
  (§ 34e Bestandsdatenabfrage),
- keine Subsidiarität: „zwingend erforderlich“
  (§ 34d TK-Unterbrechung hinsichtlich des Verantwortlichen)
- einfache Subsidiarität: „auf andere Weise aussichtslos oder wesentlich erschwert“
  (§ 34a TKÜ, 34b TK-Verkehrsdaten/Nutzungsdaten, 34c Mobilgeräte-Identifizierung/-Lokalisierung)
- mittlere Subsidiarität: „auf andere Weise unverhältnismäßig erschwert oder aussichtslos“
  (§ 35 Wohnraumüberwachung)
- strenge Subsidiarität: „durch andere Mittel nicht abgewehrt werden kann“
  (§34d TK-Unterbrechung hinsichtlich Dritter)

Die Erfahrung zeigt, dass Subsidiaritätsbestimmungen wie „wesentlich erschwert“ oder „unverhältnismäßig erschwert“ in der Praxis faktisch keinerlei begrenzende Wirkung für den
den Einsatz verdeckter Maßnahmen entfalten, weil sie zu unbestimmt sind. So gehen die Strafverfolgungsbehörden, denen ein Beurteilungsspielraum zugestanden wird, beispielsweise von einer unverhältnismäßigen Erschwerung der Ermittlungen aus, wenn alternative Aufklärungsmittel zu einem höherem Arbeitsaufwand führen und in der Konsequenz andere Ermittlungsverfahren vernachlässigt würden. Selbst gerichtlich wäre kaum nachvollziehbar überprüfbar, ob durch die erwogene Nichtanordnung eines großen Lauschangriffs eine Vernachlässigung anderen Ermittlungen zu befürchten war oder eben nicht.[8] Angesichts solcher Auslegungsschwierigkeiten bestehen berechtigte Zweifel daran, ob derart dehnbare Tatbestandsmerkmale geeignet sind, den Entscheidungsspielraum der Polizeibehörden in der Subsidiaritätsprüfung vorzugeben. Um die Wirksamkeit der Subsidiaritätsklauseln zu verbessern, sollten sie inhaltlich einheitlich und sprachlich gleich lautend formuliert werden.

Hinzu kommt: Die Arbeit der Strafverfolgungs- und Gefahrenabwehrbehörden verzeichnet seit Jahren einen Trend zu verdeckten Ermittlungsmethoden. Kontinuierlich steigen die Zahlen für Bestandsdatenabfragen, TK-Überwachungen, Funkzellenabfragen und „stille SMS“. Dieser Trend gefährdet die rechtsstaatlichen Grundlagen der Polizeiarbeit und untergräbt das Vertrauen der Bevölkerung in diese Behörde. Diese Entwicklung lässt sich nach Auffassung der Humanistischen Union nur stoppen, wenn der Gesetzgeber klare Vorgaben dafür macht, dass verdeckte Maßnahmen wieder als *ultima ratio* der Polizeiarbeit verstanden werden. Sie sind nur dann anzuwenden, wenn alle Möglichkeiten einer offenen, direkten Sachverhaltsermittlung bzw. Gefahrenbeseitigung ausgeschöpft wurden. Deshalb sollte bei allen verdeckten Datenerhebungsmethoden die strenge Subsidiarität eingeführt werden.

Empfehlung: Um den Grundsatz der offenen und transparenten Polizeiarbeit wieder zu beleben, empfehlen wir eine strikte Subsidiaritätsklausel, die einheitlich für alle zuzulas-

[8] Vgl. Roggan in: Roggan/Kutscha (Hrsg.), Handbuch der Inneren Sicherheit, 2. Auflage 2006, S. 113; Albrecht/Dorsch/Krüpe, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen - Abschlussbericht (Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht), Freiburg 2003, S. 20.

senden verdeckten Ermittlungsmaßnahmen (und unabhängig von ihren materiellen Voraussetzungen) gelten soll. Sie lautet schlicht: Die jeweilige Maßnahme ist nur zulässig, wenn die Abwehr der Gefahr auf andere Weise aussichtslos wäre.

Benachrichtigung der Betroffenen (§ 36 Abs. 3-6)

Die Benachrichtigung über heimliche Ermittlungsmaßnahmen ist aus Sicht der Betroffenen das einzig verbleibende Korrektiv, um die Zulässigkeit der Ermittlungsmaßnahmen prüfen zu lassen und ggf. die Löschung rechtswidrig erlangter Daten durchsetzen zu können.

Nach Absatz 4, Satz 2 kann die Benachrichtigung über einen früheren Einsatz verdeckter Ermittler oder von V-Leuten unterbleiben, „*wenn die Möglichkeit der weiteren Verwendung der verdeckt handelnden Personen durch die Benachrichtigung gefährdet wäre und unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber den Betroffenen das öffentliche Interesse an der Weiterverwendung überwiegt*."
Das hier in Anspruch genommene öffentliche Interesse reduziert sich – gerade angesichts der oben benannten generellen Zweifel am Einsatz von V-Leuten („Vertrauenspersonen") – vor allem auf ein polizeiliches Interesse zur weiteren Verwendung ihrer menschlichen Quelle. Dieses Interesse kann aus unserer Sicht in keinem Fall den berechtigten Anspruch auf nachträglichen Rechtsschutz aufwiegen. Das Bundesverfassungsgericht hat wiederholt darauf hingewiesen, dass den von verdeckten polizeilichen Maßnahmen Betroffenen ohne nachträgliche Information ihr Anspruch auf gerichtlichen Rechtsschutz (Art. 19 Abs. 4 GG) verwehrt bleibt. Die Einschränkung der Benachrichtigung entspreche einem doppelten Grundrechtseingriff: sie verstärke einerseits das Gewicht des materiellen Eingriffs durch die Ermittlungsmaßnahme (z.B. Artikel 10, 13 GG), zudem schränke sie die Rechtsschutzgarantie aus Art. 19 Abs. 4 GG ein.[9] Das Interesse an einer nachträglichen Benachrichtigung über heimliche, staatliche Ermittlungsmaßnahmen hat deshalb Verfassungsrang. Das behördliche Interesse am Einsatz von verdeckten Ermittlern und V-Leuten (deren Erforderlichkeit oder Alternativlosigkeit nicht einmal gesetzlich vorgeschrieben ist, s.o.) muss dahinter zurücktreten.

Empfehlung: Die Humanistische Union empfiehlt, § 36 Abs. 4 Satz 2 des PAG-E ersatzlos zu streichen.

Gemäß § 36 Absatz 5 Satz 3 PAG-E kann nach fünf Jahren der zuständige Amtsrichter in einem geheimen Verfahren die nachträgliche Benachrichtigung dauerhaft aussetzen, wenn die von der Behörde vorgebrachten Gründe weiter bestehen. Damit würde der oben beschriebene, doppelte Grundrechtseingriff abschließend goutiert, ohne dass die Betroffenen auch nur einmal angehört wurden. Aus den genannten Erwägungen ist daher eine abschließende Aussetzung der Benachrichtigung abzulehnen. Nach fünf Jahren sollte – eine hinreichende Begrenzung der polizeilichen Maßnahmen auf konkrete, gegenwärtige Gefahren vorausgesetzt – auch der eigentliche Ermittlungszweck erledigt und durch die Information an die Betroffenen nicht mehr gefährdet sein. Eine darüber hinausgehende Rückstellung der Benachrichtigung ist nicht angemessen.

Empfehlung: § 36 Abs. 5 Sätze 3 und 4 sind zu ersetzen durch „Spätestens fünf Jahre nach Beendigung der Maßnahme sind die Beteiligten gem. Abs. 3 unverzüglich zu benachrichtigen."

[9] BVerfG, 1 BvR 2378/98 vom 3.3.2004, Rn. 288ff (292).

III. Zu einzelnen Bestimmungen des PAG-E

§ 34 a Abs. 1 Überwachung der Telekommunikation

Wie eingangs ausgeführt, zeichnet sich der moderne Alltag durch die zunehmende Bedeutung der Telekommunikation (TK) für die Gestaltung sozialer Beziehungen aus. Die Überwachung der TK ist daher geeignet, Einblick in nahezu sämtliche Lebensbereiche eines Betroffenen zu verschaffen. Eine Begründung, warum zu rein präventiven Zwecken ein solch weitreichender Grundrechtseingriff notwendig sein soll, bleibt der Gesetzentwurf schuldig. Zudem ist die Maßnahme, wie oben ausgeführt, nicht auf konkrete, gegenwärtige Gefahrenlagen begrenzt, sondern würde auch langfristige „Strukturermittlungen" erlauben. Die Humanistische Union lehnt die vorgeschlagene Regelung zur präventiven Überwachung der Telekommunikation daher grundsätzlich ab.

Empfehlung: Die Humanistische Union empfiehlt, § 34a PAG-E ersatzlos zu streichen.

§ 34 a Abs. 2 und 3 Quellen-Telekommunikationsüberwachung

Das Abhören der paketvermittelten, internetgestützten Kommunikation – vor allem wenn diese in verschlüsselter Form stattfindet – stellt nicht nur besondere technische Hürden für den Zugriff auf die Inhaltsdaten auf. Diese werden bei der sog. Quellen-TKÜ dadurch zu umgehen versucht, dass zumindest ein Endgerät der beteiligten Kommunikationspartner infiltriert wird, um die Inhalte des Austauschs vor der Verschlüsselung (beim Sender) bzw. nach der Entschlüsselung (beim Empfänger) abzugreifen. Dies setzt einen Eingriff in die Integrität und Vertraulichkeit der genutzten IT-Systeme (Computer, Smartphones o.ä.) voraus, weshalb das Bundesverfassungsgericht bereits in seiner Entscheidung zur Online-Durchsuchung[10] auf die besonderen Gefahrenpotentiale einer Quellen-TKÜ eingegangen ist. Diese bestehen u.a. in:

- dem Problem der Identifizierung und Infiltration des zu überwachenden Zielsystems: insbesondere bei der Einbringung der Überwachungssoftware von außen ist vorab kaum feststellbar, ob der richtige Zielrechner kompromittiert oder unbeteiligte Dritte überwacht werden;[11]
- der technischen wie rechtlichen Absicherung, dass nur auf Inhalte der laufenden Kommunikation und nicht auf andere Daten des zu überwachenden Systems zugegriffen wird (nur unter dieser Voraussetzung lässt das BVerfG eine Infiltration des Systems nach dem Maßstäben von Art. 10 GG zu)[12]
- die Schwierigkeiten einer beweissicheren Datenerhebung: Es ist sicher zu stellen, dass die erhobenen Informationen weder von Dritten auf dem Zielsystem platziert noch durch die Quellen-TKÜ selbst (unbeabsichtigt) verändert wurden.
- die technische Absicherungen gegen den Missbrauch des Infiltrationszugangs durch Dritte.

In der bisherigen Anwendung der Quellen-TKÜ haben sich die technischen Hürden als sehr folgenreich erwiesen. Alle bisher bekannten bzw. von öffentlichen Stellen untersuch-

[10] BVerfG, 1 BvR 370/07 vom 27.2.2008.
[11] So der technische Sachverständige des BKA in der mündlichen Anhörung vor dem BVerfG zur Klage gegen die „Online-Durchsuchung" im Verfassungsschutzgesetz NRW am 10.10.2007.
[12] BVerfG, 1 BvR 370/07 vom 27.2.2008, Rn. 188-190; s.a. Ulf Buermeyer: Zum Begriff der „laufenden Kommunikation" bei der Quellen-Telekommunikationsüberwachung („Quellen-TKÜ"). Ein Beitrag zu den gebotenen legislativen Konsequenzen aus der Online-Durchsuchungs-Entscheidung des BVerfG, Strafverteidiger 7/2013, S. 470 ff.

ten Programme wiesen erhebliche Mängel auf, die keinen rechtskonformen Einsatz zur Quellen-TKÜ erlauben:[13]

- Die notwendigen Programme zur Infiltration des Zielsystems sowie der Ausleitung der Kommunikationsdaten wurden von Drittanbietern (wie DigiTask) bereitgestellt, da die öffentlichen Stellen nicht über das erforderliche Know-how verfügten.
- Einzelne Analysen der Funktionsweisen dieser Programme von Drittanbietern wiesen erhebliche Mängel hinsichtlich der o.g. Anforderungen auf: Neben den Kommunikationsdaten wurden weitere Daten aus den überwachten Computern erhoben (z.B. Screenshots), die einer Online-Durchsuchung vorbehalten wären; die ausgeleiteten Kommunikationsdaten wurden auf amerikanischen Servern zwischengespeichert; die Fernsteuerung der Überwachungsprogramme ließ sich mit einfachem Aufwand von Dritten übernehmen …
- Der Software-Quellcode dieser Programme konnte aufgrund der Schutzansprüche der Drittanbieter nicht überprüft werden (Schutz der Urheberrechte und ihrer Geschäftsgeheimnisse). Damit lässt sich jedoch nicht überprüfen, ob neben den staatlichen Behörden auch andere Personen/Stellen Zugriff auf die Überwachungsschnittstelle haben.

Wie eine Quellen-TKÜ derart technisch umgesetzt werden kann, dass sie den verfassungsrechtlichen Vorgaben des BVerfG genügt, ist derzeit nicht ersichtlich. Mit Blick auf die rechtlichen Risiken der bisherigen Lösungen sollte daher auf dieses Instrument in Gänze verzichtet werden. Angesichts der inzwischen vorhandenen Alternativen zur Quellen-TKÜ birgt ein solcher Verzicht in praktischer Hinsicht auch kein größeres Sicherheitsrisiko. So verpflichtet sich der zur Firma Microsoft gehörende Anbieter Skype (Marktführer bei den VOIP-Angeboten) wie viele andere Anbieter auch in seinen eigenen Datenschutzrichtlinien zur Zusammenarbeit mit den Strafverfolgungs- und Ermittlungsbehörden.[14] Sofern Dienstleister einen derartigen Zugang zum Abhören der verschlüsselten Internetkommunikation anbieten, müsste aus Subsidiaritätsgründen eine Quellen-TKÜ ohnehin unterbleiben, weil die Kommunikation über den weniger fehleranfälligen Weg der „normalen“ TKÜ beim Anbieter erfolgen kann.

Empfehlung: § 34 a Abs. 2 und 3 PAG-E sind ersatzlos zu streichen; die Nummerierung der nachfolgenden Sätze anzupassen und sonstige Verweise auf die beiden Absätze zu entfernen.

---

[13] Bundesbeauftragter für den Datenschutz und die Informationsfreiheit: Bericht gem. § 26 Abs. 2 BDSG über Maßnahmen der Quellen-Telekommunikationsüberwachung bei den Sicherheitsbehörden des Bundes vom 31.1.2012, unter http://linksunten.indymedia.org/de/system/files/data/2012/02/4364782314.pdf (Abruf: 7.9.2013); Bayerischer Landesbeauftragter für den Datenschutz: Prüfbericht Quellen-TKÜ vom 30.7.2012, unter http://www.datenschutz-bayern.de/0/bericht-qtkue.pdf (Abruf: 7.9.2013); Wolfgang Hoffmann-Riem: Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, Juristenzeitung 63 (21/2008), S. 1009 (mit Bezug auf die Anhörung der technischen Sachverständigen vor dem Bundesverfassungsgericht); Chaos Computer Club: Analysen zum Staatstrojaner, unter http://www.ccc.de/de/tags/staatstrojaner (Abruf: 7.9.2013).

[14] S. Microsoft, Skype-Datenschutzrichtlinien (Abschnitt 3), unter http://www.skype.com/de/legal/privacy/#disclosureOfInformation (Abruf: 7.9.2013). Die Kooperationsbereitschaft belegt auch der öffentlich gewordene Anforderungskatalog des Anbieters: Skype Communications SARL, Responding to Law Enforcement Records Requests, unter http://cryptome.org/isp-spy/skype-spy.pdf (Abruf: 7.9.2013).

§ 34 d PAG-E Unterbrechung/Verhinderung der Telekommunikation

Die Gesetzesbegründung (S. 35) sowie die herangezogene Entscheidung des Thüringer Verfassungsgerichtshofes[15] (hier unter Bezugnahme auf die IMSI-Catcher-Entscheidung des Bundesverfassungsgerichts[16]) behaupten beide, dass eine Unterbrechung bzw. Verhinderung der Telekommunikation nicht in den Schutzbereich des Fernmeldegeheimnisses (Art. 7 Landesverfassung bzw. Art. 10 GG) eingreife. Diese Verweise sind in mehrfacher Hinsicht irreführend:
Die in Bezug genommene Nichtannahme-Entscheidung des BVerfG bezieht sich auf eine Beschwerde gegen den Einsatz sog. IMSI-Catcher zur Ermittlung von Mobilgerätekennungen (IMSI/IMEI) oder zur kurzfristigen Ortung von Verdächtigen. Sie ist in rechtlicher wie tatsächlicher Form nicht mit der hier geplanten längerfristigen Unterbrechung/Verhinderung der TK vergleichbar.

a) Die damals verhandelten Rechtsgrundlagen und die entsprechenden technischen Geräte fielen nach der Argumentation des BVerfG weder unter den Schutzbereich der allgemeinen Handlungsfreiheit (Art. 2Abs. 1 GG) noch den des Fernmeldegeheimnisses (Art. 10 GG), weil ihr Einsatz nur eine kurzzeitige Störung der Empfangs- und Kommunikationsbereitschaft bewirke – während des nur wenige Sekunden dauernden Anmeldevorgangs an der polizeilichen Funkzelle.[17] Im vorliegenden Gesetzentwurf geht es jedoch um eine u.U. tagelange Blockierung der Kommunikationsbereitschaft.

b) Die damals geprüften IMSI-Catcher hatten keinerlei Einfluss auf die aktuellen Kommunikationsvorgänge (zwischen den benutzenden Menschen), sie funktionierten nach Angaben der technischen Sachverständigen des BKA sogar nur dann, wenn die Mobilgeräte sich im Standby-Betrieb befinden, also gerade keine Telefonate oder Textnachrichten ausgetauscht werden.[18] Nur so kam das Gericht zu der Einschätzung, die Maßnahme betreffe nicht den „*menschlich veranlassten Informationsaustausch*“, sondern allein eine rein technische Signalübermittlung (die Anmeldeprozedur der Geräte am Funknetz): „*Die Feststellung einer Geräte- oder Kartennummer ... durch den Einsatz eines ‚IMSI-Catchers' ist unabhängig von einem tatsächlich stattfindenden oder zumindest versuchten Kommunikationsvorgang zwischen Menschen (vgl. ...). Beim Einsatz des ‚IMSI-Catchers' ‚kommunizieren' ausschließlich technische Geräte miteinander. Es fehlt an einem menschlich veranlassten Informationsaustausch, der sich auf Kommunikationsinhalte bezieht.*“[19] Die im GE vorgeschlagene Maßnahme betrifft aber zweifelsfrei die menschliche Kommunikation wie die Kommunikationsbereitschaft und -fähigkeit.

c) Eine andauernder Eingriff in die Betriebsbereitschaft von Mobilfunkgeräten ist im Hinblick auf den Schutzbereich des relativ jungen Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme („IT-Grundrecht“) neu zu bewerten.[20] Mit seiner Entscheidung zur sog. Online-Durchsuchung von Computern reagierte 2008 das Bundesverfassungsgericht auf mehrere Entwicklungen:

---

[15] TH VerfGH 19/09, S. 26
[16] BVerfG, 2 BvR 1345/03 vom 22.8.2006
[17] „Auch ein Eingriff in die durch Art. 2 Abs. 1 GG gewährleistete allgemeine Handlungsfreiheit der Beschwerdeführer ist weder ausdrücklich vorgetragen noch sonst ersichtlich. a) Soweit durch den Einsatz des ‚IMSI-Catchers' für einige Sekunden die Herstellung einer Telekommunikationsverbindung für ein einzelnes Mobiltelefon nicht möglich ist, handelt es sich um eine Verhinderung von Telekommunikation, die nicht unter Art. 10 Abs. 1 GG fällt ...“ (BVerfG, 2 BvR 1345/03 vom 22.8.2006, Rn. 79f.)
[18] Vgl. Rosemarie Will, Kein Grundrechtsschutz für Handynutzer? In: Humanistische Union / Gustav-Heinemann-Initiative (Hrsg.), Graubuch Innere Sicherheit, Berlin 2009, S. 100ff.
[19] BVerfG, 2 BvR 1345/03 vom 22.8.2006, Rn. 57
[20] BVerfG, 1 BvR 370/07 vom 27.2.2008.

- die allgegenwärtige Präsenz und essenzielle Bedeutung der IuK-Technologien in unserem Alltag: „*Der Einzelne ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet.*“[21];
- die Unzulänglichkeit eines alleinigen Schutzes der Informationen bzw. Daten (unter Ausblendung der zugrundeliegenden Infrastruktur);
- die praktischen Schwierigkeiten eines individuellen Selbstschutzes (der das technische Sachverständnis vieler Nutzerinnen übersteigt).

In Anbetracht dieser Entwicklung leitete das Bundesverfassungsgericht aus der allgemeinen Handlungsfreiheit ein neues Grundrecht, dessen Schutzbereich[22] sich nicht auf die subjektive Seite der (missbräuchlichen) Erhebung, Speicherung und Verwendung persönlicher Daten beschränkt, sondern an den objektiven (strukturellen) Merkmalen des Vertrauens in und der Verfügbarkeit von IT-Systemen ansetzt: „*Dieses Recht fußt gleich dem Recht auf informationelle Selbstbestimmung auf Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG; es bewahrt den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit, als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten.*“[23]
Angesichts der Bandbreite möglicher Nutzungsarten, die bei heutigen Smartphones weit über das bloße Telefonieren hinausreichen, und dem hohen Verbreitungsgrad dieser Geräte kommt der Verfügbarkeit und dem sicheren Betrieb des Mobilfunknetzes eine wichtige Funktion zu. Einschränkungen des Mobilfunknetzes beeinträchtigen u.a. die Kommunikationsfreiheiten (d.h. den freien Zugang zu Online-Medien), die Informationsfreiheit (Zugang zu staatlichen Online-Informationsangeboten) und können für die betroffenen Anschlussinhaber enorme wirtschaftliche Konsequenzen haben. Das gilt umso mehr, als die Unterbrechung bzw. Verhinderung der Telekommunikation regelmäßig viele unbeteiligte Dritte betrifft, die sich in der gleichen Funkzelle aufhalten. Ein faktisches Außerkraftsetzen dieser Technologie ist deshalb nach unserer Auffassung als erheblicher Eingriff in die Handlungsfreiheit (Art. 2 Abs. 1 GG) und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) zu bewerten. Für derartige Maßnahmen sind die Eingriffsschranken insbes. aus der BVerfG-Entscheidung zur Online-Durchsuchung zu beachten. Ein zusätzlicher Richtervorbehalt für die Anordnung der Maßnahme ist aus diesem Grund unumgänglich.[24]

Empfehlung für § 34d Abs. 2: Maßnahmen nach den Absätzen 1 und 2 dürfen nur auf Antrag des Leiters der Landespolizeidirektion oder des Leiters des Landeskriminalamts oder eines besonders beauftragten Beamten des höheren Polizeivollzugsdienstes durch den Richter angeordnet werden. Die Anordnung ist auf höchstens drei Tage zu befristen.

Sven Lüders
für die Humanistische Union

[21] BVerfG, 1 BvR 370/07 vom 27.2.2008, Rn. 181.
[22] Zur Einordnung s. Oliver Lepsius, Das Computer-Grundrecht. Herleitung – Funktion – Überzeugungskraft. In: Roggan (Hrsg.), Online-Durchsuchungen. Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, Berlin 2008, S. 21ff.
[23] BVerfG, 1 BvR 370/07 vom 27.2.2008, Rn. 201.
[24] S. BVerfG, 1 BvR 370/07 vom 27.2.2008, Leitsatz 3.