Stand: 7. Februar 2018

Teil 3

Ausschussvorlage INA 19/63 – öffentlich –

Stellungnahmen der Anzuhörenden

zu dem

Gesetzentwurf
der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen
– Drucks. 19/5412 –

b|d|k RECHTSANWÄLTE

Thomas Bliwier
Fachanwalt für Strafrecht
Certified Compliance Officer

Doris Dierbach
Fachanwältin für Strafrecht
Certified Compliance Professional

Alexander Kienzle
Fachanwalt für Strafrecht

Barmbeker Straße 27a
22303 Hamburg
Tel. (040) 2702217 · 277716
Fax (040) 2792051
bdk@die-strafverteidiger.de
www.die-strafverteidiger.de

Gerichtsfach 637

b|d|k Rechtsanwälte · Barmbeker Straße 27a · 22303 Hamburg

Hessischer Landtag
-Der Vorsitzende des Innenausschusses-
-z.Hd. Frau Dr. Lindemann-
Schlossplatz 1-3

65183 Wiesbaden

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen, unsere Nachricht vom	Sekretariat	Datum
Ihr Schreiben vom 19.12.2017		Frau Peters/Frau Regewski	01.02.2018

Betr.:

Schriftliche Stellungnahme zu dem Gesetzentwurf der Fraktionen der CDU und BÜNDNIS90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen – Drucks. 19/5412 – und hierzu Änderungsantrag der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN – Drucks. 19/5782 –.

Sehr geehrte Damen und Herren,
sehr geehrter Herr Klee,
sehr geehrte Frau Dr. Lindemann,

Bezug nehmend auf Ihr vorstehend genanntes Schreiben nehme ich zu dem im Betreff genannten Gesetzentwurf nebst Änderungsantrag der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN wie folgt Stellung:

1. Allgemeines

Nach Auffassung des Verfassers erfüllt der Gesetzentwurf die ihm zugedachte Funktion einer „Neuausrichtung des Verfassungsschutzes in Hessen" nicht. Eine grundlegende Neuausrichtung, die ausweislich der Begründung des Gesetzentwurfs anhand der Maßstäbe

der höchstrichterlichen Rechtsprechung einerseits und der Lehren aus verschiedenen öffentlichkeitswirksamen Beispielen für die rechtsstaatliche Dysfunktionalität der Verfassungsschutzämter, namentlich den Erkenntnissen aus der Aufklärung des sog. NSU-Komplexes, andererseits hätte erfolgen sollen, kann das Gesetz in Form des vorliegenden Entwurfs nicht erbringen.

Dies ergibt sich aus Sicht des Verfassers daraus, dass die nachrichtendienstliche Tätigkeit durch den vorliegenden Gesetzentwurf nicht einer grundlegenden Revision unterzogen wird, sondern die bisherige Praxis der nachrichtendienstlichen Tätigkeit in Gesetzesform gegossen und fortgeschrieben werden soll.

Soweit dem Gesetz mit Blick auf die bisherige Praxis der Verfassungsschutzbehörden relevante Neuerungen zu entnehmen sind, betreffen diese zuvorderst die Ermächtigung des Landesamtes für Verfassungsschutz zur Nutzung in rechtsstaatlicher Hinsicht kritisch zu sehender oder gar abzulehnender Instrumentarien. Zu nennen sind insofern beispielsweise die sog. „Trojaner" oder die Schaffung von Eingriffsbefugnissen zulasten solcher Personen, die sich unter Förderung des Landes zur Abwehr von demokratiefeindlichen Bestrebungen engagieren.

Soweit im Übrigen eine Normierung der bereits bestehenden Praxis mit dem behaupteten Ziel unternommen werden soll, deren teils rechtsstaatlich hochgradig fragwürdige Auswüchse zu begrenzen, geht dieser Versuch in vielerlei Hinsicht fehl. Hierin liegt der Schwerpunkt der vorliegenden Betrachtung. Als beispielhaft hierfür werden insbesondere die Regelungen zu einzelnen Befugnissen des Landesamtes benannt, die nicht Lehren aus den bisher erkannten Missständen ziehen, sondern eine Fortschreibung und teilweise Vertiefung der bisherigen Missstände faktisch zu bewirken im Stande sind. Dies gilt aus Sicht des Verfassers zuvorderst für die Regelungen betreffend die Informationserhebung mit nachrichtendienstlichen Mitteln nach § 5[1] sowie Verdeckte Mitarbeiterinnen und Mitarbeiter nach § 13 und Vertrauensleute nach § 14. Daneben gilt der Befund auch für die Regelungen der Informationsweitergabe nach § 21 ff.

Selbst wenn der Gesetzentwurf entsprechend den in der Begründung eingebrachten Postulaten den Anspruch tatsächlich verfolgen sollte, das Landesamt für Verfassungsschutz als

[1] Regelungen ohne nähere Bezeichnung sind solche des Gesetzentwurfs in seiner vorliegenden Fassung.

„Dienstleister für Politik, Zivilgesellschaft und andere öffentliche Stellen"

und als

„Frühwarnsystem der Demokratie"

auszugestalten, erweist sich dieses sog. Frühwarnsystem angesichts der konkreten Regelungen als durch (Teil-) Aufgabe rechtsstaatlicher Grundsätze gekennzeichnet, die seinen Sinn insgesamt in Frage stellen.

2. Betrachtung einzelner Regelungen des Gesetzentwurfs

2.1. Präambel

Schon die Präambel des Gesetzentwurfs weist nach Auffassung des Verfassers auf ein grundlegendes Missverständnis der zu regelnden Materie hin. Es wird dabei nicht verkannt, dass es sich bei der Präambel lediglich um eine Absichtserklärung handelt, die den Rahmen für die konkrete Regelung abzustecken gedacht ist. Gleichwohl muss auch der Rahmen ohne Weiteres rechtsstaatlichen Grundsätzen entsprechen und erfüllt diese Aufgabe vorliegend nur bedingt. In rechtsstaatlicher Hinsicht hochgradig fragwürdig erweist sich aus Sicht des Unterzeichners die Formulierung, das Landesamt für Verfassungsschutz halte die

„analytischen Kompetenzen zur Beurteilung jener Gefahren vor, die Demokratie und Menschenrechten *durch extremistisches Gedankengut* drohen" (Hervorhebung nicht im Original).

Gedankengut ist im demokratischen Rechtsstaat nicht Anknüpfungspunkt einer rechtsstaatskonformen behördlichen Tätigkeit. Nicht umsonst benennt § 2 des Gesetzentwurfs als Aufgabe des Landesamts für Verfassungsschutz in dessen Abs. 1 die Abwehr von Gefahren für die freiheitlich demokratische Grundordnung sowie den Bestand und die Sicherheit des Bundes und der Länder. Zusätzlich soll nach Abs. 1 und 2 zur Aufgabe des Landesamts für Verfassungsschutz gehören, Bestrebungen und Tätigkeiten

entgegenzuwirken und diesen vorzubeugen. Ausweislich der Verweisung in § 3 Abs. 1 auf die Begriffsbestimmungen des § 4 Abs. 1 Satz 1, 2 und 4 sowie Abs. 2 des Bundesverfassungsschutzgesetzes (BVerfSchG) handelt es sich bei Bestrebungen in diesem Sinne um

> „politisch bestimmte[...], ziel- und zweckgerichtete[...] *Verhaltensweisen*" (Hervorhebung nicht im Original).

Anknüpfungspunkt einer nachrichtendienstlichen Befassung ist mithin grundsätzlich ein Handeln mit Realweltbezug, nicht Gedankengut. Es handelt sich insofern auch nicht um eine Marginalie, sondern um eine Rahmenbestimmung in der Präambel des Gesetzentwurfs, die bereits darüber Auskunft zu geben geeignet ist, dass der Gesetzentwurf rechtsstaatlich bedenklich weitgehend gerät. Dies bringt die inkorporierte Anknüpfung an das extremistische Gedankengut bereits in der Präambel auf den Punkt.

2.2. § 5 Informationserhebung mit nachrichtendienstlichen Mitteln

Diese Abkehr von in der Außenwelt grundgelegten Sachverhalten, die ein nachrichtendienstliches Tätigwerden rechtfertigen könnten, zeigt sich auch in der Regelung des § 5, der ausweislich seiner Überschrift die Informationserhebung mit nachrichtendienstlichen Mitteln regelt. Entscheidend im vorliegenden Zusammenhang ist, dass die Norm trotz aller normativen Beschränkungen dem Landesamt erlaubt, selbst Sachverhalte einer nach dem Gesetzentwurf zulässigen Erhebung personenbezogener Daten grundzulegen. Eine wirksame Beschränkung dieser Befugnis sieht der Gesetzentwurf nicht vor.

§ 5 Abs. 1 normiert die Befugnis des Landesamtes zur Erhebung von Informationen mit in Abs. 2 Satz 2 Ziff. 1 bis 12 benannten nachrichtendienstlichen Mitteln. Die allgemeine Befugnis des § 5 Abs. 1 Satz 1 zur Informationserhebung mit nachrichtendienstlichen Mitteln erfährt durch Abs. 1 Satz 2 Einschränkungen betreffend personenbezogene Daten, deren Erhebung nur zulässig sein soll in den in Ziff. 1 bis Ziff. 4 enumerierten Fällen. Während Ziff. 1, Ziff. 2 und (mit Einschränkungen) auch Ziff. 3 ausweislich des im Wortlaut vorausgesetzten Tatbestandes jeweils an einem außerhalb des Landesamtes liegenden Sachverhalt anknüpfen und die Befugnis zur Erhebung von personenbezogenen Daten von tatsächlichen Anhaltspunkten in der Außenwelt abhängig gemacht wird, gilt dies für Ziff. 4

ausdrücklich nicht. Ziff. 4 erklärt die Erhebung personenbezogener Daten für zulässig, wenn dies zur Überprüfung der Nachrichtenehrlichkeit und der Eignung von Vertrauensleuten erforderlich ist.

Die dergestalt geschaffene Zulässigkeitsregelung begegnet durchgreifenden Bedenken in mehrfacher Hinsicht. Zum einen knüpft sie an einen einzig durch das Landesamt selbst geschaffenen Tatbestand an. Das Landesamt bzw. die Behördenleitung oder ihre Vertretung selbst bestimmt ausweislich § 14 Abs. 2, mit welchen Vertrauensleuten die Zusammenarbeit erfolgen soll und erfolgt. Zur Überprüfung der Nachrichtenehrlichkeit und Eignung dieser Personen ist eine personenbezogene Datenerhebung sodann nach Ziff. 4 zulässig. Zum anderen entbehrt die Zulässigkeitsregelung einer mit Blick auf Sinn und Zweck der Normierung erforderlichen Beschränkung. Der Wortlaut der Norm lässt für sich genommen unbeschränkt die Erhebung personenbezogener Daten für die Überprüfung der Nachrichtenehrlichkeit wie der Eignung der Vertrauensperson zu. Dies bedeutet zunächst, dass auch solche personenbezogenen Daten erhoben werden dürfen, die keinerlei (personalen) Bezug zu der Vertrauensperson selbst aufweisen, sondern einzig im Zusammenhang mit den von dieser beschafften und weitergegebenen Nachrichten zu sehen sind, also im engeren Sinne die Nachrichtenehrlichkeit betreffen. Hierdurch ermächtigt der Gesetzentwurf letztlich das Landesamt für Verfassungsschutz selbst, die Voraussetzungen einer Erhebung personenbezogener Daten zu schaffen. Zur Überprüfung der Nachrichtenehrlichkeit und der Eignung einer Vertrauensperson gerät damit potentiell jede Person, über die eine Vertrauensperson berichtet, in den Fokus einer nach dem Wortlaut der Ziff. 4 zulässig personenbezogenen Datenerhebung.

Dem wirken auch die gesetzlich vorgesehenen Beschränkungen nicht wirksam entgegen. Abs. 3 Satz 1 Alt. 1 enthält eine Einschränkung betreffend einen gezielten Einsatz nachrichtendienstlicher Mittel gegen „Unbeteiligte" ausschließlich hinsichtlich Ziff. 1 und Ziff. 3, nicht indes hinsichtlich Ziff. 4. Für Ziff. 4 gelten ausweislich Abs. 3 Satz 1 Alt. 2 lediglich die allgemeinen Einschränkungen des § 4 Abs. 8 Satz 2 und Abs. 9. Demnach dürfen personenbezogene Daten Unbeteiligter insbesondere erhoben werden, wenn sie mit zur Aufgabenerfüllung erforderlichen Informationen untrennbar verbunden sind. Ein solcher untrennbarer Zusammenhang oder Verbund wird sich angesichts der schon tatbestandlich vorausgesetzten Notwendigkeit der Erhebung der personenbezogenen Daten zur Überprüfung namentlich der Nachrichtenehrlichkeit der Vertrauensperson ohne Weiteres herleiten lassen.

Es ist daher festzuhalten, dass durch § 5 Abs. 1 Satz 2 Nr. 4 eine weitreichende Befugnis des Landesamts für Verfassungsschutz geschaffen wird, selbstbestimmt die Zulässigkeit der Erhebung personenbezogener Daten (auch Unbeteiligter) zu ermöglichen. Eine gesetzgeberische Einhegung der teils verselbständigten Tätigkeit von Verfassungsschutzbehörden ist dergestalt sicher nicht zu gewährleisten.

2.3. § 13 Verdeckte Mitarbeiterinnen und Verdeckte Mitarbeiter

Mit Blick auf die bessere Kontrollierbarkeit nachrichtendienstlicher Tätigkeit sowie eine transparentere Aufgabenwahrnehmung gehen auch die von dem Gesetzentwurf vorgesehenen Regelungen betreffend Verdeckte Mitarbeiterinnen und Mitarbeiter nach Auffassung des Verfassers in vielfacher Hinsicht fehl.

2.3.1. Abs. 2 Satz 1: Steuernde Einflussnahme

So ist beispielsweise die Inkorporierung des Verbots einer „steuernden Einflussnahme" schon dem Wortlaut nach nicht geeignet, einen *erheblichen* Einfluss behördlicher Mitarbeiter auf Bestrebungen nach § 2 Abs. 2 auszuschließen, der nicht als steuernd anzusehen ist. Dies gilt jedenfalls dann, wenn – wie vorliegend – eine weitergehende Begriffsbestimmung unterbleibt.

Es handelt sich bei der in Rede stehenden Formulierung des § 13 Abs. 2 Satz 1 um den offenkundigen Versuch, eine gerade im sog. NSU-Komplex zu beobachtende „steuernde Einflussnahme" auf Bestrebungen im Sinne von § 2 Abs. 2 durch behördenassoziierte Personen zu unterbinden. Die Einschränkung eines Verbots für eine „steuernde" Einflussnahme zeigt jedoch, dass das Landesamt für Verfassungsschutz grundsätzlich ermächtigt bleiben soll, die genannten Bestrebungen zu beeinflussen. Lediglich die „steuernde" Einflussnahme wird von dem genannten Verbot erfasst. Dieser rechtsstaatlich fragwürdige Befund einer weiterhin zulässigen Einflussnahme auf Bestrebungen nach § 2 Abs. 2 durch Behördenmitarbeiter vertieft sich dadurch, dass der Gesetzentwurf darauf verzichtet, eine Legaldefinition der Einflussnahme, die steuernd und damit unzulässig zu sein geeignet ist, zu definieren. Es ist angesichts dessen mit der Schaffung eines erheblichen Graubereichs zu rechnen, der sich zwischen einer (zulässigen) Einflussnahme auf Bestrebungen im Sinne des § 2 Abs. 2 durch Verdeckte Mitarbeiterinnen und Verdeckte

Mitarbeiter und einer (unzulässigen) steuernden Einflussnahme auftut. Jede Einflussnahme birgt bereits ihrem Wortlaut nach die potentielle oder faktische Wirkung auf andere Subjekte oder Sachen in sich. Warum diese im Gegensatz zur steuernden Einflussnahme im Zusammenhang mit Bestrebungen nach § 2 Abs. 2 zulässig sein soll, erschließt sich nicht.

Insofern schafft das neue Gesetz entgegen den Postulaten der Begründung keine weitergehende Rechtssicherheit, sondern verleiht den faktisch bereits bestehenden Schwierigkeiten Gesetzesform. Mit Blick auf die bundesgesetzliche Normierung im BVerfSchG wurde insofern bereits festgehalten:

> „Wo die Grenze zwischen einsatzbedingtem Agieren und einer steuerndem Einflussnahme verläuft, ist ein tatsächliches Problem des Einzelfalls und verdeutlicht die Notwendigkeit einer effektiven operativen Kontrolle." (Bader, in: HRRS 2016, 293, 296).

Dies bedeutet nichts anderes, als dass die auch durch das Landesamt selbst wahrgenommene operative Kontrolle einziges Regulativ der Abgrenzung bleiben soll. Auch die Begründung des Gesetzentwurfs ist zur legislatorischen Abgrenzung unbehelflich. Dort heißt es:

> „Satz 1 verbietet eine steuernde Einflussnahme auf Bestrebungen i.S.v. § 2 Abs. 2. Dies gilt selbst dann, wenn die Einflussnahme mit dem Ziel erfolgt, die Bestrebung abzuschwächen [...]. Erst recht dürfen vom Landesamt solche Bestrebungen nicht initiiert werden, auch nicht zum Zwecke der Informationsgewinnung." (Gesetzentwurf S. 47)

Es bleibt also letztlich auch ausweislich der Begründung selbst dem Landesamt vorbehalten, eine begriffliche Klärung der „steuernden Einflussnahme" im Verhältnis zu anderen Einflussnahmen durch eine operative Kontrolle herbeizuführen, wobei angesichts der offenbar als erlaubt gedachten Einflussnahme bereits die begrifflichen Unklarheiten (vgl. hierzu oben) des auch ohne Steuerung ausgeübten Einflusses verbleiben. Statt also konsequenter Weise jedwede Einflussnahme durch behördliche Mitarbeiter auf Bestrebungen, denen entgegenzuwirken oder vorzubeugen ausdrückliche Aufgabe des Landesamts für Verfassungsschutz ausweislich § 2 ist, zu untersagen, verbleibt es bei einer zulässigen Einflussnahme auf dieselben durch die Behörde und ihre Mitarbeiter.

2.3.2. Abs. 2 Satz 2: Tätigwerden auch bei Verwirklichung eines Straftatbestandes

Die Inkonsequenz in der Umsetzung erkannter Notwendigkeiten zur Rückführung der Tätigkeit der Verfassungsschutzämter auf rechtsstaatlich einwandfreie Grundlage zeigt sich auch in der Schaffung der normativ als strafrechtliche Rechtfertigungsgründe gedachten Erlaubnistatbestände des § 5 Abs. 2 Satz 2 und 3. Durch die genannten Normen soll ausdrücklich ein Agieren behördlicher Mitarbeiter im (tatbestandlich) strafrechtlich relevanten Bereich ermöglicht und die Tatbestandsverwirklichung gerechtfertigt werden.

Schon die Grundentscheidung gerät insofern in höchstem Maße rechtsstaatlich bedenklich. Ein Handeln behördlicherseits entsandter Mitarbeiter im strafbaren Bereich und dessen Rechtfertigung letztlich ausschließlich zum Zwecke des Vertrauensaufbaus und der Erlangung weitergabegeeigneter Informationen gerät eines Rechtsstaats unwürdig, weil damit tatbestandlich strafbares Handeln behördlicher Mitarbeiter gezielt propagiert und gesetzgeberisch gutgeheißen wird für eine prognostisch unsichere spätere Informationserlangung. Die Brisanz dieses zunächst behördlichen und nunmehr auch gesetzgeberischen Vorgehens zeigt sich exemplarisch in einem Urteil des OLG Düsseldorf, mit dem eine im Auftrag des BND handelnde Vertrauensperson zu einer Freiheitsstrafe wegen Mitgliedschaft in einer terroristischen Vereinigung und ausländerrechtlicher Verstöße verurteilt wurde, weil die Wahrnehmung von Dienstrechten bzw. eine Amtsbefugnis für eine strafrechtliche Rechtfertigung nicht herangezogen werden konnten (OLG Düsseldorf NStZ 2013, 590 ff.). Dem soll nun durch Schaffung von gesetzlichen Rechtfertigungstatbeständen Rechnung getragen werden, ohne dass die Frage nach einer rechtsstaatlichen Vertretbarkeit noch aufgeworfen worden wäre.

Doch selbst wenn – wie in dem Gesetzentwurf vorgesehen – die Grundentscheidung dahingehend ausfällt, dass tatbestandlich strafbares Handeln behördlicher Mitarbeiter gerechtfertigt sein soll zugunsten des erstrebten Informationszuwachses, gerät die Konstruktion ausweislich des Gesetzentwurfs in mehrfacher Hinsicht rechtsstaatlich zweifelhaft. Dies gilt namentlich für die Regelung, wonach rechtfertigungsfähige Straftatbestände mangels abschließender gesetzgeberischer Regelung in Dienstvorschriften durch das Landdesamt selbst geregelt werden können. Zur Begründung dieser Selbstermächtigung wird angeführt, dass Einsatzsituationen nicht sicher vorhergesagt werden könnten und der Gegenseite durch eine abschließende Regelung kein Maßstab für die Enttarnung von betroffenen Personen an die Hand gegeben werden soll (vgl. hierzu auch

Bader, in: HRRS 2016, 293, 296). Allgemein wird aufgrund der Besonderheit der Aufgabenstellung und der operativen Ausgestaltung der Nachrichtendienste argumentiert, dass dem auch in der Gesetzgebung Rechnung getragen werden müsse (vgl. erneut Bader, in: HRRS 2016, 293, 296, unter Berufung auf Lampe, NStZ 2015, 361, 366), indem den nachrichtendienstlichen Einzelfällen in Verantwortlichkeit der Nachrichtendienste selbst und deren Dienstvorschriften adäquate (Rechtfertigungs-) Regelungen zugrunde gelegt würden.

Dem ist entgegenzutreten. Es sprechen gegen eine solche Regelungstechnik mehrere Gesichtspunkte. Zum einen ist zu bemerken, dass auch in der höchstrichterlichen Rechtsprechung die bislang unbeanstandet gebliebene vorstehende Regelungstechnik mit Blick auf die Vereinbarkeit mit rechtsstaatlichen Grundsätzen offenbar zunehmend kritisch gesehen wird (vgl. insofern BVerfG, 1 BvR 966/09 und 1 BvR 1140/09, Rn. 320, wo die genannte Regelungstechnik eigens hervorgehoben wurde; so auch Bader, in: HRRS 2016, S. 293, 297). Angesichts der Tatsache, dass ggf. auch in der verfassungsgerichtlichen Rechtsprechung für den nachrichtendienstlichen Bereich sich eine Abkehr von der Annahme einer Verfassungskonformität dieser Regelungstechnik andeutet, leuchtet nicht ein, warum neu geschaffene Gesetze – hier im Stadium des Entwurfs – eine solche Regelungstechnik noch zur Umsetzung bringen sollten. Zum anderen ist zu bemerken, dass es auch und gerade aufgrund der Lehren aus dem sog. NSU-Komplexes eines Weniger der Selbstermächtigungskompetenzen der Verfassungsschutzämter bedarf, nicht eines Mehr.

Des Weiteren lässt sich die rechtsstaatliche Zweifelhaftigkeit der Rechtfertigungsnormen exemplarisch an der Ausnahmeregelung des § 13 Abs. 2 Satz 5 verdeutlichen. § 13 Abs. 2 Satz 4 suggeriert zunächst eine über die Bundesgesetzgebung hinausgehende Lösung beim Vorliegen tatsächlicher Anhaltspunkte für die Verwirklichung eines Straftatbestandes von erheblicher Bedeutung durch Verdeckte Mitarbeiterinnen und Mitarbeiter. Im Gegensatz zu der Regelung im BVerfSchG, das insofern lediglich eine Soll-Vorschrift mit entsprechend regelhafter Anwendung vorsieht, ist § 13 Abs. 2 Satz 4 als zwingende Norm gestaltet. Demnach „wird" der Einsatz der Verdeckten Ermittlerin oder des Verdeckten Ermittlers unverzüglich beendet beim Vorliegen tatsächlicher Anhaltspunkte für die Verwirklichung eines Straftatbestandes von erheblicher Bedeutung durch den Mitarbeiter des Verfassungsschutzes. Daneben sieht die Regelung in Satz 4 die zwingende Unterrichtung der Strafverfolgungsbehörde vor. Doch schon die Regelung des § 13 Abs. 2 Satz 4 für sich genommen leidet an einer Unbestimmtheit der Begriffe der „zureichenden" tatsächlichen Anhaltspunkte sowie der „Straftatbestände von erheblicher Bedeutung", die durch die Verweisung des § 3 auf § 4 Abs. 1 Satz 1, 2 und 4, Abs. 2 BVerfSchG einer Legaldefinition

vollständig entbehren. Die Beurteilung, wie die Tatbestandsmerkmale zu definieren sein sollen und ob diese namentlich in Form der „zureichenden" tatsächlichen Anhaltspunkte im konkreten Einzelfall vorliegen, obliegt nach der derzeitigen Gesetzesfassung dem Landesamt für Verfassungsschutz und damit letztlich dem ggf. interessengeleitet agierenden Normanwender selbst. Soweit also die Gesetzesbegründung davon spricht, der Gesetzentwurf setze auf

> „eine moderne, scharf konturierte Gesetzesfassung, der eine klar strukturierte Systematik zugrunde liegt" (Gesetzentwurf S. 31),

ist dies mit Blick auf den hier in Rede stehenden Gesetzesteil gerade nicht der Fall. Darüber hinaus findet sich bereits auf dieser tatbestandlichen Ebene eine Abkehr von grundsätzlich gesicherter rechtsstaatlicher Systematik. Die Norm regelt – neben der bereits aufgezeigten Begriffsdefinition – auch die tatbestandliche Anwendung durch das Landesamt. Dies bedeutet, dass die Staatsanwaltschaften als nach §§ 152, 160 StPO zur Einhaltung des Legalitätsprinzips berufene Strafverfolgungsbehörden bei der Entscheidung betreffend diese Sachverhalte gezielt außen vorblieben. Das sonst originär in die Zuständigkeit der Staatsanwaltschaften fallende Prüfprogramm des Vorliegens eines Anfangsverdachts einer Straftatbegehung läuft durch die Einschätzungsprärogative des Landesamts (zunächst) faktisch leer. Nicht mehr die Staatsanwaltschaft, sondern das Landesamt entscheidet, wann vom Vorliegen zureichender tatsächlicher Anhaltspunkte für eine Straftatbegehung auszugehen ist. Dies wiegt umso schwerer, als „Straftaten von erheblicher Bedeutung" auch solche Straftaten umfassen können, die keinerlei Einsatzzusammenhang aufweisen (so für die Regelung im Bund Bader, in: HRRS 2016, S. 293, 297). Dies bedeutet nichts anderes, als dass das Landesamt in eigener Kompetenz entscheidet, wann zureichende tatsächliche Anhaltspunkte für eine Straftatbegehung von erheblicher Bedeutung durch eigene Mitarbeiterinnen und Mitarbeiter vorliegen mit der Konsequenz einer Unterrichtungspflicht gegenüber der Staatsanwaltschaft. Es wird dadurch ein vollkommen systemwidriges Vorprüfverfahren im Verantwortungsbereich des Landesamts geschaffen, das die genannten Sachverhalte der Einschätzung durch die hierfür nach rechtsstaatlichen Maßstäben grundsätzlich zuständige Behörde, die Staatsanwaltschaft, entzieht. Dies ist nicht hinnehmbar.

Bestehen also bereits auf der tatbestandlichen Ebene erhebliche definitorische Unsicherheiten und eine mit Blick auf die rechtsstaatliche Aufgabenzuweisung an die Staatsanwaltschaft systemwidrige Einschätzungsprärogative des Landesamts erhebliche

Probleme, gerät die zwingend anmutende Norm des § 13 Abs. 2 Satz 4 durch den folgenden Satz der Regelung vollends zur Makulatur. Durch die Regelung des Ausnahmetatbestandes in Satz 5 entscheidet selbst bei nach eigener Auffassung vorliegendem Anfangsverdacht einer durch einen Behördenmitarbeiter begangenen Straftat von erheblicher Bedeutung über den Einsatzabbruch und die Unterrichtung der Staatsanwaltschaft voraussetzungslos die Behördenleitung des Landesamts für Verfassungsschutz. Mit anderen Worten: Selbst Sachverhalte, die auf der tatbestandlichen Ebene trotz aller Unklarheiten und fehlender Konturierung der Begrifflichkeiten nicht durch das Landesamt selbst ausgesondert wurden und damit die Begehung einer Straftat von erheblicher Bedeutung durch einen Behördenmitarbeiter im Sinne eines Anfangsverdachts nahe legen, können ohne eine gesetzgeberisch formulierte Voraussetzung von den zwingenden Folgen des Satzes 4 ausgenommen werden. Dass dies bereits für sich genommen rechtsstaatlich hochgradig fragwürdig und nicht dazu angetan ist, das Vertrauen in die Verfassungsschutzbehörden zu stärken, liegt auf der Hand. Berücksichtigt man weiterhin, dass nach allgemeiner Lesart von Satz 4 und 5 auch Straftatbestände von erheblicher Bedeutung ohne Einsatzzusammenhang erfasst werden sollen (vgl. zur ähnlich gelagerten Konstellation im BVerfSchG Bader, in: HRRS 2016, S. 293, 297), ergibt sich aus der Norm ein rechtsstaatswidrig weites Potential der Abkehr vom Legalitätsprinzip. Die Behörde kann letztlich selbst bei zureichenden tatsächlichen Anhaltspunkten für eine Straftatbegehung von erheblicher Bedeutung durch einen Mitarbeiter in freiem Ermessen entscheiden, ob und ggf. wann und wie der Einsatz des Mitarbeiters beendet und ggf. die Strafverfolgungsbehörden über die zureichenden tatsächlichen Anhaltspunkte unterrichtet werden sollen. Durch eine solche gesetzliche Regelung wird sich nicht im Ansatz die Problematik minimieren lassen, die in der Intransparenz und (zumindest) Straftatnähe des Handelns der Verfassungsschutzbehörden auch und gerade im NSU-Komplex zu sehen war.

Dass die Durchbrechung dieser rechtsstaatlichen Systematik trotz aller Aufarbeitung gleichwohl von dem Gesetzentwurf bewusst vorgesehen ist, ergibt sich aus dessen Begründung. Zwar werden insofern das Regel-Ausnahme-Verhältnis und dessen betreffend die Ausnahmen restriktiv zu handhabende Anwendung betont (Gesetzentwurf S. 48). Indes lässt sich auch der Gesetzesbegründung nicht entnehmen, wann konkret eine (restriktiver Begrifflichkeit unterfallende) Ausnahme anzunehmen ist oder nicht. Es bleibt insofern bei einer voraussetzungslos gewährten Befugnis der Behördenleitung. Dies ist rechtsstaatlich kaum hinnehmbar. Die Behörde ist nach diesem gesetzlichen Regelungsgehalt also in Kenntnis über zureichende tatsächliche Anhaltspunkte für die Verwirklichung eines Straftatbestands von erheblicher Bedeutung durch einen ihrer Mitarbeiter und darf gleichwohl

frei entscheiden, hierüber Strafverfolgungsbehörden keinerlei Information zukommen zu lassen. Worin genau insofern der rechtsstaatliche Zugewinn gegenüber der bisherigen Rechtslage liegen soll, erschließt sich nicht. Zu zurückhaltend scheint daher die Maßgabe, es hätte sich *angeboten* die Unterrichtung der Strafverfolgungsbehörden nicht vom Ergebnis der Prüfung eines Anfangsverdachts durch eine Verfassungsschutzbehörde abhängig zu machen, sondern

> „diese Prüfung auch hier systemgerecht der Staatsanwaltschaft zu überlassen." (so Bader, in: HRRS 2016, S. 293, 297, für die vergleichbaren Regelungen des BVerfSchG)

Stattdessen ist die systemgerechte Unterrichtung der Strafverfolgungsbehörden und damit die Ermöglichung deren an das Legalitätsprinzip gebundene Prüfung anhand der §§ 152, 160 StPO ein unumstößliches rechtsstaatliches Gebot, das durch den vorliegenden Gesetzentwurf ebenso wenig eingehalten wird wie durch die entsprechende bundesgesetzliche Regelung.

2.4. § 14 Vertrauensleute

Die vorstehenden Probleme, die den Einsatz Verdeckter Mitarbeiterinnen und Mitarbeiter betreffen, werden durch § 14 mit Blick auf die nach dem Gesetzentwurf weiterhin zulässige Zusammenarbeit des Landesamts mit sog. Vertrauensleuten noch erheblich vertieft.

Während die Gesetzesbegründung mitteilt, die Zusammenarbeit werde durch § 14 des Gesetzesentwurfs aufgrund der Lehren, die aus dem sog. NSU-Komplex gezogen werden müssten, eingeschränkt, ist das Augenmerk zunächst darauf zu richten, dass der Gesetzentwurf grundsätzlich eine Zusammenarbeit weiterhin zulassen wird. Eine Abkehr von der Zusammenarbeit mit sog. menschlichen Quellen wird trotz aller Erkenntnisse, die zur Rechtsstaatswidrigkeit dieser Kooperationen und zur Unsicherheit dieser Art der Informationsbeschaffung auch aus dem sogenannten NSU-Komplex gewonnen werden konnten, nicht vorgesehen. Der Gesetzentwurf bleibt damit hinter den teilweise bereits gesetzgeberisch umgesetzten Fundamentalerkenntnissen weit zurück. Weiterhin soll ausweislich des Gesetzentwurfs dem Landesamt erlaubt sein, (auch) Mitglieder radikaler und extremistischer Szenen und Gruppierungen anzuwerben und dafür zu bezahlen, unter

(scheinbarer) Aufgabe ihrer politischen sich dem politischen System anzudienen, dessen Bekämpfung sie in Bestrebungen oder Tätigkeiten unternehmen.

Der Gesetzentwurf bleibt indes – selbst wenn man der Auffassung zuneigt, ohne die Abschöpfung menschlicher Quellen eine Informationsbeschaffung aus den genannten Strukturen nicht in einem ausreichenden Maße gewinnen zu können – hinter einer Lösung der sich daran anschließenden Problematiken in mehrfacher Hinsicht zurück.

2.4.1. Abs. 1: Rechtliche Gleichstellung

Dies ergibt sich zuvorderst aus der in Abs. 1 im Wege der Verweisung auf § 13 Abs. 1 bis 3 vorgesehenen rechtlichen Gleichstellung der Vertrauenspersonen mit den Verdeckten Ermittlern.

Zuvorderst ist – worüber der Gesetzesentwurf ausweislich seiner Begründung schweigt – hiermit verbunden, dass sämtliche unter 2.3. dargelegten gesetzgeberischen Defizite für den Einsatz von Vertrauenspersonen übernommen und die Regelung denselben Unwägbarkeiten und rechtsstaatlichen Defiziten unterworfen wird, die bereits hinsichtlich § 13 Geltung beanspruchen. Insofern kann auf die vorstehend beschriebenen Defizite und Problemkonstellationen „entsprechend" verwiesen werden.

Darüber hinaus fällt mit Blick auf die Vertrauenspersonen eine dem Einsatz Verdeckter Ermittlerinnen oder Ermittlern inhärente rechtsstaatliche Sicherung vollständig weg, ohne dass dies durch den vorgelegten Gesetzentwurf ansatzweise aufgefangen oder auch nur verdeutlicht würde. Trotz des Fehlens einer ausdrücklichen Legaldefinition der Verdeckten Ermittlerin oder des Verdeckten Ermittlers im Gesetzentwurf dürfte diese ähnlich ausgestaltet sein wie in vergleichbaren Regelungswerken, namentlich der StPO (so wohl auch Bader, in: HRRS 2016, 293, 296 Fn. 15, der aber zu Recht darauf hinweist, dass eine ausdrückliche Regelung auch im BVerfSchG fehle). Hinsichtlich letzterer ist ausweislich des § 110a StPO gesichert, dass Verdeckter Ermittlerinnen und Ermittler BeamtInnen des Polizeidienstes sind, die unter einer Legende ermitteln (vgl. lediglich Meyer-Goßner/Schmitt, StPO, 60. Aufl. 2017, § 110a Rn. 1 ff. m.w.N.). Wesentlich für die strafprozessuale Qualifikation als Verdeckte Ermittlerin oder Verdeckter Ermittler ist, dass

- der Ermittlungsauftrag über einzelne, konkrete Ermittlungshandlungen hinausgeht,
- eine unbestimmte Vielzahl von Personen über die wahre Identität der verdeckt operierenden Beamtin oder des verdeckt operierenden Beamten getäuscht wird und
- wegen der Art und des Umfangs des Auftrags von vornherein absehbar ist, dass die Identität der Beamtin oder des Beamten in künftigen Strafverfahren auf Dauer geheimgehalten werden muss.

Diese Grundsätze gehen zurück auf die höchstrichterliche Rechtsprechung und sind für den strafrechtlichen Bereich als geklärt anzusehen (vgl. lediglich BGHSt 41, 64, 65; Meyer-Goßner/Schmidt, StPO, 60. Auf. 2017, § 110a Rn. 2). Von herausragender Wichtigkeit ist in diesem Zusammenhang, dass strafprozessual einzig Beamtinnen und Beamte im Sinne der §§ 3, 33 ff. BeamtStG als Verdeckte Ermittlerinnen oder Verdeckte Ermittler eingesetzt werden dürfen (vgl. hierzu BGH, Beschluss vom 20.06.2007, 1 StR 251/07). Diese Anforderung ist deshalb in rechtsstaatlicher Hinsicht von elementarer Bedeutung, weil einzig durch

> „die notwendige straffe Führung und wirksame, auch disziplinarrechtliche, Dienstaufsicht" (vgl. insofern BT-Drs. 17/4333 S. 2, 3)

im Beamtenstatusverhältnis eine rechtsstaatliche Anbindung von mit behördlichem Auftrag geheim agierender Personen gewährleistet erscheint.

Diese rechtsstaatliche Sicherung entfällt mit Blick auf die Vertrauenspersonen vollständig und angesichts des vorgelegten Gesetzentwurfs ersatzlos. Was unter dem im Wege des Verweises mit erfassten (erlaubten) „Einsatz" einer Privatperson als Vertrauensperson durch eine Behörde zu verstehen sein soll, bleibt angesichts der o.g. Regelungstiefe zur Verdeckten Ermittlerin oder dem Verdeckten Ermittler vollkommen unklar. Bereits die Grundlagen der Tätigkeit der Vertrauensperson unterscheiden sich fundamental von derjenigen der Verdeckten ErmittlerInnen. Während Letztere im Rahmen eines bereits zuvor begründeten und fortbestehenden beamtenrechtlichen Rahmens tätig werden und durch diesen behördlicher Kontrolle und ggf. innerbehördlichen Sanktionierungssystemen unterliegen, gilt all dies für die Vertrauensperson gerade nicht. Diese wird angeworben wegen des – in vielen Fällen rechtswidrigen oder jedenfalls rechtswidrigkeitsnahen –

Bereichs, in dem sie sich als Privatperson bewegt. Sie unterliegt keinerlei zusätzlichen beamtenrechtlichen Bindungen, weder denen der Kontrolle und Sanktionierung, noch denen der Auftragserteilung und damit des „Einsatzes". Auch insofern greift der Gesetzentwurf angesichts des schlichten Verweises auf die Regelungen betreffend die Verdeckten Ermittlerinnen und Ermittler zu kurz. Die im Wege des Verweises vollzogene Gleichstellung von (verbeamteten) Verdeckten Ermittlerinnen und Ermittlern geht bereits dem Wortlaut der Norm, darüber hinaus aber auch ihrem Sinn und Zweck nach fehl.

Zudem ergibt sich aus der Verweisung eine noch weitergehende Rechtfertigung tatbestandlich strafbaren Verhaltens, als diese für den unmittelbar agierenden Personenkreis ausweislich des Wortlauts vorgesehen ist und bereits oben unter 2.3. als rechtsstaatlich beanstandungswürdig gekennzeichnet wurde. Durch die strafrechtsdogmatisch vorgesehene sog. limitierte Akzessorietät bedeutet der Verweis letztlich auch eine weitgehende Rechtfertigung der in der Behörde für die „Führung" der menschlichen Quellen verantwortlichen Mitarbeiter. Auch ohne ausdrückliche Erwähnung im Gesetzestext greifen die Rechtfertigungstatbestände des Gesetzesentwurfs weit über die oder den vom Wortlaut ausdrücklich erfassten Vertrauensperson hinaus: Eine Strafbarkeit wegen Anstiftung oder Beihilfe zu deren vorsätzlich begangener Straftat scheidet aufgrund der Rechtfertigung nämlich auch für die andernfalls wegen Anstiftung oder Beihilfe zu diesen Delikten strafbaren Behördenmitarbeitern aus (vgl. hierzu instruktiv Bader, in: HRRS 2016, 293). Es handelt sich also bei der im Wege des Verweises auf § 13 bewerkstelligten Schaffung der Rechtfertigungstatbestände auch für die Vertrauenspersonen um nichts weniger als die weitgehende Straffreistellung von Beamtinnen und Beamten, die in Verrichtung ihrer nachrichtendienstlichen Tätigkeit, der Beaufsichtigung, Lenkung und Steuerung von Vertrauenspersonen, die allgemeinverbindlichen Verbotsnormen ignorieren und jenseits deren Handlungsgeboten oder -verboten durch die Vertrauenspersonen agieren (lassen).

Dies muss als gesetzgeberische Grundentscheidung ebenfalls offen benannt werden, wenn es gewollt ist. Die Verweisung verbirgt insofern letztlich, dass auch diese „doppelte Rechtfertigung" bei einem tatbestandlich strafbaren Verhalten der durch den Quellen"führer" eingesetzten Vertrauensperson greift. Andernfalls werden die Rechtfertigungstatbestände gestrichen werden müssen, um nicht strafgesetzwidriges behördliches Handeln in einem Bereich, in dem eine Kontrolle ohnedies aufgrund der geltend gemachten Geheimhaltungserfordernisse nur begrenzt stattfinden kann, zu fördern.

2.4.2. Abs. 2 Satz 2, 4: Persönliche Eignung und Anwerbungsvoraussetzungen

Auch die Regelungen zu einem Anwerbungsausschluss gehen ausweislich des Wortlauts des Gesetzentwurfs an den tatsächlich in der Vergangenheit zu beobachtenden Problemen vorbei und schließen diese – wenn überhaupt – nicht mit hinreichender Klarheit aus. Exemplarisch sei dies an den folgenden Ausschlusstatbeständen verdeutlicht:

2.4.2.1. Ziff. 2: Geld- oder Sachzuwendungen auf Dauer alleinige Lebensgrundlage

§ 14 Abs. 2 Satz 2 Ziff. 2 schließt die Anwerbung solcher Vertrauenspersonen aus, die von den Geld- oder Sachzuwendungen für die Tätigkeit auf Dauer als alleinige Lebensgrundlage abhängen würden. Zwar ist insofern eine Motivation der reinen Existenzsicherung durch die Kooperation mit dem Landesamt ausgeschlossen. Indes lässt sich durch die Normierung nicht die Motivation der (zukünftigen) Quelle ausschließen, die in einer Erhöhung des Lebensstandards gesehen werden kann. Angesichts der Tatsache, dass im modernen Sozialstaat behördliche Zuwendungen in einem auf Informationsweitergabe angelegten (Vertrauens-) Verhältnis in den seltensten Fällen auf Dauer alleinige Lebensgrundlage einer Person sein dürfte, dürfte das Ausschlusskriterium weitgehend leer laufen. Dies ergibt sich auch daraus, dass bei keiner Quelle, die in Zusammenhang mit dem sog. NSU-Komplex zu bringen war, eine alleinige Abhängigkeit der Lebensgrundlage von den Zuwendungen des Bundes, Oder Landesamts für Verfassungsschutz zu beobachten war. Ein Verbot der Bezahlung menschlicher Quellen für die Informationsweitergabe wäre die einzig erkennbare akzeptable Lösung.

2.4.2.2. Ziff. 5: Eintragung im BZRA nebst Ausnahmeregelung

§ 14 Abs. 2 Satz 2 Ziff. 5 schließt die Anwerbung solcher Personen aus, in deren Bundeszentralregisterauszug eine Verurteilung wegen eines Verbrechens oder zu einer Freiheitsstrafe, deren Vollstreckung nicht zur Bewährung ausgesetzt wurde, eingetragen ist. Entscheidend erscheint insofern, dass der Gesetzentwurf auch in seiner vorliegenden Form das suggerierte Ziel, nämlich den Anwerbungsausschluss von zu den genannten Sanktionen Verurteilten, nicht zu erreichen vermag. Es ist insofern zu berücksichtigen, dass die Eintragung in das Bundeszentralregister der Verurteilung zeitlich in der Regel nicht unerheblich nachgelagert ist. Dies gilt zuvorderst hinsichtlich nicht rechtskräftiger

Verurteilungen durch das Tatgericht, die je nach Instanz des Tatgerichts in einem oder zwei Rechtsmittelinstanzen der weiteren Überprüfung unterliegen. Es vergehen daher im Fall einer erstinstanzlich landgerichtlichen Verurteilung wegen eines Verbrechenstatbestandes oder einer unbedingten Freiheitsstrafe bei einer Rechtsmitteleinlegung durch den Verurteilten in der Regel noch mehrmonatige Zeiträume, in denen eine Eintragung in das Bundeszentralregister aufgrund fehlender Rechtskraft und fortgeltender Unschuldsvermutung nicht stattfindet. Innerhalb dieses Zeitraums könnte nach dem Gesetzeswortlaut und der Anbindung des Ausschlusses an die Eintragung im Bundeszentralregister ohne Weiteres eine Anwerbung durch das Landesamt für Verfassungsschutz gleichwohl stattfinden. Zur Klarstellung: Es soll hier nicht einer „Vorverurteilung" das Wort geredet werden, die gesetzliche Tatbestände an einer erstinstanzlichen, nicht rechtskräftigen Entscheidung anbindet. Gleichwohl ist im vorliegenden Zusammenhang zu bedenken, dass ein Ausschluss von Verurteilten als Vertrauenspersonen einer staatlichen Behörde und eine Zusammenarbeit mit demselben durch den jetzigen Gesetzeswortlaut nicht ausgeschlossen werden kann. Darüber hinaus ist selbst im Falle einer rechtskräftigen Verurteilung wegen eines Verbrechens oder zu einer Freiheitsstrafe, deren Vollstreckung nicht zur Bewährung ausgesetzt worden ist, nach dem derzeitigen Gesetzeswortlaut eine Anwerbung durch das Landesamt für Verfassungsschutz nicht ausgeschlossen. Es ist insofern zu berücksichtigen, dass eine Eintragung in das Bundeszentralregister der Rechtskraft einer Verurteilung zeitlich stets nachgelagert erfolgt. Es ist insofern zunächst erforderlich, dass die rechtskräftige Verurteilung an das Bundeszentralregister gemeldet wird und dort im Wege der Sachbearbeitung eingetragen wird. Für die Zwischenzeit greifen die hier in Rede stehenden Ausschlusskriterien ebenfalls nicht. Auch der weitergehende Ausschluss eines Einsatzes der (bereits angeworbenen) Vertrauensperson bei Vorliegen der Ausschlusskriterien hindert ein Tätigwerden auf diesem Hintergrund nicht vollständig. So scheinen durchaus Konstellationen denkbar, in denen eine Anwerbung und ein Einsatz nach einer (erst-, zweitinstanzlichen oder rechtskräftigen) Verurteilung erfolgt und in Kenntnis derselben fortgesetzt wird bis zu einem Eintrag der Verurteilung in das Bundeszentralregister und der Kenntnisnahme des Landesamts für Verfassungsschutz hiervon, die als ungeschriebenes Tatbestandsmerkmal offenkundig ebenfalls vorliegen muss.

Eine Alternative zu der vom Wortlaut des Gesetzentwurfs vorgesehenen Vorgehensweise scheint zu sein, einen Anwerbeausschluss bereits für den Fall vorzusehen, dass im Einzelnen zu definierende offene Ermittlungs- oder Gerichtsverfahren gegen die anzuwerbende oder einzusetzende Vertrauensperson vorliegen. Angesichts der Tatsache,

dass ein am Nichtvorliegen solcher offenen Verfahren orientiertes Prüfen rechtsstaatskonform beispielsweise auch bei der Prüfung einer Eignung für den offenen Strafvollzug stattfindet, dürfte dieses auch in der vorliegenden Konstellation vorzugswürdig sein. Immerhin geht es vorliegend um die Klärung der Frage, mit welchen Vertrauensleuten eine staatliche Behörde unter der Maßgabe der persönlichen Eignung und der potentiellen Nachrichtenehrlichkeit zu kooperieren vermag. Statt jedoch dieser Alternative gesetzgeberisch Vorrang einzuräumen, wird diese ausdrücklich negiert:

> „Laufende Strafverfahren sind hingegen nicht generell verpflichtungsschädlich." (Gesetzentwurf S. 50)

Eine Begründung für diese Maßgabe unterbleibt.

Auch die in dem vorgelegten Gesetzentwurf vorgesehenen Tatbestände für einen Ausschluss einer Anwerbung von als ungeeignet zu erachtenden Personen erfüllen damit den suggerierten Zweck nicht oder nur mit erheblichen Einschränkungen.

2.5. § 21 Informationsübermittlung durch das Landesamt innerhalb des öff. Bereichs

Als gerade auf dem Hintergrund der Erkenntnisse aus dem NSU-Komplex hochproblematisch anzusehen ist die gesetzgeberische Konstruktion des Dritten Teils des Gesetzentwurfes. Dies gilt insbesondere auf dem Hintergrund, dass zwar die Informationsweitergabe durch den Verfassungsschutz ausdrücklich einer gesetzgeberischen Regelung zugeführt wird. Indes werden die fakultative Informationsweitergabe nach §§ 20, 21 sowie die zwingende Weitergabe nach § 21 Abs. 2 Satz 3 durch § 24 Abs. 1 gerade in einem Bereich eingeschränkt, indem eine an nachrichtendienstlichen Interessen orientierte Informationszurückhaltung sich als hochproblematisch und teilweise als Beitrag zum Gelingen schwerster Straftaten erwiesen hat.

Namentlich die Einschränkung des § 24 Abs. 1 Ziff. 2 hebelt die zwingende Informationsweitergabe bei Vorliegen tatsächlicher Anhaltspunkte dafür, dass die Übermittlung für die Verhinderung oder Verfolgung von Staatsschutzdelikten erforderlich ist (§ 20 Abs. 1 Satz 1 BVerfSchG), unter Berücksichtigung rein nachrichtendienstlicher Interessen aus. So werden von der Norm ausdrücklich Gründe des Quellenschutzes oder des Schutzes operativer Maßnahmen als tatbestandlich begründend für ein

Übermittlungsverbot genannt. Dass damit erneut eine gesetzliche Regelung geschaffen werden soll, die aus Gründen des Quellenschutzes Verfassungsschutzämter dazu ermächtigt, für die Verhinderung oder Verfolgung schwerster gegen die freiheitlich demokratische Grundordnung gerichteter Verbrechen erforderliche Informationen gegenüber den Polizei- und Strafverfolgungsbehörden geheim zu halten, ist das Gegenteil der Umsetzung der Erkenntnisse aus den Versäumnissen im Zusammenhang mit dem nachrichtendienstlichen Agieren rund um den NSU. Statt also die in der Begründung ausdrücklich erwähnte

> „Verbesserung des Informationsaustauschs zwischen den Verfassungsschutzbehörden und den Strafverfolgungs- und Polizeibehörden" (Gesetzentwurf S. 29)

gerade hinsichtlich schwerster gegen die freiheitlich demokratische Grundordnung gerichteter Vergehen und Verbrechen zur Umsetzung zu bringen, wird diese neuerlich neben anderem unter den Vorbehalt einer ausschließlich an den Interessen der Verfassungsschutzbehörden orientierten Einschränkung versehen. Da diese Einschränkung namentlich auch den Quellenschutz als Grundlage einer Informationsvorenthaltung benennt, wird eine der im Zusammenhang mit dem sog. NSU-Komplex erkannten wesentlichen Problemkonstellationen gesetzgeberisch fortgeschrieben: Nach wie vor soll der Schutz auch in rechtsstaatlicher Perspektive hochgradig zweifelhafter Quellen Grund für Intransparenz und Geheimhaltung sein. Erneut wird der nachrichtendienstlichen Interessenwahrnehmung ein unbedingter Vorrang vor der Verhinderung und Verfolgung von Straftaten eingeräumt.

Auch insofern bleibt der vorgelegte Gesetzentwurf hinter einer wirksamen Aufarbeitung von Lehren aus den bekannten Problemkonstellationen weit zurück.

3. Fazit

Der Gesetzentwurf verfehlt – wie an den vorstehenden Regelungsbereichen exemplarisch aufgezeigt – die an ihn in rechtsstaatlicher Hinsicht zu stellenden Anforderungen. Die Berufung auf einen

> „signifikanten Reformbedarf, der bei der Zusammenarbeit von Nachrichtendiensten, Polizei- und sonstigen Sicherheitsbehörden besteht, [...] spätestens bei der politischen Aufarbeitung der Taten des

> sogenannten „Nationalsozialistischen Untergrunds“ (NSU) zutage getreten [ist]“ (Gesetzentwurf S. 29)

entpuppt sich angesichts der vorstehend dargestellten Probleme, die sich mit dem Gesetzentwurf in seiner vorliegenden Fassung verbinden, als gesetzgeberisches Postulat, dessen Umsetzung durch diesen nicht erreicht werden wird. Es handelt sich mit Blick hierauf um einen Entwurf der verpassten Chancen. Der Entwurf orientiert sich an einer minimalistisch rechtsstaatliche Vorgaben berücksichtigenden Bundesgesetzgebung und schreibt diese fort. Statt die teils erheblichen strukturellen wie spezifischen Probleme, die sich mit der Tätigkeit der Verfassungsschutzämter ergeben, gesetzgeberisch aufzuarbeiten und – wo erforderlich – auszuräumen, verbleibt er hinter diesen Zielen weit zurück. Statt beispielsweise den Einsatz von behördlichen Mitarbeitern und das Anwerben und Einsetzen von Vertrauenspersonen gesetzgeberisch aufzuarbeiten und diese – bis hin zu einem Verbot einer solchen behördlichen Kooperation – zu regeln, wird lediglich die normative Mindestvoraussetzung normiert. Kein anderer gesetzgeberischer Wille scheint dem Gesetzentwurf zugrunde zu liegen, wenn es dort in der Begründung heißt:

> „Besonders hohen Wert legt der Gesetzentwurf darauf, bundeseinheitliche Standards für den Einsatz von Verdeckten Mitarbeiterinnen, Verdeckten Mitarbeitern und Vertrauensleuten zu normieren. Daher übernimmt der Entwurf die entsprechenden Vorschriften des Bundes (§§ 9a und 9b des Bundesverfassungsschutzgesetzes) weitestgehend wörtlich (§§ 13 und 14).“ (Gesetzentwurf S. 33)

Dass damit erhebliche Probleme fortgeschrieben und teilweise erhebliche neue erst geschaffen werden, war darzulegen.

Mit freundlichen Grüßen
b|d|k Rechtsanwälte

Alexander Kienzle

Deutscher Gewerkschaftsbund

I I
An den Innenausschuss des Hessischen Landtags
Herrn Horst Klee

Schriftliche Stellungnahme zum Gesetzesentwurf der Fraktionen CDU und BÜNDNIS 90/ DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen und dem Änderungsantrag (Drucksache 19/5412 und 19/5782)

1. Februar 2018

Helena Müller
Öffentlicher Dienst/ Beamte Hessen

helena.mueller@dgb.de

Telefon: 069 27 30 05 -33

Mobil: 0151 14 80 60 72

Sehr geehrter Herr Klee,

für die Übersendung und Möglichkeit der schriftlichen Stellungnahme zum Gesetzesentwurf der Fraktionen CDU und BÜNDNIS 90/ DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen bedanken wir uns.

Unsere Stellungnahme untermauert einen Beschluss der DGB Bezirkskonferenz Hessen – Thüringen vom 9.12.2017 in Frankfurt am Main. Außerdem ist zu erwähnen, dass im Rahmen der Anhörung, unsere Fachgewerkschaft GdP, Gewerkschaft der Polizei Hessen eine eigene fachliche Stellungnahme abgibt. Diese enthält weitergehende Anforderungen, welche sich aus der fachlichen Sicht und Stellung der GdP in der Gesamtkomplexität des zu behandelnden Themas ergeben.

Der DGB und seine Mitgliedsgewerkschaften engagieren sich in Hessen in vielfältiger Form und auf breiter gesellschaftlicher Ebene gegen Rassismus, Antisemitismus und jede Form gruppenbezogener Menschenfeindlichkeit. Wir treten für eine plurale, demokratische und weltoffene Gesellschaft ein.

Neben dem umfangreichen Engagement des DGB und seiner Mitgliedsgewerkschaften auf betrieblicher Ebene zählt hierzu sowohl die Unterstützung lokaler Bündnisse gegen Rechts als auch die Mitarbeit in zahlreichen Begleitausschüssen der lokalen „Partnerschaften für Demokratie", die Teil des Bundesprogamms „Demokratie leben" sind. Diese werden auch von der hessischen Landesregierung gefördert. Darüber hinaus unterstützen der DGB und die DGB-Jugend seit 2007, also von Beginn an, die Arbeit des „Beratungsnetzwerks" auf Landesebene. In all diesen Jahren haben sich die zuständigen MitarbeiterInnen des DGB aktiv für die Stärkung und Weiterentwicklung der dortigen Initiativen und Programme eingesetzt. Das „Netzwerk Demokratie und Courage", das jährlich über 100 antirassistische und demokratiefördernde Workshops an allgemein- und berufsbildenden Schulen umgesetzt hat und von 2004 bis 2015 ein Projekt der DGB-Jugend Hessen war, ist seit 2016 Teil des Landesprogramms „Hessen – aktiv für Demokratie und gegen Extremismus". Seit Dezember 2017 ist der Bildungsträger „Arbeit und Leben", eine Weiterbildungseinrichtung,

die vom DGB und dem Deutschen Volkshochschulverband (DVV) getragen wird, mit dem Projekt „Arbeitswelt und Rechtspopulismus" beauftragt, Bildungsarbeit gegen Rassismus und Ausgrenzung und für demokratisches Bewusstsein in den Betriebe umzusetzen – und in diesem Kontext die Zusammenarbeit von Kommunen mit Unternehmen in Bezug auf die Integration von Geflüchteten zu fördern. Die GEW Hessen ist außerdem Mitinitiatorin des „Bündnisses gegen Berufsverbote Hessen". Zur Stärkung unserer Demokratie beteiligen sich der DGB und seine Mitgliedsgewerkschaften gerne an politischen Programmen des Bundes und des Landes.

Der vorliegende Gesetzesentwurf betrifft und besorgt uns vor dem geschilderten Hintergrund in besonderem Maße. Statt denjenigen Menschen und Organisationen den Rücken zu stärken, die sich schon jetzt unter widrigen Umständen dem zunehmendem Rechtspopulismus und der zu beobachtenden Akzeptanz menschenfeindlicher Ideologien die Grundwerte eines friedlichen demokratischen Zusammenlebens entgegenstellen, werden diese Personen hier unter Generalverdacht gestellt. Dabei sprechen wir an dieser Stelle keineswegs nur für den DGB, sondern auch für die zahlreichen ehrenamtlichen Aktiven und mehr als drei Dutzend zivilgesellschaftlichen Träger des Beratungsnetzwerks. Ohne deren Engagement würde die Arbeit gegen menschenverachtende Einstellungen in der Gesellschaft, gegen Diskriminierung und gegen die extreme Rechte in Hessen keineswegs die Qualität aufweisen, auf die die Landesregierung gerne hinweist.

Mit Sorge müssen wir feststellen, dass trotz des gesellschaftlichen Drucks in den letzten Wochen die Regierungsfraktionen nicht von ihrer Linie abweichen, Überprüfungen der „Zuverlässigkeit" von Einzelpersonen und Trägern vorzunehmen. Wir beziehen uns hierbei explizit auf §21, Abs. 1, Nr. 2 Buchst. i. Bei der Formulierung dieses Absatzes bleiben – trotz einiger Änderungsvorschläge weitere Fragen offen:

Wann genau wird ein Anlass definiert um Personen oder Organisationen auf ihre Zuverlässigkeit zu überprüfen? Was genau sind „begründete Einzelfälle"?

Die „anlassbezogene Überprüfung" beruht auf Kriterien, Perspektiven und Erkenntnissen des Landesamtes für Verfassungsschutz. Das Vorgehen stellt für uns gerade vor dem Hintergrund der intransparenten Vorgehensweise und Speicherpraxis der Verfassungsschutzbehörden einen nicht zu rechtfertigenden Eingriff in das informationelle Selbstbestimmungsrecht und den Schutzbereich der ArbeitnehmerInnen dar.

Diese juristische Ungenauigkeit bietet unserer Auffassung nach Spielräume, die – wie in einem Fall vom Frühjahr letzten Jahres[1] – zu Verleumdungen und erheblichen Eingriffen in die Persönlichkeitsrechte auf Arbeitnehmendenseite führen können. Zudem würde das LfV mit einer solchen Überprüfung – und vor allem dann, wenn eine solche Überprüfung negativ für die Arbeitnehmenden ausfallen sollte und diese damit aus Sicht des LfV nicht mehr weiter beschäftigt werden könnten – direkt in die Autonomie der Träger in Personalfragen

[1] http://www.fr.de/frankfurt/frankfurt-streit-um-suspendierungen-a-1020531

eingreifen. Die angesprochene Intransparenz wird dadurch noch verstärkt, dass künftig Personen nur Auskunft über die abgespeicherten Daten erhalten sollen, wenn die betroffene Person „auf einen konkreten Sachverhalt hinweist [...]" (§27, Abs.1).

Neben dem nicht nachzuvollziehenden Misstrauen werden im §21, Abs. 1, Nr. 2 Buchst. i. Delegitimierungskampagnen von AfD und extrem rechten Organisationen Tür und Tor geöffnet. Diese versuchen schon heute in Hessen, so in verschiedenen kommunalen Parlamenten seit März 2016 geschehen, Zweifel an der Eignung der Träger und ihrer MitarbeiterInnen zu säen und diese per se als „Linksextreme" zu brandmarken. Dass allerdings genau diese Menschen und Träger in ihrer alltäglichen Arbeit für Menschenrechte, demokratische Werte und den Rechtsstaat einstehen und dafür teils bedroht werden, sollte für die Regierung eine Aufforderung sein, genau jene zu unterstützen und ihnen wertschätzend den Rücken zu stärken.

Deswegen fordern wir die ersatzlose Streichung des §21, Abs. 1, Nr. 2 Buchst. i.

Indes fordern wir, dass die Vergabe von Landesmitteln des Projekts „Hessen aktiv für Demokratie und gegen Extremismus" nicht erneut an das Bekenntnis der Träger zur „freiheitlich demokratischen Grundordnung" gekoppelt wird. Das „uneingeschränkte Eintreten für die fdGO" (freiheitlich-demokratische Grundordnung) ist bisweilen in den Zuwendungsbescheiden fixiert, die die Träger unterschreiben müssen. Die Vergabebedingungen formulieren zudem eine Neutralitätspflicht der beteiligten Träger im Rahmen ihrer Projekte. Zweifelsohne besteht diese Pflicht für den Staat. Er kann sie aus unserer Sicht jedoch nicht auf den einzelnen Träger und einzelne Projekt übertragen. Das Prinzip der Trägerpluralität hat sich seit mehr als 70 Jahren bewährt. Die darin zu erkennenden unterschiedlichen demokratietheoretischen Vorstellungen müssen auch weiterhin Teil des demokratischen Diskurses bleiben.

Mit freundlichen Grüßen

Helena Müller

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Prof. Dr. Jan Dirk Roggenkamp
Fachbereich 5
Polizei und Sicherheitsmanagement
Campus Lichtenberg
Alt-Friedrichsfelde 60
10315 Berlin

jan.roggenkamp@hwr-berlin.de

Gutachterliche Stellungnahme

anlässlich der öffentlichen Anhörung im Innenausschuss des Hessischen Landtages

am 8. Februar 2018

zu dem

Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen - Drucks. 19/5412

sowie

Änderungsantrag der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN - Drucks. 19/5782

Überblick

Einleitung

Der mir zur schriftlichen Stellungnahme vorgelegte Gesetzentwurf zur Neuausrichtung des Verfassungsschutzes in Hessen (LT-Drs. 19/5142 hierzu Änderungsantrag LT-Drs. 19/5782) enthält - das folgt bereits aus dem Titel des Gesetzentwurfs - umfangreiche Neuregelungen im hessischen Verfassungsschutzgesetz (i.W. HVerfSchG). Daneben wird auch das Hessische Sicherheits- und Ordnungsgesetz (i.W. HSOG) umfangreich erweitert und novelliert. Angesichts der postlaufzeit- und weihnachtsunterbrechungsbedingt kurzen Bearbeitungszeit kann und soll die vorgelegte Stellungnahme nur zu spezifischen Punkten erfolgen.

Teil 1 Regelungen im neuen HVerfSchG

I. Quellen-Telekommunikationsüberwachung, § 6 Abs. 2 HVerfSchG

1. Ausgangslage

a. Regelung

> **§ 6 (2) HVerfSchG**
>
> Um eine Maßnahme nach § 1 Abs. 1 Nr. 1 des Artikel-10-Gesetzes durchzuführen, darf das Landesamt unter den Voraussetzungen des § 3 des Artikel-10-Gesetzes ohne Wissen der betroffenen Person mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingreifen, wenn
> 1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und
> 2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

b. Regelungsinhalt

Nach dem neuen § 6 Abs. 2 HVerfSchG darf ein heimlicher Zugriff auf *„von der Person genutzte informationstechnische Systeme"* erfolgen um eine Telekommunikationsüberwachungsmaßnahme (TKÜ) nach § 1 Abs.1 Nr. 1 Artikel 10-Gesetz durchzuführen. Es handelt sich um eine Befugnis zur Durchführung einer sog. Quellen-Telekommunikationsüberwachung (i.W. Quellen-TKÜ), mit deren Hilfe auf Kommunikation zugegriffen werden soll, die auf Grund der verschlüsselten Übermittlung (z.B. durch Nutzung sog. Messengersysteme) im Rahmen einer „herkömmlichen" TKÜ nicht zur Kenntnis genommen werden kann.

Voraussetzung für eine Maßnahme nach § 6 Abs. 2 HVerfSchG ist, dass *„1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und 2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen."*.

2. Kritikpunkt 1: Explizite Rechtsgrundlage

Es ist zu begrüßen, dass eine explizite Befugnis zur Durchführung einer Quellen-TKÜ geschaffen wird.

Da die Quellen-TKÜ einen Grundrechtseingriff darstellt, der qualitativ über den der „einfachen" TKÜ hinausgeht, ist eine explizite Regelung erforderlich.[1] Dies hat auch der Bundesge-

[1] Vgl. bereits (für die StPO) *Braun/Roggenkamp*, K&R 2011, 681, 682f.

setzgeber für die StPO so gesehen und jüngst die dortige Regelung zur TKÜ (§ 100a StPO) u.a. wie folgt erweitert:

> § 100a Abs. 1 S. 2, 3 StPO:
>
> *Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. Auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.*
>
> § 100a Abs. 5 StPO:
>
> *Bei Maßnahmen nach Absatz 1 Satz 2 und 3 ist technisch sicherzustellen, dass*
>
> *1. ausschließlich überwacht und aufgezeichnet werden können:*
> *a) die laufende Telekommunikation (Absatz 1 Satz 2), oder*
> *b) Inhalte und Umstände der Kommunikation, die ab dem Zeitpunkt der Anordnung nach § 100e Absatz 1 auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können (Absatz 1 Satz 3),*
> *2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und*
> *3. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.*
> *Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.*

Vorbildfunktion für diese Regelung hatte - wie auch für den hier gegenständlichen § 6 Abs. 2 HVerfSchG - der § 20 l Abs. 2 S. 1 BKAG, der wie folgt gefasst ist:

> *„Die Überwachung und Aufzeichnung der Telekommunikation darf ohne Wissen des Betroffenen in der Weise erfolgen, dass mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn*
> *1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und*
> *2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen."*

3. Kritikpunkt 2: Gesetzgebungskompetenz

Für eine Regelung zur Quellen-TKÜ im Landesrecht besteht keine Gesetzgebungskompetenz.

Es stellt sich allerdings die Frage, ob § 6 Abs. 2 HVerfSchG tatsächlich - wie es die Entwurfsbegründung suggeriert - lediglich die Funktion erfüllt *„die Bestimmtheit der gesetzlichen Be-*

fugnisse zu erhöhen und die Rechtsicherheit" zu verbessern und sie nur *„darauf abzielt, die technischen Voraussetzungen für die eigentliche Telekommunikationsüberwachung"* zu schaffen.[2] Aus diesem Grund stünden, so die Begründung weiter, *„die bundesgesetzlichen Regelungen des Artikel-10-Gesetzes einer landesgesetzlichen Regelung nicht entgegen."*

Diese Einschätzung wird hier nicht geteilt. Wie auch § 100a Abs. 2 S. 2 StPO und § 20 l Abs. 2 BKAG handelt es sich bei § 6 Abs. 2 HVerfSchG um eine *„besondere Ermächtigungsgrundlage"*[3] für die Überwachung und Aufzeichnung von Kommunikationsinhalten auf einem informationstechnischen System des Betroffenen. Sie enthält wie § 20 l Abs. 2 BKAG *„zusätzliche weitere Voraussetzungen"* unter denen die Durchführung der Quellen-TKÜ erst *„erlaubt"* ist.[4]

Für eine solche „besondere" TKÜ-Regelung lässt das Artikel-10-Gesetz aber neben §§ 1, 3 Artikel-10-Gesetz, die bereits die TKÜ regeln, keinen Raum[5].

4. Kritikpunkt 3: Anforderungen an die verwendete Software

Es sollte klargestellt werden, dass nur eine Quellen-TKÜ-Software eingesetzt werden darf, die vorab von einer unabhängigen Stelle auf Einhaltung der verfassungsrechtlichen Anforderungen überprüft (und ggf. zertifiziert) werden sollte.

Im Gegensatz zur herkömmlichen TKÜ ist es im Rahmen der Quellen-TKÜ erforderlich, auf das zur Telekommunikation genutzte informationstechnische System (z.B. Smartphone, PC) zuzugreifen, um dort die noch unverschlüsselte Kommunikation abzufangen und auszuleiten. Hierfür ist die Installation einer Software auf dem Zielsystem erforderlich, was mit tatsächlichen Risiken behaftet ist. Diese hat das BVerfG in der sog. „Online-Durchsuchungs"-Entscheidung[6] wie folgt dargestellt:

> *„Wird ein komplexes informationstechnisches System zum Zweck der Telekommunikationsüberwachung technisch infiltriert („Quellen-Telekommunikationsüberwachung"), so ist mit der Infiltration die entscheidende Hürde genommen, um das System insgesamt auszuspähen. Die dadurch bedingte Gefährdung geht weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist. Insbesondere können auch die auf dem Personalcomputer abgelegten Daten zur Kenntnis genommen werden, die keinen Bezug zu einer telekommunikativen Nutzung des Systems aufweisen. Erfasst werden können beispielsweise das Verhalten bei der Bedienung eines Personalcomputers für eigene Zwecke, die Abrufhäufigkeit bestimmter Dienste, insbesondere auch der Inhalt angelegter Dateien oder – soweit das infiltrierte informationstechnische System auch Geräte im Haushalt steuert – das Verhalten in der eigenen Wohnung.*
>
> *Nach Auskunft der in der mündlichen Verhandlung angehörten sachkundigen Auskunftspersonen kann es im Übrigen dazu kommen, dass im Anschluss an die Infiltration*

[2] LT-Drs. 19/5412, Begründung, S. 32; wortgleich auch die Begründung zu BayLT-Drs. 17/11609, S. 22 zu Art. 13 BayVSG.
[3] BT-Drs. 18/12785 zu § 100a Abs. 1 S. 2 StPO.
[4] Vgl. BVerfG, Urteil vom 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09 - „BKAG" - Rn. 234
[5] Zu berücksichtigen ist in diesem Zusammenhang die Auffassung, nach welcher der § 3 Artikel-10-Gesetz selbst kompetenzwidrig erlassen wurde (*Roggan*, G-10-Gesetz, § 3 Rn. 3 m.w.N.). In diesem Fall wäre § 6 Abs. 2 HVerfSchG ebenfalls verfassungswidrig, da er bezüglich seiner Voraussetzungen auf diesen verweist.
[6] BVerfG, Urteil vom 27. 2. 2008 - 1 BvR 370/07, 1 BvR 595/07 - die folgenden Zitate finden sich in Rn. 188 und 189.

> *Daten ohne Bezug zur laufenden Telekommunikation erhoben werden, auch wenn dies nicht beabsichtigt ist. In der Folge besteht für den Betroffenen – anders als in der Regel bei der herkömmlichen netzbasierten Telekommunikationsüberwachung – stets das Risiko, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere persönlichkeitsrelevante Informationen erhoben werden."*

Damit Art. 10 Abs. 1 GG *„der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer ‚Quellen-Telekommunikationsüberwachung'"* bleibt, muss durch *„technische Vorkehrungen und rechtliche Vorgaben"* sichergestellt sein, dass sich die Überwachung *„ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt"*.[7]

Diese Vorgaben des BVerfG greift der Entwurf - wie auch die Vorbildregelung in § 20l Abs. 2 BKAG - auf, indem er sie schlicht in Gesetzesform wiedergibt. Das soll nach Auffassung des BVerfG ausreichend sein:

> *„Ob oder wie sich durch technische Maßnahmen sicherstellen lässt, dass ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet wird, betrifft die Anwendung der Norm, nicht aber ihre Gültigkeit."*[8]

Zu berücksichtigen ist aber, dass nach dem BVerfG das zur Quellen-TKÜ verwendete Programm so auszugestalten ist, *„dass es - hinreichend abgesichert auch gegenüber Dritten - den mit der Überwachung betrauten Mitarbeiterinnen und Mitarbeitern [...] inhaltlich eine ausschließlich auf die laufenden Kommunikationsinhalte begrenzte Kenntnisnahme ermöglicht"*.

Mit anderen Worten: es bedarf einer streng monofunktionalen[9] Software[10] deren Existenz bislang nicht belegt (und technisch auch schwer vorstellbar) ist.[11]

Mit Hilfe dieser Software dürfte *nicht* übermittelt werden, ob beispielsweise das überwachte Smartphone an- oder ausgeschaltet ist. Ebenfalls dürften keine Standortdaten übermittelt werden, sofern sie nicht Umstände konkreter Kommunikation sind. Eine Screenshotfunktion wäre unzulässig, da diese auch Nachrichten abbilden könnte, die der Nutzer nur formuliert, dann aber nicht absendet.[12] Die Möglichkeit eines Zugriffs auf Daten zurückliegender, also nicht mehr laufender Kommunikation (hierzu noch sogleich) müsste ausgeschlossen sein.

Es wird weder aus dem Gesetzestext noch aus der Begründung deutlich, wie diese Vorgaben eingehalten werden bzw. wer oder wie die Einhaltung überprüft werden sollen.

Zu begrüßen ist es, dass eine Verpflichtung zur *„Protokollierung des eingesetzten technischen Mittels"* in § 6 Abs. 4 Satz 1 Nr. 1 HVerfSchG vorgesehen ist. Diese Protokollierungspflicht wird jedoch verwässert, wenn - wie es die Begründung klarstellt *„lediglich allgemein verständliche Angaben zum Funktionsumfang"*[13] - festgehalten werden sollen.

---

[7] BVerfG, Urteil vom 27. 2. 2008 - 1 BvR 370/07, 1 BvR 595/07 - Rn. 190.
[8] BVerfG, Urteil vom 20.04.2016 - 1 BvR 966/09, 1 BvR 1140/09 - „BKAG" - Rn. 234.
[9] Die Software müsste zudem den allgemeinen datenschutzrechtlichen Anforderungen entsprechen.
[10] *Roggenkamp*, in: Peters/Kersten/Wolfenstetter (Hrsg.), Innovativer Datenschutz, 2012, S. 267, 273 f.
[11] Ob die derzeit offenbar bereits eingesetzten Lösungen (vgl. *Pinkert/Tanriverdi*, „Polizei spioniert Handynutzer mit Trojaner aus", Süddeutsche Zeitung v. 26.1.2018 - http://www.sueddeutsche.de/digital/ueberwachung-polizei-spioniert-handynutzer-mit-trojaner-aus-1.3842439) diesen Anforderungen gerecht werden, ist nicht bekannt.
[12] Vgl. BayLfD, Prüfbericht Quellen-TKÜ, S. 27.
[13] LT-Drs. 19/5412, Begründung, S. 33.

Die Überprüfung der Einhaltung der verfassungsrechtlichen Anforderungen kann nicht der anordnenden oder gar der die TKÜ durchführenden Stelle überlassen werden.[14] An geeigneter Stelle sollte klargestellt werden, dass nur eine vorab von einer unabhängigen Stelle entsprechend überprüfte (und ggf. zertifizierte) Quellen-TKÜ Software eingesetzt werden darf.

5. Kritikpunkt 4: Keine retrograde Erhebung

Es ist zu begrüßen, dass § 6 Abs. 2 HVerfSchG keine dem § 100a Abs. 1 S. 3 StPO entsprechende Befugnis enthält.

Eine solche Befugnis, die dem Zugriff auf Kommunikationsinhalte dient, die im Zeitraum zwischen Anordnung der Maßnahme und tatsächlicher Aufnahme der Überwachung erfolgt sind, wäre nicht mit den Vorgaben des BVerfG vereinbar, nach der lediglich die „laufende Kommunikation" im Rahmen der Quellen-TKÜ überwacht werden darf.[15]

6. Kritikpunkt 5: Begleitmaßnahmen / Ausnutzung von Sicherheitslücken

Eine erforderliche Eingrenzung der möglichen und ein klarer Ausschluss unzulässiger Maßnahmen zur Installation der für die Durchführung einer Quellen-TKÜ benötigten Software fehlt bislang. Insbesondere ist die Ausnutzung von bisher unbekannten Sicherheitslücken auszuschließen.

Weder Gesetzentwurf noch Begründung enthalten Regelungen oder Hinweise, über welche Mittel und Wege die Quellen-TKÜ Software auf das informationstechnische System aufgespielt werden darf. Als unbedenklich werden das heimliche Aufspielen etwa bei einer Grenzkontrolle als auch das Zusenden einer E-Mail mit einem getarnten Staatstrojaner angesehen, soweit dieser E-Mail-Anhang keine Sicherheitslücken ausnutzt[16]. Als verfassungsrechtlich unzulässig stellt sich in diesem Zusammenhang das heimliche Eindringen in Wohnräume - und der damit verbundene Eingriff in Art. 13 GG - dar, um die Software zu installieren. Dies sollte zumindest in der Begründung klargestellt werden. Vorbildfunktion kann hier die Begründung zur Neuregelung des § 100a Abs. 1 S. 2 StPO entfalten. Dort heißt es:

> *„Jeder Zugriff auf ein informationstechnisches System des Betroffenen zum Zweck der Aufbringung der Überwachungssoftware darf grundsätzlich nur auf technischem Wege oder mittels kriminalistischer List erfolgen. Eine Befugnis, die Wohnung des Betroffenen zu diesem Zweck heimlich zu betreten, ist mit der Befugnis nach § 100a Absatz 1 Satz 2 StPO nicht verbunden."*[17]

Aber auch die technischen Wege der Infiltration sind zu begrenzen. Die Ausnutzung von Sicherheitslücken in Hard- und Software ist nur als zulässig anzusehen, wenn es sich um bereits bekannte Lücken handelt. Die Ausnutzung von eigens ermittelten oder „angekauften" Informationen über noch unbekannte Sicherheitslücken (sog. zero day exploits) stünde im Widerspruch zur staatlichen Verpflichtung zum Schutz der Bevölkerung vor möglichen Be-

---

[14] Vgl. *Roggan*, StV 2017, 821, 824.
[15] *Roggan*, StV 2017, 821.
[16] *Buermeyer*, Stellungnahme zur Öffentlichen Anhörung zur „Formulierungshilfe" des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess v. 29.5.2017, Ausschuss-Drucksache - 18(6)334, S. 21.
[17] BT-Drs. 18/12785, S. 52.

einträchtigungen der IT-Infrastruktur.[18] Diese Verpflichtung folgt aus dem Recht auf Gewährleistung von Integrität und Vertraulichkeit informationstechnischer Systeme[19] (i.W. IT-Grundrecht). Dieses ist nicht nur Abwehrrecht des Bürgers gegen den Staat. Es enthält auch einen verfassungsrechtlichen Schutz- und Gewährleistungsauftrag zur Verwirklichung der Wertvorstellungen des Grundrechts.[20]

Hingewiesen sei in diesem Zusammenhang auf eine Empfehlung der Expertengruppe der Vereinten Nationen „on Developments in the Field of Information and Telecommunications in the Context of International Security", die unter deutscher Beteiligung u.a. formuliert hat:

> *„States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure."*[21]

II. Online-Durchsuchung

1. Ausgangslage

Der Entwurf des § 8 HVerfSchG enthält eine Regelung zur Durchführung einer sog. Online-Durchsuchung.

a. Regelung

§ 8 HVerfSchG-Entwurf Verdeckter Zugriff auf informationstechnische Systeme

(1) Das Landesamt darf nach Maßgabe des § 7 mit technischen Mitteln verdeckt auf informationstechnische Systeme zugreifen, um
1. Zugangsdaten und verarbeitete Daten zu erheben oder
2. zur Vorbereitung einer Maßnahme nach Nr. 1 spezifische Kennungen sowie den Standort eines informationstechnischen Systems zu ermitteln.

(2) Durch technische Maßnahmen ist sicherzustellen, dass
1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen.
Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) § 6 Abs. 4 gilt entsprechend.

b. Regelungsinhalt

Es handelt sich hierbei um eine Befugnis zu einem Eingriff in das IT-Grundrecht. [22]

---

[18] Vgl. auch *Buermeyer*, Stellungnahme, S. 21f. mit Formulierungsvorschlag auf S. 23.
[19] Grundlegend BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370, 595/07 - „Online-Durchsuchung".
[20] *Heckmann*, in: Heckmann, jurisPK-Internetrecht, 5. Aufl. 2017, Kap. 5 Rn. 125
[21] Vereinte Nationen, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security v. 22.7.2015 - A/70/174, S. 8 Punkt 13 (j) - abrufbar unter: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.
[22] Vgl. BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370, 595/07 - „Online-Durchsuchung".

Die verfassungsrechtlichen Anforderungen an Befugnisse zur Online-Durchsuchung hat das BVerfG bereits in zwei Entscheidungen[23] konkretisiert. Die Begründung lässt erkennen, dass die entsprechenden Vorgaben beachtet werden sollen, indem beispielsweise ein Richtervorbehalt und Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung vorgesehen sind. Zudem besteht ein Bewusstsein dahingehend, dass es sich bei einer Online-Durchsuchung um einen *„mitunter tief in die Privatsphäre reichenden Eingriff"* handelt, der nur *„ausnahmsweise und einzelfallbezogen"* vorgenommen werden soll.[24]

2. Kritikpunkt 1: Geschützte Rechtsgüter

Die in § 7 Satz 1 genannten Schutzgüter, zu deren Zweck eine Online-Durchsuchung stattfinden kann, sind teilweise unscharf bzw. missverständlich und sollten klarer gefasst werden.

Wie die Gesetzesbegründung zutreffend ausführt, stellt das BVerfG an die Angemessenheit einer Eingriffsbefugnis erhöhte Anforderungen:

> *„Der Grundrechtseingriff, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, entspricht im Rahmen einer präventiven Zielsetzung angesichts seiner Intensität nur dann dem Gebot der Angemessenheit, wenn bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen, selbst wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt."*[25]

Nach § 8 Abs. 1 HVerfSchG darf ein verdeckter Zugriff auf informationstechnische Systeme *„nach Maßgabe des § 7"* erfolgen. Das bedeutet, dass die gleichen Voraussetzungen vorliegen müssen wie bei einer technischen Wohnraumüberwachungsmaßnahme nach § 7 HVerfSchG. Erforderlich ist danach das Vorliegen *„tatsächlicher Anhaltspunkte für eine dringende Gefahr für 1. den Bestand oder die Sicherheit des Bundes oder eines Landes, 2. Leib, Leben oder Freiheit einer Person oder 3. Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist"*.

Zumindest missverständlich ist die Nennung der Rechtsgüter *„Leib einer Person"* sowie *„Sachen von bedeutendem Wert"*. Bei ersterem könnte der unbefangene Leser den Eindruck gewinnen, dass auch der Schutz vor leichten und leichtesten Körperverletzungen erfasst wäre. Bei letzterem läge es nahe, den tatsächlichen Sachwert eines Gegenstandes zum maßgeblichen Kriterium zu machen. In beiden Fällen stellte sich die Frage, ob tatsächlich ein *„überragend wichtiges Rechtsgut"* geschützt werden soll.

Zwar hat das BVerfG zu beiden Begriffen in ähnlichem Kontext[26] bereits befunden:

> *„Erlaubt sind Zugriff und Nutzung der Daten nur zum Schutz besonders gewichtiger Rechtsgüter, das heißt zunächst zum Schutz von Leib, Leben, Gesundheit oder Freiheit von Personen. Ersichtlich sind im Kontext dieser Norm unter Gesundheitsbeeinträchtigungen* ***nur schwerwiegende Gesundheitsverletzungen mit dauerhaften Folgen*** *gemeint. Soweit die Vorschrift darüber hinaus auch den Schutz von Sachen mit erhebli-*

---

[23] BVerfG, Urteil vom 27.02.2008 – 1 BvR 370, 595/07 - „Online-Durchsuchung" sowie BVerfG, Urteil vom 20.04.2016 - 1 BvR 966/09, 1 BvR 1140/09 - „BKAG".
[24] LT-Drs. 19/5412, Begründung, S. 34.
[25] BVerfG, Urteil vom 27.02.2008 – 1 BvR 370, 595/07 - „Online-Durchsuchung" - Rn. 242.
[26] Dem § 5 Abs. 2 Satz 1 ATDG.

chem Wert vorsieht, stellt der Gesetzgeber klar, dass es ***nicht um den Schutz des Eigentums oder der Sachwerte als solcher geht****, sondern um Sachen, „deren Erhaltung im öffentlichen Interesse geboten ist" (§ 5 Abs. 2 Satz 1 ATDG).* ***Gemeint sind im Zusammenhang mit der Terrorismusabwehr etwa wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen.***"[27]

Mit Blick auf das Gebot der Normenklarheit und die Tatsache, dass es sich bei der referenzierten Aufzählung „nur" um „besonders gewichtige" (und nicht „überragend wichtige") Rechtsgüter handelt, erscheint eine Klarstellung in § 7 erforderlich.

Es wird angeregt, die Nrn. 2 und 3 entsprechend klar(er) zu formulieren.

3. Kritikpunkt 2: Zweck der Maßnahme

Es ist ausdrücklich klarzustellen, dass eine initiale Datenerhebung durch eine Online-Durchsuchung nur „zum Zweck der Abwehr von Gefahren im Sinne von § 7 Satz 1 HVerfSchG" zulässig ist.

Um den Anforderungen des BVerfG an Maßnahmen zur Datenerhebung zu genügen, muss der Gesetzgeber u.a. den Verwendungszweck *„bereichsspezifisch und präzise"* bestimmen.[28] Diesen Anforderungen wird § 8 HVerfSchG nicht gerecht, da eine konkrete Zweckbestimmung für die Erhebung[29], die in der Abwehr der Gefahren für die in § 7 Satz 1 HVerfSchG liegen muss, zumindest nicht *„präzise"* erkennbar ist. Es wird dementsprechend eine Klarstellung angeregt.

4. Kritikpunkt 3: Mögliche Zielpersonen bzw. -systeme

Es ist klarzustellen, wer mögliche Zielpersonen einer Online-Durchsuchung sind. Die derzeitige Verweisung über § 7 Satz 2 HVerfSchG auf § 3 Abs. 2 Artikel-10-Gesetz ist unzureichend, unpassend und zu weit. Es wird eine Neuformulierung angelehnt an § 20k Abs. 4 BKAG / § 49 Abs. 3 Satz 1 BKAG-2018 bzw. § 15b Abs. 4 HSOG angeregt. Eine Zugriffsmöglichkeit auf informationstechnische System anderer Personen muss den erhöhten Anforderungen der verfassungsrechtlichen Rechtsprechung entsprechen.

Bezüglich der möglichen Zielpersonen einer Online-Durchsuchung findet ebenfalls § 7 Anwendung. Dieser verweist u.a. auf die Regelungen des § 3 Abs. 2 Artikel-10-Gesetz. Dort ist bestimmt:

„(2) [1]Die Anordnung ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. ***[2]Sie darf sich nur gegen den Verdächtigen oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Verdächtigen bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Verdächtige ihren Anschluss benutzt.*** *[3]Maßnahmen, die sich auf Sendungen beziehen, sind nur hinsichtlich solcher Sendungen zulässig, bei denen Tatsachen die Annahme rechtfertigen, dass sie von dem, gegen den sich die Anordnung richtet, herrühren oder für ihn bestimmt sind. [4]Abgeordnetenpost von Mitgliedern des Deutschen Bundestages*

[27] BVerfG, Urteil vom 24.04.2013 - 1 BvR 1215/07 - „ATDG" - Rn. 191 - Hervorhebung nur hier.
[28] BVerfG, Urteil vom 15.12.1983 - 1 BvR 209/83, 1 BvR 484/83, u.a. - „Volkszählung" - Rn. 179.
[29] Die Regelungen zur Zweckänderung in § 9 Abs. 3 HVerfSchG entsprechen den Anforderungen.

und der Parlamente der Länder darf nicht in eine Maßnahme einbezogen werden, die sich gegen einen Dritten richtet." (Hervorhebung nur hier)

Da Voraussetzung für eine Online-Durchsuchung (und auch für eine verdeckte Wohnraumüberwachung) das Vorliegen einer *„dringenden Gefahr"* für ein in § 7 Satz 1 HVerfSchG genanntes Rechtsgut und nicht der *„Verdacht einer Straftat"* ist, ist die Adressatenregelung in § 3 Abs. 2 Satz 2 Artikel-10-Gesetz ungeeignet, da dort auf *„den Verdächtigen"* abgestellt wird. Gemeint ist offenbar die für die Gefahr verantwortliche Person. Eine entsprechende Klarstellung könnte in Anlehnung an § 20k Abs. 4 Satz 1 BKAG / § 49 Abs. 3 Satz 1 BKAG-2018 bzw. § 15b Abs. 4 HSOG lauten, *„Die Maßnahme darf sich nur gegen eine Person richten, die entsprechend § 6 oder § 7 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung verantwortlich ist"*[30].

Darüber hinaus gestattet § 3 Abs. 2 Satz 2 Artikel-10-Gesetz eine Maßnahme gegen Personen, *„von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Verdächtigen bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Verdächtige ihren Anschluss benutzt"*. Hierdurch wird die Möglichkeit eingeräumt sog. Nachrichtenmittler oder Anschlussüberlasser in eine Maßnahme mit einzubeziehen. Die Regelung ist jedoch auf TKÜ-Maßnahmen zugeschnitten und macht - auch in entsprechender Anwendung - weder bei einer Online-Durchsuchung, noch bei einer Wohnraumüberwachung Sinn. Es fehlt also auch hier an der für eine Datenerhebungsmaßnahme, die zudem einen derart schweren Grundrechtseingriff darstellt, erforderlichen Klarheit.

Für den Fall der Wohnraumüberwachung hat das BVerfG ausgeführt:

> *„Nicht zu beanstanden ist gleichfalls, dass § 20h Abs. 2 BKAG dabei die Überwachung solcher Personen nicht nur in deren eigener Wohnung, sondern auch in der Wohnung Dritter erlaubt, wenn sich die Zielperson dort aufhält und Maßnahmen in der Wohnung der Zielperson allein nicht zur Abwehr der Gefahr führen werden.* ***Allerdings hat das Bundesverfassungsgericht für solche Überwachungsmaßnahmen in Wohnungen Dritter eingrenzende Maßgaben zur Auslegung vorgeschrieben. Es bedarf insoweit eines konkretisierten Verdachts, dass sich die Zielperson zur Zeit der Maßnahme in der Wohnung des Dritten aufhält.*** *Dies ist gegebenenfalls durch andere Maßnahmen, wie eine Observation, sicherzustellen. Nicht auf konkrete Anhaltspunkte gestützte Vermutungen für die Anwesenheit der Zielperson in der Wohnung des Dritten reichen für den Beginn der Maßnahme nicht aus (vgl. BVerfGE 109, 279 <356>).* ***Darüber hinaus muss eine hinreichende Wahrscheinlichkeit bestehen, hierbei verfahrensrelevante Informationen zu gewinnen. Erforderlich sind auch insoweit tatsächliche Anhaltspunkte dafür, dass die Zielperson in den zu überwachenden Räumlichkeiten im Überwachungszeitraum verfahrensrelevante und im weiteren Verfahren verwertbare Gespräche führen wird.*** *Bloße Vermutungen und eine Überwachung ins Blaue hinein, allein getragen von der Hoffnung auf Erkenntnisse, genügen nicht (vgl. BVerfGE 109, 279 <356 f.>)."*[31]

Diesen erhöhten Anforderungen an den Eingriff in Grundrechte letztlich nicht für die Gefahr verantwortlicher Personen wird bereits die Regelung für die verdeckte Wohnraumüberwachung in § 7 Satz 2 HVerfSchG iVm. § 3 Abs. 2 Artikel-10-Gesetz nicht gerecht. Es bedarf ei-

---

[30] Einen entsprechenden Verweis auf §§ 17, 18 BPolG in § 20h BKAG hat das BVerfG nicht beanstandet, vgl. BVerfG, Urteil vom 20.04.2016 - 1 BvR 966/09, 1 BvR 1140/09 - „BKAG" - Rn. 187.

[31] BVerfG, Urteil vom 20.04.2016 - 1 BvR 966/09, 1 BvR 1140/09 - „BKAG" - Rn. 188 - Hervorhebungen nur hier.

ner Regelung, wie sie sich z.B. in § 46 Abs. 2 BKAG-2018 findet. Für die Online-Durchsuchung müssen, auf Grund der Vergleichbarkeit der Schwere der Eingriffsintensität mit der verdeckten Wohnraumüberwachung, die gleichen Grundsätze gelten.

Eine (entsprechende) Anwendung der Adressatenregelung - auch einer Neuregelung in der angeregten Form - verbietet sich allerdings für Maßnahmen nach § 8 HVerfSchG. Die Maßnahmen sind in tatsächlicher Hinsicht nicht vergleichbar, da es bei der Online-Durchsuchung nicht um die Überwachung einer Wohnung, sondern eines informationstechnischen Systems geht. Nach hier vertretener Auffassung ist - wie es auch im Fall der Regelung der Online-Durchsuchung in § 100b StPO (dort Abs. 3) geschehen ist - die Schaffung einer eigenständigen Adressatenregelung erforderlich, soll ein Zugriff auf informationstechnische Systeme Nichtverantwortlicher gestattet werden.

Ein Zugriff auf informationstechnische Systeme „anderer Personen" darf nur zulässig sein, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass die Zielperson informationstechnische Systeme der anderen Person (auch) benutzt. Zudem muss eine hinreichende Wahrscheinlichkeit dafür bestehen, dass hierbei Informationen gewonnen werden können, die für die Abwehr der Gefahr erforderlich sind und die auf andere Weise nicht gewonnen werden können.

5. Kritikpunkt 4: Begleitmaßnahmen

Eine erforderliche Eingrenzung der möglichen und ein klarer Ausschluss unzulässiger Maßnahmen zur Installation der für die Durchführung einer Online-Durchsuchung benötigten Software fehlt bislang. Auch hier (zur Parallelproblematik bei der Quellen-TKÜ s.o.) ist die Ausnutzung von bisher unbekannten Sicherheitslücken zu untersagen.

Auch die Online-Durchsuchung erfordert das Aufspielen einer Software auf dem informationstechnischen System der Zielperson. Es gilt das zur Quellen-TKÜ Gesagte entsprechend.

III. Ortung von Mobilfunkendgeräten, § 10 HVerfSchG

Die Regelung zur Ortung von Mobilfunkendgeräten durch sog. IMSI-Catcher ist sowohl mit Blick auf die Tatbestandsvoraussetzungen als auch die möglichen Adressaten zu unbestimmt.

Der Einsatz eines IMSI-Catchers, der zwar „nur" einen Eingriff in das Recht auf informationelle Selbstbestimmung und nicht Art. 10 Abs. 1 GG darstellt, aber regelmäßig eine Vielzahl von Personen betrifft, soll nur zulässig sein *„soweit tatsächliche Anhaltspunkte für eine schwerwiegende Gefahr für die von § 2 umfassten Schutzgüter vorliegen"*. Welche Schutzgüter gemeint sind, wird bei Lektüre des § 2 - der die Aufgaben des Landesamtes umschreibt - nicht mit der hinreichenden Präzision deutlich. Es wird angeregt, diese unmittelbar in § 10 HVerfSchG zu formulieren.

Zudem findet sich auch hier wieder (vgl. oben zur Parallelproblematik bei der Online-Durchsuchung) ein Verweis auf § 3 Abs. 2 Artikel-10-Gesetz, der unpassend und auch in entsprechender Anwendung zu unpräzise ist, da er auf die Verdächtigeneigenschaft einer Person abstellt.

Teil 2 Neuregelungen des HSOG

Durch das Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen wird auch das Hessische Gesetz über die öffentliche Sicherheit und Ordnung (i.W. HSOG) geändert und ergänzt.

I. Erweiterung Zuverlässigkeitsüberprüfung (§ 13b HSOG)

1. Ausgangslage

Die in § 13b HSOG enthaltene Regelung zur Zuverlässigkeitsüberprüfung bei Veranstaltungen in privater Trägerschaft soll erweitert werden.

a. Änderungen/Ergänzungen im Überblick

§ 13b Abs. 1 HSOG - aktuelle Fassung	**§ 13b Abs. 1 HSOG-Entwurf** - inhaltliche Änderungen/Ergänzungen gelb markiert
Eine Zuverlässigkeitsüberprüfung kann durchgeführt werden bei Personen, für die ein privilegierter Zutritt zu einer besonders gefährdeten Veranstaltung in nicht öffentlicher Trägerschaft beantragt wird. Die Polizeibehörde hört den Hessischen Datenschutzbeauftragten an, wenn eine Zuverlässigkeitsüberprüfung nach Satz 1 beabsichtigt ist.	Eine Zuverlässigkeitsüberprüfung kann durchgeführt werden bei Personen, für die ein privilegierter Zutritt zu einer besonders gefährdeten Veranstaltung in nicht öffentlicher Trägerschaft beantragt wird. Bei sonstigen Veranstaltungen in nicht öffentlicher Trägerschaft kann eine Zuverlässigkeitsüberprüfung bei Personen im Sinne des Satz 1 durchgeführt werden, wenn dies zum Schutz der Veranstaltung erforderlich ist. Die Polizeibehörde hört den Hessischen Datenschutzbeauftragten an, wenn eine Zuverlässigkeitsüberprüfung nach Satz 1 oder 2 beabsichtigt ist.

b. Regelungsinhalt

Durch die Ergänzung in § 13b Abs. 1 Satz 2 HSOG werden die Voraussetzung für die Durchführung einer Zuverlässigkeitsüberprüfung von Personen, denen ein *„privilegierter Zutritt"* zu einer Veranstaltung *„in nicht öffentlicher Trägerschaft"* beantragt wird, abgesenkt.

2. Kritikpunkt: Unbestimmtheit / Uferlosigkeit

Im Rahmen der Erweiterung wird versäumt bestehende Unklarheiten bezüglich der verwendeten Begriffe zu klären. Die Erweiterung selbst ist in ihrer jetzigen Fassung zu unbestimmt und damit zu weit gefasst und bedarf der Ergänzung.

Bereits die bestehende Regelung sah und sieht sich Kritik[32] ausgesetzt. Ungeklärt ist und bleibt, wie die verwendeten Begriffe *„privilegierter Zutritt"* oder *„besonders gefährdete Veranstaltung"* zu verstehen sind. Letztere ist nunmehr von der *„sonstigen Veranstaltung"* abzugrenzen, bei der jedoch - damit eine *„Zuverlässigkeitsüberprüfung"* zulässigerweise durchgeführt werden kann - diese *„zum Schutz der Veranstaltung erforderlich"* sein muss.

Lediglich aus der Begründung wird deutlich, dass ein Schutz vor Gefahren insbesondere *„im Zusammenhang mit dem islamistischen Terrorismus"*[33] intendiert ist. Die Formulierung *„zum Schutz der Veranstaltung erforderlich"* suggeriert jedoch, dass auch ein Schutz vor Gefahren

[32] Hierzu BeckOK PolR Hessen/*Bäuerle* HSOG § 13b Rn. 4f.
[33] LT-Drs. 19/5412, Begründung, S. 54.

unterhalb der Schwelle der erheblichen Gefahr ausreichen soll. Das dem offenbar nicht so sein soll, ist in der Norm klarzustellen.

Insofern durch die Erweiterung einer vermeintlich *„abstrakt hohen Gefährdungslage"*[34] begegnet werden soll, sollte dies ebenfalls in der Regelung selbst reflektiert werden. Die Zulassung einer Zuverlässigkeitsüberprüfung hat nicht unerhebliche Eingriffe in das Recht auf informationelle Selbstbestimmung zur Folge. Daran ändert auch die Überprüfung mit *„Einwilligung der betroffenen Person"* (§ 13a Abs. 2 Satz 2 HSOG) nichts, da die *„Einwilligung"* nicht den datenschutzrechtlichen Anforderungen an eine wirksame Einwilligung entspricht:

> *„Denn in aller Regel wird diese allein deshalb erfolgen, da ansonsten eine Tätigkeit im gewünschten Bereich nicht möglich ist, was u. a. auch Konsequenzen für ein bestehendes Arbeitsverhältnis haben könnte."*[35]

II. Rasterfahndung, § 26 HSOG

Die (Wiedereinführung) des Richtervorbehalts bei Durchführung einer Rasterfahndung ist aus verfassungsrechtlicher Sicht zu begrüßen.

Die Notwendigkeit einer richterlichen Anordnung wird in § 26 Abs. 4 HSOG (wieder) eingeführt. Damit werden, wie beabsichtigt[36], die Bedenken bezüglich der verhältnismäßigen Ausgestaltung der Rasterfahndung in verfahrensrechtlicher Hinsicht ausgeräumt.

III. Elektronische Aufenthaltsüberwachung, § 31a HSOG

1. Ausgangslage

Durch § 31a HSOG wird die rechtliche Grundlage für eine „Elektronische Aufenthaltsüberwachung" (i.W. „EAÜ" - missverständlich auch „elektronische Fußfessel" genannt) einschließlich Begleitmaßnahmen geschaffen. Die Regelung lehnt sich ausdrücklich[37] an § 20z BKAG / § 56 BKAG-2018 an und ergänzt diese für den Zuständigkeitsbereich des Landes. Sie stellt - je nach konkreter Ausgestaltung - einen Eingriff sowohl in die Freizügigkeit (Art. 11 GG) als auch die Freiheit der Person (Art. 2 Abs. 2 Satz 2 GG)[38] dar.[39] Zudem wird durch die mit ihr verbundene Datenerhebung in erheblicher Weise in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG) eingegriffen.[40]

2. Kritikpunkt 1: Geeignetheit

Die EAÜ ist zur Zielerreichung geeignet.

Die Sinnhaftigkeit der EAÜ ist durchaus umstritten. Insbesondere wird bezweifelt, ob sie zur Erreichung des Ziels der Verhütung terroristischer Straftaten tatsächlich geeignet ist.[41]

---

[34] LT-Drs. 19/5412, Begründung, S. 54.
[35] 44. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, LT-Drs. 19/3510, S. 36 f.
[36] LT-Drs. 19/5412, Begründung, S. 56.
[37] LT-Drs. 19/5412, Begründung, S. 56.
[38] Zu Fragen der Konkurrenz BeckOK Grundgesetz/*Baldus* GG Art. 11 Rn. 33.
[39] *Lindner/Bast*, DVBl. 2017, 291, 292; Das Grundrecht auf Freiheit der Person ist als eingeschränktes Grundrecht ebenfalls in Art. 4 zu zitieren. Insofern der Änderungsantrag in LT-Drs. 19/5782 in Nr. 3 diese Zitierung nunmehr vorsieht, sollte dies auch in Bezug auf § 31a erfolgen.
[40] *Guckelberger*, DVBl. 2017, 1121, 1124.
[41] Vgl. z.B. *Krone*, „Warum elektronische Fußfesseln keine Attentate verhindern können", br.de vom 1.2.2017 - https://www.br.de/puls/themen/welt/elektronische-fussfessel-terror-100.html.

Die Geeignetheit ist jedoch zu bejahen. Die Frage, ob eine Maßnahme zur Erreichung des angestrebten Ziels geeignet ist, bemisst sich allein danach, ob zumindest ein Beitrag zur Zielerreichung geleistet werden kann[42]. Es erscheint nicht ausgeschlossen, dass die ständige Überwachung des Aufenthaltsorts von Personen, die durch die EAÜ ermöglicht wird, eine Verhütung von Straftaten zumindest fördert. Die EAÜ kann einerseits abschreckende Wirkung entfalten und andererseits zu Erkenntnissen führen, die ein rasches Eingreifen ermöglichen.[43]

3. Kritikpunkt 2: Erforderlichkeit

Die EAÜ kann auch als erforderlich, ggf. sogar als gegenüber anderen Maßnahmen vorzugswürdig angesehen werden.

Als alternative Maßnahmen zur EAÜ kommen die Observation (§ 15 HSOG) oder die Ingewahrsamnahme[44] (§ 32 HSOG) in Betracht. Es handelt sich hierbei jedoch nur bedingt um gleichermaßen zur Zielerreichung geeignete Maßnahmen, die zudem regelmäßig mit einem intensiveren Eingriff in die Rechte des Betroffenen einhergehen als die EAÜ.

So kann eine Observation (ggf. in Verbindung mit einem Aufenthaltsverbot und/oder einer Meldeauflage) nur sehr viel aufwändiger realisiert werden. Insbesondere ist die Gewährleistung einer gleichermaßen „flächendeckenden" Aufenthaltsüberwachung durch menschliche Beobachtung nur schwer vorstellbar. Damit diese überhaupt realisierbar ist, wäre ein Verfolgen „auf Schritt und Tritt" erforderlich. Zudem würde die Observation - insbesondere wenn sie heimlich erfolgt - einen im Ergebnis stärkeren Eingriff in die Persönlichkeitsrechte des Betroffenen bedeuten. Gegenstand einer Observation sind typischerweise nicht nur der Aufenthaltsort, sondern auch die Umstände des Aufenthalts (konkrete Tätigkeiten, Gesprächspartner, Verhalten).

Eine Ingewahrsamnahme stellt einen stärkeren Eingriff in die Freiheit der Person des Betroffenen dar, da sie stets eine Freiheitsentziehung bedeutet. Auch wenn die EAÜ mit einem Verbot, einen bestimmten Bereich (z.B. das Grundstück der betroffenen Person) nicht ohne Erlaubnis der Polizeibehörden zu verlassen „kombiniert" wird (vgl. § 31a Abs. 2 Nr. 1 HSOG), stellt sich dies dennoch als weniger einschneidende Einschränkung dar, als der Aufenthalt in einem Gewahrsamsraum. Schließlich beträgt die höchstens zulässige Dauer des Unterbindungsgewahrsams de lege lata (§ 35 Abs. 1 Nr. 4 HSOG) sechs Tage und ist nur zulässig, wenn die Begehung einer Straftat *„mit erheblicher Bedeutung für die Allgemeinheit"* unmittelbar bevorsteht, also in allernächster Zeit zu erwarten ist.[45]

4. Kritikpunkt 3: Angemessenheit

Die geplante Regelung stellt sich auch als angemessen und verhältnismäßig ausgestaltet dar.

Die EAÜ dient der Verhütung von terroristischen Straftaten und ist nur zum Schutz höchstrangiger Rechtsgüter zulässig. Die mit ihr einhergehenden Einschränkungen der Grundrechte der betroffenen Person stehen nicht in erkennbarem Missverhältnis zu diesem Ziel.

---

[42] Vgl. z.B. BVerfG NVwZ 1997, 1109, 1111 m.w.N.
[43] Wie hier *Guckelberger*, DVBl. 2017, 1121, 1125.
[44] *Lindner/Bast*, DVBl. 2017, 291, 292 - „aliud zum polizeirechtlichen Gewahrsam".
[45] *Meixner/Fredrich*, HSOG-Kommentar, § 32 Rn. 13.

Die Regelung ist zudem verhältnismäßig ausgestaltet. Für alle Maßnahmen nach § 31a Abs. 1 und 2 HSOG ist ein Richtervorbehalt und eine grundsätzliche Befristung auf drei Monate vorgesehen. Die Daten müssen - sollten sie nicht (mehr) zu den genau festgelegten Zwecken benötigt werden - *„spätestens zwei Monate"* nach Erhebung gelöscht werden.

Zu begrüßen ist die Einschränkung in Abs. 4 Satz 3, nach welchem im Rahmen der technischen Möglichkeiten[46] sicherzustellen ist, *„dass innerhalb der Wohnung der Person keine über den Umstand ihrer Anwesenheit hinausgehenden Aufenthaltsdaten erhoben werden"*. Diese wird durch die Regelung in Abs. 4 Satz 9 ergänzt: *„Werden innerhalb der Wohnung der betroffenen Person über den Umstand ihrer Anwesenheit hinausgehende Aufenthaltsdaten erhoben, dürfen diese nicht verwendet werden und sind unverzüglich nach Kenntnisnahme zu löschen."*.

5. Kritikpunkt 4: Ergänzende Anordnungen

Die in § 31a Abs. 2 HSOG vorgesehenen „ergänzenden Anordnungen" sind teilweise zu unbestimmt. Sie sollten mit bereits bestehenden bzw. vorgeschlagenen Standardmaßnahmen abgestimmt werden. Insb. § 31a Abs. 2 Nr. 3 HSOG erscheint zu pauschal und überflüssig.

Nach der Begründung knüpfen die nach § 31a Abs. 2 HSOG möglichen ergänzenden Anordnungen *„im Hinblick auf ihre Voraussetzungen an Abs. 1 an. Sie sind aber nicht nur zusätzlich zu einer Maßnahme der elektronischen Aufenthaltsüberwachung zulässig, sondern können auch unabhängig davon angeordnet werden"*[47].

Insbesondere die nach § 31a Abs. 2 Nr. 3 HSOG mögliche Auflage, *„sich zu bestimmten Zeiten bei einer Polizeidienststelle zu melden"* erscheint allerdings - insb. im Vergleich zur neugeregelten „allgemeinen" Meldeauflage (hierzu sogleich) - zu pauschal und unbestimmt. In Fällen, in denen eine EAÜ stattfindet, dürfte eine entsprechende Anordnung überflüssig sein, da ja eine permanente Standortüberprüfung möglich ist. In anderen Fälle dürfte die allgemeine Meldeauflage ausreichend sein.

Die in § 31a Abs. 2 Nr. 2 HSOG vorgesehene Möglichkeit der Anordnung *„sich nicht an bestimmten Orten aufzuhalten, die [ihr] Gelegenheit oder Anreiz zu Straftaten bieten können"* ist ebenfalls zu unbestimmt formuliert. Systematisch ist diese Maßnahme beim Aufenthaltsverbot (§ 30 Abs. 3 HSOG) zu verorten und auch im Zusammenhang mit diesem zu regeln.

6. Kritikpunkt 5: Flankierende Regelung

Die den § 31a HSOG flankierenden Regelungen in §§ 32 und 43b HSOG begegnen keinen Bedenken.

Die Erweiterung der Regelung zum sog. Durchsetzungsgewahrsam in § 32 auf Fälle der EAÜ und Maßnahmen nach § 31a Abs. 2 HSOG begegnen keinen Bedenken. Ein Durchsetzungsgewahrsam ist danach nur zulässig, wenn die *„Unerlässlichkeit"* (zur Erreichung des mit der EAÜ angestrebten Ziels[48]) der mit der Maßnahme verbundenen Freiheitsentziehung - deren

---

[46] Derzeit realisiert durch eine sog. Home-Unit.
[47] LT-Drs. 19/5412, S. 57.
[48] Der Durchsetzungsgewahrsam darf - wie auch bei Verstößen gegen § 30 HSOG - nicht zur Sanktionierung missbraucht werden.

maximale Dauer mit zehn Tagen in Anbetracht der Gewichtigkeit der zu schützenden Rechtsgüter nicht zu beanstanden ist - durch einen Richter bestätigt wurde.

Die an § 145a StGB / § 87 BKAG-2018 angelehnte Strafvorschrift begegnet ebenfalls keinen Bedenken. Durch das Erfordernis der (vorsätzlichen) Zweckgefährdung wird vermieden, dass jeder Verstoß gegen eine Anordnung nach § 31a HSOG gewissermaßen automatisch eine Strafbarkeit nach sich zieht. Geringfügige Verstöße und/oder Verstöße, bei denen eine Kausalität für die Gefährdung nicht feststellbar ist, führen nicht zu einer Strafbarkeit.[49]

IV. Erweiterung der offenen Videoüberwachung, § 14 Abs. 3, 4 HSOG

1. Ausgangslage

Die bestehenden Regelungen des § 14 Abs. 3 und Abs. 4 HSOG sollen zum Zweck der Erweiterung der offenen Videoüberwachung geändert werden.

a. Änderungen/Ergänzungen im Überblick

§ 14 Abs. 3, 4 HSOG - aktuelle Fassung	**§ 14 Abs. 3, 4 HSOG-Entwurf** - inhaltliche Änderungen/Ergänzungen gelb markiert
(3) Die Polizeibehörden können zur Abwehr einer Gefahr oder wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Straftaten drohen, öffentlich zugängliche Orte mittels Bildübertragung offen beobachten und aufzeichnen. Der Umstand der Überwachung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen. Fest installierte Anlagen dürfen unabhängig davon, ob die Voraussetzungen für ihre Errichtung nach Satz 1 noch vorliegen, zwei Jahre lang betrieben werden; die Frist verlängert sich entsprechend, wenn die Voraussetzungen weiterhin vorliegen. Abs. 1 Satz 2 und 3 sowie § 15 des Hessischen Datenschutzgesetzes gelten entsprechend. (4) Die Gefahrenabwehrbehörden können mittels Bildübertragung offen beobachten und aufzeichnen: 1. zur Sicherung öffentlicher Straßen und Plätze, auf denen wiederholt Straftaten begangen worden sind, sofern tatsächliche Anhaltspunkte für weitere Straftaten bestehen, 2. zum Schutz besonders gefährdeter öffentlicher Einrichtungen, 3. zur Steuerung von Anlagen zur Lenkung oder Regelung des Straßenverkehrs, soweit Bestimmungen des Straßenverkehrsrechts nicht entgegenstehen. Gefahrenabwehrbehörde im Sinne der Nr. 2 ist auch der Inhaber des Hausrechtes. Abs. 1 Satz 2 und 3, Abs. 3 Satz 2 und 3 sowie § 15 des Hessischen Datenschutzgesetzes gelten entsprechend.	(3) Die Gefahrenabwehr- und die Polizeibehörden können zur Abwehr einer Gefahr oder wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Straftaten drohen, öffentlich zugängliche Orte mittels Bildübertragung offen beobachten und aufzeichnen. Der Umstand der Überwachung sowie der Name und die Kontakdaten der oder des Verantwortlichen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen. Fest installierte Anlagen dürfen unabhängig davon, ob die Voraussetzungen für ihre Errichtung nach Satz 1 noch vorliegen, zwei Jahre lang betrieben werden; die Frist verlängert sich entsprechend, wenn die Voraussetzungen weiterhin vorliegen. Abs. 1 Satz 2 und 3 ~~sowie § 15 des Hessischen Datenschutzgesetzes~~ gelten entsprechend. (4) Die Gefahrenabwehr- und die Polizeibehörden können mittels Bildübertragung offen beobachten und aufzeichnen: ~~1. zur Sicherung öffentlicher Straßen und Plätze, auf denen wiederholt Straftaten begangen worden sind, sofern tatsächliche Anhaltspunkte für weitere Straftaten bestehen,~~ 1. zum Schutz besonders gefährdeter öffentlicher Einrichtungen oder Räumlichkeiten, 2. zur Steuerung von Anlagen zur Lenkung oder Regelung des Straßenverkehrs, soweit Bestimmungen des Straßenverkehrsrechts nicht entgegenstehen. Soweit der Inhaber des Hausrechts nicht Gefahrenabwehr- oder Polizeibehörde ist, gilt er im Fall des Satz 1 Nr. 1 als Gefahrenabwehrbehörde. Abs. 1 Satz 2 und 3 und Abs. 3 Satz 2 und 3 ~~sowie § 15 des Hessischen Datenschutzgesetzes~~ gelten entsprechend.

[49] Vgl. zu § 145a StGB BeckOK StGB/*Heuchemer* StGB § 145a Rn. 7, 10.

b. Regelungsinhalt

Durch die vorgesehene Änderung ist insbesondere die Absenkung der Anforderungen an die offene Videoüberwachung durch die Gefahrenabwehrbehörden intendiert. Wie im Fall der Videoüberwachung durch die Polizei soll nunmehr auch diesen die Überwachung sämtlicher öffentlich zugänglicher Orte (bisher *„öffentliche Straßen und Plätze"*) möglich sein.

Voraussetzung ist nicht mehr, dass es sich bei der zu beobachtenden Straße bzw. dem zu beobachtenden Platz um eine Straße bzw. einen Platz handelt, *„auf denen wiederholt Straftaten begangen worden sind"* und bei denen *„tatsächliche Anhaltspunkte für weitere Straftaten"* vorliegen (§ 14 Abs. 4 Nr. 1 HSOG a.F.). Ausreichend ist nun auch für die Gefahrenabwehrbehörden - zumindest nach dem Wortlaut der Neufassung - das der Zweck der Gefahrenabwehr verfolgt wird oder *„tatsächliche Anhaltspunkte"* dafür vorliegen, dass Straftaten *„drohen"*.

c. Grundrechtsrelevanz

Schon die bloße Beobachtung durch Videotechnik stellt einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar.[50] Mit guten Argumenten wird vertreten, dass bereits bei Bestehen der technischen Möglichkeit der Beobachtung ein Eingriff vorliegt.[51] Die Aufzeichnung bzw. Speicherung ist zudem ein Eingriff in das Recht am eigenen Bild. Darüber hinaus werden verfassungsrechtliche Bedenken mit Blick auf die Versammlungsfreiheit geäußert.[52]

Der mit der Videoüberwachung verbundene Eingriff ist von hohem Gewicht, da es sich um einen Eingriff großer Streubreite handelt, der eine Vielzahl von Personen betrifft, die keinen Anlass für die Überwachung gegeben haben.

> *„Verdachtslose Eingriffe mit großer Streubreite, bei denen zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben, weisen grundsätzlich eine hohe Eingriffsintensität auf [...]."*[53]

Insbesondere besteht bei Videoaufzeichnungen eine erhöhte Gefahr des Missbrauchs zum Nachteil der gefilmten Personen. Bereits 2007 hat das BVerfG zutreffend festgestellt:

> *„Durch die Aufzeichnung des gewonnenen Bildmaterials werden die beobachteten Lebensvorgänge technisch fixiert und können in der Folge abgerufen, aufbereitet und ausgewertet sowie mit anderen Daten verknüpft werden. So kann eine Vielzahl von Informationen über bestimmte identifizierbare Betroffene gewonnen werden, die sich im Extremfall zu Profilen des Verhaltens der betroffenen Personen in dem überwachten Raum verdichten lassen."*[54]

---

[50] BeckOK PolR Nds/*Roggenkamp/Albrecht* Nds. SOG § 32 Rn. 3 m.w.N.; VG Hannover, Urteil v. 09.06.2016 - 10 A 4629/11.
[51] So z.B. *Roggan*, NVwZ 2001, 134, 136 m.w.N. auch zur aA.
[52] *Hornmann*, HSOG, § 14 Rn. 34.
[53] BVerfG NVwZ 2007, 688, 691.
[54] BVerfG NVwZ 2007, 688, 690.

Die mit einer offenen Videoüberwachung und -aufzeichnung einhergehenden Gefährdungen des Persönlichkeitsrechts insb. durch Verknüpfung mit anderen Datenquellen haben sich durch den technischen Fortschritt in den vergangenen Jahren vervielfacht. Es ist inzwischen technisch ohne weiteres möglich in kürzester Zeit ein umfangreiches Persönlichkeitsprofil einer Person zu erstellen. Moderne hochauflösende und in unmittelbar digital verarbeitbarer Form speichernde Videoüberwachungslösungen sind hierfür eine Schlüsseltechnologie.[55]

Analog zu den technischen Möglichkeiten müssen auch die Anforderungen an eine Befugnis zur Videoüberwachung steigen, um den aus dem Grundrecht auf informationelle Selbstbestimmung folgenden Schutzauftrag ausreichend Rechnung zu tragen.

2. Kritikpunkt 1: Nicht-Heilung faktischer Tatbestandslosigkeit

Durch die Erweiterung des § 14 Abs. 3 HSOG wird die überfällige Heilung der verfassungsrechtlich nicht hinnehmbaren, faktischen Tatbestandslosigkeit der Norm versäumt. Es wird angeregt die Regelung dahingehend verfassungskonform auszugestalten, dass eine Videoüberwachung nur zur Abwehr von erheblichen Gefahren oder zur Verhütung von Straftaten von erheblicher Bedeutung an sog. Kriminalitätsbrennpunkten zulässig ist.

Die Regelungen zur offenen Videoüberwachung in § 14 Abs. 3 HSOG wird bereits seit vielen Jahren als *„faktisch tatbestandslos"* kritisiert, da sie eine *„Videoüberwachung von jedermann an jedem öffentlichen Ort"* gestattet.[56]

Die Kritik ist begründet. Die Tatbestandsvoraussetzungen sind denkbar weit. Das Ziel der Abwehr einer (nicht weiter eingegrenzten) Gefahr (§ 14 Abs. 3 Satz 1 1. Alt HSOG) für die öffentliche Sicherheit oder die öffentliche Ordnung oder die tatsachenbasierte Annahme, dass (nicht weiter eingegrenzte) Straftaten drohen (§ 14 Abs. 3 Satz 1 2. Alt HSOG), soll bereits ausreichen.

a. § 14 Abs. 3 Satz 1 1. Alt

Die Regelung des § 14 Abs. 3 Satz 1 1. Alt HSOG ist in der jetzigen Form nicht mit der Verfassung vereinbar.

Nach der Rechtsprechung des BVerfG[57] kann eine Videoüberwachung mit Aufzeichnung des gewonnenen Bildmaterials (nur) auf der Grundlage einer hinreichend bestimmten und normenklaren Ermächtigungsgrundlage materiell verfassungsgemäß sein, *„wenn für sie ein hinreichender Anlass besteht und Überwachung sowie Aufzeichnung insbesondere in räumlicher und zeitlicher Hinsicht und im Hinblick auf die Möglichkeit der Auswertung der Daten das Übermaßverbot wahren"*. Das Vorliegen einer konkreten Gefahr als Tatbestandsvoraussetzung erfüllt die Anforderungen an die hinreichende Bestimmtheit insbesondere aber den „hinreichenden Anlass" nicht.

---

[55] Die realen Möglichkeiten (und Gefahren) moderner Videoüberwachung - insbesondere in Kombination mit Gesichtserkennungstechniken - zeigen sich derzeit eindrücklich in China. Hierzu *Denyer*, „China's watchful eye", Washington Post v. 7.1.2018 - https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/?utm_term=.a3f57a52ebbb.

[56] *Hornmann*, HSOG, § 14 Rn. 35.

[57] BVerfG NVwZ 2007, 688, 691.

Mit Blick auf die oben dargestellte Intensität des Eingriffs darf nach hier vertretener Auffassung ein Eingriff nur zur Abwehr erheblicher Gefahren zugelassen werden.[58] Es wird im Zuge der Neuregelung eine entsprechende Klarstellung angeregt.

Hinzuweisen ist in diesem Zusammenhang auf den Umstand, dass das Erfordernis des Vorliegens einer konkreten Gefahr (*„zur Abwehr einer Gefahr"*) eine dauerhaft angelegte stationäre Videoüberwachung zur Gefahrenabwehr ausschließt.[59] § 14 Abs. 3 Satz 1 1. Alt HSOG ist damit praktisch bedeutungslos.[60]

b. § 14 Abs. 3 Satz 1 2. Alt

Bezüglich § 14 Abs. 3 Satz 1 2. Alt HSOG vertritt die wohl h.M. die Auffassung, dass die Regelung *„verfassungskonform"* dahingehend ausgelegt werden kann (und muss), dass Straftaten mit erheblicher Bedeutung i.S.d. § 13 Abs. 3 HSOG drohen müssen[61] und es sich bei den zu beobachtenden Orten zudem belegbar um *„Kriminalitätsbrennpunkte"* handeln muss.[62]

Diese Behelfslösung, die insb. auf eine Entscheidung des VGH Mannheim[63] aus dem Jahr 2003 gestützt wird, kann nicht überzeugen. § 14 Abs. 3 Satz 1 2. Alt HSOG ist in seiner derzeitigen Fassung nicht mit Verfassungsrecht vereinbar. Die der Entscheidung zu Grunde liegende Regelung des § 21 Abs. 3 BadWürttPolG a.F. war - im Gegensatz zur hier gegenständlichen - tatbestandlich zumindest auf sog. gefährliche Orte i.S.d. § 26 I Nr. 2 BadWürttPolG (vergleichbar mit der Regelung in § 18 Abs. 2 Nr. 1 HSOG) beschränkt, also einen Ort *„an dem erfahrungsgemäß Straftäter sich verbergen, Personen Straftaten verabreden, vorbereiten oder verüben, sich ohne erforderlichen Aufenthaltstitel oder ausländerrechtliche Duldung treffen oder der Prostitution nachgehen"*. Der § 14 Abs. 3 HSOG enthält bis dato nicht einmal eine solche (immer noch unzureichende) Einschränkung. In Reaktion auf die o.g. Entscheidung des VGH Mannheim wurde der Tatbestand des § 21 Abs. 3 BadWürttPolG entsprechend enger gefasst.[64] Er lautet nunmehr:

> *„Der Polizeivollzugsdienst oder die Ortspolizeibehörden können an öffentlich zugänglichen Orten Bild- und Tonaufzeichnungen[65] von Personen anfertigen, wenn sich die Kriminalitätsbelastung dort von der des Gemeindegebiets deutlich abhebt und Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit der Begehung von Straftaten zu rechnen ist."*

Eine derartige Reaktion ist im hessischen Polizeirecht überfällig. Es wird angeregt, gerade auch mit Blick auf die geplante (vermeintliche - hierzu sogleich) Absenkung der Eingriffsvoraussetzungen für die Gefahrenabwehrbehörden, nunmehr eine entsprechende „Modernisierung" vorzunehmen.

---

[58] Vgl. zur sog. Vorratsdatenspeicherung BVerfG NJW 2010, 833, 841 - Rn. 231.
[59] BeckOK PolR Hessen/*Bäuerle* HSOG § 14 Rn. 72.1.
[60] Nach *Hornmann*, HSOG, § 14 Rn. 42 kann dem § 14 Abs. 3 Satz 1 1. Alt *„so gut wie keine praktische Bedeutung zukommen"*.
[61] *Hornmann*, HSOG, § 14 Rn. 43.
[62] BeckOK PolR Hessen/*Bäuerle* HSOG § 14 Rn. 76.
[63] VGH Mannheim, Urteil vom 21. 7. 2003 - 1 S 377/02.
[64] BadWü-LT-Drs. 15/3165, S. 42.
[65] Die Sinnhaftigkeit von Tonaufzeichnungen zur Straftatenverhütung soll hier nicht weiter erörtert werden, da die hessische Regelung eine solche Befugnis nicht enthält.

In diesem Zusammenhang sei darauf hingewiesen, dass das BVerwG[66] die Regelung des § 8 Abs. 3 Satz 1 HbgPolDV[67] für hinreichend bestimmt erachtet hat. Diese Regelung, die entgegen einer teilweise vertretenen Auffassung[68] bislang nicht *„im Wesentlichen"* dem § 14 Abs. 3 HSOG entspricht, kann ebenfalls „Vorbildfunktion" erfüllen. Beide Regelungen verzichten i.Ü. auf die bedeutungslose (siehe bereits oben) und inhaltlich zu unbestimmte Tatbestandsalternative des Vorliegens einer konkreten Gefahr.

3. Kritikpunkt 2: Absenkung der Vorgaben für Gefahrenabwehrbehörden

Die intendierte Absenkung der Vorgaben für eine Videoüberwachung öffentlich zugänglicher Orte durch Gefahrenabwehrbehörden wird de facto nicht erreicht. Da die Verhütung von Straftaten Aufgabe der Polizei ist, ist der Anwendungsbereich gering.

Nach der Neuregelung sollen für Gefahrenabwehrbehörden nunmehr die gleichen Voraussetzungen für die Durchführung einer Videoüberwachung gelten wie für die Polizei (im Einzelnen siehe bereits oben).

Begründet wird dies damit, dass *„die Befugnisse im HSOG den Polizeibehörden grundsätzlich gleichermaßen zugewiesen sind"*[69]. Zu berücksichtigen ist hierbei, dass die Einrichtung einer offenen Videoüberwachung regelmäßig als Maßnahme anzusehen sein wird, die der Verhütung zu erwartender Straftaten dient und somit in das Aufgabenfeld der Polizeibehörden fällt (§ 1 Abs. 4 HSOG). Der Anwendungsbereich der Videoüberwachung zur (verfassungsrechtlich problematischen - dazu bereits oben) allgemeinen Abwehr konkreter Gefahren scheint gering (siehe oben).

Freilich ist auch eine Videoüberwachung durch Gefahrenabwehrbehörden auf Grundlage des § 14 Abs. 3 HSOG nur zulässig, wenn die Regelung entsprechend dem oben Gesagten verfassungskonform modernisiert wird. Insofern kann von einer Absenkung der Anforderungen nicht die Rede sein, da auch die bisherigen Anforderungen des § 14 Abs. 4 Nr. 1 HSOG als zu niedrigschwellig anzusehen sind.

V. Erweiterung der Einsatzmöglichkeiten der sog. „Body-Cam", § 14 Abs. 6

1. Ausgangslage

Die bestehende Regelung des § 14 Abs. 6 HSOG, auf dessen Grundlage insb. sog. Body-Cams[70], eingesetzt werden, soll neu gefasst und erweitert werden.

a. Änderungen/Ergänzungen im Überblick

§ 14 Abs. 6 HSOG - aktuelle Fassung	**§ 14 Abs. 6 HSOG-Entwurf** - inhaltliche Änderungen/Ergänzungen gelb markiert
Die Polizeibehörden können an öffentlich zugänglichen Orten eine Person, deren Identität nach diesem Gesetz oder anderen Rechtsvorschriften festgestellt werden soll, mittels Bild- und Tonübertragung kurzfristig tech-	Die Polizeibehörden können an öffentlich zugänglichen Orten eine Person, deren Identität nach diesem Gesetz oder anderen Rechtsvorschriften festgestellt werden soll, mittels Bild- und Tonübertragung

[66] BVerwG, Urteil vom 25. 1. 2012 – 6 C 9/11.
[67] Diese lautet *„Die Polizei darf zur vorbeugenden Bekämpfung von Straftaten öffentlich zugängliche Straßen, Wege und Plätze mittels Bildübertragung offen beobachten und Bildaufzeichnungen von Personen anfertigen, soweit an diesen Orten wiederholt Straftaten der Straßenkriminalität begangen worden sind und Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit der Begehung derartiger Straftaten zu rechnen ist."*
[68] *Meixner/Fredrich*, § 14 HSOG, Rn. 20.
[69] LT-Drs. 19/5782, S. 4.
[70] Zum Zwecke der Datenerhebung am Körper getragene Kameras.

nisch erfassen, offen beobachten und dies aufzeichnen, wenn dies nach den Umständen zum Schutz von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten oder Dritten gegen eine Gefahr für Leib oder Leben erforderlich ist. Dabei können personenbezogene Daten auch über dritte Personen erhoben werden, soweit dies unerlässlich ist, um die Maßnahme nach Satz 1 durchführen zu können. Sind die Daten für Zwecke der Eigensicherung oder der Strafverfolgung nicht mehr erforderlich, so sind sie unverzüglich zu löschen.	1. kurzfristig technisch erfassen, wenn dies aufgrund tatsächlicher Anhaltspunkte zum Schutz von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten oder Dritten gegen eine Gefahr für Leib, Leben oder Freiheit erforderlich erscheint; 2. offen beobachten und dies aufzeichnen, wenn dies nach den Umständen zum Schutz von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten oder Dritten gegen eine Gefahr für Leib, Leben oder Freiheit erforderlich ist. Soweit es für die Durchführung von Maßnahmen nach Satz 1 unerlässlich ist, können personenbezogene Daten auch über dritte Personen erhoben werden. Sind die Daten für Zwecke der Eigensicherung oder der Strafverfolgung nicht mehr erforderlich, so sind sie unverzüglich zu löschen.

b. Tatbestandsvoraussetzungen de lege lata

Der Einsatz sog. Body-Cams ist de lege lata nur zulässig, wenn sie

1. *„an öffentlich zugänglichen Orten"* stattfindet,
2. eine Identitätsfeststellung stattfinden soll und
3. *„dies nach den Umständen zum Schutz von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten oder Dritten gegen eine Gefahr für Leib oder Leben erforderlich ist"*.

Die Datenerhebung erfolgt *„mittels Bild- und Tonübertragung"* und zwar entweder in Form einer *„kurzfristigen technischen Erfassung"*, einer *„offenen Beobachtung"* oder einer *„Aufzeichnung"* dieser Beobachtung.

c. Grundrechtsrelevanz

In jedem dieser drei Fälle liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung bzw. das Recht am eigenen Bild all der Personen vor, deren Abbild bzw. Stimme aufgezeichnet wird.[71]

2. Insbesondere Pre-Recording (de lege lata)

Nur durch Lektüre der Gesetzesbegründungen wird deutlich, dass mit dem *„kurzfristigen technischen Erfassen"* - welches offenbar auch verdeckt möglich sein soll - die Nutzung der sog. Pre-Recording Funktion der derzeit genutzten Body-Cams gemeint ist.

Nach Darstellung in der LT-Drs. 19/1979 (dort S. 30) ist die Pre-Recording Funktion (derzeit) wie folgt ausgestaltet:

> *„Beim Pre-Recording wird das Videobild beim Einschalten der Pre-Recording-Funktion auf ein flüchtiges Speichermedium mit begrenzter Speicherkapazität, wie den RAM-*

[71] Zutreffend *Kipker*, Stellungnahme zur öffentlichen Anhörung des Innenausschusses des Hessischen Landtags am 10. September 2015 zum Gesetzentwurf der Landesregierung für ein Gesetz zur Änderung des Melderechts, des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und des Hessischen Glücksspielgesetzes vom 19. 5. 2015, LT-Drs. 19/1979, S. 7.

Speicher, abgelegt, wobei die Kamera kontinuierlich Videobilder auf diesem Speicher ablegt. Der Speicher verliert die Daten automatisch etwa beim Abschalten des Geräts, beim Überschreiben der Daten oder beim Stoppen des Pre-Recordings. Sobald die Aufnahmefunktion des Kamerasystems eingeschaltet wird, kopiert das System die noch vorhandenen Daten des RAM-Speichers auf ein dauerhaftes Speichermedium, wie beispielsweise eine SD-Karte, und schreibt die neuen Videodateien direkt dahinter. Die aus dem Pre-Recording gespeicherten Videodaten stehen dabei in sehr engem zeitlichem Zusammenhang mit der durch die Betätigung der Aufnahmefunktion der Body-Cam ausgelösten Aufzeichnung und umfassen lediglich einen kurzen Zeitraum."

De lege lata ist auch dieses *„kurzfristige technische Erfassen"* erst zulässig, wenn alle o.g. Tatbestandsvoraussetzungen vorliegen.

3. Kritikpunkt 1: Unbestimmtheit des Begriffs „technische Erfassung"

Die Verwendung des Begriffs „technische Erfassung" für die Pre-Recording-Funktion ist zumindest missverständlich und sollte überdacht werden.

Der Begriff *„technische Erfassung"* soll offenbar suggerieren, dass keine (grundrechtlich relevante) Datenerhebung und -speicherung stattfindet. Es scheint eine Gleichsetzung mit der vom BVerfG in gewissen Konstellationen für zulässig gehaltenen Kennzeichenerfassung[72] beabsichtigt zu sein. Diese Vergleichbarkeit ist jedoch nicht gegeben. Im Gegensatz zur KFZ-Kennzeichenerfassung erfolgt eine Speicherung der Daten für mindestens ca. 30-60 Sekunden im RAM der Kamera[73] und nicht nur für Sekundenbruchteile.

Die *„Erfassung"* im Rahmen des Pre-Recordings dient zudem nicht lediglich dem rein technischen Abgleich mit bestimmten Suchkriterien, sondern erfolgt gewissermaßen „auf Vorrat" ohne dass bereits ein konkreter Verwendungszweck zum Zeitpunkt der Speicherung feststeht. Die jederzeit mögliche Perpetuierung der im RAM abgelegten Video- und Audiodaten steht im konkreten Einzelfall im „Ermessen" der die Body-Cam bedienenden Person.

Es muss auch der Umstand Berücksichtigung finden, dass moderne Body-Cams nicht nur im Nahbereich des sie tragenden Beamten aufzeichnen, sondern eine Identifizierung von Personen ermöglichen, die sich zehn oder mehr Meter entfernt aufhalten.[74] Es werden nicht gezielt - wie bei der Kennzeichenerfassung - Buchstaben- und Zahlenkombinationen erhoben, sondern detaillierte Aufnahmen der Umgebung des Kameraträgers gemacht.

4. Kritikpunkt 2: Unbestimmtheit der zeitlichen Grenzen

Es fehlt eine klare zeitliche Begrenzung der *„kurzfristigen"* technischen Erfassung. Es ist eine entsprechende Klarstellung im Gesetz vorzusehen.

Der Gesetzgeber ist verpflichtet, die Grenzen eines Eingriffs in das Recht auf informationelle Selbstbestimmung *„hinreichend bereichsspezifisch, präzise und normenklar festzulegen"*[75]. Die zeitliche Einschränkung *„kurzfristig"* entspricht diesen Vorgaben nicht, kann sie doch einen Zeitraum von wenigen Sekunden bis hin zu mehreren Minuten betragen. Unterstellt, der

---

[72] BVerfG, Urteil vom 11. 3. 2008 - 1 BvR 2074/05, 1 BvR 1254/07.

[73] Vgl. z.B. Produktbeschreibung der Kamera DrivePro Body 30 - https://www.bodycam24.de/produkt/transcend-bodycam-drivepro-body-30/.

[74] BeckOK PolR NRW/*Arzt* PolG NRW § 15c Rn. 10 mwN.

[75] Std. Rsp. BVerfG, vgl. z.B. BVerfG, Urteil vom 11.03.2008 - 1 BvR 2074/05, 1 BvR 1254/07 - Rn. 94 m.w.N.

Einsatz der Pre-Recording Funktion wird überhaupt als erforderlich angesehen, wäre zu prüfen, welche Dauer maximal erforderlich ist und eine entsprechende Begrenzung im Gesetzestext vorzusehen.

Das eine solche Klarstellung bei der Neufassung des § 14 Abs. 6 HSOG nicht in Erwägung gezogen wurde verwundert, da der Entwurf sich mit Blick auf die Erweiterung der zu schützenden Rechtsgüter um das Rechtsgut „Freiheit" explizit an § 27a BPolG orientiert. Dieser enthält in Abs. 3 eine diesbezüglich klare Regelung.

5. Kritikpunkt 3: Verdeckte Erhebung

Der verdeckte Einsatz der Pre-Recording Funktion ist verfassungsrechtlich unzulässig. Es wird ist nur der offene Einsatz der Pre-Recording Funktion zuzulassen.

Das *„kurzfristige technische Erfassen"* soll offenbar auch verdeckt erfolgen dürfen. Das ergibt sich aus der Formulierung des § 14 Abs. 6 HSOG (sowohl geltende Fassung als auch Entwurf), nach welchem nur das *„Beobachten"* und *„Aufzeichnen"* ausdrücklich offen erfolgen sollen.

Eine tragfähige verfassungsrechtliche Rechtfertigung für ein Abweichen vom Grundsatz der offenen Datenerhebung ist nicht ersichtlich.[76]

Der Einsatz von Body-Cams soll abschreckende bzw. deeskalierende Wirkung entfalten und potentielle Aggressoren einschüchtern. Ein verdeckter Einsatz von Body-Cams - und sei es nur in Form des kurzfristigen Pre-Recordings - kann zur Erreichung dieses Ziels nicht beitragen, wäre also ungeeignet.

Einziger Zweck einer verdeckten Aufnahme kann die Verfolgungsvorsorge sein. Diesbezüglich ist es jedoch zumindest fraglich, ob hier überhaupt eine entsprechende Gesetzgebungskompetenz besteht. Das BVerfG[77] hat hierzu im Zusammenhang mit Regelungen der präventiven Telekommunikationsüberwachung im Niedersächsischen SOG ausgeführt:

> *„Die Vorsorge für die spätere Verfolgung von Straftaten ist kompetenzmäßig dem „gerichtlichen Verfahren" i.S. des Art. 74 I Nr. 1 GG zuzuordnen. Die gesetzliche Ermächtigung bezweckt die Sicherung von Beweisen für ein künftiges Strafverfahren. Allerdings fehlt es im Zeitpunkt der Überwachungsmaßnahme, anders als für die Strafverfolgung im herkömmlichen Sinne, an einer bereits begangenen Straftat. Die Verfolgungsvorsorge erfolgt in zeitlicher Hinsicht präventiv, betrifft aber gegenständlich das repressiv ausgerichtete Strafverfahren. Die Daten werden zu dem Zweck der Verfolgung einer in der Zukunft möglicherweise verwirklichten konkreten Straftat und damit letztlich nur zur Verwertung in einem künftigen Strafverfahren, also zur Strafverfolgung, erhoben. Dabei knüpft die Ermächtigung zur Erhebung personenbezogener Daten in § 33a I Nrn. 2 und 3 NdsSOG an das erwartete Handeln von Personen an, bei denen Tatsachen die Annahme rechtfertigen, dass sie Straftaten von erheblicher Bedeutung begehen werden. Eine Verwertung der erhobenen Daten für diesen Zweck kommt erst in Betracht, wenn tatsächlich eine Straftat begangen wurde und daraus strafprozessuale Konsequenzen gezogen werden. Die der Verfolgungsvorsorge zugeordneten Daten und Informationen sind insofern dazu bestimmt, in ungewisser Zukunft in ein Ermittlungs- und Hauptver-*

[76] Vgl. BeckOK PolR Hessen/*Bäuerle* HSOG § 14 Rn.
[77] BVerfG, Urteil vom 27. 7. 2005 - 1 BvR 668/04 - auch für die folgenden Zitate.

fahren einzufließen. Es geht - jenseits eines konkreten Anfangsverdachts [...] - um die Beweisbeschaffung zur Verwendung in künftigen Strafverfahren, nicht um eine präventive Datenerhebung zur Verhütung von Straftaten. Eine solche Verfolgungsvorsorge gehört zum gerichtlichen Verfahren i.S. des Art. 74 I Nr. 1 GG."

Eine Gesetzgebungskompetenz des Landes besteht nicht, wenn der Bundesgesetzgeber von seiner konkurrierenden Gesetzgebungskompetenz in abschließender Weise Gebrauch gemacht hat. Dies wurde vom BVerfG mit Blick auf die Regelungen der Telekommunikationsüberwachung in der StPO bejaht. Es scheint naheliegend, dass die Regelungen zur Herstellung von Bildaufnahmen nach § 100h Abs. 1 Nr. 1 StPO und § 81b StPO ebenfalls eine solche, abschließende Regelung darstellen.

Das BVerwG hat in einer Entscheidung zur Zulässigkeit der offenen (!) Videoüberwachung der Reeperbahn auf Grundlage des § 8 Abs. 3 HbgPolDVG eine solche abschließende Regelung im Wesentlichen mit der Begründung verneint, dass es sich bei den Maßnahmen nach der StPO gerade um verdeckte Maßnahmen handele, *„die im Hinblick auf ihr äußeres Gepräge, ihren Einsatzzweck und die grundrechtliche Betroffenheit der observierten Person bedeutsame Unterschiede zur offenen Beobachtung*" aufweise. Diese Unterschiede sind nicht mehr klar erkennbar. Das gilt umso mehr, weil es sich beim Pre-Recording gerade nicht um eine offene Maßnahme handelt.

6. Insb. Pre-Recording (de lege ferenda)

Auf die o.g. Kritikpunkte[78] an der bestehenden Regelung geht der Entwurf der Erweiterung bedauerlicherweise nicht ein. Im Gegenteil: es ist intendiert *„die Funktion des Pre-Recordings bereits unterhalb der Schwelle für das offene Beobachten und Aufzeichnen*" (Drs. 19/5782, S. 5) zu ermöglichen.

7. Kritikpunkt 4: Unbestimmte/nicht erforderliche Erweiterung

Die in § 14 Abs. 6 Nr. 1 HSOG-Entwurf enthaltene „Erweiterung" ist missverständlich und führt nicht zum angestrebten Ziel.

Durch die Einführung der Möglichkeit des (weiterhin verdeckt möglichen) Einsatzes der Pre-Recording Funktion in Fällen, in denen dies aufgrund tatsächlicher Anhaltspunkte zum Schutz gegen eine Gefahr für Leib, Leben oder Freiheit *„erforderlich erscheint*" wird die Unbestimmtheit der Befugnisnorm erweitert, ohne dass das Ziel der Ermöglichung der Nutzung der Pre-Recording Funktion unterhalb der Schwelle für das offene Beobachten und Aufzeichnen nach § 14 Abs. 6 Nr. 2 HSOG-Entwurf erreicht würde.

Die derzeitige Regelung ist bereits sehr weit gefasst. Der (offene wie auch verdeckte) Einsatz muss lediglich *„nach den Umständen*" zum *„Schutz [...] gegen eine Gefahr*" erforderlich sein. Die Schwelle zum Vorliegen einer konkreten Gefahr muss also noch nicht überschritten sein.[79] Das kann bei einem offenen Einsatz als sinnvoll erachtet werden, soll doch durch den Einsatz der Body-Cam eine konkrete Gefahr nicht nur abgewehrt, sondern idealerweise be-

---

[78] Zu weiteren Kritikpunkten, die ebenfalls nicht adressiert werden vgl. die Auflistung von *Kipker* unter https://community.beck.de/2016/10/12/datenschutz-und-body-cams-nicht-nachvollziehbare-bedenken.

[79] Vgl. BeckOK PolR Hessen/*Bäuerle* HSOG § 14 Rn. 106; VG Frankfurt, Urteil vom 03.07.2013 - 5 K 1101/13.F; zur Unschärfe dieser Formulierung ausführlich *Arzt*, Stellungnahme Innenausschuss Bürgerschaft HH am 18.11.2014: Einführung von Bodycams, S. 8 ff.

reits deren Entstehung verhindert werden.[80] *Martini/Nink/Wentzel* umschreiben dies treffend wie folgt

> *„Die Wendung „nach den Umständen" geht auf das gesetzgeberische Bemühen zurück, der Unsicherheit Rechnung zu tragen, die beim Einschalten der Kamera im Hinblick auf eine Gefährdung besteht: Die Aufzeichnung soll nicht erst nach dem Beginn eines gewalttätigen Übergriffs (oder wenn dieser unmittelbar bevorsteht) zulässig sein, sondern schon in einer Situation, die aufgrund polizeilichen Erfahrungswissens auf eine Eskalationsgefahr schließen lässt."*[81]

Werden nunmehr in § 14 Abs. 6 Nr. 1 HSOG-Entwurf als Tatbestandsvoraussetzung *„tatsächliche Anhaltspunkte"* gefordert, auf Grund derer der Einsatz der Body-Cams zum Schutz gegen eine Gefahr erforderlich *„erscheinen"* muss, so ist das - entgegen der Intention des Entwurfs - sogar ein Mehr als das Erfordernis des Vorliegens von bloßen *„Umständen"*.

Es macht darüber hinaus keinen Unterschied, ob formuliert wird *„wenn dies aufgrund tatsächlicher Anhaltspunkte [...] erforderlich* ***erscheint****"* oder *„wenn dies aufgrund tatsächlicher Anhaltspunkte [...] erforderlich* ***ist****"*. Auch wenn eine Maßnahme „nur" zulässig ist, wenn sie auf Grund tatsächlicher Anhaltspunkte zur Abwehr einer Gefahr erforderlich ist, ist Voraussetzung lediglich die auf einer subjektiven Prognose angenommene „Wahrscheinlichkeit" des Schadenseintritts[82]:

> *„Der Begriff der polizeilichen Gefahr enthält eine Prognose, das heißt eine auf Tatsachen gegründete subjektive Einschätzung über einen zukünftigen Geschehensablauf. Das Urteil, welches das Vorliegen einer Gefahr (also der Wahrscheinlichkeit eines Schadenseintritts) bejaht oder verneint, beruht zum Teil auf sicherem Wissen, zum Teil auf Ungewißheit und zum Teil auf einer aus Erfahrung gespeisten bewertenden Einschätzung der bekannten Umstände. Insofern dem Gefahr-Begriff ein an einen bestimmten Wissensstand gebundenes Wahrscheinlichkeitsurteil zugrunde liegt, ist der Begriff notwendig ein „subjektiver"."*[83]

8. Kritikpunkt 5: Erforderlichkeit der intendierten Erweiterung

Es ist nicht ersichtlich, wieso ein Einsatz der Pre-Recording Funktion *„unterhalb der Schwelle für das offene Beobachten und Aufzeichnen"* für Eigensicherungszwecke erforderlich ist.

Ungeachtet dessen, dass das Ziel des Einsatzes von Body-Cams - nämlich die Abschreckung potentieller Gewalttäter - durch den verdeckten Einsatz der Pre-Recording Funktion nicht zumindest gefördert werden kann (hierzu bereits oben), bleibt die Frage unbeantwortet, wieso ein Einsatz *„unterhalb der Schwelle für das offene Beobachten und Aufzeichnen"* erforderlich ist.

Der Begründung (S. 5) ist lediglich zu entnehmen, dass diese Erweiterung erfolgt, *„um eine zielführende Nutzung dieser Funktion und der Body-Cam zu ermöglichen."* Das erscheint unter

---

[80] Vgl. im anderen Kontext *Wehr*, BPolG, § 43 Rn. 9; die Zulässigkeit des verdeckten Einsatzes u.a. aus diesem Grund ablehnend BeckOK PolR Hessen/*Bäuerle* HSOG § 14 Rn. 100.
[81] *Martini/Nink/Wentzel*, NVwZ-Extra, 24/2016, Fn. 96.
[82] Vgl. z.B. die Legaldefinition der konkreten Gefahr im § 2 Nr. 1 a Nds. SOG.
[83] *Denninger*, in: Lisken/Denninger, Handbuch des Polizeirechts, Teil D, Rn. 46.

Berücksichtigung der grundrechtlichen Tragweite der Eingriffserweiterung zu unsubstantiiert.

9. Kritikpunkt 6: Erweiterung um das Rechtsgut „Freiheit"

Die Erweiterung der Befugnis um das Rechtsgut *„Freiheit"*, die in Anlehnung an den neuen § 27a BPolG erfolgt, ist nachvollziehbar und nicht zu beanstanden.

Es handelt sich bei dem Rechtsgut der Freiheit (der Person) um ein hochrangiges Rechtsgut[84], welches mit dem der körperlichen Unversehrtheit auf einer Stufe steht.

VI. Meldeauflage, § 30a HSOG

1. Ausgangslage

Mit § 30a HSOG wird die sog. „Meldeauflage" im HSOG ausdrücklich geregelt.

> **§ 30a HSOG-Entwurf - Meldeauflagen**
>
> Die Polizeibehörden können zur Verhütung von Straftaten eine Person anweisen, sich an bestimmten Tagen bis zu zweimal zu bestimmten Zeiten bei einer bestimmten polizeilichen Dienststelle zu melden (Meldeauflage), wenn Tatsachen die Annahme rechtfertigen, dass sie außerhalb ihres gewöhnlichen Aufenthaltsorts im Zusammenhang mit einer Veranstaltung eine Straftat begehen wird.
>
> Die Meldung hat bei der Polizeistation oder bei dem Polizeirevier des gewöhnlichen Aufenthaltsortes zu erfolgen; mit Einverständnis der betroffenen Person kann auch eine andere Dienststelle einer Polizeibehörde des Bundes oder der Länder bestimmt werden.
>
> Die Meldeauflage ist auf die Veranstaltung oder eine zusammenhängende Serie von Veranstaltungen zu beschränken, deren Gesamtdauer sechs Wochen nicht überschreitet.
>
> § 31a Abs. 2 Nr. 3 bleibt unberührt.

2. Kritikpunkt: Ausdrückliche Regelung

Die ausdrückliche Regelung der Meldeauflage in § 30a HSOG ist zu begrüßen. Sie erscheint in ihrer Ausgestaltung überlegt und verhältnismäßig.

Bislang wird die Auferlegung von sog. Meldeauflagen, also der Verpflichtung sich an bestimmten Tagen bei einer Polizeidienststelle zu melden, auf die Befugnisgeneralklausel (§ 11 HSOG) gestützt.

Diese Praxis ist insb. in der Literatur auf teilweise starke Kritik gestoßen.[85] Einfache Meldeauflagen (bis zu drei Tage) auf Basis der Generalklausel werden als *„rechtswidrige Vorladungen"* angesehen.[86] Qualifizierte Meldeauflagen (ab vier Tage) bedürften schon wegen ihrer Eingriffsintensität einer ausdrücklichen Regelung.[87]

Mit § 30a HSOG wird die Meldeauflage als „Standardmaßnahme" etabliert. Das ist uneingeschränkt zu begrüßen.

---

[84] BeckOK Grundgesetz/*Lang* GG Art. 2 Rn. 84.
[85] Vgl. insb. *Arzt*, Die Polizei 2006, 156.
[86] *Schucht*, NVwZ 2011, 709, 713.
[87] *Schucht*, NVwZ 2011, 709, 713 mit weiteren Argumenten.

Die konkrete Ausgestaltung der Regelung erscheint angemessen und überlegt:

- Da es sich um eine Maßnahme der Straftatenverhütung handelt, ist konsequenterweise nur die Polizei befugt eine Meldeauflage zu erlassen.
- Die Tatbestandsvoraussetzung *„wenn Tatsachen die Annahme rechtfertigen, dass sie außerhalb ihres gewöhnlichen Aufenthaltsorts im Zusammenhang mit einer Veranstaltung eine Straftat begehen wird"* erscheint zunächst weit, da keinerlei Eingrenzung bezüglich der Schwere der befürchteten Straftaten (eine Formalbeleidigung oder einfache Sachbeschädigung würde ausreichen) vorgenommen wird. Bei verhältnismäßiger Anwendung dürfte dies aber noch hinnehmbar sein.
- Die vorgesehenen Ermächtigungsbegrenzungen - Meldung bis zu zweimal sowie maximale Gesamtdauer von sechs Wochen - erscheinen angemessen.
- Die ausdrückliche Möglichkeit mit Einverständnis der betroffenen Person eine andere Dienststelle als die am gewöhnlichen Aufenthaltsort zu bestimmen, trägt den an eine Meldeauflage in der Rechtsprechung[88] und Literatur formulierten Anforderungen Rechnung, dass es dem Adressaten freistehen müsse, alle Orte aufzusuchen die nicht für ihn „gesperrt" sind.[89] Welche Dienststellen hier in Betracht kommen, kann im Rahmen der Anhörung klargestellt werden.[90]

Berlin, 4.2.2018

Prof. Dr. Jan Dirk Roggenkamp

[88] BVerwG NVwZ 2007, 1439, 1442.
[89] *Rachor*, in: Lisken/Denninger, Handbuch des Polizeirechts, Teil E, Rn. 775.
[90] *Rachor*, in: Lisken/Denninger, Handbuch des Polizeirechts, Teil E, Rn. 775.

Chaos Computer Club

STELLUNGNAHME

zum Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen,

Drucksache 19/5412,

an den Hessischen Landtag, Innenausschuss

4. Februar 2018

Constanze Kurz, Marco Holz, Justus Hoffmann, Lukas Laufenberg

Gerne kommen wir Ihrer Bitte um Stellungnahme zum Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen nach.

Diese Stellungnahme beschäftigt mit dem geplanten Einsatz von staatlicher Spähsoftware (Staatstrojaner) zur sog. „Quellen-Telekommunikationsüberwachung" (Quellen-TKÜ) und zur „Online-Durchsuchung" informationstechnischer Systeme. Sie konzentriert sich auf die technischen Realitäten bei Entwicklung und Einsatz solcher Staatstrojaner und deren rechtliche, gesellschaftliche und wirtschaftliche Implikationen. Auch andere der vorgesehenen Maßnahmen im Gesetzesentwurf sind kritisch zu sehen, werden hier jedoch nicht betrachtet.

Einleitung

Der vorliegende Gesetzesentwurf bedeutet eine Ausweitung der Befugnisse des Landesamts für Verfassungschutz. Das LfV soll danach die Befugnis und die Mittel erhalten, zur Informationsgewinnung Computersysteme zu hacken.

In §§ 6 bis 9 des vorliegenden Gesetzesentwurfes ist der verdeckte Zugriff auf informationstechnische Systeme geregelt. Spionagesoftware soll dazu dienen, Computer oder andere informationstechnische Systeme dauerhaft zu infiltrieren, um Kommunikations- oder andere Daten auszuleiten. Damit greift sie in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ein. Befindet sich das angegriffene informationstechnische System in einer Wohnung, liegt zusätzlich ein Eingriff in Art. 13 Abs. 1 GG vor.

Praktisch geschieht ein solcher Zugriff, indem eine oder mehrere bestehende Sicherheitslücken ausgenutzt werden, um die Überwachungssoftware heimlich aus der Ferne oder durch direkten Zugriff auf das Gerät zu installieren und danach fest im System zu verankern. Das betroffene Endgerät ist nach dem Aufbringen des Trojaners kompromittiert, eine sichere und vertrauenswürdige Informationsverarbeitung und -übertragung nicht mehr gewährleistet. Betroffene bemerken diese Maßnahme in der Regel nicht.

Die Entwicklung eines Trojaners, der alle nötigen rechtlichen Vorgaben erfüllt, stellte Behörden in der Vergangenheit vor große Probleme. Alle bisherigen Versuche, Staatstrojaner für deutsche Behörden zu entwickeln und einzusetzen, sind entweder gescheitert oder als rechtswidrig eingestuft worden. Aktuell wird in den Medien über den Einsatz von zugekauften Trojanern des Bundeskrimininalamtes spekuliert.[1] Der in Hessen entwickelte Staatstrojaner aus dem Jahre 2011 war nicht nur rechtswidrig eingesetzt

[1] Vgl. Innenministerium gibt Staatstrojaner FinSpy offenbar frei – aber noch kein Einsatz, https://www.heise.de/newsticker/meldung/Innenministerium-gibt-Staatstrojaner-FinSpy-offenbar-frei-aber-noch-kein-Einsatz-3959660.html vom 2. Februar 2018.

worden,[2] sondern schuf auf den infiltrierten Rechnern aufgrund von groben Design- und Implementierungsfehlern weitere Lücken, die auch Dritte ausnutzen konnten.[3]

1) Risiken beim Einsatz von Staatstrojanern

1a) Ausnutzen von Sicherheitslücken

Um einen Staatstrojaner zur „Online-Durchsuchung" oder „Quellen-TKÜ" aus der Ferne auf ein informationstechnisches System aufspielen zu können, ist eine Sicherheitslücke erforderlich. Eine Sicherheitslücke ist in diesem Zusammenhang in der Regel ein Programmierfehler, durch den es Angreifern möglich ist, die Kontrolle über das System zu übernehmen. Sie könnenn dann beispielsweise Daten aufspielen, verändern, herunterladen oder die Funktionsweise des Systems beliebig verändern. Sicherheitslücken finden sich in zahlreicher alltäglicher Software.

Hier wird ein genereller Konflikt offenkundig, in den sich der hessische Gesetzgeber begibt: Spionagesoftware benötigt eine Schwachstelle im angegriffenen Computersystem, die vom Besitzer des Systems nicht geschlossen wurde und daher heimlich genutzt werden kann. Jeder Einsatz eines Staatstrojaners erfordert, dass eine Schadcode-Komponente unbemerkt bei der verdächtigen Person installiert wird. Denn eine Sicherheitslücke sowie der Schadcode bilden das Einfallstor für die Spionagesoftware.

Erfahren die Hersteller oder die Entwickler der betroffenen Software von einer solchen Schwachstelle, steht in der Regel nach kurzer Zeit eine Aktualisierung bereit, welche die Lücke schließt. Durch das absichtliche Offenhalten der Lücken untergräbt der Staat jene Vertrauenswürdigkeit, die er eigentlich zu schützen hat.

Zudem schafft er erhebliche sekundäre Gefahren: Werden Lücken nicht geschlossen, entsteht ein enormer Schaden für die IT-Sicherheit bei Privatpersonen und Unternehmen. Hohe Sicherheitsstandards sind gerade für Unternehmen essentiell, um keine Angriffsfläche für nachhaltig rufschädigende Datenpannen und für Wirtschaftsspionage zu bieten.[4] Darüber hinaus könnten Kriminelle oder Terroristen eine solche Lücken nutzen, um kritische Infrastruktur anzugreifen. Das Vorhandensein einer Sicherheitslücke in einer Software stellt eine Gefahr für alle Nutzer dieser Software dar.

---

[2] Vgl. LG Landshut, 4 Qs 346/10.

[3] Vgl. Chaos Computer Club analysiert Staatstrojaner, https://www.ccc.de/de/updates/2011/staatstrojaner vom 8. Oktober 2011.

[4] Vgl. IT-Sicherheitsleitfaden des Landes Hessen, https://www.hessen.de/pressearchiv/pressemitteilung/sicherheitsluecken-schaden-betrieben-0 vom 16. September 2015.

1b) Veränderte Ausgangslage bei Schadsoftware

Seit die Diskussion in Deutschland um die Einführung einer gesetzlichen Erlaubnis zum staatlichen Hacken vor mehr als zehn Jahren begann, hat sich das Gesamtbild in der IT-Sicherheit und bezüglich der Verbreitung, des Handels und der Abwehr von Schadsoftware stark gewandelt. In der jüngeren Vergangenheit ist staatliche Schadsoftware in zunehmendem Maße in die Hände Krimineller gelangt. Diese haben die Sicherheitslücken, die von staatlicher Seite geheimgehalten worden waren, genutzt, um in großem Umfang Computer mit Erpressungstrojanern[5] zu infizieren.

Das geplante Gesetz fördert den Schwarzmarkt für noch nicht geschlossene Sicherheitslücken mit Steuergeldern und erodiert damit insgesamt die IT-Sicherheit. Kriminelle profitieren von offenen Sicherheitslücken und gestohlenen Staatstrojanern – Opfer ist die Allgemeinheit.

Die internationalen Schadenssummen durch Spionagesoftware, welche von staatlichen Akteuren oder in deren Auftrag entwickelt wurde, sind stark gestiegen und liegen im Bereich von vielen Millionen Euro jedes Jahr. Nicht gemeldete Sicherheitslücken gelangten in die Hände von Dritten und schädigten in der Folge Millionen Computersysteme. Im Jahr 2017 richtete die bislang größte Welle von Schadsoftware, die aus einem staatlichen Schadsoftware-Arsenal entwendet wurde, unter dem Namen „Wannacry" bei Unternehmen, Behörden und Privatleuten enormen Schaden an. Vergleichbares gilt für die Angriffswelle mit der Malware „NotPetya".[6] Die Schadenssumme allein bei „Wannacry" wird international auf über vier Milliarden Euro taxiert. Alarmierend ist dabei die Tatsache, dass in Großbritannien insbesondere Krankenhausinfrastrukturen davon betroffen und Leben und Gesundheit von Menschen gefährdet waren.

1c) Folgeschäden für Wirtschaft und Privatpersonen

Die Regelungen im Gesetzesentwurf implizieren das absichtliche Offenhalten von Sicherheitslücken in IT-Systemen durch staatliche Stellen. Gleichzeitig wird allerdings die eigentlich zwingend notwendige Einschätzung der möglichen Folgeschäden unterlassen und ist auch für den Einzelfall nicht im Gesetzesentwurf vorgesehen.

Für den Einsatz in einem Staatstrojaner sind Sicherheitslücken in besonders weitverbreiteter Software attraktiv, etwa in gängigen Betriebssystemen (Windows, Android, iOS) oder Browsern (Chrome, Firefox): Hiermit können viele verschiedene Geräte angegriffen werden, ohne den Staatstrojaner grundlegend umprogrammieren zu müssen.

---

[5] Ein Erpressungstrojaner ist eine Schadsoftware, die auf einem Rechner gespeicherte Daten verschlüsselt und erst nach Kauf eines Passworts wieder freigibt.

[6] Vgl. Ransomware-Attacke, http://www.zdnet.de/88324525/ransomware-attacke-4000-server-und-45-000-pcs-neu-installiert/ vom 26. Januar 2018.

Für Kriminelle sind solche Lücken aus demselben Grund ebenfalls interessant. Es existiert daher ein florierender Grau- und Schwarzmarkt, auf dem Informationen über Sicherheitslücken gehandelt werden. Der Staat gerät hier folglich in einen Zielkonflikt: Auf der einen Seite will er ein möglichst hohes IT-Sicherheitsniveau für Bürger und Wirtschaft garantieren; auf der anderen Seite hat er ein Interesse an offenen Sicherheitslücken in möglichst vielen und verbreiteten Systemen, um diese bei Bedarf zum Zwecke der „Online-Durchsuchung" oder „Quellen-TKÜ" ausnutzen zu können.

Der Weg vom staatlichen zum kriminellen Trojaner kann kurz sein, wenn die Schadsoftware abhanden kommt oder von den Überwachten auf dem eigenen Rechner entdeckt wird.[7] Da staatliche Akteure Geld für Informationen über noch unbekannte Sicherheitslücken ausgeben, um diese Lücken für Staatstrojaner nutzen zu können, wächst das Volumen der Schwarzmärkte, auf denen diese Informationen gehandelt werden. Die Hersteller der verwundbaren Software könnten diese Lücken eigentlich zum Schutz aller Nutzer bei Kenntnis durch Updates schließen. Da die Informationen über Existenz und Art der Lücke auf dem Schattenmarkt jedoch oftmals an den Meistbietenden für bis zu sechs- oder siebenstellige Eurobeträge verkauft werden, erfahren Softwarehersteller nicht von kritischen Lücken in ihren Produkten. Alle ihre Kunden bleiben damit verwundbar.

Staatliche Schadsoftware unterminiert die IT-Sicherheit damit strukturell, da ihre Entwicklung die Anreize dafür setzt, Sicherheitslücken anzubieten, zu verkaufen und nicht schließen zu lassen. Daher ist bei der Bewertung des Gesetzentwurfes nicht nur der Kostenaufwand für das Bereitstellen und den Einsatz der Software selbst zu betrachten, sondern es sind auch die Risiken zu kalkulieren, die dabei entstehen. Durch die Finanzierung und das damit einhergehende Setzen falscher Anreize beim Umgang mit Sicherheitslücken hat sich bereits eine ganze Branche entwickelt, die aktiv unser aller Sicherheit gefährdet und die Wirtschaft sowie öffentliche Stellen buchstäblich viele Millionen kostet. Eine verantwortungsvolle IT-Sicherheitspolitik zielt auf die Schließung von Lücken ab, statt sich noch an der fragwürdigen Praxis des Handels mit Schwachstellen zu beteiligen und indirekt kriminelle Händler zu unterstützen.

Der Gesetzesentwurf gibt keine Anhaltspunkte dafür, dass die dargestellten Risiken der Schadsoftware minimiert werden. Der Staat sollte seine Bürger und die Wirtschaft vor Schadsoftware schützen sowie das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme verwirklichen.[8] Das heißt ganz praktisch auch, von der Entwicklung und Finanzierung von Schadsoftware abzusehen.

---

[7] Vgl. Motherboard: Cryptocurrency Mining Malware That Uses an NSA Exploit Is On the Rise https://motherboard.vice.com/en_us/article/yw5yp7/monero-mining-wannamine-wannacry-nsa vom 30. Januar 2018.

[8] Zur allgemeinen Verbesserung der IT-Sicherheit sollten kritische Softwarekomponenten mit Hilfe öffentlicher Gelder auf Schwachstellen überprüft werden, als Vorbild könnte hier das Projekt „EU-FOSSA" https://joinup.ec.europa.eu/collection/eu-fossa der Europäischen Kommission dienen.

An einem Großteil der heute verbreiteten Schadsoftware, die entdeckt und analysiert wurde, waren staatliche Stellen beteiligt, ob als Auftraggeber oder direkt bei der Entwicklung. Die bisher gefährlichsten bekannten Digitalwaffen („Stuxnet", „Flame", „Duqu" und „Regin") sind allesamt in staatlichem Auftrag entstanden.[9] Mittelbar trägt der Staat als Auftraggeber damit eine Mitschuld an der Existenz und Verbreitung solcher Digitalwaffen.

Die Auswirkungen von staatlich finanzierter Entwicklung von Schadsoftware, die sämtliche Bereiche der Wirtschaft, die öffentliche Infrastruktur und Millionen Privatleute gefährdet, können nicht mehr ignoriert werden, wenn sich nun das Bundesland Hessen anschickt, ebenfalls eine gesetzliche Grundlage zu schaffen, die diese Fehlentwicklung vorantreiben wird. Denn die Entwicklung von Spionagesoftware kann leicht zum Boomerang werden, wenn die Malware den Besitzer wechselt.

Der Zweitverwertungsmarkt für Sicherheitslücken und Trojaner ist erheblich angewachsen. So könnten auch repressive Regimes im Ausland die von Steuergeldern in Deutschland finanzierten Hacking-Tools zum Ausspähen von Journalisten, Oppositionspolitikern und unterdrückten Minderheiten nutzen.[10] Die Technologie-Zulieferer solcher Regierungen sitzen oft in Europa, wirksame Exportverbote gibt es bisher nicht.[11]

Prinzipiell ist das Ausnutzen von Sicherheitslücken von staatlicher Seite nicht wünschenswert, da es im Interesse aller Behörden liegen sollte, diese Lücken konsequent und zeitnah schließen zu lassen. Das Interesse von Behörden muss es nicht nur sein, die eigenen Systeme zu sichern, sondern auch Folgeschäden ihres Tuns für Wirtschaft und Privatpersonen zu vermeiden. Einem Fortbestand von Sicherheitslücken, die staatlichen Stellen bekanntgeworden sind, muss daher konsequent entgegengewirkt werden. Dazu muss in den Gesetzesentwurf mindestens eine Meldepflicht für das LfV aufgenommen werden, insbesondere bei Sicherheitslücken, die in weitverbreiteter und sicherheitskritischer Software bestehen. Solche Lücken stellen eine enorme Gefährdung für eine große Zahl von Geräten dar.

Warum in Hessen oder in Deutschland finanzierte Hacking-Tools gegen eine spätere missbräuchliche Nutzung besser geschützt sein sollen als etwa die Arsenale von anderen Geheimdiensten, ist nicht ersichtlich.[12]

---

[9] Vgl. Regin: Top-tier espionage tool enables stealthy surveillance, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf vom 27. August 2015.

[10] Vgl. etwa bei der Spähsoftware Pegasus, https://citizenlab.ca/2017/07/mexico-disappearances-nso/ vom 10. Juli 2017.

[11] Vgl. Europas Exportkontrollen für digitale Waffen versagen, http://www.zeit.de/digital/datenschutz/2017-02/ueberwachung-technik-exporte-europa-kontrolle-versagt vom 24. Februar 2017.

[12] Auch finanziell und personell gut ausgestatteten Behörden wie der NSA ist es wiederholt nicht gelungen, die Geheimhaltung der von ihnen genutzten Spionagesoftware sicherzustellen, vgl. Hackers Stole NSA Cybertools In Another Breach Via Another Contractor, https://www.npr.org/2017/10/05/555922305/report-hackers-stole-nsa-cybertools-in-another-breach-via-another-contractor vom 5. Oktober 2017 sowie NSA's EternalBlue exploit, http://www.zdnet.com/article/a-giant-botnet-is-forcing-windows-servers-to-mine-cryptocurrency/ vom 1. Februar 2018.

Im Gesetzesentwurf fehlt eine Regelung, die fordert, eine genutzte Schwachstelle und die zugehörige Schadsoftware im Einzelfall einem Richter oder einer anderen unabhängigen Stelle vorzulegen sowie eine Prognose zu erstellen, ob die jeweilige Schwachstelle dazu geeignet ist, bei Geheimhaltung einen großen Anteil der Bevölkerung, kritische Infrastrukturen oder die Wirtschaft in besonderer Weise zu schädigen. Ohne eine solche Prüfung, und zwar bevor die Lücke in einem Trojaner genutzt wird, kann die Wahrscheinlichkeit von eintretenden Pannen und Zweckentfremdungen des Trojaners nicht reduziert werden. Zusätzlich kann eine derartige Regelung im Missbrauchsfall Verantwortlichkeiten klären.

1d) Missbrauchsprävention

Missbrauchsfälle sind nicht theoretisch. Die umfassende Spionage, die durch einen Staatstrojaner ermöglicht wird, ist geeignet, Menschen mit Informationen zu erpressen oder ihnen durch Identitätsdiebstahl Schaden zuzufügen. Im Rahmen der Snowden-Veröffentlichungen war bekanntgeworden, dass NSA-Mitarbeiter ihre Spionagewerkzeuge routinemäßig für private Zwecke missbraucht haben.[13] Öffentlich bekannte Fälle in Deutschland betrafen etwa Polizeibehörden, die Staatstrojaner einsetzten.[14]

Für Geheimdienste wie das Landesamt für Verfassungsschutz, die weniger öffentlichen und justiziellen Kontrollen unterliegen als Polizeibehörden, muss ein höheres Schutzniveau gegen Missbrauch angestrebt werden. Aus den Fällen in der Vergangenheit sollte die Lehre gezogen werden, dass eine Spionagesoftware wie ein Staatstrojaner in keinem Fall durch Einzelpersonen im LfV missbräuchlich nutzbar sein darf. Entsprechende Maßnahmen und konkrete Lösungsansätze, die dem entgegenwirken, fehlen im Gesetzesentwurf.

Gefährdet ist auch der Hessische Landtag selbst sowie die Mitglieder des Parlamentarischen Kontrollgremiums, die zur Erfüllung ihrer Aufgaben ebenfalls verbreitete Standardsoftware einsetzen. Das ist genau die Art von Software, die primäres Ziel eines Staatstrojaners ist. Der vom Parlament kontrollierte Geheimdienst wird mit dem Gesetzesentwurf quasi in die Lage versetzt, die eigene Kontrollinstanz zu hacken. Auch dieses Risiko ist nicht

---

[13] Vgl. NSA staff used spy tools on spouses, ex-lovers, https://www.reuters.com/article/us-usa-surveillance-watchdog/nsa-staff-used-spy-tools-on-spouses-ex-lovers-watchdog-idUSBRE98Q14G20130927 vom 27. September 2013.

[14] In der „Patras"-Affäre war 2012 bekanntgeworden, dass ein Polizeibeamter eine Schadsoftware der Bundespolizei zur Überwachung seiner jugendlichen Tochter zweckentfremdet hatte. Auf deren Rechner war der Trojaner später von einem Freund entdeckt worden, dem es in der Folge gelang, Systeme der Bundespolizei zu kompromittieren. Vgl. Patras – Vater-Tochter-Streit löst Angriff auf Bundespolizei aus, https://www.golem.de/1201/88870.html vom 8. Januar 2012.

theoretisch, sondern wurde von „befreundeten" Geheimdiensten bereits praktiziert.[15]

Abschließend bleibt festzustellen, dass im Entwurf zum Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen keine Vorkehrungen geschaffen werden, die einem Missbrauch aktiv entgegenarbeiten oder anderweitig risikomindernd wirken. Das LfV soll zwar unter bestimmten Bedingungen Computer und weitere informationstechnische Systeme ausspähen dürfen, allerdings keinen speziellen Regelungen unterworfen werden, die einem Missbrauch präventiv begegnen.

2) Staatstrojaner im hessischen Gesetzesentwurf

2a) Begrenzung auf laufende Gespräche bei der „Quellen-TKÜ"

Im Zielsystem vorhandene Schwachstellen werden sowohl für die „Quellen-Telekommunikationsüberwachung" nach § 6 Abs. 2, dessen Funktionsumfang auf das Abhören von Gesprächen reduziert sein soll, als auch für die „Online-Durchsuchung" des gesamten informationstechnischen Systems nach § 8 benötigt. Beide Maßnahmen unterscheiden sich nur im Umfang der abgegriffenen Daten. Die Notwendigkeit der Kompromittierung der Systeme ist bei „Online-Durchsuchung" und „Quellen-TKÜ" technisch identisch.

Aus technischer Sicht bestehen erhebliche Zweifel daran, ob die Überwachung bei der sogenannten „Quellen-TKÜ" präzise auf laufende Gespräche eingrenzbar ist. Die Frage, wie laufende Kommunikation treffsicher von anderen auf dem Gerät stattfindenden Datenverarbeitungsprozessen unterschieden werden kann, ist technisch nicht befriedigend gelöst. Der Grund dafür ist, dass eine Bestimmung, wann eine Äußerung an einem Computer zu einer Kommunikation wird, nicht immer leicht zu treffen ist: Praxisnahe Beispiele dafür sind der Entwurf einer E-Mail, die vom informationstechnischen System erfasst, aber nie gesendet wird, oder das Eintippen einer Whatsapp-Nachricht, ohne diese abzusenden. Wird im Rahmen einer „Quellen-TKÜ" ein solcher nicht gesendeter Entwurf erfasst, handelt es sich jedoch nicht um Kommunikation, sondern gleichsam um das Festhalten von Gedanken. Praktisch geschieht dies etwa, wenn die Spionagesoftware Bildschirmfotos anfertigt, wie es von Staatstrojanern zur „Quellen-TKÜ" in der Vergangenheit bereits durchgeführt wurde.

Der hessische Gesetzgeber versucht bei der Regelung zur „Quellen-TKÜ" den gefährlichen Irrweg zu beschreiten, den schon der Bundesgesetzgeber in der Neuregelung des Staatstrojaners in der Strafprozessordnung beschritten hat: Er behandelt das staatliche Hacken eines informationstechnischen Geräts für den Fall der „Quellen-TKÜ" als eine Art Fortschreibung der herkömmlichen Telekommunikationsüberwachung. Diese unterscheidet

[15] Vgl. CIA admits to spying on Senate staffers, https://www.theguardian.com/world/2014/jul/31/cia-admits-spying-senate-staffers vom 31. Juli 2014.

sich technisch gesehen jedoch fundamental von einer Spionagesoftware, da erstere mit Hilfe des Kommunikationsanbieters durchgeführt wird. Die „Quellen-TKÜ" ist hingegen ein Einbruch in ein Computersystem mit allen damit einhergehenden Risiken und Nebenwirkungen und darf daher nicht als bloße Telekommunikationsüberwachung missverstanden werden. Eine rechtliche Gleichsetzung beider Maßnahmen verbietet sich daher.

2b) Vorgesehene Bedingungen zur „Online-Durchsuchung"

Der hessische Gesetzesentwurf missachtet das Urteil des Bundesverfassungsgerichts, das den Einsatz von Staatstrojanern an Bedingungen knüpft: „Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen".[16] Im vorliegenden Gesetzesentwurf erfolgt diese Einschränkung im Bezug auf die „Online-Durchsuchung" nicht. Insbesondere erfolgt noch nicht einmal eine Einschränkung auf Straftaten nach § 3 Abs. 1 des G10-Gesetzes, wie es für die „Quellen-TKÜ" nach § 6 der Fall ist. Fragwürdig ist zudem, ob die Maßgabe einer „dringenden Gefahr für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist" nach § 7 für Wohnraumüberwachung und „Online-Durchsuchung" mit Blick auf das Urteil rechtmäßig ist. Die Erlaubnis des Trojaner-Einsatzes bei „Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist", stellt eine erhebliche Erweiterung dar und ist zu weitgehend.

Betrachtet man zudem die Realität des Einsatzes eines Staatstrojaners, ist es ohnehin widersinnig, einen Landesgeheimdienst mit der Aufgabe der Infektion eines Computersystems zu betrauen, wenn eine konkrete Gefahr für ein überragend wichtiges Rechtsgut droht. Denn das staatliche Hacken benötigt eine Reihe von vorbereitenden Handlungen und das Sammeln von Informationen über das anzugreifende System. Die Installation der Schadsoftware muss immer vorbereitet werden, damit das Zielsystem analysiert, sicher identifiziert und entlang der rechtlichen Vorgaben dann infiziert werden kann.

Diese Prozeduren sind zeitaufwendig und daher bei Gefahr im Verzug nicht mehr sinnvoll durchführbar, wenn es um eine konkrete Gefahrensituation geht, in der ein überragend wichtiges Rechtsgut wie beispielweise ein Menschenleben bedroht ist. Zwar kann nach § 9 Abs. 1 bei „Gefahr im Verzug" auf den eigentlich vorab vorgesehenen Richtervorbehalt verzichtet und der Trojanereinsatz stattdessen erst einmal von der Behördenleitung genehmigt werden, der Staatstrojaner ist als Ultima Ratio zum Schutz vor konkreten Gefahren aber aufgrund der nötigen Vorlaufzeiten kein geeignetes Mittel.

---

[16] Urteil des Ersten Senats vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07, 2. Leitsatz.

Genauso ist ein Geheimdienst in solchen Fällen nicht die adäquate Behörde, die eingeschaltet werden sollte.

Das staatliche Hacken weiter in den präventiven Bereich auszudehnen, widerspricht den Vorgaben des Bundesverfassungsgerichts. Das LfV ist schon wegen seiner typischen Aufgaben keine geeignete Behörde, um Staatstrojaner einzusetzen. Denn wenn wie vom Bundesverfassungsgericht gefordert, die „Online-Durchsuchung" auf die Abwehr von Gefahren für Leib und Leben zu beschränken ist, sollten solche Situationen nicht dem LfV überlassen werden.

2c) Trennungsgebot zwischen polizeilicher und geheimdienstlicher Arbeit

Der Gesetzesentwurf sieht in § 21 Abs. 2 vor, dass Abhör-Daten des LfV an andere Behörden weitergegeben werden können. Dadurch ist das Trennungsgebot tangiert, das geheimdienstliche von polizeilicher Arbeit abkoppeln soll. Folge der Regelung zu den Datenaustauschmöglichkeiten ist eine Aushebelung datenschutzrechtlicher Schutzvorschriften.

Das Trennungsgebot kann auch berührt sein, wenn im LfV die vom Bundeskriminalamt entwickelte Software „Remote Communication Interception Software" mitbenutzt werden sollte. Es ist inakzeptabel, dass gemäß dem Gesetzesentwurf nicht dokumentiert werden muss, welche Spionagesoftware vom LfV verwendet wird, insbesondere bei der Mitwirkung externer Dienstleister. Ebenfalls fehlt ein Verbot zur Zusammenarbeit mit Unternehmen, die ihre Hacking-Werkzeuge auch an Staaten anbieten, die Menschenrechte und demokratische Standards missachten.

2d) Richtervorbehalt und Prüfung

Nach dem Gesetzesentwurf soll ein Richter gemäß § 9 den Einsatz der Schadsoftware kontrollieren. Konkret ist für diese Prüfung das Amtsgericht Wiesbaden vorgesehen. Eine besondere Qualifikation, um die technische Wirkmächtigkeit des Spionagewerkzeugs sowie die praktischen Abläufe zu verstehen, ist dabei nicht vorgesehen. Das gilt auch für die zweite richterliche Prüfung bei der Verwertung der erhobenen Daten.

Eine Rechtmäßigkeitsüberprüfung durch Richter erfordert auch eine technische Prüfung des Trojaners. Diese ist ohne eine Pflicht zum Hinterlegen des Trojaners samt Quelltext nicht möglich. Das dient zugleich der Qualitätssicherung, um rechtlichen und technischen Problemen aufgrund schlampiger und fehlerhafter Programmierung vorzubeugen, die in früher

eingesetzten Versionen von Staatstrojanern der Firma Digitask mit Sitz in Haiger (Lahn-Dill-Kreis) belegt wurden.[17]

Desweiteren fehlt auch eine Regelung, dass dem Verfassungsschutz der Quelltext des Trojaners überhaupt bekannt sein muss. Es ist zu befürchten, dass wie in der Vergangenheit proprietäte Software von kommerziellen Anbietern eingekauft wird, die aufgrund schlampiger Programmierung selbst unsicher ist und die zugehörigen Serverssysteme des Landesamts für Verfassungsschutz selbst angreifbar macht. Trotz dieser Gefahren ist eine Dokumentation auch durch eventuell hinzugezogene externe Dienstleister nicht vorgeschrieben.

Den Richtern des Amtsgerichts Wiesbaden wird die Verantwortung für Entscheidungen auferlegt, die ohne Kenntnis des technischen Sachverhaltes aber gar nicht adäquat zu treffen sind. Der Gesetzesentwurf verkennt die Notwendigkeit technischer Kenntnisse zur rechtlichen Bewertung des Trojanereinsatzes, so dass sich die Richter auf die Aussagen von Mitarbeitern des LfV oder deren externer Dienstleister verlassen müssen. Zudem ist wegen der vorab vorzunehmenden Kernbereichsprognose bei Einsatz des Spionageprogramms eine Kammer einem einzelnen Richter vorzuziehen.

Die technische Prüfung, ob mittels Staatstrojaner erhobene Daten authentisch (und damit nach Weitergabe an Polizeibehörden oder Staatsanwaltschaften gemäß § 21 Abs. 2 in einem Gerichtsverfahren verwertbar) sind, dürfte in den meisten Fällen unmöglich sein: Dass der Zugriff mittels Staatstrojaner über eine Sicherheitslücke möglich war, beweist schließlich, dass das Gerät zu diesem Zeitpunkt kompromittierbar war. Es ist daher nicht nachweisbar, ob gefundene Beweise tatsächlich vom überwachten Nutzer stammen oder von Dritten dort hinterlegt oder manipuliert wurden.

2e) Rechtsstaatliche Kontrolle und Prüfung

Der Gesetzesentwurf wirft die generelle Problematik der Prüfung der Rechtmäßigkeit bei konkreten Einsätzen des Staatstrojaners durch den hessischen Verfassungsschutz auf. Anders als in der Polizeiarbeit, bei der regelmäßig Ermittlungsmethoden der Prüfung durch Gerichte, Strafverteidiger und die Beschuldigten selbst stattfinden, arbeitet ein Geheimdienst unter weit geringerer öffentlicher Kontrolle. Vergangene Geheimdienstskandale lassen auch nicht erkennen, warum der hessischen Behörde ein besonderes Vertrauen entgegengebracht werden sollte. Das hessische LfV hat im Rahmen des parlamentarischen Untersuchungsausschusses im Wiesbadener Landtag zum NSU-Skandal und zum ehemaligem V-Mann-Führer Andreas Temme wenig Anlass für Vertrauensvorschuss geboten.

---

[17] Vgl. Chaos Computer Club analysiert Staatstrojaner, http://ccc.de/de/updates/2011/staatstrojaner vom 27. Juni 2012.

Ein Aspekt der Prüfung des rechtmäßigen Einsatzes ist die Aufzeichnung der Verfahrensschritte. Die im Gesetzesentwurf vorgesehene Protokollierung von „nichtflüchtigen Änderungen" nach § 6 Abs. 4 Satz 1 Nr. 5 ist unzureichend. Eine Änderung ist im technischen Sinne „flüchtig", wenn sie nur auf den Arbeitsspeicher des Rechners angewendet wird. Dieser wird normalerweise beim Herunterfahren oder Neustarten des Systems verworfen. Demgegenüber stehen nichtflüchtige Änderungen, welche auf Festplatten, SSDs oder Speicherkarten angewendet werden. Diese Speichermedien behalten ihre Daten auch dann, wenn das Gerät ausgeschaltet wird. Eine „nichtflüchtige" Änderung bleibt also auf unbegrenzte Zeit bestehen.

Eine eindeutige Trennung zwischen flüchtigen und nichtflüchtigen Änderungen ist beim Trojanereinsatz in der Praxis jedoch aus zweierlei Gründen nicht möglich: Zum einen werden die meisten Smartphones, Server und Router sowie viele PCs und Laptops selten oder nie neu gestartet.[18] Eine technisch gesehen „flüchtige" Änderung kann deshalb monate- oder jahrelang fortbestehen. Zum anderen sind die Systeme, in die der Verfassungsschutz mit dem Trojaner einbrechen soll, so komplex, dass es nicht möglich ist, alle Wechselwirkungen zwischen Trojaner und angegriffenem System abzusehen. Das versehentliche Hinterlassen von nichtflüchtigen Veränderungen durch den Verfassungsschutz ist daher sehr wahrscheinlich.

Folglich könnte ein von staatlichen Stellen eingesetzter Trojaner erhebliche Veränderungen am System vornehmen, die nicht von der Protokollierungspflicht nach § 6 (4) umfasst wären. Dass flüchtige Veränderungen generell nicht dokumentiert werden müssen, ist daher unzureichend. Hierbei ist auch zu bedenken, dass mittlerweile Schadsoftware im Umlauf ist, die sich ausschließlich im flüchtigen Speicher des Systems aufhält. Das zeigt, dass eine Schadsoftware nicht weniger problematisch ist, nur weil sie im technischen Sinne „flüchtig" ist.

Der vorliegende Gesetzesentwurf liefert keine ausreichenden Regelungen zur besonderen rechtsstaatlichen Kontrolle des Einsatzes von geheimdienstlichen Trojanern. Für Maßnahmen nach § 6 Abs. 2 des Verfassungschutzgesetzes („Quellen-TKÜ" mit Trojanereinsatz) sind im Verfassungschutzkontrollgesetz keine Berichtspflichten an das parlamentarische Kontrollgremium vorgesehen.

In § 6 Abs. 4 werden keine Dokumentationspflichten über die Herkunft der genutzten Sicherheitslücke und ggf. der Vertragspartner bzw. die unterstützende Behörde bei Zulieferung der Spionagesoftware angeführt. Das Kontrollgremium und der hessische Datenschutzbeauftragte können somit keinen Einblick nehmen und die Gefahren für Privatpersonen und Wirtschaft durch das Ausnutzen der Sicherheitslücke nicht einschätzen.

---

[18] Das Aktivieren des Ruhezustands ist kein Ausschalten des Systems. Hierbei wird der Inhalt des flüchtigen Speichers auf den nichtflüchtigen Speicher kopiert und nachträglicher Analyse sogar nach einem späteren Ausschalten zugänglich gemacht.

Wie bei jeder geheimen Überwachung sollte sich das LfV einer unabhängigen Kontrolle stellen müssen: sowohl bei Entwicklung und Nutzung von Trojanern als auch durch gerichtliche Prüfung der Einsatzprotokolle. Welche Daten von den Geräten gewonnen oder in diese eingespielt und welche konkreten Maßnahmen ergriffen wurden, um einen Missbrauch der Spionagesoftware durch Dritte zu vermeiden, muss im Einzelfall dokumentiert werden.

Diese Dokumentation wäre zudem einer Evaluation des Gesetzes dienlich, welche aufgrund der Schwere der vorgesehenen Grundrechtseingriffe dringend geboten ist. Eine Befristung des Gesetzes ist daher sinnvoll und würde spätere Korrekturen auf der Basis dokumentierter Fakten ermöglichen.

2f) Besondere Benachteiligung von Menschen mit Behinderung

Generell finden sich keine Regelungen zur Sicherstellung der Integrität und Funktionalität des betroffenen informationstechnischen Systems im Gesetzesentwurf. Wie bereits vom Arbeitskreis barrierefreies Internet e. V. kritisiert,[19] stellt dies eine besondere Beeinträchtigung Behinderter dar, da Veränderungen an Systemen mit spezialisierter Software schnell dazu führen können, dass diese Systeme aufgrund des Verlusts der Barrierefreiheit nicht mehr genutzt werden können. Da sich sowohl Überwachungssoftware als auch sog. Screenreader („Bildschirmvorleser") und vergleichbare Assistenzsysteme in dieselben Schnittstellen des Betriebsystems integrieren, wäre hier eine Software-Inkompatabilität denkbar und nicht unwahrscheinlich. Anders als unter Punkt G auf Seite 3 des Gesetzesentwurfs behauptet, liegen demnach besondere Auswirkungen auf behinderte Menschen vor. Hier ist eine erneute Prüfung des Entwurfs nach den Maßstäben der UN-Behindertenrechtskonvention nötig.

Darüber hinaus sei darauf hingewiesen, dass eine Beeinträchtigung der Funktionalität des kompromittierten informationstechnischen Systems dazu führen wird, dass der Einsatz der Software zur „Online-Durchsuchung" bzw. „Quellen-TKÜ" nicht unbemerkt bleibt. Sowohl die Maßnahme an sich als auch die vom Trojaner genutzte Sicherheitslücke könnten dadurch öffentlich werden.[20]

---

[19] Vgl. Arbeitskreis barrierefreies Internet e. V.: Hessentrojaner bedroht Behinderte, http://akbi.de/2017/12/22/pm-37-hessentrojaner-bedroht-behinderte-akbi-schliesst-sich-gemeinsamer-erklaerung-gegen-verfassungsschutzgeset-z-an/ vom 22. Dezember 2017.

[20] Zur Gefahr für die Bevölkerung durch offene Sicherheitslücken in kritischer Infrastruktur siehe auch Abschnitt 1c, Seite 4.

2g) Unverhältnismäßige Grundrechtseingriffe

Aufgrund der zentralen Rolle, die insbesondere Smartphones für die höchstpersönlichen Beziehungen vieler Menschen spielen, darf die „Quellen-TKÜ" nicht als eine Fortsetzung der Telefonüberwachung mit anderen Mitteln missverstanden werden (vgl. Abschnitt 2a, S. 8f.). Wenn eine staatliche Stelle durch Schadsoftware den Zugriff auf ein Smartphone erlangt, ist das nicht einfach nur das Äquivalent einer abgehörten Telefonleitung. Das digitale Abbild vieler Lebensaspekte der Person ist mit dem informationstechnischen System verbunden: höchstpersönliche Gespräche mit Partnern, Familienmitgliedern und Freunden, besuchte Webseiten, Suchbegriffe und Aufenthaltsorte.

Beispielhaft zu bedenken ist hier, dass Menschen auch intime Beziehungen über informationstechnische Systeme anbahnen und private Nachrichten als Texte, Bilder oder Videos mit höchstpersönlichem Inhalt mittels Computern und Smartphones erstellen und versenden. Ähnliches gilt für das Teilen und Diskutieren religiöser und weltanschaulicher Überzeugungen oder die vertrauliche Kommunikation mit Geistlichen oder Berufsgeheimnisträgern. Es ist unvermeidbar, dass derartige Nachrichten bei einer „Online-Durchsuchung" oder „Quellen-TKÜ" ebenfalls erfasst werden können.

Eingriffe in den besonders geschützten Kernbereich der privaten Lebensgestaltung müssen zum einen wirksam verhindert werden. Zum anderen müssen kernbreichsrelevante Daten zusätzlich gegen missbräuchliche Verwendung gesichert werden. Fälle, in denen derartige Überwachungsinstrumente missbraucht wurden, sind nicht theoretisch und bei „befreundeten" Geheimdiensten auch öffentlich geworden.[21] Der damalige Datenschutzbeauftragte Peter Schaar hat in seinem Bericht über „Maßnahmen der Quellen-Telekommunikationsüberwachung bei den Sicherheitsbehörden des Bundes" in deutlichen Worten bemängelt, dass bei einem mittels „Quellen-TKÜ" abgehörten Skype-Gespäch rechtswidrig auch Liebesbeteuerungen, erotische Gespräche und Selbstbefriedigungshandlungen abgehört und sogar noch gespeichert und protokolliert worden waren.[22]

Manche Kommunikationsendgeräte werden von mehreren Personen verwendet. Damit sind beim Trojanereinsatz auch deren Grundrechte zu berücksichtigen. Es ist für einen Überwachungstrojaner nicht erkennbar, wer gerade vor dem Gerät sitzt. Wird also der Computer einer Zielperson mit einem Trojaner infiziert, können private Daten von Dritten ebenfalls betroffen sein, ebenso wird ein Eingriff in deren höchstpersönlichen Lebensbereich möglich.

---

[21] In NSA-Büros wurden intime Fotos abgefangen und herumgereicht, vgl. The NSA Shared Sexually Explicit Photographs, Says Edward Snowden, http://time.com/3010649/nsa-sexually-explicit-photographs-snowden/ vom 21. Juli 2014.

[22] Vgl. Bericht von Peter Schaar, abrufbar unter https://www.ccc.de/system/uploads/103/original/Schaar-Bericht.pdf vom 31. Januar 2012.

2h) Zugriff auf beliebige informationstechnische Systeme

Dem Gesetzesentwurf fehlt in den §§ 6 und 8 eine Eingrenzung der informationstechnischen Systeme, in die eingegriffen werden darf. Aufgrund der immer weiter zunehmenden Vernetzung von Gebrauchsgegenständen und medizinischen Geräten erscheint eine Einschränkung jedoch zwingend nötig. Ein Eingriff in Systeme mit Bezug zu kritischer Infrastruktur (etwa Stromnetze, Internetknotenpunkte), aber auch beispielsweise Industrieanlagen und Maschinensteuerungen, Fahrzeugelektronik, Behördennetze sowie medizinisch genutzte Computersysteme (Herzschrittmacher, lebenserhaltende Maschinen, elektronische Implantate) ist mit unkalkulierbaren Risiken für die Betroffenen oder gar für die gesamte Bevölkerung verbunden. Eine solche Maßnahme sollte daher vom Gesetzgeber präventiv unterbunden werden. Beim Einsatz von Schadsoftware bleibt jedoch immer ein Restrisiko, auch solche Systeme versehentlich zu beeinträchtigen.

Der Gesetzesentwurf erlaubt nach §§ 6 und 8 die Kompromittierung informationstechnischer Systeme Dritter, sofern diese Systeme durch von der Maßnahme betroffenen Personen genutzt werden. Hier liegt nicht nur ein gravierender Eingriff in die Rechte einzelner Dritter vor. Dies kann auch Systeme betreffen, die von einer größeren Anzahl von Personen genutzt werden, etwa Serversysteme wie E-Mail-Server. Die Gefährdung der Funktionsfähigkeit und auch die Erfassung von Daten vieler Unbeteiligter kann dabei nicht ausgeschlossen werden soll. Eine definitorische Beschränkung ist daher in den Gesetzesentwurf aufzunehmen.

In § 8 liegt zudem gar keine Eingrenzung der zu kompromittierenden Systeme vor, so dass nicht einmal die Nutzung des informationstechnischen Systems durch Zielpersonen Bedingung für einen Eingriff ist. Nach den Vorausetzungen des § 3 Abs. 2 des G10-Gesetzes können sich die getroffenen Maßnahmen auch „gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Verdächtigen bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben". Diese Regelung war ursprünglich für die Telekommunikationsüberwachung ohne den Einsatz von Staatstrojanern vorgesehen. Sie ist zu weitgehend, wenn sie ebenfalls auf die aktive Kompromittierung von Computersystemen unbeteiligter Dritter (etwa auch Internetdiensteanbieter) angewandt wird. Dieses Problem wird dadurch verstärkt, dass ein bloßer Verdacht, auf einem System könnten sich relevante Daten befinden, zur Anwendung der Trojaner-Maßnahme ausreicht. Eine Schadsoftware in ein solches System einzuspielen, gefährdet jedoch die Sicherheit aller seiner Nutzer und nimmt Grundrechtsverletzungen bei völlig unbeteiligten Personen billigend in Kauf.

Zusammenfassung

Nach dem geplanten Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen soll das LfV die Befugnis erhalten, sich heimlich in Computersysteme zu hacken. Sowohl der Einsatz als auch die Entwicklung der dafür benötigten Schadprogramme bringen erhebliche Gefahren mit sich, denen der Gesetzesentwurf nur unzureichend Rechnung trägt.

Da für Trojaner Sicherheitslücken benötigt werden, müssen diese gefunden oder erworben werden. Solche Sicherheitslücken, die absichtlich geheimgehalten werden, stellen eine erhebliche Gefährdung für kritische Infrastrukturen, Behörden, Wirtschaft und Privatpersonen dar. Vorfälle wie die rasante Ausbreitung der Schadsoftware „Wannacry", bei der eine von der NSA geheimgehaltene Sicherheitslücke ausgenutzt wurde, zeigen, wie unmittelbar diese Bedrohung ist. Im Gesetzesentwurf fehlen Maßnahmen, die diese Risiken mindern könnten. Dem Missbrauch von staatlicher Schadsoftware wird zudem nicht ausreichend vorgebeugt. Eine wirksame Kontrolle des Trojanereinsatzes kann aufgrund lückenhafter Protokollierungspflichten nicht erfolgen.

Die Eingriffshürden für Maßnahmen nach §§ 6 und 8 („Quellen-TKÜ" und „Online-Durchsuchung") sind nicht ausreichend. Angesichts der Schwere der Grundrechtseingriffe, auch in den Kernbereich der privaten Lebensgestaltung, wären Nachbesserungen am Gesetzesentwurf zwingend.

Die Entwicklung und der Einsatz von Schadsoftware durch den Staat sind aufgrund der dargestellten erheblichen und strukturellen Risiken für die IT-Sicherheit auch grundsätzlich abzulehnen. Die entsprechenden Paragraphen sind zu streichen.

Stellungnahme

zu dem

Gesetzentwurf

der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein

Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen

- Drucks. 19/5412-

hierzu:

Änderungsantrag

der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN

- Drucks. 19/5782 -

zur Vorbereitung der öffentlichen Anhörung des
Innenausschusses des Hessischen Landtages
am 8. Februar 2018

vorgelegt von

Prof. Dr. Ralf Poscher
und
Dr. Benjamin Rusteberg
Institut für Staatswissenschaft und Rechtsphilosophie
an der Albert-Ludwigs-Universität Freiburg

im Februar 2018

A. Einleitung

Der vorliegende Gesetzentwurf – Drucks. 19/5412 – für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen enthält in Artikel 1, der den Schwerpunkt des Gesetzes bildet, ein neues Hessisches Verfassungsschutzgesetz (HVSG). Ergänzt wird dieses in Artikel 2 durch ein Gesetz zur parlamentarischen Kontrolle des Verfassungsschutzes in Hessen (Verfassungsschutzkontrollgesetz). Artikel 3 fügt in Verbindung mit dem Änderungsantrag – Drucks. 19/5782 – neue Befugnisnormen in das Hessische Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) ein und nimmt weitere Änderungen daran vor.

Durch das Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen soll die Arbeit des Landesamts für Verfassungsschutz auf eine neue gesetzliche Grundlage gestellt werden. Als Ziele nennt der Entwurf[1]

- eine Verbesserung der Zusammenarbeit der Nachrichtendienste, Polizei- und sonstigen Sicherheitsbehörden im Verhältnis von Bund und Ländern, auch auf der Grundlage der politischen Aufarbeitung der Mordserie der rechtsextremistischen Terrorgruppe des sogenannten „Nationalsozialistischen Untergrunds" (NSU);
- Umsetzung der auf Bund- und Länderebene, insbesondere durch die Expertenkommission der Hessischen Landesregierung, erarbeiteten Handlungsempfehlungen;
- Anpassung der hessischen Vorschriften an die Rechtsprechung des Bundesverfassungsgerichts, insbesondere das in der Entscheidung zum Antiterrordateigesetz entwickelte „informationelle Trennungsprinzip" sowie an die Vorgaben aus dem Urteil zum BKA-Gesetz;
- Schaffung einer gesetzlichen Grundlage, die die Befugnisse des Landesamts und deren Grenzen klar definiert;
- Orientierung an bundeseinheitlich geltenden rechtsstaatlichen Standards, wie sie insbesondere im Artikel-10-Gesetz und dem überarbeiteten Bundesverfassungsschutzgesetz niedergelegt seien;
- Stärkung der parlamentarischen Kontrolle;
- Verbesserung der Verhütung von Straftaten durch die Aufnahme zusätzlicher Befugnisse und Ergänzung vorhandener Regelungen im HSOG.

Angesichts des Umfangs der Neuregelung und der für die Stellungnahme zur Verfügung stehenden Zeit kann vorliegend nicht auf alle, auch nicht auf alle möglicherweise problematischen Punkte des Entwurfs eingegangen werden. Die im Folgenden genannten Punkte erscheinen jedoch besonders erwähnungsbedürftig.

[1] Drucks. 19/5412, S. 1 ff., 24 ff.

B. Hessisches Verfassungsschutzgesetz (HVSG)

I. Regelungstechnik

1. Neugliederung

Das aktuelle Hessische Gesetz über das Landesamt für Verfassungsschutz (VerfSchG HE 1990) stammt aus dem Jahre 1990 und ist seitdem viele Male geändert und ergänzt worden. Statt weitere punktuelle Änderungen vorzunehmen, setzt der vorliegende Gesetzentwurf deshalb auf eine vollständige Neuregelung. Durch eine „verbesserte Normenklarheit soll die Rechtssicherheit erhöht und die Grundlage für eine stärkere gesellschaftliche Akzeptanz geschaffen werden."[2]

In seiner Systematik hält der Gesetzentwurf an der bisherigen Gliederung in vier Teile fest, strukturiert aber deren Inhalte neu. Die bislang zusammenhängend geregelten Aufgaben und Befugnisse werden nunmehr getrennt normiert: Der Erste Teil des neuen HVSG regelt die Organisation und die Aufgaben des Landesamts, der Zweite Teil dessen Befugnisse bei der Informationserhebung. Im Dritten Teil sind die Regelungen zur Speicherung, Sperrung, Löschung sowie vor allem zur Übermittlung personenbezogener Daten normiert. Im abschließenden Vierten Teil finden sich die Schlussvorschriften.[3] Die gesetzlichen Regelungen über die parlamentarische Kontrolle des Verfassungsschutzes, die im VerfSchutzG HE 1990 bislang ebenfalls enthalten war, werden nun mit dem Verfassungsschutzkontrollgesetz in ein eigenständiges Gesetz überführt.

Die durch den Gesetzentwurf vorgenommene Neugliederung ist grundsätzlich zu begrüßen. Das neue HVSG gewinnt insofern an Übersichtlichkeit gegenüber der Vorgängerreglung.

2. Enumeration statt Generalklausel

Die Technik des Gesetzentwurfs, die Zahl der verwendeten Generalklauseln zu reduzieren und durch Enumerationen zu ersetzen, ist ebenfalls grundsätzlich positiv zu bewerten.

§ 5 Abs. 2 S. 2 HVSG enthält nunmehr in Satz 1 eine Legaldefinition der nachrichtendienstlichen Mittel sowie in Satz 2 eine abschließende Aufzählung derjenigen nachrichtendienstlichen Mittel, die das Landesamt einsetzen darf. Die allgemeinen Voraussetzungen für diesen Einsatz sind zudem in den Absätzen 1 und 3 des § 5 HVSG geregelt. Für einzelne nachrichtendienstliche Mittel finden sich weitergehende Anforderungen in den folgenden Paragraphen.

---

[2] Drucks. 19/5412, S. 26.
[3] Drucks. 19/5412, S. 26.

Nach Ansicht des Entwurfs soll durch diese Regelung der grundrechtlichen Relevanz nachrichtendienstlicher Mittel stärker Rechnung getragen werden. Der Einsatz nachrichtendienstlicher Mittel müsse normenklar geregelt und kontrollierbar sein.[4]

Die Möglichkeit einer solchen abschließenden Aufzählung der nachrichtendienstlichen Mittel war im Bereich des Nachrichtendienstrechts schon lange in der Diskussion, wurde aber vielfach als nicht praktikabel zurückgewiesen.[5] Der vorliegende Entwurf zeigt nun, dass eine solche Aufzählung möglich ist. Dabei darf allerdings nicht übersehen werden, dass mit dieser Aufzählung kein weitergehender Gestaltungsanspruch verbunden ist. Diese scheint insbesondere nicht darauf angelegt, bislang in der Praxis eingesetzte Mittel nunmehr aus dem Kreis zulässiger Maßnahmen auszuscheiden. Insofern handelt es sich – wie so oft im Bereich der personenbezogenen Prävention – eher um eine nachlaufende gesetzgeberische Kodifikation einer etablierten behördlichen Praxis. Ihr Nutzen liegt somit vor allem darin zu verhindern, dass nachrichtendienstliche Mittel, die aufgrund voranschreitender technischer Entwicklung oder innovativer Praxis dem Landesamt potentiell zur Verfügung stünden, auch nicht vorübergehend auf eine Generalklausel gestützt werden können – anders als etwa im Polizeirecht unter der Geltung der polizeilichen Generalklausel. Es bedarf nunmehr also in jedem Fall eines neuen gesetzgeberischen Entscheids, um die Liste der zulässigen nachrichtendienstlichen Mittel zu erweitern. Hierin liegt nicht zuletzt auch eine Stärkung der parlamentarischen Kontrolle des Verfassungsschutzes, wie ihn der Gesetzentwurf ausdrücklich anstrebt.

§ 21 HVSG regelt die Informationsübermittlung durch das Landesamt innerhalb des öffentlichen Bereichs. § 21 Abs. 1 Nr. 2 HVSG enthält nun ebenfalls eine Enumeration der möglichen Verwendungszwecke, für die das Landesamt Informationen an inländische öffentliche Stellen zu vermitteln befugt ist. Anders als bei § 5 Abs. 2 S. 2 HVSG ist die hier vorgenommene Aufzählung allerdings nicht abschließend („insbesondere"). Dennoch ist der gewählte Regelungsansatz auch hier zu begrüßen, da er erstmals eine differenzierte Auseinandersetzung mit den einzelnen Übermittlungsanlässen bzw. mit der nachfolgenden Verarbeitung der Information ermöglicht. Auf die dabei bestehenden materiellrechtlichen Probleme wird noch einzugehen sein.[6]

---

[4] Drucks. 19/5412, S. 31.
[5] Vgl. zur Diskussion schon Schlink NJW 1981, 565 ff.; Gusy NVwZ 1983, 322 ff.
[6] Vgl. unten B.III.2.

3. Verweisungen

a) Zweckmäßigkeit

Um das HVSG stärker in den Regelungskomplex einzubinden, den der Bundesgesetzgeber für die Zusammenarbeit innerhalb des Verfassungsschutzverbunds geschaffen hat, und dessen Anwendung zu erleichtern, übernimmt der Gesetzentwurf an zahlreichen Stellen bundesrechtliche Regelungen.[7] Dies geschieht zum Teil durch textgleiche Regelungen – vgl. § 2 Abs. 2 HVSG der weitgehend § 3 Abs. 1 BVerfSchG entspricht – vielfach aber auch durch Verweisungen, seien es statische – vgl. § 3 Abs. 1 HVSG, der bestimmt dass die „Begriffsbestimmungen des § 4 Abs. 1 Satz 1, 2 und 4 sowie Abs. 2 des Bundesverfassungsschutzgesetzes" Anwendung finden – oder auch dynamische Verweisungen – § 11 Abs. 3 HVSG verweist etwa auf das Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Gesetz vom 27. Juni 2017 (BGBl. I S. 1963), in der jeweils geltenden Fassung; § 11 Abs. 8 HVSG verweist auf die Nachrichtendienste-Übermittlungsverordnung vom 11. Oktober 2012 (BGBl. I S. 2117), zuletzt geändert durch Gesetz vom 23. Dezember 2016 (BGBl. I S. 3346), in der jeweils geltenden Fassung.

Eine derartige Übernahme der Regelungen eines anderen Normgebers kann sich durchaus als zweckmäßig darstellen. Sie kann Ausdruck von „Gesetzesökonomie"[8] sein, indem sie die einheitliche Anwendbarkeit der jeweiligen Regelungen sicherstellt und unnötige Dopplungen sowie damit evtl. verbundene unbeabsichtigte Abweichungen vermeidet.

Eine derartige Regelungstechnik kann allerdings auch mit erheblichen Nachteilen verbunden sein. So ist mit der bloßen Übernahme von Bundesrecht ein weitgehender Verzicht auf einen eigenständigen landesrechtlichen Regelungsansatz verbunden. Dabei verbleibt dem Gesetzgeber bei der Regelung der nachrichtendienstlichen Informationserhebung und -verarbeitung, trotz der zahlreichen Vorgaben des Bundesverfassungsgerichts, durchaus ein eigenständiger Spielraum.[9] Dies gilt umso mehr, soweit es ihm darum geht, einen über das Mindestmaß hinausgehenden Schutz der durch die Maßnahmen beeinträchtigten Grundrechte sicherzustellen. Durch die schlichte Übernahme der bundesgesetzlichen Regelungen macht der Entwurf freilich nur sehr eingeschränkt von diesem Spielraum Gebrauch. Dies ist auch deshalb bedauerlich, weil damit zugleich einer der großen rechtstechnischen Vorteile des föderalen Systems der Bundesrepublik nicht ausgeschöpft wird, nämlich die Möglichkeit eine

[7] Drucks. 19/5412, S. 26.
[8] Begriff bei Brugger, VerwArch 78 (1987), S. 1 (7).
[9] Übersicht über die Rechtsprechung bei Tanneberger, Die Sicherheitsverfassung, 2014.

„best practice“ aus den unterschiedlichen Regelungsansätzen in Bund und Ländern zu entwickeln. Davon, dass sich eine solche „best practice“ im Bereich des Nachrichtendienstrechts bereits herausgebildet hätte, kann angesichts der Bewegung, die in diesem Rechtsgebiet momentan herrscht, auch längst noch keine Rede sein.

Schließlich führt eine derartige Verweisungstechnik, die eben in der Regel auch nur eine „entsprechende“ Anwendung der in Bezug genommenen Vorschriften erlaubt, zu neuen Unbestimmtheiten, die nicht zuletzt für den rechtsunterworfenen Bürger eine Nachvollziehbarkeit des Gesetzes erschweren. Dies wird insbesondere bei den weiteren Ausführungen zu den Maßnahmen der Informationserhebung noch deutlich werden.[10]

b) Verweisungen auf das Artikel 10-Gesetz

(I) Vorliegen Dynamischer Verweisungen?

Die Entwurfsbegründung gibt an, dass der Gesetzentwurf „[h]insichtlich der materiellen Grenzen (Schutz des Kernbereichs privater Lebensführung, Schutz zeugnisverweigerungsberechtigter Personen, Eingriff als ‚ultima ratio‘ etc.) und des Verfahrens (Antrag, Durchführung, Mitteilung an Betroffene etc.) [...] soweit möglich dynamische Rechtsgrundverweisungen auf das Gesetz zur Beschränkung des Brief-, Post und Fernmeldegeheimnisses - Artikel-10-Gesetz“ verwende. Dieses enthalte „eine bundesweit geltende Grundlage für Maßnahmen der Nachrichtendienste sowohl des Bundes als auch der Länder im Schutzbereich des Art. 10 des Grundgesetzes“ und sei daher „aus diesem Bereich den Mitarbeiterinnen und Mitarbeitern des Landesamts bereits vertraut“.[11] Etwas später führt die Entwurfsbegründung zudem aus, dass so eventuelle Änderungen durch den Bundesgesetzgeber, die durch die Fortentwicklung der Rechtsprechung des Bundesverfassungsgerichts ausgelöst werden, automatisch in das Landesrecht übernommen werden könnten, der Landtag aber dennoch jederzeit die Möglichkeit habe, auf unerwünschte Änderungen im Bundesrecht durch eine Änderung der Verweisungsnormen im Landesrecht zu reagieren.[12]

Diese Ausführungen verwundern insofern, als eine dynamische Verweisung auf das Artikel 10-Gesetz im Normtext an keiner Stelle explizit gemacht wird. Soweit der Gesetzesentwurf an anderer Stellen deutlich macht, dass er sich dynamischer Verweisungen bedient, verweist er nicht lediglich auf die entsprechende Norm, sondern zitiert den vollständigen Gesetzestitel

[10] Vgl. insbesondere unten B.II.2.b)(II).
[11] Drucks. 19/5412, S. 27.
[12] Drucks. 19/5412, S. 27.

mit der jeweiligen letzen Änderung sowie den entsprechenden Veröffentlichungsstellen und verwendet dabei den Zusatz „in der jeweils geltenden Fassung".[13] Entsprechende Bestimmungen finden sich an den Stellen, in denen der Entwurf auf das Artikel 10-Gesetz Bezug nimmt, d.h. insbesondere bei den §§ 6 ff. HVSG, allerdings nicht.

Eine dynamische Verweisung auf die jeweils aktuelle Version des Bundesgesetzes würde nach gegenwärtigem Stand also nicht erfolgen. Im Falle veränderter Vorgaben durch das Bundesverfassungsgericht müsste der Hessische Landesgesetzgeber weiterhin selbst aktiv werden.

(II) Verfassungsmäßigkeit derartiger dynamischer Verweisungen

Im Gegensatz zu dynamischen würden derartige statische Verweisungen auf das Artikel 10-Gesetz allerdings auch keine weitergehenden verfassungsrechtlichen Fragen aufwerfen. Denn während sich bloße textliche Übernahmen und sogenannte statische Verweisungen grundsätzlich als verfassungsrechtlich unproblematisch darstellen, ist die Verfassungsmäßigkeit dynamischer Verweisungen – soweit sie auf Regelungen anderer Normgeber Bezug nehmen – traditionell umstritten.[14]

Nach der Rechtsprechung des Bundesverfassungsgerichts darf ein Gesetzgeber im Rahmen seiner Regelungen zwar grundsätzlich auch „im Wege der Verweisung auf Vorschriften eines anderen Normgebers Bezug nehmen."[15] Jedoch müssen derartige Verweisungen in Hinblick auf das Bestimmtheitsgebot „hinreichend klar erkennen lassen, welche Vorschriften im einzelnen gelten sollen."[16] In der Literatur werden hier zum einen Anforderungen an die hinreichende Bestimmtheit der Verweisungsklausel und zum anderen an die hinreichende Publikation der in Bezug genommenen Vorschriften formuliert.[17] In dieser Hinsicht bestehen für die im vorliegenden Gesetzentwurf enthaltenen Regelungen allerdings keine Bedenken.

Über die bloße Normenklarheit hinaus bestehen jedoch noch weitere Anforderungen. Die Verweisung „auf andere Vorschriften in ihrer jeweils geltenden Fassung (dynamische Verweisung)", könne dazu führen, dass der eigentlich zuständige Gesetzgeber „den Inhalt seiner Vorschriften nicht mehr in eigener Verantwortung bestimmt und damit der

[13] Neben den oben unter B.I.3.a) zitierten Stellen vgl. auch § 6 Abs. 1 HVSG in Bezug auf das Hessische Ausführungsgesetz zum Artikel 10-Gesetz.
[14] Zur Debatte Sachs, in: ders. (Hrsg.), GG. Grundgesetz Kommentar, 7. Aufl. 2014, Art. 20 Rn. 123a; in der Rechtsprechung zuletzt BVerfG, Beschl. vom 17. Februar 2016 – 1 BvL 8/10 –, Rn. 75, m.w.N.
[15] BVerfG, Beschluss vom 25. Februar 1988 – 2 BvL 26/84 –, Rn. 16 (= BVerfGE 78, 32 [35 f.]).
[16] Ebd.
[17] Clemens, AöR 111 (1986), 63 (83 ff.; 86 ff.).

Entscheidung Dritter überläßt."[18] Damit seien dynamische Verweisungen zwar nicht schlechthin ausgeschlossen, „aber nur in dem Rahmen zulässig, den die Prinzipien der Rechtsstaatlichkeit, der Demokratie und der Bundesstaatlichkeit ziehen".[19] Grundrechtliche Gesetzesvorbehalte könnten diesen Rahmen zusätzlich einengen.[20]

Dabei könnte für den vorliegenden Gesetzentwurf nicht davon ausgegangen werden, dass diese Anforderungen im Falle einer Interpretation der Verweisungen auf das Artikel 10-Gesetz als dynamische Verweisungen ohne Weiteres erfüllt wären.

So bedient sich der Gesetzentwurf etwaiger Verweisungen auf das Artikel 10-Gesetz gerade bei Maßnahmen, die eine besonders hohe Eingriffsintensität aufweisen. Nach der sogenannten Wesentlichkeitslehre bedarf es allerdings gerade in diesen Fällen einer selbstständigen Entscheidung des eigentlich verantwortlichen Gesetzgebers.[21] Dem widerspricht auch nicht, dass sich die Verweise vorliegend lediglich auf die Ausgestaltung des Verfahrens beziehen, das bei der Anwendung der jeweiligen Maßnahmen zu beachten ist, während die materiellen Tatbestandsvoraussetzungen durch das HVSG selbst geregelt werden. Denn bei verdeckt ausgeführten Maßnahmen der Informationserhebung kommt der Ausgestaltung des Verfahrens für den Grundrechtsschutz eine wesentliche Bedeutung zu, nicht zuletzt in Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung.

Für die Zulässigkeit einer dynamischen Verweisung soll jedoch sprechen, wenn dem Normgeber, auf den die Verweisung Bezug nimmt, lediglich ein bereits vorstrukturierter Entscheidungsspielraum zusteht, bei der die formal-dynamische Verweisung sich der Sache nach als material-gebundene Verweisung darstellt, die eine vorhersehbare und angemessene Regelung erwarten lässt.[22] Eine solche lässt sich auch im Fall des Verweises auf das Artikel 10-Gesetz annehmen, da die wesentlichen Grundzüge der Verfahrensausgestaltung durch die Entscheidungen des Bundesverfassungsgerichts vorgegeben sind und auch keineswegs damit zu rechnen ist, dass der Bundesgesetzgeber hinter den hier gesetzten Standard zurückfallen wird. Insofern könnten auch dynamischen Verweisungen auf das Artikel 10-Gesetz noch als verfassungsgemäß angesehen werden.

---

[18] Ebd.
[19] Ebd.
[20] Ebd.
[21] Brugger, VerwArch 78 (1987), S. 1 (24).
[22] Brugger, VerwArch 78 (1987), S. 1 (24 f.).

II. § 4 ff. HVSG: Informationserhebung

1. Übersicht

Der Entwurf nimmt die Neuregelung des Hessischen Verfassungsschutzgesetzes zum Anlass, mit der sogenannten Quellen-TKÜ in § 6 Abs. 2 HVSG und dem verdeckten Zugriff auf informationstechnische Systeme in § 8 HVSG neue Befugnisse zur Informationserhebung für das Landesamt einzuführen. Zudem nimmt der Entwurf mit den § 13 und § 14 erstmals eine explizite Regelung des Einsatzes Verdeckter Mitarbeiterinnen und Mitarbeiter bzw. von sogenannten Vertrauensleuten vor. Schließlich finden sich bei den bereits existierenden Ermächtigungen zur Informationserhebung weitere Änderungen im Detail.

Nicht alle der im Rahmen der Neuregelung vorgenommenen Änderungen sind als verfassungsgemäß einzustufen. Insbesondere versäumt es der Gesetzentwurf – trotz gegenteiliger Beteuerung[23] – an zahlreichen Stellen, die notwendigen Konsequenzen aus der Entscheidung des Bundesverfassungsgerichts zum BKA-Gesetz zu ziehen.[24]

2. §§ 7 ff. HVSG: Besonders intensive Überwachungsmaßnahmen

a) Überblick

Die Maßnahmen des verdeckten Einsatzes technischer Mittel zur Wohnraumüberwachung und des verdeckten Zugriffs auf informationstechnische Systeme, die im Entwurf in § 7 bzw. § 8 geregelt sind, hat das Bundesverfassungsgericht in seiner Entscheidung zum BKA-Gesetz als „besonders intensive Überwachungsmaßnahmen“ gekennzeichnet.[25]

Für den verdeckten Einsatz technischer Mittel zur Wohnraumüberwachung existiert mit § 5a VerfSchutzG HE 1990 eine entsprechende Vorläuferregelung sowie mit § 9 Abs. 2 BVerfSchG eine entsprechende Regelung auf Bundesebene. Für den verdeckten Zugriff auf informationstechnische Systeme gibt es hingegen bislang keine Regelung in Hessen; auch auf Bundesebene existiert eine entsprechende Befugnis nur für das BKA, nicht aber für den Verfassungsschutz.

b) Eingriffsvoraussetzungen

Hinsichtlich der zu schützenden Rechtsgüter sowie der zulässigen Adressaten entsprechen die Regelungen der §§ 7 ff. HVSG grundsätzlich den Anforderungen, wie sie das

[23] Drucks. 19/5412, S. 28.
[24] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220.
[25] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 302; dazu Rusteberg, KritV 2017, S. 24 (30).

Bundesverfassungsgericht zuletzt in seiner Entscheidung zum BKA-Gesetz formuliert hat.[26] Sie weisen in der konkreten Ausgestaltung jedoch Mängel auf.

Hinsichtlich der notwendigen Eingriffsschwelle ist die Regelung als solche zwar verfassungskonform. Die diesbezüglich vorgenommenen Erwägungen im Gesetzentwurf gehen jedoch von verfassungswidrigen Voraussetzungen aus.

(I) Schutzgüter

Für Maßnahmen, die der Gefahrenabwehr dienen und damit präventiven Charakter haben, kommt es nach der Rechtsprechung des Bundesverfassungsgerichts in Hinblick auf ihre Rechtfertigung unmittelbar auf das Gewicht der zu schützenden Rechtsgüter an. Heimliche Überwachungsmaßnahmen, die tief in das Privatleben hineinreichen, sind nur zum Schutz besonders gewichtiger Rechtsgüter wie Leib, Leben und Freiheit der Person sowie der Bestand oder die Sicherheit des Bundes oder eines Landes zulässig.[27] § 7 S. 1 Nr. 1 u. 2 HVSG erfüllen diese Anforderungen offensichtlich, indem sie diese Anforderungen wortgleich ins einfache Recht übertragen.

Differenziert ist demgegenüber § 7 S. 1 Nr. 3 HVSG zu beurteilen, der eine Überwachung auch zulässt zum Schutz von „Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist". Eine entsprechende Formulierung des Schutzguts hat das Bundesverfassungsgericht in seiner Entscheidung zur Antiterrordatei zwar zur Rechtfertigung besonders eingriffsintensiver Maßnahmen als noch ausreichend angesehen. Dies jedoch gerade nur, da die Formulierung zum Ausdruck bringe, dass es nicht um den Schutz des Eigentums oder der Sachwerte als solcher gehe, sondern um das öffentlichen Interesse an der Erhaltung dieser Sachen. Im Zusammenhang mit der Terrorismusabwehr seien damit etwa „wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen" gemeint.[28]

Damit lässt sich zwar auch § 7 S. 1 Nr. 3 HVSG in dem oben beschriebenen Sinne noch verfassungskonform auslegen. Zweckmäßiger erscheint jedoch eine Formulierung, die den eigentlichen Bezugspunkt dieser Regelung bereits im Wortlaut deutlich erkennen lässt, so dass eine Auslegung auch ohne zusätzlichen Rückgriff auf die Rechtsprechung des Verfassungsgerichts gelingen kann.

---

[26] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 103 ff.; dazu Rusteberg, KritV 2017, S. 24 (30 f.).
[27] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 106.
[28] BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/07 –, Rn. 203; vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn.183.

(II) Adressaten

Die gezielte Anwendung der besonders eingriffsintensiven Überwachungsmaßnahmen auf Dritte sieht das Bundesverfassungsgericht als unverhältnismäßig an.[29] Die Überwachung eines Dritten könne nur erlaubt werden, „wenn aufgrund bestimmter Tatsachen vermutet werden kann, dass die Zielperson sich dort zur Zeit der Maßnahme aufhält, sie dort für die Ermittlungen relevante Gespräche führen wird und eine Überwachung ihrer Wohnung allein zur Erforschung des Sachverhalts nicht ausreicht. Ebenso kann eine Online-Durchsuchung auf informationstechnische Systeme Dritter erstreckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Zielperson dort ermittlungsrelevante Informationen speichert und ein auf ihre eigenen informationstechnischen Systeme beschränkter Zugriff zur Erreichung des Ermittlungsziels nicht ausreicht."[30]

Auch wenn die Entwurfsbegründung diese Problematik nicht diskutiert, versucht der Gesetzentwurf grundsätzlich diesen Anforderungen Rechnung zu tragen. An dieser Stelle zeigen sich jedoch die praktischen Probleme einer Regelungstechnik, die derart großzügig von Verweisungen Gebrauch macht, besonders deutlich:

Die §§ 7 ff. HVSG machen selbst keine direkten Vorgaben bezüglich der möglichen Maßnahmenadressaten.

Gem. § 5 Abs. 1 S. 2 HVSG darf das Landesamt personenbezogene Daten mit nachrichtendienstlichen Mitteln jedoch nur unter den Voraussetzungen von Satz 2 Nr. 1 bis 5 erheben. Diese setzen mindestens voraus, dass (1.) bei der betroffenen Person tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 vorliegen, (2.) tatsächliche Anhaltspunkte dafür vorliegen, dass auf diese Weise die zur Erforschung von Bestrebungen und Tätigkeiten nach § 2 Abs. 2 erforderlichen Quellen gewonnen werden können, (3.) die Maßnahme zum Schutz des Landesamts gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten erforderlich ist oder (4.) dies zur Überprüfung der Nachrichtenehrlichkeit und der Eignung von Vertrauensleuten erforderlich ist.

Gem. § 5 Abs. 3 S. 1 HVSG dürfen in den Fällen des Absatzes 1 Satz 2 Nr. 1 und 3 zudem „nachrichtendienstliche Mittel nicht gezielt gegen Unbeteiligte eingesetzt werden; im Übrigen gilt § 4 Abs. 8 Satz 2 und Abs. 9." Gem. § 4 Abs. 8 S. 2 HVSG dürfen personenbezogene Daten Unbeteiligter „auch erhoben werden, wenn sie mit zur Aufgabenerfüllung erforderlichen Informationen untrennbar verbunden sind." Gem. § 4 Abs. 9 HVSG sind

[29] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 115, 191 f.
[30] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 115.

Daten, die für das Verständnis der zu speichernden Informationen nicht erforderlich sind, unverzüglich zu löschen. Einzelheiten regelt nach § 5 Abs. 3 S. 2 HVSG „das für den Verfassungsschutz zuständige Ministerium durch Dienstvorschrift".

Aufgrund dieser Regelungen wäre in den Fällen des Absatzes 1 Satz 2 Nr. 2 und 4 der gezielte Einsatz von eingriffsintensiven Maßnahmen also grundsätzlich auch gegen „Unbeteiligte" möglich. Nun ließe sich zwar überlegen, inwieweit bei diesen Varianten überhaupt eine Gefährdung der nach § 7 HVSG erforderlichen Rechtsgüter möglich ist; vollkommen ausgeschlossen erscheint dies freilich nicht.

§ 7 S. 2 HVSG normiert zusätzlich folgendes: „§ 3 Abs. 2 und die §§ 3a und 3b des Artikel-10-Gesetzes finden zum Schutz des Kernbereichs privater Lebensgestaltung und zeugnisverweigerungsberechtigter Personen entsprechende Anwendung." Gem. § 3 Abs. 2 G10 ist die Anordnung „nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. Sie darf sich nur gegen den Verdächtigen oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Verdächtigen bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Verdächtige ihren Anschluss benutzt. Maßnahmen, die sich auf Sendungen beziehen, sind nur hinsichtlich solcher Sendungen zulässig, bei denen Tatsachen die Annahme rechtfertigen, dass sie von dem, gegen den sich die Anordnung richtet, herrühren oder für ihn bestimmt sind. [...]"

Hier ergeben sich weitere Probleme:

So erscheint bereits der Wortlaut der Verweisung missverständlich. Denn anders als dies der Wortlaut eigentlich nahe legt, trifft § 3 Abs. 2 G10 gerade keine Regelungen zum Kernbereichsschutz, sondern enthält eben eine Regelung bzgl. der zulässigen Adressaten.

Wie § 7 S. 2 HVSG selbst normiert, kommt zudem lediglich eine entsprechende Anwendung des § 3 Abs. 2 G10 in Betracht, da dieser sich – entsprechend des Regelungsgegenstandes des G10 – auf Maßnahmen zur Überwachung von Telekommunikations- und Postverkehr bezieht, nicht aber auf die Wohnraumüberwachung oder den verdeckten Zugriff auf informationstechnische Systeme. Zudem bezieht sich der Begriff des Verdächtigen in § 3 Abs. 2 G10 auf den in § 3 Abs. 1 G10 normierten Katalog an Straftaten, während § 7 HVSG sich nunmehr an den gefährdeten Rechtsgütern orientiert.

Eine angepasste Auslegung erscheint insofern zwar grundsätzlich möglich. Dies jedoch vor allem dann, wenn sie nicht allein auf der Grundlage des Gesetzestexts erfolgt, sondern zugleich die bundesverfassungsgerichtlichen Vorgaben mit einbezieht.

Dementsprechend wäre zu überlegen, ob es tatsächlich das Ziel sein kann, eine Neuregelung von Anfang an mit derartigen Auslegungsproblemen zu befrachten. Eine normenklare eigenständige Regelung für die bei den §§ 7 ff. HVSG in Frage kommenden Adressaten erscheint hier vorzugswürdiger.

(III) Eingriffsschwelle

Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Erhebung von Daten durch heimliche Überwachungsmaßnahmen mit hoher Eingriffsintensität im Bereich der Gefahrenabwehr zum Schutz der genannten Rechtsgüter grundsätzlich nur verhältnismäßig, „wenn eine Gefährdung dieser Rechtsgüter im Einzelfall hinreichend konkret absehbar ist und der Adressat der Maßnahmen aus Sicht eines verständigen Dritten den objektiven Umständen nach in sie verfangen ist."[31] Für die „besonders tief in die Privatsphäre eindringenden Eingriffe der Wohnraumüberwachung" verweist das Gericht auf Art. 13 Abs. 4 GG, der explizit eine „dringende Gefahr" verlangt. Diese nehme im Sinne des qualifizierten Rechtsgüterschutzes nicht nur auf das Ausmaß, sondern auch auf die Wahrscheinlichkeit eines Schadens Bezug.[32]

Die §§ 7 u. 8 HVSG verlangen nun für die Anwendbarkeit der entsprechenden eingriffsintensiven Maßnahmen ihrerseits ausdrücklich das Vorliegen einer „dringenden Gefahr". Insoweit kann an der Verfassungsmäßigkeit der Regelungen eigentlich kein Zweifel bestehen.

Problematisch sind allerdings die Ausführungen, die die Entwurfsbegründung zur Bedeutung dieser Eingriffsschwelle macht. So führt sie in Bezug auf § 7 HVSG aus, „dieser schaffe die verfassungsrechtlich ausgewogene, zugleich aber auch hinreichend praktikable Rechtsgrundlage für jene Lebenssachverhalte, in denen sich ein zum Schaden führender Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, aber bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Mit den flankierenden Verfahrensregelungen des § 9 schafft die Vorschrift nunmehr diejenige Eingriffsgrundlage, mit der einem schweren Missbrauch des Wohnungsgrundrechts für extremistisch-terroristische Bestrebungen und Aktivitäten adäquat

[31] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 109.
[32] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 110.

begegnet werden kann. Eine Wohnraumüberwachung kann als ultima ratio etwa dann in Betracht kommen, wenn Privaträume für Missionierungs- bzw. Radikalisierungszwecke genutzt werden. Es entspricht dabei nachrichtendienstlichem Erfahrungswissen, dass entsprechende extremistische Bestrebungen insbesondere dann in den nicht öffentlichen Raum wie etwa Privaträume und angemietete Hallen verlagert werden, wenn der sicherheitsbehördliche Verfolgungsdruck steigt."[33]

Zur verfassungsrechtlichen Absicherung verweist die Begründung auf ein „vom Bundesverfassungsgericht fortentwickelte[s] sicherheitsrechtliche[s] Gefahrenabwehrmodell[...]".[34] Danach sei der Gesetzgeber „nicht von vornherein für jede Art der Aufgabenwahrnehmung auf die Schaffung von Eingriffstatbeständen beschränkt, die dem tradierten sicherheitsrechtlichen Modell der Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren entsprechen. Vielmehr kann er – insbesondere im Kontext der Terrorismusbekämpfung – die Grenzen für bestimmte Bereiche mit dem Ziel der Straftatenverhütung auch weiter ziehen, indem er die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziert. In Bezug auf terroristische Straftaten, die oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, können Überwachungsmaßnahmen auch dann erlaubt werden, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird."[35]

Obwohl die Rechtsprechung des Bundesverfassungsgerichts hier formal korrekt wiedergegeben wird, sind diese Ausführungen in Verbindung mit dem, was zuvor über die praktische Bedeutung der Maßnahmen für das Landesamt gesagt wurde, mindestens missverständlich: Zum einen hat der Gesetzentwurf von der vom Bundesverfassungsgericht eröffneten Möglichkeit, statt auf eine dringende Gefahr, auf das individuelle Verhalten einer Person abzustellen (vgl. demgegenüber etwa § 20h Abs. 1 Nr. 1 b BKAG) gerade nicht Gebrauch gemacht. Zum anderen entsprechen die in der Entwurfsbegründung genannten Beispiele, d.h. die Nutzung von Privaträumen für Missionierungs- bzw. Radikalisierungszwecke, gerade nicht den Voraussetzungen, die das Bundesverfassungsgericht an die Nutzung derart eingriffsintensiver

[33] Drucks. 19/5412, S. 34.
[34] Drucks. 19/5412, S. 34.
[35] Drucks. 19/5412, S. 33 f.

Überwachungsmaßnahmen stellt. Bei der „Missionierung- bzw. Radikalisierung" geht es um geistige Einwirkungen auf Dritte. Weder diese Einwirkung noch „das missioniert bzw. radikalisiert werden" lässt sich damit als ein individuelles Verhalten einer Person beschreiben, welches die *konkrete Wahrscheinlichkeit* begründet, dass die Person *in überschaubarer Zukunft* terroristische Straftaten begehen wird, welche die in § 7 S. 1 HVSG genannten Rechtsgüter verletzen. Durch die in der Entwurfsbegründung genannten Beispiele entsteht der Eindruck, dass die besonders eingriffsintensiven Überwachungsmaßnahmen durch das Landesamt in einem informatorischen Vorfeld eingesetzt werden sollen, in dem sie nach der Rechtsprechung des Bundesverfassungsgerichts gerade nichts zu suchen haben.

Nicht umsonst hat etwa das Land Niedersachsen die Wohnraumüberwachung aus dem Arsenal der nachrichtendienstlichen Mittel gestrichen.[36] Bei einer konkreten Gefahr werde der Vorgang in allen vorstellbaren Fallkonstellationen bereits bei der Polizei in Bearbeitung sein. Dementsprechend habe die niedersächsische Verfassungsschutzbehörde von diesem Mittel niemals Gebrauch gemacht und es werde auch zukünftig keine Anwendungsmöglichkeit für dieses Mittel gesehen. Es seien auch zukünftig keine Sachverhalte vorstellbar, in denen bei Vorliegen einer konkreten Gefahr die Verfassungsschutzbehörde den Fall nicht bereits an die für die Gefahrenabwehr zuständige Polizei abgegeben hätte.[37]

Nichts anderes gilt auch für die Variante, in der das individuelle Verhalten einer Person die *konkrete Wahrscheinlichkeit* begründet, dass die Person *in überschaubarer Zukunft* terroristische Straftaten begehen wird. Das Gericht hat vielmehr herausgearbeitet, dass die Konkretheit des Gefahrurteils sich auf zwei unterschiedliche Aspekte bezieht.[38] Zum einen auf die Konkretheit des Wahrscheinlichkeitsurteils, dass anders als bei der abstrakten Gefahr nicht von gefahrrelevanten Aspekten des konkreten Sachverhalts abstrahieren darf. Zum anderen auf die Konkretisierung des Schadensereignisses, auf das sich das Wahrscheinlichkeitsurteil bezieht.

In den in Bezug genommenen Ausführungen geht es dem Verfassungsgericht nicht um den ersten Aspekt. Es geht ihm nicht darum, die Anforderungen an die Konkretheit und das erforderliche Maß der Wahrscheinlichkeit oder die geforderte zeitliche Nähe abzusenken. Vielmehr geht es dem Gericht lediglich um den zweiten Konkretisierungspunkt. Für die Annahme einer konkreten Gefahr muss nicht immer schon ein „seiner Art nach

[36] Gesetz zur Neuausrichtung des Verfassungsschutzes im Land Niedersachsen, NDS GVBl. 2016, 194 ff.
[37] NDS LT Drucks. 17/2161, 26 f.
[38] Vgl. bereits Poscher, Die Verwaltung 2008, 345 (355 f.).

konkretisiertes und zeitlich absehbares Geschehen" in seinen Grundzügen feststehen.[39] In Hinblick auf die Konkretisierung des Schadensereignisses lässt das Gericht alternativ genügen, dass aufgrund des Verhaltens der Person des Maßnahmeadressaten die *konkrete Wahrscheinlichkeit* besteht, dass dieser *in überschaubarer Zukunft* eine terroristische Straftat begehen wird, deren genauer Ablauf jedoch noch nicht abgesehen werden kann.[40]

Während in dem einen Fall also die *konkrete Wahrscheinlichkeit* bestehen muss, dass *zeitlich absehbar* ein in seinen *Grundzügen feststehendes Schadensereignis* eintreten wird, kann in dem anderen Fall das konkrete Schadensereignis zwar offen bleiben. Dafür muss aber die *konkrete Wahrscheinlichkeit* bestehen, dass eine *bestimmte Person* in *überschaubarer Zukunft* irgendeine *terroristische Straftat* begehen wird und diese Wahrscheinlichkeit muss sich gerade mit dem *Verhalten* dieser Person begründen lassen.

Die Möglichkeit zum Einsatz dieser Überwachungsmaßnahmen im Vorfeld konkreter Gefahren ergibt sich hieraus also gerade nicht.

c) Verfahren

In Hinblick auf das Verfahren zur Anwendung der besonders eingriffsintensiven Überwachungsmaßnahmen und die darin enthaltenen Vorkehrungen zum Schutz des Kernbereichs der privaten Lebensgestaltung bestehen grundsätzlich keine verfassungsrechtlichen Bedenken, die über das bereits Gesagte hinausreichen würden. Hinsichtlich dreier Punkte bedarf es jedoch zumindest kurzer Anmerkungen:

(I) § 9 Abs. 2 HVSG: Antrag auf Anordnung der Überwachung

Nach der Rechtsprechung des Bundesverfassungsgerichts hat der Gesetzgeber das Gebot einer vorbeugenden und unabhängigen Kontrolle beim Einsatz besonders intensiver Überwachungsmaßnahmen in spezifischer und normenklarer Form mit strengen Anforderungen an den Inhalt und die Begründung der gerichtlichen Anordnung zu verbinden.[41] Diesem Gebot ist – unter den entsprechenden Vorbehalten bzgl. der verwendeten Verweisungstechnik – mit § 9 Abs. 2 S. 2 HVSG und dem darin enthaltenen Verweis auf § 10 Abs. 2 u. 3 G10 Genüge getan.

Aus dem Gebot folgt nach Ansicht des Gerichts aber zugleich das Erfordernis einer hinreichend substantiierten Begründung und Begrenzung des Antrags auf Anordnung, die es dem Gericht oder der unabhängigen Stelle erst erlaubt, eine effektive Kontrolle auszuüben.

[39] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 112.
[40] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 112.
[41] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 118.

Insbesondere bedarf es der vollständigen Information seitens der antragstellenden Behörde über den zu beurteilenden Sachstand.[42]

Entsprechende Regelungen finden sich im HVSG bislang nicht, insbesondere wird auch § 9 Abs. 3 G10 durch § 9 Abs. 2 S. 2 HVSG nicht in Bezug genommen.

(II)§ 9 Abs. 3 HVSG: Datenverwendung

Entgegen seines Wortlauts regelt § 9 Abs. 3 HVSG weniger die Verwendung der erhobenen Daten, als vielmehr die Voraussetzungen ihrer Übermittlung bzw. Weiter-Verwendung im Rahmen einer Zweckänderung.

In Hinblick auf die § 9 Abs. Nr. 1 u.3 HVSG bestehen dabei keine Bedenken.

§ 9 Abs. Nr. 2 HVSG ist jedoch verfassungswidrig und dies gleich in doppelter Hinsicht:

Zum einen kommt nach der Rechtsprechung des Bundesverfassungsgerichts eine Übermittlung von Daten, die aus besonders eingriffsintensiven Überwachungsmaßnahmen herrühren, in Bezug auf die Verhinderung von Straftaten nur dann in Betracht, wenn sich aus ihnen zumindest ein *konkreter Ermittlungsansatz* für die Aufdeckung entsprechender Straftaten ergibt. Soweit ein Gesetz jedoch eine Übermittlung allgemein „zur Verhütung" von Straftaten erlaubt, fehle es an jeder eingrenzenden Konkretisierung des Übermittlungsanlasses und Informationen könnten, auch wenn sie aus eingriffsintensiven Maßnahmen stammen, schon mit Blick auf einen nur potentiellen Informationsgehalt als Spurenansatz übermittelt werden. Diese Eingrenzung gilt dabei unabhängig von der Schwere der in Bezug genommenen Straftaten.[43]

Indem § 9 Abs. Nr. 2 HVSG eine Verwendung der erhobenen Daten allgemein zur Verhinderung und Verhütung von Straftaten im Sinne von § 100b Abs. 2 StPO zulässt, verstößt er gegen diese Voraussetzungen.

Aber auch der von § 9 Abs. Nr. 2 HVSG in Bezug genommene Straftatenkatalog des § 100b Abs. 2 StPO dürfte als einschränkendes Merkmal der Übermittlungsvoraussetzungen nicht ausreichen. So hat das Bundesverfassungsgericht als Übermittlungsvoraussetzung nicht ausreichen lassen, dass die in Bezug genommenen Straftaten im Höchstmaß mit mindestens

[42] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 118.
[43] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 313.

fünf Jahren Freiheitsstrafe bedroht sind, da insoweit auch Delikte eingeschlossen seien, die nur zur mittleren Kriminalität zu rechnen sind.[44]

Der von § 9 Abs. Nr. 2 HVSG in Bezug genommene § 100b Abs. 2 StPO bezeichnet die dort genannten Straftaten zwar seinem Wortlaut nach als „besonders schwer". Dies ändert jedoch nichts daran, dass zahlreiche der dort genannten Straftatbestände nach der Wertung des StGB noch nicht einmal als Verbrechen gem. § 12 Abs. 1 StGB zu qualifizieren sind, da sie lediglich eine Mindeststrafe von sechs Monaten aufweisen. Auch folgt der Strafrahmen der von § 100b Abs. 2 StPO in Bezug genommenen Delikte oftmals erst aus ihrer gewerbs- oder bandenmäßigen Begehung. Auch in diesen Fällen ist aber nicht ersichtlich, inwieweit etwa Diebstahl, Hehlerei oder die Verleitung zur missbräuchlichen Asylantragstellung eine den Schutzgütern des § 7 Satz 1 HVSG vergleichbares Gewicht erlangen sollten. Inwieweit hieraus auch eine (partielle) Verfassungswidrigkeit des § 100b StPO folgt, kann vorliegend dahinstehen.

(III) § 9 Abs. 4 HVSG: Eigensicherung

§ 9 Abs. 4 HVSG sieht in Anlehnung an Art. 13 Abs. 5 GG eine Anordnung der Maßnahmen nicht durch den Richter, sondern durch „die Behördenleitung oder ihre Vertretung" für den Fall vor, dass „der Einsatz technischer Mittel nach den §§ 7 und 8 ausschließlich dem Schutz der für den Verfassungsschutz bei einem Einsatz in Wohnungen tätigen Personen" dient. Die Entwurfsbegründung verweist diesbezüglich auf „abgeschwächte Voraussetzungen, da diese Personen selbst von den Vorgängen in der Wohnung Kenntnis erlangen".[45]

Eine Parallelregelung für den verdeckten Zugriff auf informationstechnische Systeme gem. § 8 HVSG erscheint jedoch verfassungsrechtlich nicht angebracht. Zum einen ist schon nicht absehbar, wie eine Eigensicherung mittels eines solchen Zugriffs aussehen sollte. Zum anderen ist die für die Regelung des Art. 13 Abs. 5 GG maßgebliche Abschwächung des Schutzinteresses nicht gegeben, da eine vergleichbare Kenntnisnahme des Computersystems durch für den Verfassungsschutz tätige Personen nicht vorliegt. Soweit 9 Abs. 4 HVSG sich auf den verdeckten Zugriff auf informationstechnische Systeme gem. § 8 HVSG bezieht, ist er demnach selbst nach dem Begründungsansatz des Gesetzentwurfs verfassungswidrig.

---

[44] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 316. Dabei ging es zwar nicht um die „Verhütung", sondern um die „Verfolgung" von Straftaten. In der Sache ändert dies aber nichts.
[45] Drucks. 19/5412, S. 37.

3. § 11 HVSG: Besondere Auskunftsersuchen

§ 11 HVSG regelt die sogenannten besonderen Auskunftsersuchen grundsätzlich in enger Anlehnung an § 4a VerfSchG HE 1990 sowie §§ 8a ff. BVerfSchG.

Ohne dass dies in der Entwurfsbegründung ausreichend kenntlich gemacht würde, enthält § 11 Abs. 2 Nr. 1 HVSG allerdings eine erhebliche Ausweitung der Befugnis des Landesamts, verpflichtende Auskunftsersuchen an private Infrastrukturdienstleister zu richten. Während sich die Auskunftsverpflichtung bislang ausschließlich auf Luftfahrtunternehmen sowie die Betreiber von Computerreservierungssystemen und Globalen Distributionssystemen erstreckte, wird diese nunmehr auf sämtliche „Verkehrsunternehmen" ausgeweitet.

Probleme dürften hier zunächst hinsichtlich der Bestimmtheit entstehen, da unklar ist, wie weit der Begriff des „Verkehrsunternehmens" reicht. Dies gilt etwa in Hinblick auf Car-Sharing-Angebote oder Vermittlungen von Mitfahrgelegenheiten.

Vor allem findet aber auch qualitativ eine erhebliche Ausweitung der mit der Befugnis verbundenen Eingriffsintensität statt. Bislang war mit dem Luftverkehr ausschließlich ein Verkehrsmittel erfasst, das nur einen sehr geringen Teil der individuellen Mobilität abdeckt und noch dazu Einsatz vor allem bei Auslandsreisen findet. Durch die Erweiterung ermächtigt die Befugnis aber nunmehr zu einer nahezu lückenlosen Kontrolle des individuellen Bewegungsverhaltens, sofern dies über Verkehrsdienstleister und nicht lediglich zu Fuß oder unter Nutzung eines eigenen Fahrzeugs stattfindet.

Dessen sollte sich der Gesetzgeber jedenfalls bewusst sein, wenn er eine entsprechende Änderung beschließt.

4. § 12 HVSG: Ton- und Bildaufzeichnungen außerhalb der Schutzbereiche der Art. 10 und 13 des Grundgesetzes

§ 12 HVSG erlaubt dem Landesamt bereits dann das nicht öffentlich gesprochene Wort außerhalb des Schutzbereichs der Art. 10 und 13 GG mit oder ohne Inanspruchnahme technischer Mittel mitzuhören, abzuhören oder aufzuzeichnen, wenn dies im Einzelfall zur Erfüllung seiner Aufgaben nach § 2 Abs. 1 und 2 erforderlich ist. Dies gilt entsprechend für einen verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen.

Die Regelung verstößt insoweit gegen die Vorgaben des Bundesverfassungsgerichts, als sie keine Vorkehrungen zum Kernbereichsschutz enthält. Die insoweit entsprechende Vorschrift des § 20g BKAG hatte das Bundesverfassungsgericht zwar nicht unmittelbar den besonders

eingriffsintensiven Überwachungsmaßnahmen zugerechnet. Wohl ermögliche die Regelung aber Überwachungsmaßnahmen, die typischerweise tief in die Privatsphäre eindringen könnten. Auch außerhalb von Wohnungen könnten „mit einiger Wahrscheinlichkeit höchstvertrauliche Situationen erfasst werden [...], die dem Kernbereich privater Lebensgestaltung zuzurechnen sind." Die Vorschrift weise demnach insoweit eine Kernbereichsnähe auf, die eine ausdrückliche gesetzliche Regelung zum Schutz des Kernbereichs privater Lebensgestaltung erforderlich mache. Der Gesetzgeber habe hierzu in normenklarer Weise Schutzvorschriften sowohl auf der Ebene der Datenerhebung als auch auf der Ebene der Datenauswertung und Datenverwertung vorzusehen.[46]

Da es vorliegend an einer entsprechenden Regelung fehlt, ist § 12 HVSG insoweit verfassungswidrig. Für Abhilfe könnte hier entweder eine auf § 12 HVSG zugeschnittene Regelung sorgen. Alternativ ließe sich auch an eine Regelung denken, die – vergleichbar § 10 NDS VerfSchG – allgemein und für alle im Gesetz vorgesehenen Maßnahmen den Schutz des Kernbereichs regelt.

5. § 13 u. § 14 HVSG: Verdeckte Mitarbeiterinnen und Verdeckte Mitarbeiter; Vertrauensleute

a) Überblick

Der Einsatz verdeckter Mitarbeiterinnen und Mitarbeiter, noch mehr aber der Einsatz von Vertrauensleuten gehören zu den Bereichen, die rechtlich wie faktisch für einige der größten Probleme und Skandale im Bereich des Nachrichtendienstwesens verantwortlich gewesen sind. Insofern sollte es eigentlich eine rechtstaatliche Selbstverständlichkeit darstellen, dass in dem Fall, dass ein Gesetz ihren Einsatz überhaupt für zulässig erachtet, eine möglichst detaillierte Regelung der entsprechenden Befugnisnormen erfolgt.[47] Umso erstaunlicher ist es, dass in der Praxis die zuständigen Gesetzgeber erst seit einigen Jahren überhaupt dazu übergegangen sind, entsprechende Regelungen eines Einsatzes vorzunehmen. Von einer Erprobung oder Bewährung dieser Vorschriften kann deshalb momentan auch noch keine Rede sein.

Insofern ist es besonders bedauerlich, dass sich der vorliegende Entwurf für den Bereich verdeckter Mitarbeiterinnen und Mitarbeiter und Vertrauensleute ganz weitgehend damit

[46] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn 176.
[47] Das BVerfG fordert im Sicherheitsrecht grundsätzlich einen besonders hohen Grad der Bestimmtheit der Regelungen, da dort anders als im Übrigen Verwaltungsrecht unbestimmte Rechtsbegriffe „nur sehr eingeschränkt im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle konkretisiert werden können". BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 94; dazu Rusteberg, KritV 2017, S. 24 (33).

begnügt, die Regelungen des Bundesverfassungsschutzgesetzes zu übernehmen. Denn damit werden zugleich die erheblichen Defizite übernommen, die diese Regelungen momentan aufweisen. Noch bedenklicher ist, wenn die Änderungen, *die* vorgenommen wurden, im Wesentlichen in einer weiteren Ausweitung der Befugnisse bestehen.

b) Einsatzvoraussetzungen

(I) Einsatz gegen nicht gewaltorientierte Bestrebungen

Das Bundesverfassungsschutzgesetz beschränkt den Einsatz verdeckter Mitarbeiterinnen und Mitarbeiter sowie von Vertrauensleuten gem. § 9a Abs. 1 S. 2 BVerfSchG grundsätzlich auf Bestrebungen von erheblicher Bedeutung, die insbesondere gegeben sein sollen, wenn diese darauf gerichtet sind, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten.

§ 13 HVSG verzichtet hingegen darauf, eine entsprechende Einschränkung vorzunehmen. Der Entwurf begründet diesen Verzicht damit, dass die bundesrechtliche Begrenzung im Rahmen der „arbeitsteiligen Zusammenarbeit der Verfassungsschutzbehörden von Bund und Ländern [...] zwangsläufig einen erweiterten Beobachtungsauftrag aufseiten der Landesverfassungsschutzbehörden zur Folge [habe], der auch nicht gewaltorientierte Bestrebungen einbezieht."[48]

Diese Begründung überrascht insofern, als Verhältnismäßigkeitsgesichtspunkte vollkommen außer Betracht bleiben. Sie behandelt den Einsatz von verdeckten Mitarbeiterinnen und Mitarbeitern bzw. von Vertrauensleuten quasi als Selbstverständlichkeit, obwohl es sich um einen schwerwiegenden und damit besonders begründungsbedürftigen Grundrechtseingriff handelt. Ein einfacher Schluss von der Aufgabe auf die Befugnis ist hier – wie stets im Öffentlichen Recht – jedoch ausgeschlossen.

Dementsprechend hatte der Bundesgesetzgeber einen Einsatz von verdeckten Mitarbeiterinnen und Mitarbeitern bzw. von Vertrauensleuten gegen nicht gewaltorientierte Bestrebungen gerade auch deshalb abgelehnt, weil er ihn als nicht angemessen ansah.[49]

(II) Ausschlussgründe für den Einsatz bestimmter Personen

Der Einsatz von Vertrauensleuten stand nicht zuletzt deswegen immer wieder in der Kritik, weil hierzu auch erheblich vorbestrafte Personen angeworben wurden oder bereits für die Nachrichtendienste tätige Vertrauensleute erhebliche Straftaten begingen. Insofern ist eine

[48] Drucks. 19/5412, S. 40.
[49] Entwurf eines Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes, BT Drucks. 18/4654, S. 26.

gesetzliche Beschränkung derjenigen Personen, die überhaupt für einen Einsatz als V-Person in Betracht kommen, grundsätzlich ein Schritt in die richtige Richtung.

Dieser Schritt ist allerdings ein kleiner. Denn die Vorgaben des § 14 Abs. 2 HVSG sind zunächst recht unbestimmt, insoweit Satz 2 fordert, dass Vertrauensleute „nach ihren persönlichen und charakterlichen Voraussetzungen für die Zusammenarbeit mit dem Verfassungsschutz geeignet sein" müssen. Soweit in Satz 4 dann einzelne Ausschlussgründe normiert sind, dürften diese in ihrer praktischen Reichweite recht beschränkt bleiben. Vor allem wird die wohl wichtigste Vorgabe des Satz 4 Nr. 5, wonach Personen, die wegen eines Verbrechens verurteilt worden sind oder zu einer Freiheitsstrafe, deren Vollstreckung nicht zur Bewährung ausgesetzt worden ist, nicht als Vertrauensleute angeworben werden dürfen, umgehend durch die Ausnahmebestimmung des § 14 Abs. 2 S. 5 HVSG konterkariert.

Entsprechendes gilt für § 13 Abs. 2 S. 4 u. 5 HVSG, wonach der Einsatz einer Verdeckten Mitarbeiterin oder eines Verdeckten Mitarbeiters unverzüglich beendet und die Strafverfolgungsbehörde unterrichtet wird, sofern zureichende tatsächliche Anhaltspunkte dafür bestehen, dass rechtswidrig ein Straftatbestand von erheblicher Bedeutung verwirklicht wurde. Auch hier sieht Satz 5 mögliche Ausnahme von dieser Regel vor.

Rechtsklarheit und -sicherheit wird durch eine derartige Regelung nicht geschaffen. Erschwerend kommt hinzu, dass die Vorschrift keine korrespondierenden Protokollierungspflichten vorsieht, wie dies etwa bei anderen, besonders intensiven Eingriffsmaßnahmen der Fall ist.

c) Strafbewehrte Handlungen im Einsatz

(I) Überblick

Auch in Hinsicht auf die Ermöglichung strafbewehrter Handlungen für verdeckte Mitarbeiterinnen und Mitarbeiter sowie für Vertrauensleute orientiert sich der vorliegende Entwurf eng an der Regelung des Bundesverfassungsschutzgesetzes. Diesem liegt ein zweiteiliger Regelungsansatz zu Grunde:

Zunächst sieht § 9a Absatz 2 BVerfSchG eine Rechtfertigung von Handlungen vor, die (1.) nicht in Individualrechte eingreifen, die (2.) von den an den Bestrebungen Beteiligten derart erwartet werden, dass sie zur Gewinnung und Sicherung der Informationszugänge unumgänglich ist, und die (3.) nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts stehen.

In § 9a Absatz 3 BVerfSchG wird zudem zusätzlich die Möglichkeit geschaffen, dass die Staatsanwaltschaft von der Verfolgung bestimmter im Einsatz begangener Vergehen absehen oder eine bereits erhobene Klage in jeder Lage des Verfahrens zurücknehmen und das Verfahren einstellen kann. Voraussetzung ist hier, dass (1.) der Einsatz zur Aufklärung von Bestrebungen erfolgte, die auf die Begehung von in § 3 Absatz 1 des Artikel 10-Gesetzes bezeichneten Straftaten gerichtet sind, und (2.) die Tat von an den Bestrebungen Beteiligten derart erwartet wurde, dass sie zur Gewinnung und Sicherung der Informationszugänge unumgänglich war. Bei der Entscheidung soll das Verhältnis der Bedeutung der Aufklärung der Bestrebungen zur Schwere der begangenen Straftat und Schuld des Täters zu berücksichtigen sein. Ein Absehen von der Verfolgung ist hingegen ausgeschlossen, wenn eine höhere Strafe als ein Jahr Freiheitsstrafe zu erwarten ist oder zu erwarten ist, dass die Strafe nicht zur Bewährung ausgesetzt wird.

§ 13 Abs. 2 HVSG entspricht § 9a Abs. 2 BVerfSchG mit einem lediglich geringfügig anderen Wortlaut.

§ 13 Abs. 3 HVSG enthält hingegen lediglich einen Verweis auf § 9a Abs. 3 BVerfSchG, wonach dieser bei Einsätzen zur Erfüllung der Aufgabe nach § 2 Abs. 2 Nr. 5 HVSG – dieser bezieht sich auf die Sammlung von Information über die sogenannte Organisierte Kriminalität – entsprechende Geltung erhalten soll. Dies erklärt sich daraus, dass bereits nach § 9a Abs. 3 S. 5 BVerfSchG die Regelungen des Absatzes auch „in Fällen der Landesbehörden für Verfassungsschutz“ gelten sollen.

(II)Formelle Verfassungswidrigkeit des § 13 Abs. 3 HVSG

Die Regelung des § 13 Abs. 3 HVSG ist verfassungswidrig, da es dem Land Hessen insoweit an der notwendigen Gesetzgebungskompetenz mangelt. Zwar sieht § 74 Abs. 1 Nr. 1 GG eine konkurrierende Gesetzgebungskompetenz für das gerichtliche Verfahren vor, zu der auch die Regelung des Strafprozesses zählt.[50] Nach den §§ 3; 6 EG StPO ist jedoch davon auszugehen, dass der Bund von dieser Gesetzgebungskompetenz abschließend Gebrauch gemacht hat.

Anders als von der Entwurfsbegründung angenommen,[51] kommt es somit auch nicht darauf an, ob der Bundesgesetzgeber mit dem Erlass der §§ 9a, 9b BVerfSchG eine abschließende Regelung hinsichtlich des Einsatzes von verdeckten Mitarbeiterinnen und Mitarbeitern sowie Vertrauensleuten beabsichtigte – insoweit dürfte dem Bund auch seinerseits die Gesetzgebungskompetenz fehlen. Entscheidend ist vielmehr, dass er den Ländern auch

[50] Seiler, in: Epping/Hillgruber (Hrsg.), BeckOK Grundgesetz, 35. Edition, Art. 74 Rn. 11.
[51] Drucks. 19/5412, S. 42

insoweit keine zusätzliche Kompetenz zur Regelung des Strafverfahrens einräumen wollte. Den Ländern verbleibt insoweit kein eigenständiger Regelungsspielraum hinsichtlich der Möglichkeit zur Einstellung eines Strafverfahrens.

Für Einsätze im Bereich des § 2 Abs. 2 Nr. 5 HVSG kommt eine Anwendung des § 9a Abs. 3 BVerfSchG also nur in Betracht, soweit diese Einsätze zugleich gem. § 9a Abs. 3 S. 1 Nr. 1 BVerfSchG zur Aufklärung von Bestrebungen erfolgen, die auf die Begehung von in § 3 Absatz 1 G10 bezeichneten Straftaten gerichtet sind.

Entsprechendes gilt für § 13 Abs. 4 HVSG, wobei hier schon zweifelhaft ist, inwieweit Mitarbeiterinnen und Mitarbeiter, die verdeckt Informationen in sozialen Netzwerken und sonstigen Kommunikationsplattformen im Internet erheben, überhaupt durch die Regelung des § 9a Abs. 3 BVerfSchG erfasst werden. Jedenfalls kann auch hier der Hessische Landesgesetzgeber keine Erweiterung der bundesgesetzlich geregelten Einstellungsmöglichkeiten vorsehen.

(III) Materiell: Verfehlter Regelungsansatz

Materiell können weder § 9a Abs. 2 BVerfSchG bzw. § 13 Abs. 2 HVSG noch § 9a Abs. 3 BVerfSchG überzeugen. Der von ihnen jeweils gewählte Regelungsansatz ist zu unbestimmt und von Wertungswidersprüchen durchzogen.

§ 9a Abs. 2 BVerfSchG bzw. § 13 Abs. 2 HVSG setzen für eine Rechtfertigung der begangenen Handlung jeweils voraus, dass diese (1.) nicht in Individualrechte eingreift, (2.) von den an den Bestrebungen Beteiligten derart erwartet wird, dass sie zur Gewinnung und Sicherung der Informationszugänge unumgänglich ist, und (3.) nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts steht. Die Begründung des Gesetzesentwurfs, mit dem § 9a in das Bundesverfassungsgesetz eingeführt wurde, sowie der vorliegende Gesetzesentwurf nennen als entsprechende Beispiele etwa das Verwenden von Kennzeichen verfassungswidriger Organisationen oder den Verstoß gegen das versammlungsrechtliche Vermummungsverbot.[52]

Der Anwendungsbereich der Regelung geht nach ihrem Wortlaut aber weit über die genannten Beispiele hinaus. Denn hiernach erlaubt § 9a Abs. 2 BVerfSchG bei entsprechender Bedeutung des aufzuklärenden Sachverhalts selbst schwerste Straftaten, solange sie „von den an den Bestrebungen Beteiligten derart erwartet [werden], dass sie zur Gewinnung und Sicherung der Informationszugänge unumgänglich“ sind und nicht zugleich

[52] Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes, BT-Drucks. 18/4654, S. 26; Drucks. 19/5412, S. 40.

in Individualgüter eingreifen. Die Regelung stellt sich somit als eine Art Blankobefugnis für die Begehung jeglicher Straftat dar, die sich nicht unmittelbar gegen Leib und Leben, Freiheit oder Eigentum des Einzelnen richtet. Davon erfasst wären etwa Falschaussage, Meineid und Beweisunterdrückung, alle Arten des Waffen- und Drogenhandels bis hin zur Weitergabe von Massenvernichtungswaffen.[53]

Zu diesem Befund tritt noch hinzu, dass diese Rechtfertigungsgründe ja keineswegs nur für die verdeckten Mitarbeiterinnen und Mitarbeiter des Verfassungsschutzes gelten, sondern auch für die sogenannten Vertrauensleute. Diese können ihre zuvor rechtswidrig ausgeübten Taten der schweren und schwersten Kriminalität nunmehr unter dem Deckmantel des Hessischen Verfassungsschutzes gerechtfertigt weiterführen.

Auf der anderen Seite erscheint es wenig überzeugend, wenn zugleich selbst die Beschädigung geringwertiger Sachen aus dem Bereich der zu rechtfertigenden Delikte herausgenommen und dem Ermessen der Staatsanwaltschaft überstellt wird. In dieser Hinsicht stellt die Regelung des § 9a Abs. 3 BVerfSchG auch für die Mitarbeiterinnen und Mitarbeiter des Verfassungsschutzes eine erhebliche Belastung dar, als vorab eben nicht abgesehen werden kann, inwiefern eine entsprechende Straftat tatsächlich verfolgt werden wird.

Zugleich sind aber auch die Regelungen des § 9a Abs. 3 BVerfSchG so offen formuliert, dass bei den Delikten, die sich gegen individuelle Rechtsgüter richten, selbst Verbrechen – gem. § 12 Abs. 1 StGB Delikte, die mit einer Mindeststrafe von einem Jahr oder darüber bedroht sind – nach dieser Regelung unverfolgt bleiben können, wenn die Straferwartungen entsprechend angepasst werden.

§ 9a Abs. 3 BVerfSchG entfaltet nach Satz 5 seine Wirkung für das Hessische Landesamt zwar auch ohne weiteres Zutun des Hessischen Gesetzgebers. Die Wertungswidersprüche zu § 13 Abs. 2 HVSG bleiben aber insofern bestehen und in das HVSG übernommen.

d) Fehlender Kernbereichsschutz

Die Regelungen der §§ 13, 14 HVSG sind auch insofern verfassungswidrig, als es ihnen an Regelungen zum Schutz des durch die Menschenwürde geschützten Kernbereichs der privaten Lebensgestaltung mangelt. Bei den in der Öffentlichkeit bekanntgewordenen Fällen, in denen verdeckte Ermittler eingesetzt wurden, ist es regelmäßig dazu gekommen, dass diese sexuelle oder sogar partnerschaftliche Beziehungen zu den von ihnen beobachteten Personen eingegangen sind.

[53] Dass dies keineswegs rein hypothetisch bleiben muss, verdeutlicht etwa die sogenannte Plutonium-Affäre des BND, https://de.wikipedia.org/wiki/Plutonium-Aff%C3%A4re.

Einsätze, bei denen unter Legende derartig intime Beziehungen mit den zu beobachtenden Personen eingegangen werden, zeigen sich im Hinblick auf den durch die Menschenwürde geschützten Kernbereich privater Lebensgestaltung als besonders problematisch, da Überwachungsmaßnahmen grundsätzlich so auszugestalten sind, dass sie die Erhebung von Kernbereichsdaten vermeiden müssen,[54] der Aufbau intimer oder gar partnerschaftlicher Beziehung jedoch gerade auf das Eindringen in den Kernbereich zielt.[55] Jedenfalls ohne rechtliche Vorkehrungen zu seinem Schutz sind sie mit dem Grundgesetz nicht vereinbar.

Abhilfe könnte hier entweder eine gesondert auf die Situation der §§ 13; 14 HVSG zugeschnittene Regelung zum Kernbereichsschutz schaffen. Alternativ ließe sich auch an eine Regelung denken, die – vergleichbar § 10 NDS VerfSchG – allgemein und für alle im Gesetz vorgesehenen Maßnahmen den Schutz des Kernbereichs regelt.

III. § 16 ff. HVSG: Informationsübermittlung:

Die Informationsübermittlung an und durch das Landesamt ist nun in den §§ 16 ff. geregelt. Zahlreiche Regelungen waren an die zwischenzeitlich ergangene Rechtsprechung des Bundesverfassungsgerichts, insbesondere zur Antiterrordatei und zum BKA-Gesetz anzupassen.[56] Zudem hat der Entwurf die Gelegenheit genutzt, einige Regelungen neu zu strukturieren, zusammenzufassen und zu vereinheitlichen.

1. § 19 HVSG: Informationsübermittlung durch öffentliche Stellen an das Landesamt

§ 19 HVSG entspricht in seinem Gehalt grundsätzlich § 8 VerfSchG HE 1990. Die wesentliche Änderung besteht darin, dass den dort genannten Behörden und sonstigen öffentlichen Stellen des Landes bei der Frage, ob sie Informationen an das Landesamt übermitteln, kein Ermessen mehr zusteht, sondern sie nunmehr zur Informations- und Datenübermittlung verpflichtet sind, wenn tatsächliche Anhaltpunkte dafür bestehen, dass die Übermittlung für die Erfüllung der Aufgaben der Verfassungsschutzbehörde erforderlich ist.[57]

Rein rechtlich gesehen dürfte hierin zwar tatsächlich eine eher geringfügige Änderung zu sehen sein, da auch bislang nur wenige Gründe existiert haben dürften, die es der jeweiligen Behörde erlaubt hätten, eine Übermittlung zu unterlassen, obwohl entsprechende Anhaltspunkte vorlagen. Praktisch dürfte die Neuregelung aber zu einer nicht unerheblichen Zunahme an Übermittlungen führen, da die Behördenmitarbeiterinnen und -mitarbeiter

---

[54] BVerfGE 120, 274 (337).
[55] Vgl. Hohnerlein, NVwZ 2016, S. 511 (514), auch zu entsprechenden Beispielen.
[56] BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/07 sowie BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09.
[57] Drucks. 19/5412, S. 46.

nunmehr befürchten müssen einen Rechtsbruch zu begehen, wenn sie auf die Vornahme von Übermittlungen verzichteten. Dieser Effekt dürfte dadurch verstärkt werden, dass es im Gesetz an jeglicher Konkretisierung mangelt, welche Informationen für die Erfüllung der Aufgaben der Verfassungsschutzbehörde erforderlich sein könnten.

Nicht zuletzt wegen dieser mangelnden Bestimmtheit ergeben sich auch für die betroffenen Bürgerinnen und Bürger erhebliche Abschreckungs- und Einschüchterungseffekte, wenn sie künftig davon ausgehen müssen, dass praktische jeder Behördengang an das Landesamt gemeldet werden wird. Spätestens wenn dadurch besonders grundrechtssensible Bereiche betroffen werden – wie etwa beim Anmelden einer Versammlung –, ist die Verhältnismäßigkeit einer solchen Regelung in Frage gestellt.

2. § 21 HVSG: Informationsübermittlung durch das Landesamt innerhalb des öffentlichen Bereichs

Wie oben bereits ausgeführt, ist es grundsätzlich zu begrüßen, dass § 21 Abs. 1 HVSG es nunmehr unternimmt, die Voraussetzungen, unter denen das Landesamt Informationen innerhalb des öffentlichen Bereichs übermitteln kann, einzeln aufzulisten. Es bedarf jedoch einiger Anmerkungen, was die Reichweite und Konsequenzen dieser Tatbestände betrifft.

Überschaubar wären diese lediglich dann, wenn § 21 HVSG als bloße Übermittlungsvorschrift bewertet wird, die es dem Landesamt zwar grundsätzlich ermöglicht, im Rahmen seiner Aufgabenerfüllung nach § 2 Abs. 3 HVSG Informationen an die zuständigen Behörden zu übermitteln, umgekehrt aber keine Ermächtigung für die jeweiligen Behörden beinhaltet, die entsprechenden Informationen beim Landesamt nachzufragen. Nach dem sogenannten Doppeltürprinzip bedürfte es dann weiterer gesetzgeberischer Konkretisierungen, die die Voraussetzungen einer solchen Abfrage regeln.

Wird § 21 HVSG hingegen zugleich als Ermächtigung gedeutet, in den genannten Fällen Informationen beim Landesamt abzufragen, wird das Instrument der Regelanfrage beim Landesamt für Verfassungsschutz in einem lange Zeit nicht vorstellbaren Maße ausgeweitet bzw. perpetuiert. Warum demgegenüber gem. § 21 Abs. 2 HVSG ausgerechnet Übermittlungen an Staatsanwaltschaft, Polizeien etc. nur eingeschränkt möglich sein sollen, lässt sich dann auch mit dem Hinweis auf das Trennungsgebot nicht mehr sinnvoll erklären, bietet doch gerade das Strafverfahren sehr viel bessere verfassungsrechtliche Sicherungen als die von § 21 Abs. 1 HVSG in Bezug genommenen Verwaltungsverfahren.

Mit einer entsprechenden Ausweitung der Regelanfrage wären zudem zahlreiche Folgefragen verbunden, die in dem vorliegenden Entwurf bislang nicht berücksichtigt werden. So weist die Entwurfsbegründung explizit darauf hin, dass die Aufgabe des Landesamts in der nachrichtendienstlichen Sammlung und Auswertung von Informationen bestehe, weshalb im Rahmen der Informationsübermittlung keine Rohdaten, sondern Erkenntnisse der Auswertungen weitergegeben würden.[58] Hieraus ergibt sich aber etwa die Frage, inwieweit die Behörde, an die eine Übermittlung erfolgt, in Fällen, in denen sie eine Ermessensentscheidung zu tätigen hat, dieses ordnungsgemäß ausüben kann, ohne dass sie selbst in der Lage wären, eine Beurteilung der erhaltenen Informationen vorzunehmen, etwa hinsichtlich ihrer Stichhaltigkeit, Verlässlichkeit oder Vollständigkeit.

Darüber hinaus stellt sich auch die Frage, inwieweit die jeweiligen Informationen ggf. in einem anschließenden Verfahren vor den Verwaltungsgerichten Verwendung finden können, wenn nicht zugleich die jeweiligen Quellen, aus denen die Informationen stammen, vollständig offen gelegt werden. Selbst im Falle der erfolgreichen Durchführung des sogenannten in-camera-Verfahrens nach § 99 VwGO dürfen die zu Recht nicht vorgelegten Vorgänge „nur unter strengen Voraussetzungen zu Lasten eines Rechtsschutzsuchenden bei der Sachentscheidung berücksichtigt werden. Nicht gerichtsverwertbare Tatsachen müssen als solche unberücksichtigt bleiben."[59] Welches Gewicht den Angaben des Landesamts dann zukommen kann, obwohl diese nicht entsprechend durch Beweismittel belegt werden können, wäre dann jeweils im Einzelfall ggf. unter Berücksichtigung von Beweislastregeln zu beurteilen.

IV. § 27 HVSG: Auskunft

Nach der Rechtsprechung des Bundesverfassungsgerichts hat der Gesetzgeber zur Flankierung informationsbezogener Eingriffe Auskunftsrechte vorzusehen. Denn Vornahme und Umfang derartiger Eingriffe seien für die Betroffenen nicht sicher abzuschätzen. Einschränkungen seien nur zulässig, „wenn sie gegenläufigen Interessen von größerem Gewicht dienen." Gesetzliche Ausschlusstatbestände müssen deshalb sicherstellen, „dass die betroffenen Interessen einander umfassend und auch mit Blick auf den Einzelfall zugeordnet werden." Dies ändert sich auch nicht dadurch, dass das Gericht es im Ergebnis als verfassungsrechtlich hinnehmbar erachtet, wenn im Ergebnis „die praktische Wirksamkeit solcher Auskunftsrechte angesichts der Art der Aufgabenwahrnehmung – wie bei der

[58] Drucks. 19/5412, S. 48.
[59] Schoch/Schneider/Bier/Rudisile, VwGO, 33. EL Juni 2017, § 99 Rn. 49.

heimlichen Datenverarbeitung zur Abwehr von Gefahren durch den internationalen Terrorismus – sehr begrenzt bleibt".[60]

§ 27 Abs. 2 HVSG enthält in seinen Nummern 1 bis 4 weitreichende Gründe, aus denen eine Auskunft abzulehnen ist. Die Auskunft erstreckt sich nach § 27 Abs. 1 S. 3 HVSG zudem von vorneherein nicht auf (1.) die Herkunft der Daten und die Empfänger von Übermittlungen und (2.) Daten, die nicht strukturiert in automatisierten Dateien gespeichert sind.

Insofern ist es nicht nachvollziehbar, wenn der vorliegende Gesetzentwurf die Geltendmachung eines Auskunftsbegehrens zusätzlich dadurch erschwert, dass gem. § 27 Abs. 1 S. 1 HS. 2 HVSG „die betroffene Person hierzu auf einen konkreten Sachverhalt hinweist und ein besonderes Interesse an einer Auskunft" darlegen muss. Daran ändert auch der Umstand nichts, dass § 15 Abs. 1 BVerfSchG eine entsprechende Regelung vorsieht.

Zum einen ist bereits nicht erkennbar, welche nicht selbst inkriminierenden Angaben eine Person machen könnte, die auf diese Art um Auskunft hinsichtlich der über sie gespeicherten Daten ersucht. Zum anderen ist auch nicht erkennbar, wie ansonsten „ein unverhältnismäßigen Verwaltungsaufwand" entstehen könnte, wie ihn die Entwurfsbegründung befürchtet.[61] So sind nach Auskunft der Bundesregierung in dem Zeitraum von 2015 bis 2017 beim Bundesamt für Verfassungsschutz im Schnitt weniger als 300 Auskunftsersuchen pro Jahr eingegangen.[62] Beim hessischen Landesamt dürfte diese Zahl noch entsprechend geringer ausfallen. Soweit die Gesetzesbegründung einer „Ausforschungsgefahr" begegnen will,[63] kann dies im Einzelfall durch den Versagungsgrund des § 27 Abs. 2 Nr. 2 HVSG geschehen.

In Bezug auf den § 27 Abs. 2 Nr. 2 HVSG ebenfalls nicht nachvollziehbar ist, dass die Entwurfsbegründung von „einem Ausforschungsversuch oder einer rechtsmissbräuchlichen Ausübung des Auskunftsrechts" ausgeht, soweit „öffentlich zu einer ‚Auskunftskampagne' aufgerufen" werde.[64] Zum einen ist in der Ausschlussregelung des § 27 Abs. 2 HVSG die Variante einer „rechtsmissbräuchlichen Ausübung des Auskunftsrechts" überhaupt nicht enthalten. Zum anderen ist auch nicht ersichtlich, inwieweit es rechtsmissbräuchlich sein sollte, wenn etwa Bürgerrechtsorganisationen dazu aufrufen und es den Betroffenen ggf.

[60] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 137.
[61] Drucks. 19/5412, S. 52.
[62] BT-Drucks. 19/490, S. 2; insgesamt gab es in dem genannten Zeitraum 895 Auskunftsersuchen.
[63] Drucks. 19/5412, S. 53.
[64] Drucks. 19/5412, S. 53.

technisch erleichtern, von ihren verfassungsrechtlich verbürgten Rechten Gebrauch zu machen.

C. Verfassungsschutzkontrollgesetz

Das Bundesverfassungsgericht hat in seiner Rechtsprechung immer wieder betont, dass die Defizite die im Bereich der polizei- und nachrichtendienstlichen Informationsvorsorge hinsichtlich subjektiver Rechtsschutzmöglichkeiten bestehen, durch eine wirksame aufsichtliche Kontrolle und Transparenz des Behördenhandelns gegenüber der Öffentlichkeit kompensiert werden müssen.[65] Insofern ist das geäußerte Anliegen des Gesetzentwurfs, die parlamentarische Kontrolle zu stärken, vollumfänglich zu begrüßen. Dieses Ziel ist jedoch nur teilweise erreicht worden.

I. § 3 Abs. 2 Verfassungsschutzkontrollgesetz: Umfang der Unterrichtungspflicht

§ 3 Abs. 2 Verfassungsschutzkontrollgesetz sieht vor, dass „Zeit, Art und Umfang der Unterrichtung der Parlamentarischen Kontrollkommission [...] unter Beachtung des notwendigen Schutzes der Quellen durch die politische Verantwortung der Landesregierung bestimmt" werden. Die Regelung entspricht dabei wortgleich § 22 Abs. 2 VerfSchutzG HE 1990 und gibt der Landesregierung demnach einen weiten Spielraum über die Reichweite der Unterrichtung zu bestimmen, in den neben rechtlichen, auch politische Aspekte mit einbezogen werden können. Die in § 3 Abs. 1 Verfassungsschutzkontrollgesetz normierte Pflicht, die Parlamentarische Kontrollkommission umfassend zu unterrichten, wird damit empfindlich eingeschränkt.

Demgegenüber sieht § 6 Abs. 2 PKGrG, an das der Entwurf des Verfassungsschutzkontrollgesetz ansonsten weitgehend angelehnt ist, eine Einschränkung der Unterrichtungspflicht – soweit die jeweiligen Informationen und Gegenstände überhaupt der Verfügungsberechtigung der Nachrichtendienste unterliegen – nur insoweit vor, als „dies aus zwingenden Gründen des Nachrichtenzugangs oder aus Gründen des Schutzes von Persönlichkeitsrechten Dritter notwendig ist oder wenn der Kernbereich der exekutiven Eigenverantwortung betroffen ist". Macht die Bundesregierung von diesen Rechten Gebrauch, besteht zudem eine Begründungspflicht gegenüber dem Parlamentarischen Kontrollgremium.

Vorliegend ist nicht ersichtlich, warum das Land Hessen hinter diesem Kontrollniveau zurückstehen sollte.

---

[65] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 135.

II. §§ 5a; 5b und § 8 PKGrG: Ständiger Bevollmächtigter und Eingaben

Soweit es die Verfasser des Gesetzentwurfs mit ihrem Anliegen, die parlamentarische Kontrolle zu stärken, ernst meinen, ist zudem unverständlich, wieso die auf Bundesebene durch das Gesetz zur weiteren Fortentwicklung der parlamentarischen Kontrolle der Nachrichtendienste des Bundes[66] neu eingeführten bzw. noch einmal gestärkten Institute des Ständigen Bevollmächtigten (§§ 5a, 5b PKGrG) sowie der unmittelbaren Eingabe an das Parlamentarische Kontrollgremium durch die Angehörigen der Nachrichtendienste (§ 8 Abs. 1 PKGrG) nicht in den vorliegenden Entwurf übernommen wurden.

[66] BGBl. I 2016, 2746.

D. Zusammenfassung

1. Die Ziele, die sich der vorliegende Entwurf eines Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen gesetzt hat (S. 2 f.), kann er nur teilwiese erfüllen.

2. Zu begrüßen ist die verbesserte Systematik des HVSG, die zu einer verbesserten Übersicht und erleichterten Anwendbarkeit des Gesetzes beiträgt (S. 4 f.). Das großzügige Gebrauchmachen von Verweisungen im Regelungstext verursacht allerdings neue Unklarheiten (S. 6 ff.).

3. Die Anpassung der Regelungen zur Informationserhebung an die seit dem Erlass des VerSchG HE 1990 erfolgte Rechtsentwicklung, insbesondere an die Vorgaben, die das Bundesverfassungsgericht in seiner Entscheidung zum BKA-Gesetz für staatliche Überwachungsmaßnahmen gemacht hat, ist nur teilweise gelungen.

4. Die Regelungen zu den besonders intensiven Überwachungsmaßnahmen der Wohnraumüberwachung und des verdeckten Zugriffs auf informationstechnische Systeme in den §§ 7 ff. HVSG erfüllen sowohl in Hinblick auf die Eingriffsvoraussetzungen als auch auf die Regelung des Anwendungsverfahrens weitestgehend die verfassungsrechtlichen Anforderungen (S. 10 ff.). In Bezug auf die in Frage kommenden Schutzgüter (S. 11) und zulässigen Adressaten (S. 12) bedarf es jedoch teilweise einer verfassungskonformen Auslegung. Im Bereich des Anwendungsverfahrens sind die Regelungen zum Antrag auf Anordnung der Überwachung (S. 17), zur Datenverwendung (S. 18) und zur Eigensicherung (S. 19) zumindest in Teilen verfassungswidrig.

5. In Bezug auf die notwendige Eingriffsschwelle für den Einsatz der besonders intensiven Überwachungsmaßnahmen ist der Gesetzestext als solcher zwar verfassungskonform. Die Entwurfsbegründung geht jedoch hinsichtlich der hiernach möglichen Szenarien zum Einsatz dieser Maßnahmen von falschen Voraussetzungen aus. Wohnraumüberwachung und verdeckter Zugriff auf informationstechnische Systeme setzen für ihren Einsatz jeweils eine konkrete Gefahr voraus; ein Einsatz zur bloßen Informationsvorsorge scheidet hingegen nach der Rechtsprechung des Bundesverfassungsgerichts ausdrücklich aus. Die Sinnhaftigkeit, das Landesamt mit derartigen Befugnissen auszustatten, ist damit nachdrücklich in Frage gestellt (S. 14 ff.).

6. Bei den besonderen Auskunftsersuchen nach § 11 HVSG nimmt der Gesetzentwurf eine wesentliche Ausweitung der Befugnisse und der mit diesen verbundenen Eingriffsintensität vor. Während sich die Auskunftsverpflichtung bislang auf Luftfahrtunternehmen sowie die

Betreiber von Computerreservierungssystemen und Globalen Distributionssystemen beschränkte, wird diese nunmehr auf sämtliche „Verkehrsunternehmen“ erstreckt (S. 20).

7. Bei den Regelung zur Ton- und Bildaufzeichnung außerhalb der Schutzbereiche der Art. 10 u. 13 GG nach § 12 HVSG fehlt es an der notwendigen Regelung zum Schutz des Kernbereichs privater Lebensgestaltung (S. 20).

8. Bei der Regelung des Einsatzes von verdeckten Mitarbeiterinnen und Mitarbeitern sowie von Vertrauensleuten gem. § 13 u. § 14 HVSG übernimmt der Gesetzentwurf mit den bundesrechtlichen Regelungen zugleich die erheblichen Defizite, die diese in Hinblick auf die Eingriffsvoraussetzungen (S. 22) und die Regelung strafbewehrter Handlungen im Einsatz (S. 23) aufweisen. Zudem fehlt es an einer Regelung zum Kernbereichsschutz (S. 26).

9. Die Regelungen zur Informationsübermittlung in den §§ 16 ff. HVSG sind grundsätzlich verfassungskonform. Allerdings werfen die Regelung zur Informationsübermittlung durch öffentliche Stellen an das Landesamt gem. § 19 HVSG und zur Informationsübermittlung durch das Landesamt innerhalb des öffentlichen Bereichs gem. § 21 HVSG zahlreiche Folgefragen auf, die im Entwurf bislang nicht berücksichtigt werden (S. 27).

10. Die Anforderungen zur Auskunftserteilung nach § 27 HVSG sind unnötig restriktiv und insoweit verfassungswidrig (S. 29).

11. Die insbesondere mit dem Erlass eines eigenständigen Verfassungsschutzkontrollgesetzes verfolgte Absicht einer Stärkung der parlamentarischen Kontrolle des Landesamts ist ausdrücklich zu begrüßen. Mit diesem Ziel ist es allerdings nicht zu vereinbaren, dass der Umfang der Unterrichtungspflicht der Landesregierung gem. § 3 Abs. 2 Verfassungsschutzkontrollgesetz in nicht nachvollziehbarer Weise beschränkt wird. Ferner sollten die Regelungen zur Ernennung eines Ständigen Bevollmächtigen sowie zu Eingaben an das Kontrollgremium aus dem Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes entsprechend übernommen werden.

beratungsNetzwerk hessen
Gemeinsam für Demokratie und gegen Rechtsextremismus

Reiner Becker | Philipps-Universität – FB 21 - 35032 Marburg

An den
Hessischen Landtag
Herrn Horst Klee

65183 Wiesbaden

beratungsNetzwerk hessen
Gemeinsam für Demokratie und gegen Rechtsextremismus

Demokratiezentrum
Dr. phil. Reiner Becker
Tel.: 06421 / 28-24535
Fax: 06421 / 28-24577
E-Mail: reiner.becker@staff.uni-marburg.de
Anschrift: Philipps-Universität Marburg
Wilhelm-Röpke-Straße 6, Raum 00B02
D - 35032 Marburg
Web: www.beratungsnetzwerk-hessen.de
www.facebook.com/Beratungsnetzwerk

Marburg, 05.02.2018

Stellungnahme zur Öffentlichen Anhörung des Innenausschusses des Hessischen Landtages zum Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen – Drucks. 19/5412 – hierzu: Änderungsantrag der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN – Drucks. 19/5782

Sehr geehrter Herr Klee,

Das Beratungsnetzwerk Hessen – gemeinsam für Demokratie und gegen Rechtsextremismus bietet seit 2007 ein umfangreiches Angebot an, um demokratische Strukturen zu stärken, Rechtsextremismus vorzubeugen sowie Betroffenen Hilfe zu geben. Das Netzwerk berät hessenweit Schulen, Eltern und Familienangehörige, Kommunen, Vereine und weitere Hilfesuchende nach Vorfällen mit einem rechtsextremen, antisemitischen oder rassistischen Hintergrund. Das an der Philipps-Universität Marburg ansässige Demokratiezentrum Hessen fungiert als Fach- und Geschäftsstelle und arbeitet im Auftrag des Hessischen Kompetenzzentrums gegen Extremismus (HKE) im Hessischen Ministerium des Innern und für Sport. Das Demokratiezentrum vermittelt kompetente Ansprechpartner vor Ort, koordiniert die Beratung und Vernetzung und dokumentiert die Arbeit des Netzwerks. Seit 2015 ist das Demokratiezentrum auch zuständig für die Bündelung und Entwicklung von Angeboten zur Demokratieförderung und Prävention insbesondere von Rechtsextremismus und extremistischem Salafismus. Das Demokratiezentrum und das Beratungsnetzwerk werden finanziert durch das Bundesprogramm „Demokratie leben! Aktiv gegen Rechtsextremismus, Gewalt und Menschenfeindlichkeit“ sowie durch das Landesprogramm „Hessen – aktiv für Demokratie und gegen Rechtsextremismus“.

Die folgenden Ausführungen beziehen sich auf Artikel 1 des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen, §21, Abs.1, Nr. 2, Buchstabe i.

Das Demokratiezentrum begrüßt die Vereinbarungen, die im Rahmen eines Gespräches am 11.12.2017 zwischen dem Hessischen Ministerium des Innern und für Sport, dem Demokratiezentrum und den vom Landesprogramm geförderten Träger getroffen wurden, die vorsehen, dass grundsätzlich von dem Vorhaben zur Überprüfung der Zuverlässigkeit Abstand genommen wird, wie es im ersten Entwurf des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen in Artikel 1, §21, Abs.1, Nr. 2, Buchstabe i formuliert war. Diese Überprüfung sollte Bestandteil der Allgemeinen Nebenbestimmungen des Landesprogramms „Hessen – aktiv für Demokratie und gegen Extremismus" werden und die Zustimmung der Träger hierzu Voraussetzung für die Auszahlung von Fördermittel sein. In dem besagten Artikel war vorgesehen, die Zuverlässigkeit von Personen mit deren Einwilligung zu überprüfen

1. die in mit Landesmitteln geförderten Beratungsstellen zur Prävention und Intervention gegen verfassungsfeindliche Bestrebungen oder in mit Landesmitteln eingesetzten geförderten Projekten eingesetzt sind oder eingesetzt werden sollen,
2. die als Mitwirkende in beratenden Gremien zur Prävention und Intervention gegen verfassungsfeindliche Bestrebungen tätig sind oder tätig werden wollen.[1]

Die konkreten Anlässe und der einhergehende Druck auf die Verantwortungsträger, die zu diesem Gesetzesvorhaben führten, waren immer nachvollziehbar; erinnert sei an die Vorwürfe gegenüber dem Deutsch-Islamischen-Verband (DIV) im Sommer 2016, der eine Modellprojektförderung durch das Bundesprogramm „Demokratie leben!" erhalten hatte oder an die Vorwürfe gegenüber Mitarbeitern des Violence Prevention Networks (VPN) im Frühjahr 2017, die sich als unhaltbar erwiesen haben. In beiden Fällen bestand ein enormer öffentlicher Druck auf die Verantwortlichen in den Ministerien und im Falle von VPN auf den Träger und das gesamte Team, wie ich es in meiner langjährigen Tätigkeit noch nicht erlebt habe.

In der Perspektive einer sicherheitsbehördlichen Logik scheint die einfache Überprüfung zwar hilfreich für einen Umgang nach Anlässen zu sein, die von einem öffentlichen Druck begleitet sind. Die aus diesen Anlässen gezogenen Schlüsse, Zuverlässigkeitsüberprüfungen in geplanter Weise einzuführen, waren und sind jedoch aus verschiedenen prinzipiellen Gründen nicht nachvollziehbar:

1. Dem Demokratiezentrum und den geförderten Trägern wurde in den vergangenen Jahren über das Bundes- und Landesprogramm deutlich mehr Mittel für die politische Bildung, Prävention und für die unterschiedlichen Beratungsangebote zur Verfügung gestellt. Dank der guten Kooperation zwischen staatlichen und zivilgesellschaftlichen Trägern in Hessen seit 2007 ist es allen Beteiligten gemeinsam gelungen, die Angebote und Handlungsmöglichkeiten in einem kurzen Zeitraum quantitativ und qualitativ deutlich auszuweiten. Insbesondere in Hessen waren dabei seit 2007 der Netzwerkgedanke und die Partnerschaft zwischen Staat und Zivilgesellschaft im Vergleich zu vielen anderen Bundesländern sehr ausgeprägt. Dies war mithin ein wesentlicher Grund dafür, auch in sehr kurzer Zeit, viele neue Angebote zu schaffen. Durch die ursprüngliche Fassung des §21 drohte eine enorme Schieflage in diesem Verhältnis, denn fortan hätte der

[1] Vgl. Artikel 1, §21, Abs.1, Nr. 2, Buchstabe i im Gesetzesentwurf zur Neuausrichtung des Verfassungsschutzes in Hessen, Drucksache 19/5412

Verfassungsschutz als nachgeordnete Behörde des HMdIS quasi einen festen Platz in den Personalbüros der geförderten zivilgesellschaftlichen Träger gehabt, sei es bei der Auswahl von Personal, sei es bei der Überprüfung bereits beschäftigter Mitarbeiter und Mitarbeiterinnen. Obwohl die beteiligten Träger auch unter dem Gesichtspunkt der Zuverlässigkeit bei der Personalauswahl sich nach vorhandenen Standards zu richten haben, da sie etwa anerkannte Träger der Weiterbildung oder der Kinder- und Jugendhilfe sind, hätte eine solche Regelung zur Folge gehabt, dass ihnen die Verantwortung bei der Personalauswahl und gegenüber ihren Mitarbeiter_innen letztlich genommen worden wäre.

2. In der ersten Fassung des §21 des Verfassungsschutzgesetzes war vorgesehen, dass die Zuverlässigkeit von Mitwirkenden in beratenden Gremien zur Prävention und Intervention ebenfalls überprüft werden sollte. Dies hätte grundsätzlich die Teilnehmer_innen von unseren Vernetzungstreffen (im Schnitt 80 Personen), die der Lenkungsgruppe, die Mitglieder im Fachbeirat des Netzwerks gegen Salafismus ebenso betroffen, wie die Begleitausschüsse der 29 Partnerschaften für Demokratie in Hessen, die zum größten Teil eine Kofinanzierung des Landes erhalten. All dies sind Gremien, in denen keine sicherheitssensiblen Informationen weitergegeben werden, sondern es sind Gremien, die wesentlich zum Gelingen der verschiedenen Maßnahmen im Landes- und Bundesprogramm dank ihrer jeweiligen Expertise beitragen. Auch wenn es so nicht intendiert war und ist, so steht für die betroffenen Träger und auch für die betroffenen Kooperationspartner in den verschiedenen Gremien mit der Frage ihrer Zuverlässigkeit ein starkes Gefühl des Misstrauens im Raum.

3. Auch im Kontext des Landesprogramms „Hessen – aktiv für Demokratie und gegen Extremismus" und auch des Bundesprogramms „Demokratie leben" gibt es Arbeitsbereiche, in denen zivilgesellschaftliche Träger tätig sind, die sicherheitssensibel sind und die daher eine Überprüfung der entsprechenden Mitarbeiter und Mitarbeiterinnen notwendig machen (z.B. Projekte, die in Justizvollzugsanstalten tätig sind). Hier ist es aus fachlichen Gründen nachvollziehbar, dass eine Zuverlässigkeitsüberprüfung vorgenommen wird. Doch die große Mehrheit der geförderten Projekte in Hessen arbeiten nicht in solch sicherheitssensiblen Bereichen; sie führen vielmehr Bildungsprojekte an Schulen durch, beraten Kommunen bei der Integration von Flüchtlingen oder bieten Fortbildungsangebote für Mitarbeiterinnen und Mitarbeiter der kommunalen Jugendarbeit an, zeitlich befristet und in Teams. Jede Lehrerin, jeder Lehrer in Hessen, jede Jugendpflegerin, jeder Jugendpfleger oder jede Mitarbeiterin, jeder Mitarbeiter in der Erwachsenenbildung haben regelmäßigeren Kontakt zu den unterschiedlichen Zielgruppen – doch hier finden keine Überprüfungen der Zuverlässigkeit statt. Worin unterscheiden sich die Mitarbeiter_innen in den hier betroffenen Projekten von z.B. Pädagog_innen und Lehrer_innen in den Regelstrukturen? In dieser Perspektive verstößt aus unserer Sicht eine Überprüfung der Zuverlässigkeit gegen das Prinzip der Verhältnismäßigkeit.

4. Die Diskussion um die Einführung einer Zuverlässigkeitsüberprüfung in Hessen hat auch bundesweit für Aufmerksamkeit gesorgt. Das Demokratiezentrum hat von Februar bis November 2017 versucht, intern eine Klärung zwischen den hessischen Trägern und dem HMdIS zu suchen; erst nach Scheitern dieses internen Prozesses sind Träger in die Öffentlichkeit gegangen. Zahlreiche Stellungnahmen von Trägern und Verbänden aus dem gesamten Bundesgebiet wurden danach veröffentlicht, da die Befürchtung bestand, dass die „hessische Lösung" eine Blaupause für politische Verantwortungsträger in anderen Bundesländern sein könnte. Hier wurde die Erinnerung an die Auseinandersetzung zur so

genannten „Extremismusklausel" wach[2], die 2011 vom BMFSFJ und dem BMI für die damaligen Bundesprogramme eingeführt und 2014 von beiden Häusern nach juristischen Auseinandersetzungen in einer sehr abgeschwächten Form zur so genannten Demokratieerklärung umgewidmet wurde. Das BMFSFJ fügt seitdem seinen Zuwendungsbescheiden im Rahmen des Bundesprogramms „Demokratie leben!" ein ausführliches Begleitschreiben bei, in dem die Letztempfänger für die Fragen der Zuverlässigkeit und für die mögliche Zusammenarbeit mit Personen und Organisationen mit einem extremistischen Hintergrund sensibilisiert werden. Das BMFSFJ wirbt insbesondere für diese Fragen um die Kooperation und Zusammenarbeit zwischen Ministerium und Letztempfängern, „um gemeinsam dafür Sorge zu tragen, dass eine Unterstützung extremistischer Gruppen durch die Gewährleistung materieller Leistungen (hier: Mittel des Bundes) oder immaterieller Leistungen vermieden wird."[3] Es ist selbstverständlich auch im Interesse der Träger in Hessen, dass sie keine Mitarbeiter_innen beschäftigen oder mit Organisationen zusammenarbeiten, welche die Ziele des Grundgesetzes nicht teilen. Hierfür kommen die Standards dieser Träger zum Tragen, die sich aus den jeweiligen gesetzlichen Verpflichtungen im Rahmen ihrer Anerkennung ergeben, zum Beispiel in der Personalgewinnung und -führung. Der vorliegende Änderungsantrag zur Neuausrichtung des Verfassungsschutzes in Hessen berücksichtigt dies nun und sollte daher nun eine hinreichende Ausgangsbasis für die Kooperation zwischen Staat und Zivilgesellschaft zum Thema Zuverlässigkeit sein, wie sie auch im Bundesprogramm „Demokratie leben!" praktiziert wird.

5. Die Motivation zur Einführung von Zuverlässigkeitsüberprüfungen rühren vor allem aus Vorkommnissen bzw. Vorwürfen gegenüber Trägern und Mitarbeiter_innen, die im Themenfeld des militanten Islamismus bzw. Salafismus tätig sind und die, wie die o.g. Beispiele zeigen, eine sehr große Öffentlichkeit finden - woran könnte das liegen?

Die unterschiedlichen Aktivitäten zur politischen Bildung, Prävention und Beratung im Themenfeld Rechtsextremismus gehen auf ein z.T. langjähriges zivilgesellschaftliches Engagement der verschiedenen Initiativen und Träger zurück. Das Engagement im Themenfeld des militanten Islamismus/Salafismus kennt eine solche Tradition nicht, vielmehr waren es staatliche Akteure, die hier die Impulse setzten, das Geld in die Hand genommen haben und wegen einer erhöhten Sensibilität der Öffentlichkeit seit dem 11. September 2001 und den nachfolgenden Terroranschlägen in Europa den Aufbau von Projekten, ihre finanzielle Förderung und die Kooperation mit Trägern im Rahmen dieser Aktivitäten bundesweit aus einer sehr starken sicherheitspolitischen Brille betrachten. Es besteht vielerorts im Vergleich zu den meisten Trägern im Themenfeld Rechtsextremismus oftmals eine Unsicherheit bei staatlichen Verantwortungsträgern gegenüber Personen und Trägern z.B. aus der muslimischen Community, die dann in

[2] Im Wortlaut: „Hiermit bestätigen wir, dass wir uns zur freiheitlichen demokratischen Grundordnung der Bundesrepublik Deutschland bekennen und eine den Zielen des Grundgesetzes förderliche Arbeit gewährleisten. Als Träger der geförderten Maßnahmen haben wir zudem im Rahmen unserer Möglichkeiten und auf eigene Verantwortung dafür Sorge zu tragen, dass die als Partner ausgewählten Organisationen, Referenten etc. sich ebenfalls den Zielen des Grundgesetzes verpflichten. Uns ist bewusst, dass keinesfalls der Anschein erweckt werden darf, dass eine Unterstützung extremistischer Strukturen durch die Gewährung materieller oder immaterieller Leistungen Vorschub geleistet wird." Vgl. https://www.gera.de/fm/sixcms/193/Demokratieerklaerung_01.pdf (Datum des Zugriffs: 30.01.2018)

[3] Begleitschreiben des Bundesministeriums für Familie, Senioren, Frauen und Jugend zum Zuwendungsbescheid im Rahmen des Bundesprogramms „Demokratie leben! Aktiv gegen Rechtsextremismus, Gewalt und Menschenfeindlichkeit", 19.01.2015.

Krisensituationen zum Tragen kommen. Wir erleben ja nicht nur Gewalt mit einem militanten-islamistischen Hintergrund: trotz der nach wie vor hohen Zahl von politisch motivierten Straf- und Gewalttaten mit einem rechtsextremistischen Hintergrund sind es aber ausgerechnet Projekte gegen den militanten Islamismus, die einer kritischen und manchmal einer gar hysterischen medialen Öffentlichkeit ausgesetzt sind und die damit einhergehend unter einem Rechtfertigungsdruck mit Blick auf die Fragen von Zuverlässigkeit stehen können und zwar deutlich stärker, als es bei Projekten im Bereich Rechtsextremismusprävention (bisher) der Fall war. Das sollte zu denken geben.

Hier gilt es grundsätzlich, das Binnenverhältnis zwischen Staat und zivilgesellschaftlichen Trägern im Themenfeld des militanten Islamismus/Salafismus zu prüfen, denn es droht sich der Eindruck zu verfestigen, dass der Staat in diesem Themenfeld zwar auf das zivilgesellschaftliche Knowhow dieser Träger setzt, den handelnden Personen aber misstraut. Die sicherheitspolitische Brille abziehen würde bedeuten, dass nicht jedes geförderte Präventionsprojekt ein staatlich gefördertes Projekt zur Extremismus- oder gar Terrorbekämpfung ist, sondern viele Projekte (wie im Themenfeld Rechtsextremismus auch) niedrigschwellige Maßnahmen zur Förderung von Demokratie anbieten. Ein zu hoher Erwartungs- und Erfolgsdruck, möglicherweise gepaart mit o.g. Unsicherheit, lassen den noch recht jungen Projekten im Themenfeld des militanten Islamismus wenig Zeit und Luft, ihre Ansätze zu entwickeln, zu erproben und zu evaluieren. Bliebe es bei der konstatierten „Vertrauensschieflage", so sollte konsequenterweise der Staat selbst und nicht zivilgesellschaftliche Organisationen Träger solcher Maßnahmen sein.

6. In dem vorliegenden Änderungsantrag für das Verfassungsschutzgesetz heißt es in Artikel 1, §21 Abs. 1. Nr. 2 Buchstabe i nun, dass in „begründeten Einzelfällen" Personen und Organisationen einer anlassbezogenen Überprüfung der Zuverlässigkeit unterzogen werden können. Wohl wissend, dass en détail nicht alles im Gesetzestext ausformuliert werden kann, so ist es dringend vonnöten, nachvollziehbare Kriterien zu entwickeln, was „begründete Einzelfälle" sind. Die o.g. Beispiele für Vorkommnisse in Hessen rühren z.T. aus Presseartikeln und Veröffentlichungen in Internetblogs, die wiederum in sozialen Netzwerken geteilt und kommentiert wurden. Sind solche öffentlich formulierten Verdachtsfälle Begründung genug, um eine Zuverlässigkeitsüberprüfung zu verlangen? Viele Träger befürchten, dass in Zukunft Presseartikel oder (Mikro)Shitstorms in Sozialen Netzwerken dafür ausreichen. Aus der Erfahrung in anderen Bundesländern ist damit zu rechnen, dass auch in Hessen nach den Landtagswahlen 2018 die Arbeit der Träger im Kontext des Landesprogramms über parlamentarische Anfragen in den besonderen Fokus geraten. Neben den Kriterien für „begründete Einzelfälle" ist es daher wichtig, dass bei öffentlich formulierten Verdachtsfällen gegenüber geförderten Projekten ein enger Austausch (Stichwort „Krisenkommunikationsplan") zwischen staatlichen und zivilgesellschaftlichen Verantwortungsträgern zur kommunikativen Bewältigung solch akuter Krisen besteht, die zum einen möglichst Schaden vom verantwortlichen Ministerium und vom verantwortlichen Träger abzuwenden sucht, aber zum anderen auch die in den öffentlichen Fokus geratenen Teams und die einzelnen betroffenen Mitarbeiter_innen schützt.

Einleitung

Hinter dem Verbund aus Betriebssystem, der darauf installierten Anwendung und den passenden Geräten steckt die Arbeit von Menschen. Ähnlich wie ein Autor ein Buch schreibt erstellen Entwickler Betriebsanleitungen, mit dem Laptops, Desktops, Smartphones oder die Rechner in Firmen genutzt werden können. Mit „Betriebsanleitung“ sind hier der Quell- oder Sourcecode gemeint als Grundlage der damit erstellten Betriebssysteme und ihrer Anwendungen.

Heute existieren unübersehbar viele Varianten von Betriebssystemen und den dazu passenden Anwendungen und Geräten. In Lehre und Forschung, in der Energieversorgung, oder an einem zeitgemäßen Arbeitsplatz ist dieser Verbund aus Betriebssystem, Anwendungen und dem passenden Gerät zu finden. Daraus ergeben sich sehr viele Varianten von Fehlerursachen.

Ein solcher Verbund ist z.B. als Desktop oder Laptop bekannt. Uns begleitet das Smartphone sogar rund um die Uhr fast überall hin.

Die Anzahl an Kombinationen aus Betriebssystem, Anwendung und dem dazu passenden Gerät ist unübersehbar. Alleine für das Betriebssystem Android mit den dazu passenden Smartphones existieren über 10.000 Varianten.

Wir reden hier von sogenannten informationstechnischen (IT) Anwendungen, die von Menschen gemacht werden, und die in diesem komplexen Zusammenspiel niemals fehlerfrei sind. Bei der Erstellung dieser Anwendungen durch Entwickler passieren Fehler, die trotz Nachkontrolle und extrem aufwändigen Maßnahmen zur Qualitätssicherung unentdeckt bleiben, oft über viele Jahre. Die möglichst zeitnahe Behebung von erkannten Fehlern in Betriebssystemen, ihren Anwendungen wie auch den dazu passenden Geräten ist die bestmögliche Garantie für funktionierende informationstechnische Systeme und damit für deren Betriebssicherheit. Grundlage dafür ist, dass Informationen über Fehler offen für den Markt (vor allem für Hersteller, die Nutzer, die Anbieter und den Handel) kommuniziert werden.

Stellungnahme

Der Gesetzentwurf zur Neuregelung des Verfassungsschutzes in Hessen möchte unter anderem eine gesetzliche Grundlage dafür schaffen, dass Fehler in Betriebssystemen, ihren Anwendungen und den passenden Geräten zur Verfolgung und Aufklärung von bestimmten, schweren Straftaten genutzt werden können, indem durch Ausnutzung von Fehlern Überwachungsanwendungen auf den Geräten von z.b. mutmaßlich Verdächtigen installiert werden können.

Im folgenden wird auf die informationstechnischen Besonderheiten des Entwurfs Bezug genommen.

Konkret sollen mit dem Gesetz spezielle IT Anwendungen auf den IT Systemen von mutmaßlichen Verdächtigen zum Einsatz kommen, genauer Überwachungsanwendungen auf z.B. dem Smartphone oder z.B. dem Laptop des Verdächtigen so installiert werden, dass ihre Existenz und Funktion für den Verdächtigen und sein Umfeld unbemerkt bleibt. Diese speziellen Anwendungen zur Überwachung nutzen Fehler im Betriebssystem des Geräts oder den darauf installierten Anwendungen.
Je nach der zu Grunde liegenden Technologie werden zur genaueren Ordnung der Überwachungsanwendungen Begriffe wie z.b. „Trojaner“ verwendet, wobei die Liste der verwendeten Bezeichnungen und ihrer Abkürzungen und Ableitungen ständig wächst, und mittlerweile der Begriff „Hessentrojaner“ als ein einführter Begriff verstanden werden kann.

Hier wurde der Begriff Überwachungsanwendung als Sammelbegriff für Anwendungen gewählt, die auf staatlicher Seite zum Einsatz kommen sollen, und als eine bestimmte informationstechnische Variante im Gesetz zur Neuregelung des Verfassungsschutzes erkannt werden können.

Naturgemäß sind die den Überwachungsanwendungen zu Grunde liegenden Fehlfunktionen in Betriebssystemen oder ihrer Anwendung nur nutzbar, wenn sie entweder der breiten Öffentlichkeit unbekannt sind oder dem Entwicklerteam, bzw. dem Hersteller von staatlicher Seite untersagt wird, die Fehlfunktion zu reparieren (fixen) und die Nutzer der fehlerhaften Anwendungen darüber überhaupt erstmal zu informieren.

In der Realität sind Tausende von Fehlern, die von Überwachungsanwendungen ausgenutzt werden könnten, nur einem kleinen Kreis von IT Spezialisten bekannt.

Derartige Informationen werden in gesonderten Teilen des Internets als wertvolles Wissen angeboten, und durchaus gewerblich orientiert an jeden meistbietenden Käufer verdeckt weitergegeben, manchmal für Beträge über 100.000 € . Diese gesonderten Teile des Internet zur Abwicklung des Handels sind als das „darknet“ bekannt geworden.

Daneben arbeiten reguläre spezialisierte Firmen mit eigenen Entwicklerteams an Anwendungen, die die forensische Analyse und weitergehend das Ausnützen von Fehlern integriert anbieten, und somit einen komfortablen Werkzeugkasten bereitstellen, mit dem informationstechnische System forensisch analysiert und danach mit geeigneten Überwachungsanwendungen von staatlicher Seite für eine Überwachung geöffnet werden kann.

Vom den mutmaßlich Verdächtigen unbemerkt werden also mit der Installation von Überwachungsanwendungen auf z.B. Smartphones diese soweit geöffnet, dass vermutlich konkrete Beweise für Straftaten wie Bilder oder Erkenntnisse über mögliche weitere Beteiligte durch Videomitschnitt gesichert werden können.

Das Problem dabei ist, dass diese speziellen Anwendungen mit ihrem Start auf dem Laptop, dem Desktop oder dem Smartphone des Verdächtigen tiefgreifende Zugriffsrechte auf dem Gerät erhalten müssen um ihren Zweck zu erfüllen, und dass die Überwachung 24 Stunden rundum die Uhr an nahezu jedem Ort weltweit möglich ist. Das „Gesetz zur Neuregelung des Verfassungsschutzes“ soll dafür ausreichende Rechtsgrundlagen schaffen.

Beispiel Smartphone

Bei einem Smartphone im mutmaßlichen Besitz eines Verdächtigen kann dies bedeuten, dass mit der erfolgreichen Installation der Überwachungsanwendung alle Dateien des Geräts und das Gerät selbst mit allen technischen Eigenschaften genutzt werden könnten.

Damit könnte die Überwachungsanwendung beispielsweise

- den Aufenthaltsort des Smartphone auf wenige Meter genau bestimmen
- die Umgebung des Smartphone mit Kamera und Mikrophon überwachen
- an das Smartphone angeschlossene Komponenten wie Fitness Armbänder auslesen
- die Dateien auf dem Smartphone lesen, verändern, kopieren, löschen oder neue Dateien auf das Gerät aufspielen
- die Einstellungen zur Nutzung auf dem Smartphone so verändern, dass dieses sich in der Kommunikation mit unbeteiligten Dritten als das Smartphone eines beliebigen Dritten ausgibt. Dazu könnten durch die Überwachungsanwendung neue Inhalte auf das

Smartphone kopiert werden. Nur durch den Stand der Technik limitierte Inhalte wie Videos, Sprachdateien oder Nachrichten in einem Chatablauf können eine andere Identität als den tatsächlichen Nutzer des Smartphones als plausibel erscheinen lassen, sowohl für die Überwacher wie auch jeden Kommunikationspartner des Smartphones

- verschlüsselte Anwendungen auf dem Smartphone überwachen und z.b. von verschlüsselten Nachrichtendiensten wie Whatsapp vom Verdächtigen unbemerkt Bildschirmfotos mit den lesbaren Nachrichteninhalten übertragen, während der Verdächtige Whatsapp nutzt

Unbefugte Weiterverwendung

Die Überwachungsanwendung ist dabei grundsätzlich nicht davor geschützt, selbst vom Verdächtigen auf dem Smartphone entdeckt zu werden und anschließend wie jede andere Anwendung aus z.B. dem Smartphone heraus kopiert zu werden; zur beliebigen weiteren Verwendung durch den Verdächtigen selbst.
Also könnte dem Verdächtigen so ein Werkzeug zur Überwachung von anderen Smartphones bereitgestellt werden, ohne dass diese unerlaubte Weiterverwertung des Anwendungsprogramms von staatlicher Seite bemerkt, rechtssicher protokolliert oder verhindert werden könnte.
Ebenso kann die Kommunikation des Anwendungsprogramms mit den informationstechnischen Einrichtungen der staatlichen Seite durch den mutmaßlichen Verdächtigen selbst mißbraucht werden, um einen unentdeckten Zugriff auf die Systeme der staatlichen Seite zu starten, mit allen sich daraus ergebenden Konsequenzen für die weitere strafrechtliche Würdigung der Ermittlungen selbst und die Betriebssicherheit der informationstechnischen Systeme auf staatlicher Seite.

Wer soll überwacht werden und wer wird tatsächlich überwacht?

Die Überwachungsanwendung weiß selbst nichts darüber, wer das Smartphone gerade nutzt, und zu welchem Zweck. So können unbeteiligte Kollegen am Arbeitsplatz, Bekannte im Verein oder die Familie unabsichtlich überwacht werden, wenn z.B. das überwachte Smartphone des mutmaßlich Verdächtigen von Dritten ausgeliehen wurde, um damit ein Telefonat mit dem Lebenspartner zu führen, oder das Bankkonto zu verwalten. Im Rahmen einer Überwachung rund um die Uhr wird üblicherweise eine Vielzahl von Personen im Umfeld des Verdächtigen durch die Überwachungsanwendung erfasst werden. Für die staatliche Seite wird so jeder denkbare Gesetzesverstoß von eigentlich unbeteiligten Dritten im Umfeld einer entsprechend arbeitenden Überwachungsanwendung als sogenannter Beifang offengelegt.

Unerwünschte Modifikationen

Die konkreten technischen Eigenschaften der Überwachungsanwendung sind nach der Installation auf z.b. dem Smartphone des Verdächtigen modifizierbar. Damit ist gemeint, dass jede Person mit Zugriff auf das Smartphone die darauf installierte Überwachungsanwendung so abändern kann, dass von der Überwachungsanwendung Informationen übertragen werden, die vereinfacht ausgedrückt erfunden sind. Oder die zugreifende Person kann tatsächlich aus dem Smartphone ausgelesene Informationen so abändern und zur Übertragung bereitstellen, dass sich aus der Auswertung der Informationen strafwürdige Tatbestände ergeben könnten, die so nie passiert sind. Die Überwachungsanwendung kann grundsätzlich nicht davor geschützt werden, aus z.B. dem Smartphone des Verdächtigen von diesem oder Dritten manipulierte Daten auszulesen und diese als quasi „echte“ Daten z.B. der Kamera an die staatliche Seite zu kommunizieren.

Darknet und Wiederverkauf

Die angekaufte Überwachungsanwendung soll für die staatlichen Seite als Auftraggeber bestimmte Funktionen und Dienste bereitstellen. Um nach dem heutigen Stand der Technik sicherzustellen, dass nur die gewünschten Funktionen und Dienste des Überwachungsprogramms tatsächlich zur Anwendung kommen, und diese nach dem Start möglichst fehlerfrei laufen, wäre angesichts der strafrechtliche relevanten Bedeutung der Überwachungsmaßnahme eine fachkundige Prüfung der Bauanleitung des eingesetzten Überwachungsanwendung durch unabhängige und in ihrer Kompetenz anerkannte Dritte anzuraten.
Ohne eine solche Prüfung muss die Überwachungsanwendung als eine in ihrer Zuverlässigkeit und Betriebssicherheit eher kritische Komponente der Überwachungsmaßnahme bewertet werden. Insbesondere sollte vor dem Start der Überwachungsmaßnahme berücksichtigt werden, dass regelmäßig wesentliche Bestandteile von Überwachungsanwendungen aus dem sogenannten „darknet", also von unbekannten Personen mit unbekannter Herkunft im Internet erworben werden, und der Anbieter der Überwachungsanwendung hierzu üblicherweise keine Rechenschaft ablegt.

Die Qualitätssicherung der Überwachungsanwendung, ihre wirkliche Funktionsweise und belastbare vertragliche Vereinbarungen zur Nachbesserung bei erkannten Fehlfunktion der Überwachungsanwendung sind insbesondere im darknet marktunüblich und kaum einforderbar.

Systemrelevante Risiken

Marktüblich kann eine mehrfache Verwertung der Überwachungsanwendung durch jeden Anbieter vermutet werden. Dieselbe Überwachungsanwendung, die eine Fehlfunktion z.B. auf dem Betriebssystems des Verdächtigen nutzt, um den Zugriff auf den Desktop zu bekommen könnte an anderer Stelle von Dritten genutzt werden, um den Zugriff auf Rechner von Krankenhäusern oder Kraftwerken im dortigen Betriebssystem zu bekommen, mit unabsehbaren Risiken für die Betriebssicherheit von z.B. systemrelevanten Einrichtungen wie Kraftwerken, Flughäfen oder Krankenhäusern.
Dieses Risiko kann nur verringert werden, wenn Fehler in informationstechnischen Systemen unmittelbar nach dem Bekanntwerden beim Hersteller oder den Entwicklern nachgebessert werden dürfen. Dazu dürfen die bekannt gewordenen Informationen zu Fehlern von staatlicher Seite nicht unterdrückt bzw. verboten werden. Vielmehr sollten die Risiken derartiger Fehler qualifiziert bewertet werden, damit bei erkennbar systemrelevanten Fehlern in informationstechnischen Systemen deren Heilung unbedingten Vorrang hat.
Zu diesen systemrelevanten Risiken bleibt der Gesetzentwurf zur Neuregelung des Verfassungsschutzes offen. Somit ist ungeklärt, ob oder ab wann z.B. kommerziell agierende Anbieter von Überwachungsanwendungen einer notwendigen Informationspflicht entdeckter Fehler gegenüber den Herstellern nachkommen sollen.

Darmstadt, im Februar 2018

Peter Löwenstein

Geschäftsführer Loenco GmbH

Eine Liste von Quellenmaterial und Belegen zur ergänzenden Darstellung kann vom Autor bereitgestellt werden.

Stiftung
Neue
Verantwortung

Stellungnahme

für die öffentliche Anhörung im Hessischen Landtag

zum Gesetzentwurf der Fraktionen CDU und BÜNDNIS 90/DIE GRÜNEN zur Neuausrichtung des Verfassungsschutzes in Hessen (Drucksache 19/5412)

Autoren:
Kilian Vieth
Dr. Thorsten Wetzling

Kontakt:
Stiftung Neue Verantwortung
Berliner Freiheit 2
10785 Berlin

kvieth@stiftung-nv.de
twetzling@stiftung-nv.de

Berlin, den 5. Februar 2018

1. Einleitung

Mit dem Entwurf zur Neuausrichtung des Verfassungsschutzes in Hessen (Drucksache 19/5412) soll auf den „signifikanten Reformbedarf"[1] im Bereich des Hessischen Landesverfassungsschutzes reagiert und Erkenntnisse aus diversen parlamentarischen Untersuchungen[2] umgesetzt werden. Jetzt steht der Innenausschuss des Hessischen Landtags in der Pflicht, die grundlegende Reform des Landesverfassungsschutzes und seiner Kontrolle zu beraten.

Wir bedanken uns für die Möglichkeit, eine Reihe von Verbesserungsmöglichkeiten im Rahmen dieser Stellungnahme aufzuzeigen. Wir konzentrieren uns auf die Ausgestaltung der Instrumente und Mechanismen für eine effektive und demokratische Kontrolle über die nachrichtendienstlichen Tätigkeiten der Hessischen Landesregierung. Eine erschöpfende Stellungnahme zu anderen wichtigen Aspekten dieses Gesetzentwurfs kann und soll hier nicht geleistet werden.

Die Fokussierung auf Problemzonen der Kontrolle bedeutet gleichwohl nicht, dass jegliche nachrichtendienstliche Befugnis durch bessere Kontrolle zu legitimieren ist. Präzise gesetzliche Grundlagen, Transparenz und Kontrolle sind vielmehr unverzichtbare Grundvoraussetzung für einen demokratischen und effektiven Verfassungsschutz.

In der jetzigen Form fehlen dem Gesetzentwurf aber wichtige rechtsstaatliche Absicherungen um die Verhältnismäßigkeit und Legitimität von geheimen Überwachungsbefugnissen zu wahren. Der Entwurf versäumt es aus unserer Sicht leider, für ausreichende Transparenz zu sorgen und die parlamentarische und juristische Kontrolle entscheidend zu stärken. So stehen beispielsweise die unvollständigen Unterrichtungspflichten des Landesregierung, die unzureichende Berücksichtigung der Oppositionsrechte und die lückenhaften Berichtspflichten der Kontrollkommission einer effektiven parlamentarischen Kontrolle entgegen. Das nicht mehr zeitgemäße System der G10-Kontrolle und ihre technischen Defizite der Kontrolle bleiben ebenfalls unangetastet.

---

[1] Siehe Gesetzentwurfsbegründung, Drucksache 19/5412, S. 29, Abs. 1

[2] Vgl. unter anderem: 2. Bundestags-Untersuchungsausschuss BT-Drucksache 18/12950; Bericht der Expertenkommission für die Umsetzung der Empfehlungen des Zweiten BT-Untersuchungsausschusses der 17. WP; Untersuchungsausschuss 19/2 (UNA19/2) des Hessischen Landtags

2. Parlamentarische Kontrolle

Gerade weil die Arbeit des Landesamts für Verfassungsschutz (anders als anderes Regierungshandeln) vornehmlich im Geheimen stattfindet und in Grundrechte eingreift, ist die Kontrolle des Verfassungsschutzes eine der bedeutendsten Aufgaben des Hessischen Landtags. Es ist daher zu kritisieren, dass der Gesetzentwurf viele Defizite der parlamentarischen Kontrolle ungelöst lässt.

2.1. Lücken in den Unterrichtungspflichten der Landesregierung schließen

Der Gesetzentwurf überlässt es der Landesregierung, „Zeit, Art und Umfang der Unterrichtung" (§ 3 Abs. 2)[3] der Kontrollkommission zu bestimmen. Das erschwert eine wirksame Kontrolle ungemein. Nicht die Landesregierung, sondern die Kontrollkommission sollte die Rahmenbedingungen für die Prüfung relevanter nachrichtendienstlicher Vorgänge selbstständig festlegen. Zumindest sollte der Landtag den Zeitpunkt, den Gegenstand und die Form der Kontrolle selbstständig bestimmen können.

Auf Bundesebene wird die Unterrichtungspflicht über „besondere Vorgänge" präziser definiert als im hessischen Entwurf: Die Bringschuld der Bundesregierung gilt dort auch für „wesentliche Änderungen im Lagebild, behördeninterne Auswirkungen mit erheblicher Auswirkung auf die Aufgabenerfüllung sowie Einzelvorkommnisse, die Gegenstand politischer Diskussionen oder öffentlicher Berichterstattung sind" (§ 4 Abs. 1 Satz 2 PKGrG). Auch der Brandenburgische Landtag hat seine Kontrollkommission diesbezüglich selbstbewusster aufgestellt: Dort wird gesetzlich festgelegt, dass die Kontrollkommission „alle für ihre Kontrollaufgaben erforderlichen Auskünfte, Unterlagen, Akten- und Dateneinsicht, Stellungnahmen und den Zutritt zur Verfassungsschutzbehörde verlangen sowie bei besonderem Aufklärungsbedarf mit Zustimmung des Innenministers Bedienstete zum Sachverhalt befragen" kann (§ 25 Abs. 1 BbgVerfSchG). Der hessische Gesetzentwurf sollte ebenfalls um einen klaren Anspruch der Kontrollkommission auf Befragung Bediensteter ergänzt werden. Außerdem sollten der Kontrollkommission Sanktionsmöglichkeiten zur Verfügung stehen, wenn die Unterrichtung lückenhaft oder deutlich verzögert erfolgt.

Der Gesetzentwurf überlässt dem zuständigen Ministerium die Gestaltung wesentlicher Befugnisse durch Dienstvorschriften (§ 4 Abs. 1 des Artikels 1 des Gesetzentwurfs). Nachrichtendienstliche Überwachung greift besonders stark in die Grundrechte ein und muss daher unmittelbar vom Gesetzgeber und nicht durch opake Verwaltungsrichtlinien festgelegt werden. Die Landesregierung sollte die Kontrollkommission grundsätzlich über den

[3] Angaben von Paragraphen beziehen sich wenn nicht anders angegeben auf Artikel 2 des Gesetzentwurfs.

beabsichtigten Erlass oder die beabsichtigte Änderung einer Dienstvorschrift, den Einsatz aller nachrichtendienstlicher Mittel und Auskunftsersuche informieren. Genauere gesetzliche Bedingungen für den Erlass von Dienstvorschriften sind daher dringend geboten: Grundsätzlich sollten den Landesverfassungsschutz betreffende Dienstvorschriften der Kontrollkommission zur Prüfung und Zustimmung vorgelegt werden, wie es etwa in § 5 Abs. 3 Satz 3 (des Artikel 1 des Gesetzentwurfs) bereits für einen Einzelfall vorgesehen ist.

Der Entwurf lässt offen, warum bei der Berichtspflicht nur einige Befugnisse des Landesamts explizit genannt werden, anstatt alle nachrichtendienstlichen Mittel, wie sie in § 5 Abs. 2 aufgelistet werden, in die Unterrichtung mit einzuschließen. Es ist prinzipiell zu begrüßen, dass § 3 Abs. 3 Nr. 2 die Landesregierung erstmals zu einem jährlichen Bericht über die Wohnraumüberwachung, Online-Durchsuchung, die Verwendung von IMSI-Catchern und den Einsatz von verdeckten Mitarbeiter*innen und V-Leuten verpflichtet. Doch auch alle anderen nachrichtendienstlichen Befugnisse, wie Observationen oder verdeckte Ermittlungen, sind für die Kontrolle relevant. Auch wirtschaftliche Kennzahlen zu Kosten und Effektivität der Maßnahmen sowie die konkrete Auslegung gesetzlicher Befugnisse im Hinblick auf neue Überwachungstechnik sollte in die Unterrichtungspflicht aufgenommen werden. Der Kontrollkommission muss es möglich sein, sich ein vollständiges und aktuelles Bild über alle geheimen Überwachungsmaßnahmen zu verschaffen. Dies ist auch im Lichte des vom Bundesverfassungsgericht entwickelten Ansatzes der Überwachungsgesamtrechnung[4] geboten. Demnach braucht es einen gesamtheitlichen Überblick über alle schon laufenden und geplanten Überwachungsmaßnahmen um eine fundierte Bewertung aller Grundrechtseingriffe vornehmen zu können (siehe dazu Abschnitt 2.5 zur vernetzten Kontrolle). Die Landesregierung sollte dafür nicht nur jährlich, sondern mindestens alle sechs Monate umfassend berichten, wie sie es auch nach § 3 Abs. 4 gegenüber dem Parlamentarischen Kontrollgremium des Bundes im Hinblick auf „Anlass, Umfang, Dauer, Ergebnis und Kosten" der dort genannten Maßnahmen tun muss.

2.2. Kontrollinstrumente wirksamer ausgestalten

Mitglieder der Kontrollkommission sollten jederzeit und uneingeschränkt Zugang zu allen Dienststellen des Landesverfassungsschutzes haben. So ist es auch auf Bundesebene geregelt (§ 5 Abs. 1 PKGrG). Zutritt zu den Dienststellen des Landesamts für Verfassungsschutz wird den Mitgliedern bisher nur im Rahmen der Akteneinsicht gewährt (§ 4 Abs. 2 Satz 3). Diese Einschränkung ist unbegründet und schwächt die Kontrollmöglichkeiten der Kommission. Außerdem fehlen im Gesetzentwurf Vorgaben zu regelmäßigen Kontrollbesuchen vor Ort.

Die Wirksamkeit der parlamentarischen Kontrolle setzt sowohl eine eigenständige, proaktive Informationsbeschaffung durch die Mitglieder der Kommission als auch eindeutige und umfassende Zugangsrechte zu Informationen voraus. Um die Akteneinsicht (§ 4 Abs. 2) zu einem wirksamen Kontrollinstrument zu machen, braucht es klarere Regeln. Die Einsicht in

[4] GPS-Urteil (BVerfG, vom 12. April 2005 - 2 BvR 581/01)

Schriftstücke und Daten muss im Entwurf konkreter ausgestaltet werden. Datensätze und Schriftverkehr sollten in digitaler Form geführt und bereitgestellt werden um eine effiziente Untersuchung zu ermöglichen.

Die Bedingungen für die Ausgestaltung der Geschäftsordnung der Kontrollkommission (§ 1 Abs. 6) werden im Entwurf nicht ausreichend bestimmt. Sie sollten veröffentlicht werden, denn eine strukturierte Kontrolle braucht transparente Vorgaben und Regeln um Vertrauen zu schaffen. In der Geschäftsordnung sollten Jahresziele und Arbeitsschwerpunkte festgelegt werden. Neben der anlassbezogenen Kontrolle (nach Presseberichten etc.) bleibt die strukturelle Kontrolle (unabhängig von konkreten Vorkommnissen) ansonsten unausgeschöpft.

Die aufwendige und inhaltlich anspruchsvolle Kontrolltätigkeit sollte nicht allein auf den Schultern der gewählten Mitglieder beruhen. Ohne tatkräftige fachliche Unterstützung bleibt der Einfluss der parlamentarischen Kontrolle beschränkt. Daher sollte den Mitgliedern der Kontrollkommission einen Anspruch auf eine zusätzliche Mitarbeiterstelle für die Arbeit der Kontrolle eingeräumt werden. Außerdem sollte es einzelnen Mitgliedern gestattet sein, wichtige Informationen vertraulich mit ihrer Fraktionsspitze zu besprechen.[5] In Thüringen ist zum Beispiel klar geregelt, dass die Mitglieder der Kontrollkommission „unter Beachtung der Geheimhaltung den Vorsitzenden ihrer Fraktion, [...] über die wesentlichen Inhalte der Beratungen unterrichten" dürfen (§ 24 Abs. 2 Satz 2 ThürVerfSchG).

Bei den Haushaltsberatungen wird der Kontrollkommission nur ein Mitberatungsrecht gegeben (§ 4 Abs. 5). Ohne konkrete Sanktionsmöglichkeiten kann die Kontrollkommission kaum Druck gegenüber der Landesregierung aufbauen. Um die Position der Kontrollkommission zu stärken, empfiehlt es sich, ihr ein stärker ausgekleidetes Genehmigungsrecht bei der Bewilligung von zusätzlichen Haushaltsmitteln einzuräumen. Die Kontrollkommission könnte dann die Vergabe von Geldern an die Einhaltung von Rechten und Pflichten des Landesverfassungsschutzes knüpfen, was ihrer Kontrolltätigkeit zusätzliche Relevanz verleihen würde.

Der Gesetzentwurf verpasst es, einen für die Kontrolle wichtigen Whistleblowerschutz für Bedienstete des Landesverfassungsschutzes einzuführen. Das PKGr-Gesetz des Bundes erlaubt es „Angehörigen der Nachrichtendienste [...] sich in dienstlichen Angelegenheiten sowie bei innerdienstlichen Missständen [...] ohne Einhaltung des Dienstweges unmittelbar an das Parlamentarische Kontrollgremium zu wenden" (§ 8 Abs. 1 PKGrG). Diese Erlaubnis zur Eingabe sollte auch gegenüber der Kontrollkommission des Hessischen Landtags gelten.

2.3. Die Oppositionsrechte sind im Entwurf zu stärken

Der Gesetzentwurf sichert den Oppositionsfraktionen keine ausreichenden Rechte zu. Parlamentarische Regierungssysteme sind strukturell immer durch die enge Verzahnung der legislativen Regierungsmehrheit mit der exekutiven Landesregierung gekennzeichnet. Ein

[5] Siehe Expertenkommission der Hessischen Landesregierung, Empfehlung 41.05, S. 202

Großteil der Kontrollarbeit im Parlament wird in der Praxis typischerweise durch die Oppositionsfraktionen geleistet. In der Kontrollpraxis zeigt sich, dass die Qualität und Wirksamkeit der Kontrolle wesentlich von den Mitbestimmungsmöglichkeiten der parlamentarischen Minderheit beziehungsweise dem Einsatz einzelner Mitglieder der Kontrollkommission bestimmt wird. Die Oppositionsrechte sind im vorliegenden Gesetzentwurf aber zu schwach ausgeprägt. Das zeigt sich insbesondere an folgenden Beispielen:

Um die Mitbestimmung der Opposition zu gewährleisten – und die besondere Bedeutung der Kontrolltätigkeit herauszustellen – muss eine höhere Schwelle (z.B. eine zwei Drittel Mehrheit) für die Wahl der Kommissionsmitglieder angesetzt werden.[6] Die Mitglieder werden nach § 1 Abs. 4 des Artikel 2 des Gesetzentwurfs nur mit einfacher Mehrheit gewählt. Allen Fraktionen sollte zudem mindestens ein Sitz in der Kontrollkommission gesetzlich zugesichert werden.

Der Gesetzentwurf verhindert die effektive Mitsprache der Opposition bei der Dokumentation der Kontrolle. § 2 Abs. 2 regelt lediglich, dass ein Protokoll durch die Kanzlei des Landtags auf Grundlage einer Aufzeichnung der Sitzungen erstellt wird. Darüber hinaus ist es den Mitgliedern der Kontrollkommission „gestattet, sich für die Beratungen während der Sitzungen handschriftliche Notizen anzufertigen" (§ 2 Abs. 3 Satz 1). Vollständige und detaillierte Protokolle der Sitzungen der Kontrollkommission sind das Gedächtnis der Fraktionen und zentral für die Dokumentation der Kontrollarbeit. Deswegen sollten auch hier die Oppositionsrechte besser verankert werden. Eine Abstimmung über die Vollständigkeit des Protokolls und das Recht durch ein Minderheitsvotum abweichende Meinungen im Protokoll zu dokumentieren, gehören dazu und sollten in § 2 über die Arbeitsweise der Kontrollkommission aufgenommen werden.

2.4. Öffentliche Sitzungen und erweiterte Berichtspflichten

Die Kontrollkommission des Hessischen Landtags soll laut Gesetzentwurf ausschließlich geheim tagen (§ 2 Abs. 1). Doch parlamentarische Arbeit lebt von Öffentlichkeit. Deshalb sollte auch für die Kontrollkommission die Möglichkeit bestehen, öffentliche oder teilweise öffentliche Sitzungen zu beantragen und durchzuführen.[7] Das brandenburgische Landesverfassungsschutzgesetz ermöglicht etwa, dass die Kontrollkommission „auf Antrag eines Mitgliedes" beschließen kann, Öffentlichkeit herzustellen, sofern berechtigte Interessen dem nicht entgegenstehen (§ 26 Abs. 2 BbgVerfSchG). Auch in Hessen sollte eine solche Möglichkeit zur Beantragung öffentlicher Sitzung eingeführt werden.

Zudem ist der Umfang der Pflicht zur Berichterstattung im Gesetzentwurf unzureichend bestimmt. Eine öffentliche Berichterstattung ist Voraussetzung für Vertrauensbildung und ermöglicht erst demokratische Debatten. Diese Berichtspflichten der Kontrollkommission sind zu

[6] Auch die Expertenkommission der Hessischen Landesregierung empfahl eine angemessene Vertretung der Oppositionsfraktionen besser gesetzlich zu verankern, siehe Empfehlung 41.02, S. 199ff

[7] Siehe dazu auch Expertenkommission der Hessischen Landesregierung, Empfehlung 41.06, S. 203

unkonkret und werden der „gesellschaftliche Öffnung des Verfassungsschutzes"[8] nicht gerecht. Das PKGrG des Bundes spezifiziert die Berichtspflicht genauer: Der Bericht muss dort klarstellen „ob die Bundesregierung gegenüber dem Gremium ihren Pflichten, insbesondere ihrer Unterrichtungspflicht zu Vorgängen von besonderer Bedeutung, nachgekommen ist" (§ 13 PKGrG). Es bedarf klarer Anforderungen für den Inhalt der Berichterstattung, etwa bezüglich Statistiken über den Einsatz und die Entwicklung nachrichtendienstliche Maßnahmen, den Einsatz von Ressourcen und ein Protokoll des Abstimmungsverhaltens der Fraktionen in den Sitzungen der Kontrollkommission. Ein Minderheitsvotum, dass die Mitsprache und Sichtbarkeit der Opposition in den Berichten schützt, sollte ebenfalls gesetzlich verankert werden.

2.5. Der vernetzen Sicherheit eine vernetzte Kontrolle entgegenstellen

Es erstaunt, dass der Gesetzentwurf es gänzlich versäumt, Regelungen zur Zusammenarbeit mit anderen Kontrollgremien zu treffen. Verfassungsfeindliche Bestrebungen machen nicht an den Grenzen des Landes Hessens halt. Daher ist die Kooperation mit anderen Landes- und Bundesbehörden und auch internationalen Partnerdiensten wichtig. Vor diesem Hintergrund ist es aber genauso bedeutend, dass auch die Kontrollgremien sowohl auf Landes-, Bundes- und internationaler Ebene besser zusammenarbeiten um eine lückenlose und wirksame Überprüfung der länderübergreifenden Nachrichtendienstkooperation leisten zu können.[9] Ein modernes Verfassungsschutzkontrollgesetz sollte der Kontrollkommission im Rahmen ihrer Zuständigkeit eine explizite Befugnis zum Austausch mit anderen Kontrollgremien geben. Nur so kann einer vernetzter Überwachung auch eine vernetzte Kontrolle entgegengestellt und Kontrolllücken geschlossen werden.

Dabei sollte die Kooperation zwischen den verschiedenen hessischen Kontrollinstitutionen, der hessischen G10-Kommission, dem Landesdatenschutzbeauftragten und der Kontrollkommission des Landtags ebenfalls gestärkt werden. In ihrem Tätigkeitsbericht 2015-2016 hält die Bundesdatenschutzbeauftragte den Bedarf nach koordinierter Kontrolle der Nachrichtendienste ausdrücklich fest: „Den im Rahmen der Kontrolle beim BfV erstmalig verfolgten gemeinsamen Kontrollansatz mit der G-10-Kommission des Deutschen Bundestages betrachte ich als zukunftsweisendes Modell, das es zur Vermeidung kontrollfreier Räume auch künftig zu verfolgen gilt".[10] Dieser gemeinsame Kontrollansatz sollte nun auch auf Landesebene verankert werden. Da der Gesetzentwurf kein gemeinsames Prüfrecht und keine Regelungen zum Informationsaustausch zwischen Kontrollinstitutionen enthält, fehlt der Kontrolle ein gesamtheitlicher Überblick.

---

[8] Siehe Drucksache 19/5412, S. 29, Abs. 1

[9] Auch die Expertenkommission der Landesregierung empfiehlt der Kontrollkommission mit anderen Kontrollgremien in Verbindung zu treten und zusammenzuarbeiten: Empfehlung 43.01, S. 207

[10] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 26. Tätigkeitsbericht 2015-2016, S. 134

3. Juristische Kontrolle

Der Gesetzentwurf räumt dem Verfassungsschutz zusätzliche Befugnisse bei der Telekommunikationsüberwachung ein, vermeidet aber gleichzeitig eine Stärkung der juristischen Kontrolle.

Um das geheime Handeln des Verfassungsschutzes zu legitimieren, braucht es aber eine effiziente Zulässigkeits- und Notwendigkeitsprüfung von Überwachungsmaßnahmen. Der juristischen Kontrolle kommt im Gefüge der verschiedenen Kontrollinstanzen eine besonders wichtige Rolle zu. Die G10-Kommission ist die einzige Kontrollinstanz, die Abhörmaßnahmen auf ihre Vereinbarkeit mit dem Grundgesetz prüft und Maßnahmen vor dem Vollzug stoppen kann (§ 4 AG G 10, HE). Anders als bei der parlamentarischen Kontrolle, braucht die Landesregierung zur Durchführung von Maßnahmen die Vorabgenehmigung der juristischen Kontrolle.

3.1. Unzureichender Grundrechtsschutz durch G10-Kommission

Die G10-Kommission in Hessen ist in vielen Teilen analog zur G10-Kommission des Bundes gestaltet. Daher gehen wir davon aus, dass für die hessische G10-Kommission die gleichen strukturellen Defizite bestehen wie für die G10-Kommission des Bundestags. Dort ist die G10-Kommission derzeit nicht in der Lage, ihre zentrale Funktion bei der demokratischen Kontrolle der Abhöraktivitäten effektiv wahrzunehmen. Es fehlen ihr die Ressourcen und die Kompetenzen (die ihr nach § 15 Abs. 3 Artikel 10-Gesetz zustünden), um den Umgang des Verfassungsschutzes mit den erfassten Kommunikationsdaten ausreichend zu überprüfen. Auch die hessische G10-Kommission braucht bedeutend mehr technische, fachliche und personelle Kapazitäten um eine Vorprüfung der Anordnungen im Sinne des gesetzlichen Auftrags (§ 2 Abs. 2 AG G 10, HE) vornehmen zu können.

Die sogenannte Quellen-TKÜ (§ 6 Abs. 2 des Artikel 1 des Gesetzentwurfs) ist ausschließlich auf laufende Kommunikation beschränkt. Dies soll „durch technische Maßnahmen sichergestellt" sein (§ 6 Abs. 2 Nr. 1 des Artikel 1 des Gesetzentwurfs). Außerdem gilt die Bedingung, dass „der Eingriff in das informationstechnische System notwendig ist um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen" (§ 6 Abs. 2 Nr. 2 des Artikel 1 des Gesetzentwurfs). Wie die G10-Kommission diese Bedingungen praktisch prüfen kann und soll, bleibt gänzlich unklar. Technisch greift die Maßnahme zwangsläufig in die Integrität des Zielsystems ein, indem eine Software auf dem Zielsystem installiert wird. Somit steht die Quellen-TKÜ im deutlichen Gegensatz zum Abhören von Gesprächen auf dem Leitungsweg, weil eine Spionagesoftware direkt auf den Computern der Zielpersonen installiert wird. Welche Nebeneffekte dadurch entstehen ist auf Grundlage des Entwurfs nicht vorhersehbar.

Daraus ergibt sich eine eklatante Kontrolllücke. Die G10-Kommission wurde für die Prüfung und Autorisierung von Abhörmaßnahmen auf dem Leitungsweg geschaffen. Sie kann die vorgesehene Beschränkung auf laufende Kommunikation technisch und praktisch nicht effektiv kontrollieren. Das veraltete und dringend überarbeitungsbedürftige Artikel-10-Gesetz des Bundes war bisher nicht Gegenstand der Reform und stellt keinen ausreichenden Standard für eine wirksame Kontrolle dar.[11] Es ist damit nicht sichergestellt, dass die G10-Kommission die nötigen Mittel und Ressourcen hat um die vorgesehene Überwachungsbefugnis gründlich zu prüfen.

G10 Beschränkungsmaßnahmen können sich auch auf Computer-zu-Computer-Kommunikation beziehen. Dies wird zwar im Gesetzentwurf nicht explizit geregelt, geht aber aus der Begründung (S. 31) hervor. Dort heißt es, nach § 6 können auch „sog. Command&Control-Server [...] mit einer G-10-Beschränkungsmaßnahme"[12] belegt werden. Auch hier stellt sich die Frage, ob die hessische G10-Kommission die Möglichkeiten hat, solche Maßnahmen sachgerecht zu prüfen. Gerade weil Hessen ein bedeutender Serverstandort und Internetknotenpunkt ist (DE-CIX in Frankfurt), ist die effektive Kontrolle dieser Form der Internetüberwachung wichtig.

3.2. Technische Defizite der Kontrolle beseitigen

Die gleiche Problemlage gilt auch für richterliche Anordnungen, die unter anderem für die verdeckte Wohnraumüberwachung (§ 7), den Staatstrojaner (§ 8) und die Ortung von Handys (§ 10) vorgesehen sind. Das vorgesehene Genehmigungsverfahren nach § 9 des Artikel 1 des Gesetzentwurfs kann in der Praxis keine effektive Kontrolle leisten. Die sogenannten „technischen Sicherungspflichten" des Gesetzentwurfs sind bei weitem nicht ausreichend um den Schutz des Kernbereichs privater Lebensführung[13] und von Berufsgeheimnisträger*innen zu garantieren. Aus § 8 Abs. 2 des Artikel 1 des Gesetzentwurfs wird in keiner Weise klar, welche konkreten Sicherungspflichten gemeint sind und wie sie umgesetzt werden sollen.

Beispielsweise ist die Regelung, dass „nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind und die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden" (§ 8 Abs. 2 Nr. 1 und 2) zu unspezifisch. Wie kann die juristische Kontrolle überprüfen ob ausschließlich unerlässliche Veränderungen erfolgen auch wieder rückgängig gemacht werden? Diese Überprüfung und Genehmigung des Einsatzes komplexer und höchst grundrechtssensibler Überwachungstechnik kann nicht allein auf den oder die zuständigen Richter*in am Amtsgericht fallen. Um das Grundrecht auf Schutz der Integrität und Vertraulichkeit informationstechnischer

---

[11] Siehe „Das Herzstück der deutschen Geheimdienstreform: Vorschläge für eine starke G 10-Kommission", Policy Brief, 09/2015
https://www.stiftung-nv.de/de/publikation/das-herzst%C3%BCck-der-deutschen-geheimdienstreform-vorschl%C3%A4ge-f%C3%BCr-eine-starke-g-10

[12] Siehe Gesetzentwurfsbegründung, Drucksache 19/5412, S. 31

[13] Vgl. hierzu BVerfG, vom 20. April 2016, 1 BvR 966/09 u.a., Rn. 236 ff.

Systeme (Art. 1 Abs.1, Art. 2 Abs. 1 GG) zu wahren, sollte der Gesetzentwurf konkrete und überprüfbare Sicherungspflichten formulieren und eine unabhängige technische Kontrolle ermöglichen. Ansonsten ist keine ausreichende Nachvollziehbarkeit für die Kontrolle gewährleistet.

Wenn nur die Dienste, nicht aber die Kontrolle technisch voranschreitet, werden demokratische Sicherungsmechanismen sukzessive ausgehöhlt. Die Kontrolle muss daher institutionell so ausgestaltet werden, dass sie mit den technologischen Entwicklung Schritt halten kann.

4. Teilhabe und Auskunftsrechte stärken

Im Vergleich zu anderen Verfassungsschutzgesetzen, greifen die im Gesetzentwurf verankerten Transparenzregelungen und Auskunftsrechte zu kurz. In der Präambel des Gesetzentwurfs heißt es, der Verfassungsschutz „tauscht sich mit Wissenschaft und Gesellschaft aus. Hierzu gehört auch der öffentliche Diskurs". Danach findet sich aber keine Norm im Gesetzentwurf, die diesen wichtigen Grundsatz verbindlich in die Tat umsetzt. Zentrale Anspruchsgruppen wie die Zivilgesellschaft, Wissenschaft, Telekommunikationsdienstleister, Medien und Datenschutzbeauftragte (um nur einige zu nennen) haben ein berechtigtes Interesse an der Nachrichtendienstpolitik und ihrer Kontrolle. Die stärkere Öffnung und institutionalisierter Austausch sind elementar für gutes Regierungshandeln, gerade im sensiblen Bereich der Nachrichtendienste.

Die Auskunftsrechte über gespeicherte Daten für Bürger*innen sind im Vergleich zu anderen Bundesländern unnötig und ungerechtfertigt eingeschränkt. Auskunft über gespeicherte Daten wird durch den Gesetzentwurf nur gestattet, „soweit die betroffene Person hierzu auf einen konkreten Sachverhalt hinweist und ein besonderes Interesse an einer Auskunft darlegt" (§ 27 Abs. 1 des Artikel 1 des Gesetzentwurfs). Es bleibt unklar, warum ein Auskunftsinteresse mit einem konkreten Hinweis begründet werden muss. Das Niedersächsische Verfassungsschutzgesetz verpflichtet die Landesverfassungsschutzbehörde „Betroffenen auf Antrag unentgeltlich Auskunft über die zu ihrer Person gespeicherter Daten, den Zweck und die Rechtsgrundlage der Speicherung sowie die Herkunft der Daten und die Empfänger von Übermittlungen" (§ 30 Abs. 1 NVerfSchG) zu erteilen. Ein klarer gesetzlicher Auskunftsanspruch ist ein integraler Bestandteil für einen transparenten Verfassungsschutz und für individuellen Rechtsschutz. Gerade die Auskunft über die Herkunft und die Empfänger der Daten sind dafür wichtig. Im Sinne einer angestrebten Öffnung des Verfassungsschutzes sollte der Gesetzentwurf bei Auskunftsrechten nicht hinter vergleichbare Regelungen in anderen Bundesländern zurückfallen.

rote linie
Pädagogische Fachstelle
Rechtsextremismus

Öffentliche Anhörung im Innenausschuss des Hessischen Landtages

zu dem Gesetzesentwurf der Fraktionen CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen (Drucks. 19/5412) und

dem Änderungsantrag der Fraktionen CDU und BÜNDNIS 90/DIE GRÜNEN (Drucks. 19/5782)

Stellungnahme von Torsten Niebling

Rote Linie – Pädagogische Fachstelle Rechtsextremismus

Rote Linie – Pädagogische Fachstelle Rechtsextremismus
St. Elisabeth Verein e.V.
Hermann-Jacobsohn Weg 2
35039 Marburg

Tel.: 06421-948500
Mail: t.niebling@elisabeth-verein.de
www.rote-linie.net
www.elisabeth-verein.de

Inhalt

1. Die Rote Linie

Die „Rote Linie – Pädagogische Fachstelle Rechtsextremismus" wird vom St. Elisabeth-Verein e.V. mit Sitz in Marburg umgesetzt. Der St. Elisabeth-Verein e.V. ist ein 1879 gegründeter Träger der sozial-diakonischen Arbeit in der Kinder-, Jugend- und Familienhilfe, der Sozialpsychiatrie sowie in der Altenhilfe mit Angeboten in Hessen, Thüringen und Sachsen. Die Rote Linie ist seit Dezember 2009 hessenweit in dem Bereich der primären und sekundären Prävention von Rechtsextremismus bei Jugendlichen tätig.

Die „Rote Linie" ist als Fachstelle Ansprechpartner, wenn es darum geht, rechtsextreme Gefährdungen, Inszenierungen und Verfestigungen zu erkennen und frühzeitig entgegenzuwirken. Die Fachstelle berät, coacht und qualifiziert pädagogische Fachkräfte, die junge Menschen bei der Distanzwahrung bzw. Distanzierung von rechtsextremen Haltungen und Vereinnahmungen unterstützen. Die Fachstelle steht zudem beratend und coachend für Menschen, die in ihrer Arbeit vor Ort Kontakt zu Jugendlichen mit rechtsextremen Affinitäten oder Bezügen haben, zur Verfügung:

- Eltern und Angehörige
- Pädagogische Fachkräfte/Lehrkräfte
- Betriebe
- Kommunen und Ämter
- Ehrenamtliche

Die „Rote Linie" sucht den Kontakt zu rechtsaffinen jungen Menschen und arbeitet auch direkt mit rechtsextrem gefährdeten Jugendlichen, insbesondere wenn und solange (noch) keine anderen Bezugspersonen in deren Umfeld aktiviert sind. Im Rahmen der Unterstützung geht es um den ernsthaften Dialog zum Klären eigener Positionen und Fragen und die gemeinsame Suche nach Chancen für eine selbstbestimmte Zukunft – losgelöst von rechtsextremen Weltbildern und anderen einfachen Lösungsangeboten.

Die „Rote Linie" bietet zudem eine Unterstützung lokaler offener Jugendarbeit, Informationen und Beratung zum Umgang mit Hate Speech und Rechtsextremismus in Sozialen Medien sowie Bildungsangebote (Fort- und Weiterbildungen, Vorträge, Seminare).

2. Das Gesetzesvorhaben

Mit dem vorliegenden Gesetzesentwurf (HVSG-Entwurf) und dem Änderungsantrag ist eine Neuausrichtung des Hessischen Landesamts für Verfassungsschutz intendiert. Dem Gesetzesentwurf liegen mehrjährige Diskussionen über die notwendigen Entwicklungen und Korrekturen zugrunde, die u.a. auch auf Empfehlungen des NSU-Untersuchungsausschuss (Bund) zurückgehen:

- Erkenntnisübermittlungen an Strafverfolgungsbehörden
- Controlling beim Umgang mit Informationen und Daten
- Transparenz und Offenheit als Leitlinien der Neue Arbeitskultur
- Stärkung der parlamentarischen Kontrolle
- Regelungen für den Quelleneinsatz
- Intensivierter Informationsaustausch in den Abwehrzentren
- Verstärkter gegenseitiger Informationsaustausch Polizei und VS

- Verbesserung der Analyse- und Koordinierungsfähigkeit
- Zusammenarbeit der Landesämter und dem Bundesamt
- Intensivierung der Rechtsextremismusbeobachtung
- Neuorganisation und Neuausrichtung der Fortbildung
- Priorisierung der nachrichtendienstlichen Arbeit (Arbeitsteilung) sowie
- Aktive und verstärkte Öffentlichkeitsarbeit

Die Änderungen umfassen insbesondere den Aufgabenbereich, die eingesetzten Mittel, die Datenweitergabe, die Mitwirkungspflicht des Verfassungsschutzes.

2.1 Professionen - unterschiedliche Perspektiven und Verantwortlichkeiten

Im Folgenden wird das Gesetzesvorhaben dahingehend betrachtet, welche Auswirkungen sie auf Arbeitsfelder, Träger und Mitarbeiter*innen und die Umsetzung Sozialer Arbeit haben. Die Perspektive Sozialer Arbeit unterscheidet sich von der sicherheitsbehördlichen Sichtweise, ebenso die Rahmenbedingungen und Handlungsansätze. In der praktischen Arbeit gibt es gleichwohl Berührungspunkte mit den Sicherheitsbehörden, insbesondere der Polizei und aufgrund der Entstehungsgeschichte der „Roten Linie" zum Ausstiegsprogramm „IKARus".

Soziale Arbeit und Verfassungsschutz sind gesellschaftlich legitimierte und rechtlich gerahmte Interventionsformen mit ausgeprägten Unterschieden in der Beschreibung und Bewertung von Phänomenen, im Auftrag und in den Handlungsformen. Beide Professionen haben es bisweilen mit identischen Zielgruppen zu tun und sind einem öffentlich produzierten Erfolgs- und Erwartungsdruck ausgesetzt. Da jede Profession einer Eigenlogik folgt, sind Kooperation oder Zusammenarbeit voraussetzungsvoll (vgl. Niebling 2014). Hierbei gilt es, die unterschiedlichen Aufträge zu kennen, zu akzeptieren und fachliche Zuständigkeiten nicht zu verwischen. Dabei ist die Aufgabe des pädagogischen Handelns nicht in erster Linie die erfolgreiche Bekämpfung des Rechtsextremismus, sondern die Unterstützung und Hilfestellung für junge Menschen, ein Ansetzen an deren Problemlagen, Fragen und Formen der Weltaneignung.

2.2 Beispiel für unterschiedliche Sichtweisen

Als Beispiel für die konfligierenden Sichtweisen kann der §17 Abs 4 (HVSG-Entwurf) dienen: Daten über minderjährige Personen unter 14 Jahren sollen nicht nur beobachtet, sondern nun auch in Daten gespeichert werden dürfen. In den letzten Jahren wurden die Altersgrenzen von 16 Jahren auf 14 Jahre herabgesetzt, mit dem vorliegenden Gesetzesentwurf entfallen sie gänzlich. Hier stehen argumentativ Sicherheitsinteressen dem Schutz der Persönlichkeitsrechte der Kinder gegenüber, braucht es eine hohe datenschutzrechtliche Empfindlichkeit zur Prüfung der Erforderlichkeit dieser Regelung für die Aufgabenerfüllung.

Aus pädagogischer Sicht wäre zudem zu fragen: Was folgt aus den Kenntnissen und gespeicherten Daten? Was geschieht, wenn wahrgenommen wird, dass junge Menschen in ihren Herkunftsfamilien radikal erzogen werden, frühzeitig Interesse an Szenen entwickeln oder sich entsprechend inszenieren? Werden die für die Erziehung Zuständigen und Verantwortlichen – also Eltern und Jugendamt – einbezogen? Wird das Erziehungsprivileg der Eltern geachtet? Wird eine pädagogische Unterstützung empfohlen? Aus der Perspektive Sozialer Arbeit haben Kinder und Jugendliche ein Recht auf Förderung ihrer Entwicklung (SGB VIII) und der Staat ein Wächteramt. Familien, Schulen, Kinder- und Jugendhilfe, Sozialräume sind gefragt und in der Pflicht, wenn es darum geht, das

Aufwachsen junger Menschen frühzeitig zu begleiten, sie für Demokratie und gesellschaftliche Mitgestaltung zu gewinnen, zu begeistern, ihnen, wo dies noch unzureichend gelingt, Lebens- und Zukunftschancen, ergänzende Erfahrungen und Räume für Experimente, Konflikte und Identitätsbildung zu ermöglichen. Wo den Bezugspersonen und Regelstrukturen die Ressourcen fehlen, sind diese zur Verfügung zu stellen.

Das Beispiel zeigt, dass es in der Kommentierung nicht darum geht, fachliche oder politische Konflikte im Konsens aufzulösen, sondern auch zu benennen, wo es auch unterschiedliche und unvereinbare Interessen gibt und worin funktionale Alternativen liegen. Auf dieser Grundlage beschränken wir unsere Stellungnahme zum Gesetzesvorhaben auf zwei zentrale Punkte:

- Mitwirkungsaufgaben (Zuverlässigkeits- und Sicherheitsüberprüfungen)
- Die Öffnung des Verfassungsschutzes (Präventionsarbeit)

Zu fragen ist, inwieweit die Gesetzesänderungen den formulierten Anliegen gerecht werden, zielführend und aus unserer Sicht im Sinne Sozialer Arbeit angemessen sind.

3. Mitwirkungsaufgaben (Zuverlässigkeits- und Sicherheitsüberprüfungen)

Der Gesetzesentwurf sieht vor, den Katalog der Mitwirkungsaufgaben um die Befugnis zu erweitern, bei weiteren Sicherheitsüberprüfungen mitzuwirken. Benannt ist die Gruppe der „Personen, die in mit Landesmitteln geförderten Beratungsstellen zur Prävention und Intervention gegen verfassungsfeindliche Bestrebungen oder in mit Landesmitteln geförderten Projekten eingesetzt sind oder eingesetzt werden" sowie „in beratenden Gremien zur Prävention und Intervention gegen verfassungsfeindliche Bestrebungen tätig sind oder tätig werden sollen" (§21 Abs 1 Nr. 2 Buchst. l HVSG). Hier ist eine Mitwirkung bei Zuverlässigkeitsüberprüfungen vorgesehen.

Dieses Vorhaben wird begleitet durch das Vorhaben des Landes Hessen, „Sicherheitsüberprüfungen" in die Zuwendungsbestimmungen (Punkt 9) von Trägern und den Arbeitsverträgen der Personen aufzunehmen, die im Rahmen des Bundesprogramms „Demokratie Leben!" und des Landesprogramms „Hessen – Aktiv für Demokratie und gegen Extremismus" gefördert werden. Hiervon wäre der St. Elisabeth-Verein und die Beschäftigen der „Roten Linie" unmittelbar betroffen.

Mit dem Bundesprogramm „Demokratie leben! Aktiv gegen Rechtsextremismus, Gewalt und Menschenfeindlichkeit" (Laufzeit: 2015 – 2019) fördert das Bundesministerium für Familie, Senioren, Frauen und Jugend ziviles Engagement und demokratisches Verhalten auf kommunaler, Landes- und Bundesebene. Vereine, Projekte und Initiativen, die sich der Förderung von Demokratie und Vielfalt widmen und gegen Rechtsextremismus, Rassismus, Antisemitismus, islamistischen Extremismus und andere Formen von Demokratie- und Menschenfeindlichkeit, gegen Gewalt, Hass und Radikalisierung arbeiten, werden durch das Bundesprogramm unterstützt. Einige Modellprojekte widmen sich den Themenbereichen Rassismus und rassistische Diskriminierung sowie Antidiskriminierung und Frühprävention im Vorschulalter.

Zu den Zuwendungsbestimmungen haben im vergangenen Jahr Gespräche mit Vertretern des Innenministeriums und zu dem ersten Gesetzesentwurf ein Gespräch mit Herrn Staatsminister Peter Beuth stattgefunden. In diesen Gesprächen haben die Träger ihre Fragen und ihre Haltung zum Ausdruck gebracht. Eine überarbeitete Fassung der Zuwendungsbestimmungen liegt noch nicht vor.

Das aktuelle Gesetzesvorhaben regelt die Berechtigung zur Mitwirkung an Überprüfungen; es begründet nicht deren Notwendigkeit.

3.1 Demokratieförderung als Risiko- oder Gefährdungslage?

Die Schaffung eines „originären Mitwirkungstatbestand[es] im Rahmen der Präventionsaufgabe" (S. 56) setzt voraus, dass es

a) eine fachlich abgrenzbare „Präventionsaufgabe" gibt und
b) sich aus dieser Tätigkeit die Notwendigkeit einer Zuverlässigkeitsüberprüfung ergebe.

Dieses Gesetz ist nicht der richtige Ort dafür darzulegen, inwieweit die Träger oder die tätigen Personen auf Grund ihrer Tätigkeit unmittelbaren Einfluss auf die Sicherheit nehmen, so dass eine Gefährdungslage behoben oder vermieden werden muss. Festzuhalten ist jedoch, dass die Personen weder Zugang zu Sicherheitsbereichen (Flughafen, Atomanlagen,...), noch Zugriff auf Verschlusssachen haben und nicht in der Gebäudesicherung oder Detekteien tätig sind.

Vergegenwärtigt man sich die Praxis der mannigfachen Angebote der geförderten Projekte, so erkennt man, dass diese mit Angeboten der Regelstruktur eng verwandt ist und mit ihnen verzahnt sind. Hierzu zählen Veranstaltungen zur politischen Bildung, lokale Partizipationsangebote und Formen der Beratung und Unterstützung in der praktischen Jugend- und Sozialen Arbeit. Das Arbeitsfeld ist keine eigenständige „Präventionsaufgabe", sondern die Perspektive des Vermeidens ist verknüpft mit einer Perspektive des Förderns. Es handelt sich um einen Förderbereich, der reguläre Tätigkeitsfelder innerhalb der Sozialen Arbeit, der Kinder- und Jugendhilfe, der Erwachsenenbildung und der politischen Bildung unter einem spezifischen und zugleich vielfältigen thematischen Fokus unterstützt.

Ihre Arbeit besteht darin, fachliche Erkenntnisse didaktisch aufzubereiten, Foren für politische Debatten anzubieten, Vernetzung zu fördern, Opfer zu unterstützen etc. Ihre Arbeit ist zumindest in Teilen vergleichbar mit anderen Trägern der politischen Bildung, vielen Feldern der Sozialen Arbeit und Kinder- und Jugendhilfe oder der Arbeit der Landeszentrale für politische Bildung. Jede Fachkraft der Kinder- und Jugendhilfe, die dauerhaft Kontakt mit jungen Menschen hat (z.B. in Kindertagesstätten), wäre als entsprechendes „Sicherheitsrisiko" einzustufen. Im vorliegenden Fall beträfen die Überprüfungen sogar Personal außerhalb pädagogischer Tätigkeiten, z.B. der Projektadministration.

Gerade im Feld der primären „Präventionsaufgabe" finden sich zahlreiche Tätigkeiten, die andernfalls auch unter dem Label der „Förderung" oder „Bildung" umgesetzt werden. Es ist maßgeblich die politische Rahmung, die den Unterschied macht. Aus unserer Sicht ist die vorausgesetzte Plausibilität einer Notwendigkeit von Überprüfungen nicht gegeben – entsprechendes gilt für die Aufnahme dieses Träger- und Personenkreises in das Verfassungsschutzgesetz.

3.2 Qualitätssicherung

Die im Änderungsantrag vorgesehene Ausnahme etablierter und öffentlich anerkannter Träger trägt diesem Umstand insofern Rechnung, als er auf die Fachlichkeit der Träger abzielt. Träger der Sozialen Arbeit sind bereits in vielfältiger Weise engagiert, ihre Fachkräfte für Risiken und eine Kultur der Achtsamkeit zu sensibilisieren und in ihrer Fachlichkeit zu fördern. Hierzu dienen Leitbilder, Informationen, Richtlinien und Selbstverpflichtungen, kollegiale Beratungen, Supervisionen sowie

weitere Maßnahmen der Qualitätssicherung und Personalentwicklung. Die Träger haben der Öffentlichkeit gegenüber zu belegen, dass ihr Tun fachlich integer ist und dass es dem Allgemeinwohl dient. Träger und Beschäftigte sehen sich Fokus und wissen, dass jede Auffälligkeit eine hohe mediale Aufmerksamkeit nach sich ziehen kann. Überprüfungen im Vorfeld und neue Regelwerke werden daran nichts ändern. Es gilt da zu intervenieren, wo Vereinbarungen oder Recht gebrochen wird. Zur Fachlichkeit gehört aus unserer Sicht ebenso, bei einem konkreten Verdacht als Träger durch geeignete Mittel zur Aufklärung des Verdachts beizutragen sowie die Fachkräfte angemessen zu schützen.

Auch bei Trägern, die bislang nicht über die im Gesetz beschriebenen Anerkennungen oder Erfahrungen verfügen, steht aus unserer Sicht der Nachweis der Fachlichkeit im Vordergrund. Hier haben die geförderten Träger ihre Bereitschaft signalisiert, neue Träger in der Qualitätsentwicklung zu unterstützen.

3.3 Gesetzliche Grundlage und Verfahren

Aus dem Gesetzesentwurf ist nicht erkennbar, auf welcher gesetzlichen Grundlage und zur Abwendung welcher Risiken eine Zuverlässigkeitsüberprüfung durchgeführt werden soll. Damit bleiben sowohl das Überprüfungsverfahren und die Maßnahmen als auch das weitere Vorgehen zur Klärung bei vorhandenen Verdachtsmomenten oder mögliche Rechtsmittel für Betroffene und Träger offen. Hier fehlt es an einem Verweis auf eine gesetzliche Grundlage und Regelung, wie sie im Sicherheitsüberprüfungsgesetz, Luftsicherheitsgesetz oder im Waffenrecht vorliegen. „Zuverlässigkeit" selbst ist ein schwieriger und unbestimmter Rechtsbegriff, es gibt keine gesetzlichen Regeln darüber, bei welcher Straftat und Verhaltensweise jemand unzuverlässig ist, ein Umstand der zur Verhaltensunsicherheit der beschäftigten Personen führen dürfte. Die vorgesehenen Regelungen zur Sicherheits- bzw. Zuverlässigkeitsüberprüfung (§21 Abs 1 Nr. 2 Buchst. I HVSG) rufen daher rechtliche Bedenken hervor. Aus unserer Sicht bestehen Bedenken, ob diese Regelung verhältnismäßig ist.

Der praktische Zwang zur Einwilligung in eine Sicherheitsüberprüfung greift bei den Betroffenen in Art. 12 GG und bei den Trägern, die dann die betroffenen Personen nicht beschäftigen können in Art 12,14 GG ein. Wenn durch die Förderbedingungen – wie im letzten vorliegenden Entwurf – dem Projektnehmer auferlegt werden soll, Arbeitsverhältnisse mit solchen Mitarbeitenden zu kündigen, bei denen erhebliche Bedenken gegen eine Verfassungstreue bestehen oder gar Extremismus festgestellt worden ist, wird in die Rechtssphäre des Mittelempfängers in einer Art und Weise eingegriffen, die durch den Zweck der Sicherung – nämlich den adäquaten Mitteleinsatz – nicht gerechtfertigt ist. Wir sehen hier einen erheblichen Konflikt mit dem Übermaßverbot, da die Mittelvergabe davon abhängig gemacht wird, dass die Projektträger im Arbeitsvertrag bereits eine Kündigung wegen mangelnder Verfassungstreue festlegen, sich also in einer arbeitsrechtlich bedenklichen Weise vorab binden müssen (zumal im Kündigungsverfahren die Mitarbeitervertretung einzubeziehen und letztlich – wenn angerufen – das Arbeitsgericht über die Wirksamkeit entscheidet.

3.4 Kritik aus dem Feld der Distanzierungs- und Ausstiegshilfen

Distanzierungs- und Ausstiegshilfen umfassen nur einen sehr kleinen Teilbereich der Angebote die im Rahmen von Bundes- und Landesprogrammen gefördert werden. Gleichwohl liegt eine Stellungnahme der Bundesarbeitsgemeinschaft „Ausstieg zum Einstieg" e.V. vor, die sich kritisch mit den hessischen Förderrichtlinien auseinander setzt. Hier wird zu bedenken gegeben, dass diese

Überprüfung negative Auswirkungen auf zivilgesellschaftliche Distanzierungs- und Ausstiegshilfen haben, da sie geeignet sind, das Vertrauen potentieller Aussteiger*innen in die Träger zu untergraben (BAG 2017).

Der Einsatz von Aussteiger*innen ist eine sensible und fachlich verantwortungsvolle Aufgabe und findet in Hessen derzeit nicht in geförderten Projekten statt. Doch auch aus diesem Kontext liegt eine Stellungnahme zum Hessischen Gesetzesentwurf vor. Weilnböck weist auf Konflikte von Sicherheitsüberprüfungen mit Standards hin, die im Rahmen des Radicalisation Awareness Network (RAN) auf europäischer Ebene entwickelt wurden: „Die meisten der hoch entwickelten Ansätze von Prävention und Ausstiegsarbeit z.B. in den skandinavischen Ländern arbeiten auch mit sog. Ehemaligen und Ausgestiegenen bzw. mit ehemals szenenahen Personen. Dies hat in vieler Hinsicht sehr positive und integrative Wirkungen gezeitigt und wird seither als europäischer Good Practice Standard formuliert." Man werde „davon ausgehen müssen, dass dieser wichtige Einbezug von Ehemaligen/ Ausgestiegenen und ehemals szenenahen Personen stark behindert und mitunter kompromittiert würde. Denn es wäre unrealistisch anzunehmen, dass die verschiedenen Dienste auf Länder- und Bundeseben verlässlich jede*n Aussteiger*in nachrichtendienstlich verifizieren könnten – zumal bei der Masse der sog. stillen Ausstiege" (Weilnböck, 2017). Die Diskussionen im Feld der Sozialen Arbeit zielen eher darauf ab, das Potential von Distanzierungshilfen und Ausstiegsarbeit zu erweitern, z.B. durch ein Zeugnisverweigerungsrecht.

3.5 Einschätzung

Die Benennung der Träger und Personen im Rahmen der Mitwirkungspflichten drückt ein irritiertes Grundvertrauen des Staates in die Träger der Kinder- und Jugendhilfe und der politischen Bildung sowie zivilgesellschaftliche Akteure aus. Ein solcher Ausdruck staatlichen Misstrauens – im Sinne eines Generalverdachts – gegenüber den zivilgesellschaftlichen Initiativen schwächt deren Legitimation, beschädigt deren Ansehen und beschränkt deren demokratiefördernde Potentiale.

Im Gesamtbild empfehlen wir eine ersatzlose Streichung des §21 Abs 1 Nr. 2 Buchstabe i HVSG. Für das Gesetzesvorhaben stellt sich letztlich die Frage, inwieweit eine dezidierte Auflistung der Personengruppen im Rahmen dieses Gesetzes notwendig ist oder eine Benennung der berechtigenden oder verpflichtenden gesetzlichen Grundlagen für eine Mitwirkung (analog zum Niedersächsischen Verfassungsschutzgesetz,§ 3, Abs. 4) nicht zielführender ist. Im Sinne der angestrebten Transparenz böte die Gesetzesänderung Gelegenheit, Voraussetzungen, Kriterien und Maßnahmen für differenzierte Eingriffsstufen zu beschreiben. „Die Abläufe und Entscheidungskriterien sind gegenüber den Betroffenen möglichst plausibel und transparent zu machen" (AG Niedersachsen, S. 23f). Hier wirken die §§6-8 des Niedersächsischen Verfassungsschutzgesetzes deutlich kompakter.

Da die Mitwirkungsaufgaben (Sicherheitsüberprüfungen) sich in den letzten Jahren zu einem bedeutsamen Arbeitsbereich des Verfassungsschutzes entwickelt haben und mit einer entsprechenden Ressourcenbindung einhergeht, wäre auch für Hessen eine Evaluierung dieser Arbeit zu bedenken. Im Sinne der Transparenz wäre zudem gesetzlich zu regeln, dass der Verfassungsschutz in allen Phasen neben den belastenden Hinweisen auch solche recherchiert und dokumentiert, die gegen eine Einstufung als Beobachtungsobjekt sprechen (§6, Abs. 5 Nds VSG).

4. Präventions- und Öffentlichkeitsarbeit

Das Gesetzesvorhaben verfolgt das Ziel, durch „Öffnung und Transparenz" gesellschaftliches Vertrauen und Ansehen der Verfassungsschutzbehörde zu vergrößern. Gemäß dem vorliegenden Gesetzesentwurf soll die Öffentlichkeitsarbeit maßgeblich durch einen Auf- und Ausbau von Präventionsmaßnahmen befördert werden. Sie bieten Gelegenheit sich als moderne und transparente Behörde zum Schutz der Allgemeinheit darzustellen.

§2 Abs. 1 Satz 3 HVSG sieht nun einen expliziten Präventionsauftrag des Landesamtes vor. In der Begründung heißt es, damit verbunden sein soll ein „deutliches Signal zum Ausbau der amtsinternen Präventionsstrukturen in allen Phänomenbereichen [...], aber auch die Grundlage für eine effektive und dauerhafte Unterstützung des Hessischen Informations- und Kompetenzzentrums (HKE)" (HVSG-Entwurf, S. 33). Hier geht es neben der Veröffentlichung des Jahresberichtes „einerseits darum, die Öffentlichkeit über die Erscheinungen von Extremismus und Terrorismus aufzuklären" (ebd., S. 33), „andererseits ein gezieltes Tätigwerden zum Verhindern des Ausbreitens extremistischer oder terroristischer Bestrebungen" (ebd., S. 34f). Die Neufassung soll darüber hinaus „die Grundlage für weitere Präventionsprogramme und -aktivitäten" (ebd., S. 35) bilden.

4.1 Wer öffnet sich wem?

Der Verfassungsschutz ist bereits aktuell z.B. an Schulen tätig und führt Lesungen und Theaterprojekte durch („Wir gegen Salafisten"). Angesichts dieser Praxis stellt sich die Frage: Wer öffnet sich hier wem? Der Verfassungsschutz sollte sich der Gesellschaft öffnen. Diese Veranstaltungen finden aber außerhalb statt. Andere Dienste haben hier angemessenere Lösungen gefunden (z.B. Ausstellungen, eigene Veranstaltungsreihen oder das Besucherzentrum des BND). Die Gesetzesvorlage legt nahe, dass sich im Gegenteil die Schulen dem Verfassungsschutz öffnen sollen. Das Präventionsangebot enthält somit eine Handlungsaufforderung des Verfassungsschutzes an die Schulen. Hier deutet sich eine „freundliche Übernahme" der Bildungs- und Präventionsarbeit durch den Verfassungsschutz an. Diese Tätigkeit betrachten wir mit großer Skepsis und Sorge.

Es gibt bereits eine Reihe von Trägern der politischen Bildung und der Sozialen Arbeit mit ähnlichen Angeboten. Ein eigenständiges Arbeitsfeld des Verfassungsschutzes käme hier dem Aufbau einer Parallelstruktur gleich, zudem dem Ausbau eines Arbeitsfeldes, das nicht zum Kerngeschäft des Verfassungsschutzes zählt und zählen sollte. Hierauf verweist auch mit Bezug zum Bundesland Bayern Andreas Vollmer aus Sicht der Gewerkschaft der Polizei. Es sei „nicht erkennbar, wie die genannten Maßnahmen ohne Reduzierung der Kernfacharbeit umgesetzt werden können", insbesondere „die Zusatzaufgaben (wie Prävention) bedürfen einer sorgsamen Analyse."

4.2 Institutionelle Trennung und Subsidiaritätsprinzip

Für eine Umsetzung von staatlichen Aufgaben wie der politischen Bildung gilt das Subsidiaritätsprinzip. Der Staat soll Aufgaben nur dann umsetzen, wenn dies nicht durch eine kleinere, nachgeordnete Einheit erfolgen kann oder (wie im Rahmen der Jugendhilfe) keine geeigneten „Einrichtungen, Dienste und Veranstaltungen von anerkannten Trägern der freien Jugendhilfe betrieben werden oder rechtzeitig geschaffen werden können" (§ 4 Abs. 2 SGB VIII).

Die pädagogische Praxis und Erforschung der Prävention von Rechtsextremismus hat bereits eine über 20jährige Tradition, die trotz unterschiedlicher gesellschaftlicher Ursachen und Ziele z.T. auch

auf religiös begründete Phänomenbereiche übertragen werden können (Glaser/Johannson 2014). Schulen sind seit jeher Experimentierfeld aller „klassischen" Präventionsprogramme und -maßnahmen. Dabei gelten isolierte Kurzzeitmaßnahmen nicht als der Königsweg, sondern wird eine strukturelle Verankerung der schulischen Präventionsarbeit angestrebt. Insoweit kann die „Radikalisierungsprävention" aus den Fehlern der „allgemeinen" Prävention und der Kriminalprävention lernen. Vor diesem Hintergrund ist eine interdisziplinäre Klärung der Rolle des Verfassungsschutzes in der präventiven Arbeit angezeigt: Was soll, kann und muss der Verfassungsschutz leisten? Was leisten andere bereits oder könnten im Sinne der Subsidiarität andere auch leisten?

Verfassungsschutzbehörden, die politische Bildung betreiben, konkurrieren mit anderen Bildungsträgern. Selbst aus Sicht des Verfassungsschutzes wird konstatiert: „Da der Verfassungsschutz seine Leistungen üblicherweise kostenlos anbietet, kann es zu einem Verdrängungswettbewerb kommen" (Dr. Silke Wolf 2013). Aus unserer Sicht ist es bedenklich, wenn Mitarbeiter*innen des Verfassungsschutzes auf Informationsveranstaltungen für Lehrkräfte ihre Projekte mit Schüler*innen bewerben und dabei auf die vorhandenen finanzielle Mittel für Projekte an Schulen hinweisen.

Anders als im Bereich der Aufklärung der Öffentlichkeit und der Beratung von Einrichtungen über extremistische Bestrebungen kann die unmittelbare Beteiligung von Fachkräften des Verfassungsschutzes in der unmittelbaren pädagogischen Arbeit mit Jugendlichen kontraproduktiv sein. Durch die in der sicherheitsbehördlichen Präventionsarbeit angelegte „Logik des Verdachts" besteht das Risiko, die Zielgruppe negativ zu markieren bzw. zu stigmatisieren. (Dr. Wiebke Steffen 2015, S. 18) „Diese Gefahr besteht insbesondere dann, wenn über die Zielgruppe langwierige gesellschaftliche Debatten geführt werden, in der die Betroffenen als problembeladene oder gar gefährliche Gruppe dargestellt werden" (Ceylan/Kiefer 2013, S. 102).

Der Landesjugendring Rheinland-Pfalz kommentiert: „Die Verantwortung für politische Bildung liegt – nicht zuletzt aus Gründen eines Selbstverständnisses demokratischer Wertevielfalt - vor allem bei den für pädagogische Bildungsprozesse qualifizierten Organisationen wie Jugendverbänden, Schulen und den Landeszentralen und der Bundeszentrale für politische Bildung". Aus dieser Sicht ist der Verfassungsschutz aufgrund seiner Stellung im institutionellen Gefüge (und nicht auf Grund von Kenntnissen oder Kompetenzen) kein günstiger Anbieter von Bildungsmaßnahmen oder sozialer Arbeit.

Aus unserer Sicht spiegelt sich in dem angekündigten Auf- und Ausbau einer Präventionsarbeit durch den Hessischen Verfassungsschutz die Versuchung einer sicherheitspolitischen Dominanz, die Erinnerungen an Diskussionen die Anfang der 90er Jahre zur „Versicherheitlichung der Prävention" durch die Dominanz der Polizei weckt.

Präventionsangebote müssen nicht durch den Verfassungsschutz neu „erfunden" und alte Debatten nicht erneut geführt werden. „Bei dem geplanten gesetzlich verankerten Vorhaben vermischen sich dabei Aufgabengebiete, die aus guten Gründen unterschiedliche Strategien und Lösungskonzepte vorsehen. Soziale Arbeit und Sicherheitspolitik sind zwei gesellschaftlich notwendige Handlungsfelder, die jedoch unterschiedlichen Zielen folgen und diese Ziele mit verschiedenen Maßnahmen und Methoden realisieren. Eine Trennung beider Gebiete ist dringend notwendig, um weiterhin eine professionelle und gelingende Soziale Arbeit zu ermöglichen." (Stellungnahme der Deutschen Gesellschaft für Soziale Arbeit 2017)

Analoge Konfliktlinien finden sich im Feld der Ausstiegsarbeit, die wesentlich auf dem Vertrauen in die Aufrichtigkeit der Helfer und, methodisch, auf Instrumenten sozialer Arbeit beruht. Daher bezweifelt z.B. Jaschke, ob Sicherheitsbehörden die geeigneten Akteure sind und empfiehlt, diese Aufgabe den zivilgesellschaftlichen Einrichtungen zu überlassen (Jaschke 2015, 250).

Prävention ist eine Aufgabe, die landesweit einer von allen Akteursgruppen gemeinsam erarbeiteten Strategie folgen sollte. Hier wäre im Sinne von Arbeitsteilung und Kooperation zu schauen, welchen Beitrag der Verfassungsschutz leisten kann und muss - und welche Angebote andere Träger leisten können. So werden ineffektive Insellösungen und Doppelstrukturen, Finanzierungsungleichgewichte und Konkurrenzen, Deutungsdominanzen und Verdrängungseffekte vermieden.

4.3 Stärkung der Hessischen Landeszentrale für politische Bildung

Aus unserer Sicht ist es zielführender, die Hessische Landeszentrale für politische Bildung zu stärken und die Aufgaben der Demokratiestärkung, der Gewaltprävention, der politischen Bildung und der Förderung der Toleranz somit in einer Stelle außerhalb des Verfassungsschutzes zusammenzuführen und gegebenenfalls auszubauen.

„Die Hessische Landeszentrale für politische Bildung ist eine Einrichtung des Landes Hessen und unmittelbar dem Hessischen Ministerpräsidenten zugeordnet. Als einzige hessische Einrichtung führt sie politische Bildungsarbeit im öffentlichen Auftrag durch", so steht es auf ihrer Homepage. Die Hessische Landeszentrale für politische Bildung (HLZ) bearbeitet diese Aspekte z.T. seit vielen Jahren mit eigenen Referaten, einem umfangreichem Spektrum an Bildungsformaten zur Prävention und Auseinandersetzung mit fremdenfeindlichen, rassistischen und antisemitischen Verhaltens- und Denkmustern. Dabei reichen die Angebote von Print- und Multimediaangeboten über Fachtagungen, Kongresse, Qualifizierungsmaßnahmen sowie Projekte bis hin zur finanziellen Förderung von Initiativen und Trägern in den Bereichen der Extremismusprävention. In Dossiers, Publikationen und anderen Formaten wird umfassendes Informationsmaterial in Text und Bild bereitgestellt.

4.4 Einschätzung

Der hessische Verfassungsschutz hat keinen Bildungsauftrag und er sollte diesen auch nicht schleichend erhalten. Durch seine Kenntnisse und Kompetenzen ist der Verfassungsschutz ein wichtiger Partner, aber er sollte kein eigenständiger Anbieter von Angeboten der politischen Bildung sein. Der wahrgenommene Druck, neue Wege zu suchen, offen zu sein für neue Überlegungen und kreative Ideen sollte nicht – wie im Gesetzentwurf angelegt – zu einer Verschränkung von Aufgaben und damit einhergehenden Grauzonen, Konfliktpotentialen und Zuständigkeitskonflikten führen.

Öffentlichkeitsarbeit soll den Verfassungsschutz als solchen transparent werden lassen. Sie soll seine Aufgaben, deren gesetzliche Verankerung oder seine Arbeitsweise erläutern. „Neben der Fachkompetenz muss daher auch die Glaubwürdigkeit eine Rolle bei der Öffentlichkeitsarbeit der Verfassungsschutzbehörden spielen. Die Behörden müssen die Bereitschaft aufbringen, sich auch unangenehmen Fragen zu stellen. Dabei wird es aber auch darum gehen, Wege zu finden, die Erfolge der Arbeit darzustellen, um die Wirksamkeit der Institution Verfassungsschutz und seine Legitimität transparent zu machen" (Spielberg, S.110).

Dies dient dem Abbau von Vorbehalten und der Erläuterung von Aufgabe und Funktionsweise des Verfassungsschutzes als Abwehrinstrument. Auch die Informationspflicht des Verfassungsschutzes gegenüber der allgemeinen Öffentlichkeit über seine Beobachtungsfelder steht nicht in Frage.

Allein die Erziehungs- und Bildungsarbeit durch den Verfassungsschutz ist aus unserer Sicht problematisch. Die Beziehung zwischen diesen beiden gegensätzlichen Aspekten „Information und Aufklärung" und „Prävention" verlangt nicht nur nach einer Klärung, sondern nach einer institutionellen Trennung , damit eine Vermischung von Motiven und Erwartungen oder eine mangelhafte Klarheit über Motive, Handlungsweisen und deren Konsequenzen vermieden wird. Diese Aufgabe sollte bei der Hessischen Landeszentrale für politische Bildung angesiedelt sein.

5. Fazit

Aus unserer Sicht wird das Ansehen des Verfassungsschutzes zentral von der Leistungsfähigkeit in seiner Kernaufgabe, der Qualität seiner Analyse von Daten und Erkenntnissen abhängen – und davon dass diese Qualität als Beitrag zur Sicherheit aller Bürgerinnen und Bürger wahrgenommen wird.

Information und Aufklärung, nicht aber Präventionsarbeit gehört hier zu den Aufgaben. Fachlich ist Präventionsarbeit bei der Hessischen Landeszentrale für politische Bildung anzusiedeln oder subsidiär von kommunalen oder Freien Trägern umzusetzen. Eine sicherheitspolitische Dominanz pädagogischer Arbeitsfelder ist abzulehnen.

Die Benennung der Träger und Personen im Rahmen der Mitwirkungspflichten drückt ein irritiertes Grundvertrauen des Staates in die Träger der Kinder- und Jugendhilfe und der politischen Bildung sowie zivilgesellschaftliche Akteure aus. Ein solcher Ausdruck staatlichen Misstrauens – im Sinne eines Generalverdachts – gegenüber den zivilgesellschaftlichen Initiativen, schwächt deren Legitimation, beschädigt deren Ansehen und beschränkt deren demokratiefördernde Potentiale.

Vor dem Hintergrund dargelegter rechtlicher Bedenken empfehlen wir im Gesamtbild eine ersatzlose Streichung des §21 Abs 1 Nr. 2 Buchst. i HVSG und stattdessen eine Benennung der berechtigenden oder verpflichtenden gesetzlichen Grundlagen für eine Mitwirkung des Verfassungsschutzes an Sicherheits- oder Zuverlässigkeitsüberprüfungen.

6. Literatur

Arbeitsgruppe zur Reform des Niedersächsischen Verfassungsschutzes: Handlungsempfehlungen der Arbeitsgruppe zur Reform des Niedersächsischen Verfassungsschutzes. Hannover, 16.April 2014

Bundesarbeitsgemeinschaft „Ausstieg zum Einstieg": Positionspapier zum Gesetzesvorhaben „Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen" – Berlin 2017.

Ceylan, Rauf/Kiefer, Michael: Salafismus. Fundamentalistische Strömungen und Radikalisierungsprävention. Wiesbaden 2013.

Glaser, Michaela/Johansson, Susanne: Erfahrung nutzen? Übertragbarkeit von Methoden der Rechtsextremismusprävention bei der Prävention von Islamismus. Berlin 2014 [abgerufen unter www.bpb.de/186664/methoden]

Grumke, Thomas / van Hüllen, Rudolf: Der Verfassungsschutz. Grundlagen, Gegenwart, Perspektiven. - Opladen 2016.

Hessisches Landesamt für den Verfassungsschutz: Leuchtturmprojekt: „Wir gegen Salafisten" an Wiesbadener Schulen. [abgerufen unter: https://lfv.hessen.de/pr%C3%A4vention/veranstaltungen/leuchtturmprojekt-%E2%80%9Ewir-gegensalafisten%E2%80%9C-wiesbadener-schulen]

Hessische Landeszentrale für politische Bildung: Über uns. [abgerufen unter: http://www.hlz.hessen.de/hlz.html]

Jaschke, Hans-Gerd: Bekämpfung des Terrorismus – Was leisten Deradikalisierungsprogramme? Die Polizei 9. 2015, 250–255.

Landesjugendring Rheinland-Pfalz: Bildung ist keine Aufgabe des Verfassungsschutzes. Beschluss der 106. Vollversammlung des Landesjugendringes Rheinland-Pfalz. – Osthofen 2013.

Niebling, Torsten: Formen und Einflussfaktoren der Kooperation von Jugendhilfe im Kontext von Einstiegsprozessen in rechtsextreme Szenen. In: Hagen, Björn: Jugendhilfe in Kooperation. Erziehungshilfen – Kinder- und Jugendpsychiatrie – Polizei – Justiz. (Beiträge zur Theorie und Praxis der Jugendhilfe 14). Hannover 2016, S. 137-145.

Niedersächsisches Verfassungsschutzgesetz (NVerfSchG) [Online abgerufen unter http://www.schure.de/12000/nverfschg.htm#p30]

Salafismus-Prävention in der Schule. In: Gießener Allgemeine Zeitung vom 26. Mai 2017

Spielberg, Georg : Spagat zwischen „Geheim" und „Transparent". In: Verfassungsschutz 1952–2012. Festschrift zum 60. Jubiläum des Landesamts für Verfassungsschutz Baden-Württemberg. Stuttgart 2012, S. 97-110.

Steffen, Wiebke: Prävention des internationalen Terrorismus in Deutschland – eine Zustandsbeschreibung. Langfassung. – Mainz 2015.

Stellungnahme der Deutschen Gesellschaft für Soziale Arbeit (DGSA) zu den geplanten Zuwendungsrichtlinien für Demokratieförderprojekte in Hessen – Sersheim 2017.

Vollmer, Andreas: Reformen beim Verfassungsschutz. Mitarbeiter einbeziehen. In: Deutsche Polizei 2016 (2), S. 4-8.

Weilnböck, Harald: Positionspapier von Cultures Interactive e.V. zum Gesetzesvorhaben „Gesetz zur Neuausrichtung des Verfassungsschutzes" in Hessen. – Berlin 2017.

Wolf, Silke: Verfassungsschutz als Demokratiedienstleister. In: Berliner Forum Gewaltprävention, Nr. 49. – Berlin 2013, S. 61-65.

UNIKASSEL
VERSITÄT

Fachbereich
Wirtschaftswissenschaften

Institut für
Wirtschaftsrecht

Prof. Dr. Gerrit Hornung, LL.M.

Universität Kassel - FB 07 - FG Öffentliches Recht, IT-Recht und Umweltrecht
Henschelstr. 4, D-34127 Kassel

Universität Kassel
Fachgebiet Öffentliches Recht,
IT-Recht und Umweltrecht
Henschelstr. 4
34127 Kassel

gerrit.hornung@uni-kassel.de
fon +49-561 804-7923
fax +49-561 804-3621

Sekretariat: Lena Butterweck
fon +49-561 804-7924
lena.butterweck@uni-kassel.de

05.02.2018

Stellungnahme

zur öffentlichen Anhörung zu dem Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen - Drucks. 19/5412 - sowie dem Änderungsantrag der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN - Drucks. 19/5782 -

Zusammenfassung der Ergebnisse

1. Das Ziel des Gesetzentwurfs ist sehr begrüßenswert, weil die bisherigen Regelungen sowohl in der Struktur als auch in vielen Inhalten nicht mehr den verfassungsrechtlichen Rahmenbedingungen und den Erkenntnissen aus Wissenschaft und Praxis, aber auch den jüngeren politischen Bewertungen der Materie entsprechen.

2. Die Grundausrichtung der gesetzlichen Regelung (v.a. die viel präziseren Regelungen und die vielfach erreichte Harmonisierung mit dem Bundesrecht) ist nachvollziehbar und überzeugend.

3. Es sollte erwogen werden, die Aufgaben im Bereich der Organisierten Kriminalität (§ 2 Abs. 2 Nr. 5 HVSG-E) zu streichen. Sie gehören zu den klassischen Aufgaben der Polizei- und Strafverfolgungsbehörden; teilweise wird eine entsprechende Aufgabe für die Verfassungsschutzbehörden sogar für verfassungswidrig gehalten. Es handelt sich außerdem um eine Anomalie im deutschen Verfassungsschutzrecht, die es ansonsten nur in Bayern und im Saarland gibt.

4. Die Regelungen zur Quellen-Telekommunikationsüberwachung (§ 6 Abs. 2-4 HVSG-E) halten die Vorgaben des Bundesverfassungsgerichts ein. Es wird allerdings in der Praxis sehr schwer werden, die Vorgaben aus § 6 Abs. 2 Nr. 1 HVSG-E einzuhalten. Das Bundesverfassungsgericht hat explizit betont, dass dies strikt umzusetzen ist und entsprechende Ermächtigungsgrundlagen ansonsten bis auf weiteres leer laufen.

5. Angesichts der grundrechtlichen Probleme der Online-Durchsuchung, der Schwierigkeiten, ihre technischen und rechtlichen Wirkungen zu begrenzen sowie der grundsätzlichen Zuständigkeit der Polizeibehörden für die genannten Aufgaben, denen die Maßnahme dienen soll, sollte § 8 HVSG-E gestrichen werden.

6. Wenn die Bestimmungen zur Online-Durchsuchung nicht gestrichen werden, sind sie zu überarbeiten, weil sie in der vorliegenden Fassung des Gesetzentwurfs verfassungswidrig sind. Die Eingriffsschwelle ist zwar hinreichend, die zu schützenden Rechtsgüter sind jedoch durch den Verweis auf § 7 Satz 1 Nr. 3 HVSG-E zu weit gefasst. Die Weiterverweisungen auf § 3 Abs. 2 (Adressaten), § 3a (Kernbereichsschutz) und § 3b (Berufsgeheimnisträger) des Artikel 10-Gesetzes erfüllen in allen drei Fällen nicht die Vorgaben des Bundesverfassungsgerichts. Überdies sind die Regelungen in § 9 Abs. 1 Satz 2, Abs. 4 HVSG-E für die Online-Durchsuchung unverhältnismäßig.

7. Die Bestimmungen zum verdeckten Einsatz technischer Mittel zur Wohnraumüberwachung (§ 7 HVSG-E) sind ganz überwiegend verfassungskonform. Auch hier entsprechen die drei Verweise auf § 3 Abs. 2, § 3a und § 3b Artikel 10-Gesetz jedoch nicht den Vorgaben des Bundesverfassungsgerichts. Die Regelung ist insoweit verfassungswidrig.

8. Die Regelung zur automatisierten Datenanalyse (§ 25a HSOG-E in der Fassung des Änderungsantrags) ist ein begrüßenswerter Schritt hin zu einer Verrechtlichung der internen automatisierten Analysefähigkeiten der Sicherheitsbehörden in Zeiten von Big Data. Die Norm sollte aber durch verfahrensrechtliche Sicherungen ergänzt werden.

9. Die neuen Bestimmungen zum Einsatz von Vertrauensleuten (§ 14 HVSG-E) übernehmen weitgehend § 9b BVerfSchG und sind verfassungsrechtlich zulässig. Sie könnten dennoch an mehreren Punkten verbessert werden. Dies gilt insbesondere für § 14 Abs. 2 Satz 4 Nr. 2 HVSG-E, weil der Ausschlussgrund in der Praxis so gut wie immer leerlaufen wird.

10. Der Verweis auf das Hessische Datenschutzgesetz in § 16 HVSG-E muss in Abhängigkeit von dem Inhalt des aktuellen Reformprozesses (Anpassung an die Datenschutz-Grundverordnung und die JI-Richtlinie für den Datenschutz) in der Zukunft überprüft werden.

11. Die Bestimmungen zum Auskunftsanspruch in § 27 HVSG-E sind unangemessen eng. Der Auskunftsanspruch sollte - wie sonst auch - ohne besondere Begründung bestehen. Überdies sollte er zumindest in manchen Fällen auch die Herkunft über die Datenübermittlung umfassen sowie nicht auf Daten begrenzt werden, die strukturiert in automatisierten Dateien gespeichert sind. Ein Verzicht auf eine Begründung der Ablehnung des Antrags sollte nur in begründeten Einzelfällen erfolgen, nicht stets.

12. Die Neustrukturierung der parlamentarischen Kontrolle durch den Entwurf eines Verfassungsschutzkontrollgesetzes ist überaus begrüßenswert. Jedoch sollten in mehreren Punkten die Rechte der Opposition gestärkt werden (Pflicht zur angemessen Beteiligung in der Kommission, Absenkung des Mehrheitserfordernisses für die Beauftragung einer Sachverständigenperson, Möglichkeit von Sondervoten). Auch bei der personellen Ausstattung der Kontrollkommission, den Unterrichtungspflichten der Landesregierung, den Befugnissen der Kommissionsmitglieder (Herausgabe von Akten, Befragung von Mitarbeitern, Betreten der Diensträume) besteht Verbesserungsbedarf.

1. Reformbedarf und Grundausrichtung des Gesetzes

Das **Ziel des Gesetzentwurfs ist sehr begrüßenswert**. Die Grundstruktur des bisherigen Gesetzes über das Landesamt für Verfassungsschutz stammt aus dem Jahre 1990, und damit aus einer Zeit, in der noch völlig andere Vorstellungen über die verfassungsrechtlichen Anforderungen an die Arbeit der Verfassungsschutzbehörden und die grundrechtlichen Rahmenbedingungen ihrer Tätigkeit bestanden. In der Folgezeit wurde das Gesetz (wie viele andere Verfassungsschutzgesetze in Deutschland) in einer ganzen Reihe von Punkten ergänzt und erweitert, jedoch nicht systematisch überarbeitet. Dies führt zu komplexen und im Detail mit dem rechtsstaatlichen Bestimmtheitsgebot schwer zu vereinbarenden Regelungen (insbesondere Verweisungen).[1] Hinzu kommt, dass die politische Aufarbeitung, die auf verschiedenen staatlichen Ebenen zu den Taten des sogenannten „Nationalsozialistischen Untergrunds" (NSU) stattgefunden hat, einen erheblichen Reformbedarf zutage gefördert hat.[2] Dieser sollte im Rahmen des vorliegenden Gesetzgebungsverfahrens angegangen werden.

In einer **ganzen Reihe von Punkten erfüllt das Gesetz Anforderungen an ein modernes Recht der Verfassungsschutzbehörden**. Insbesondere erfolgt eine weitgehende - wenn auch nicht vollständige - Anpassung an die in der Zwischenzeit ergangene Rechtsprechung des Bundesverfassungsgerichts. Die Präzisierungen etwa bei der Aufgabenbeschreibung in § 2 HVSG-E sowie bei den nunmehr auf mehrere getrennte Normen verteilten Befugnissen sind zu begrüßen. Dies gilt beispielsweise für die Regelung der eingriffsintensiven Maßnahmen zur Informationserhebung mit nachrichtendienstlichen Mitteln in § 5 HVSG-E sowie für die nunmehr viel detaillierteren Bestimmungen zu den Informationsübermittlungen in den §§ 16 ff. HVSG-E

Auch die an vielen Punkten angestrebte **Vereinheitlichung mit dem Bundesverfassungsschutzgesetz** (etwa bei den Begriffsbestimmungen, den materiellrechtlichen Regelungen zur Informationserhebung sowie den Datenübermittlungsvorschriften) ist ein **Fortschritt**, weil die wissenschaftliche und politische Analyse der Arbeit der Sicherheitsbehörden in den letzten Jahren hier problematische Unterschiede identifiziert hatte. Freilich wird die Harmonisierung teilweise mit wiederum komplizierten Verweisungen in das Bundesrecht erkauft.

Zu begrüßen ist schließlich die Grundrichtung, das Landesamt zum einen explizit mit einer - nicht als polizeilich misszuverstehenden - Präventionsaufgabe auszustatten (§ 2 Abs. 1 Satz 2 HVSG-E) sowie es stärker an den öffentlichen Diskurs anzubinden und so auch der Kontrolle durch die demokratische Öffentlichkeit zu unterstellen. Diese Aufgabenzuweisung wird durch die Präambel freilich wieder verunklart, wenn diese sich gegen Gefahren durch „extremistisches Gedankengut" wendet. Weder Extremismus noch Gedankengut werden als Begriffe im Gesetz verwendet.[3] Wenn Bestrebungen gegen die freiheitliche demokratische Grundordnung gemeint sind, sollte dies so formuliert werden. **Allgemein erscheint die Präambel verzichtbar und in ihrer jetzigen Fassung missverständlich.**

---

[1] S. zu den verfassungsrechtlichen Grenzen von Gesetzesverweisen BVerfGE 110, 33 (61 f.).

[2] S. BT-Drs. 17/14600, insbesondere S. 861 ff.

[3] Der Begriff des Extremismus ist ohnehin unbestimmt und nach Ansicht des Bundesverfassungsgerichts von angrenzenden Bereichen wie (recht-)„radikal" oder (rechts-)„reaktionär" nur auf der Ebene des politischen Meinungskampfes und der gesellschaftswissenschaftlichen Auseinandersetzung abzugrenzen, s. BVerfG, ZUM-RD 2011, 205, 207.

An **anderen Stellen ist der Gesetzentwurf demgegenüber problematisch** - vor allem weil er die Befugnisse des Landesamts zur verdeckten und eingriffsintensiven Erhebung sensibler personenbezogener Daten ganz erheblich ausdehnt, auf hinreichende Sicherungsmaßnahmen v.a. bei der Online-Durchsuchung verzichtet und das Auskunftsrecht betroffener Personen über die Gebühr einschränkt. Auch an anderen Stellen des Gesetzesentwurfs gibt es Möglichkeiten, Regelungen präziser zu fassen und zusätzliche verfahrensrechtliche Sicherungen vorzusehen. Die Regelungen zur parlamentarischen Kontrolle sind demgegenüber eine ganz erhebliche Verbesserung gegenüber dem Status quo, können aber dennoch an wesentlichen Punkten weiter verbessert werden.

Die folgende Stellungnahme konzentriert sich auf diese problematischen und verbesserungsfähigen Punkte.

2. Aufgaben im Bereich der Organisierten Kriminalität (§ 2 Abs. 2 Nr. 5 HVSG-E)

Die Aufgabe der Sammlung und Auswertung von Informationen über Bestrebungen und Tätigkeiten der Organisierten Kriminalität im Geltungsbereich des Grundgesetzes in § 2 Abs. 2 Nr. 5 HVSG-E entspricht zwar dem bisherigen § 2 Abs. 2 Satz 1 Nr. 5, ist aber dennoch problematisch. Jenseits der räumlichen Erstreckung auf das gesamte Bundesgebiet, die bei wörtlicher Auslegung eine eindeutige Kompetenzüberschreitung wäre, handelt es sich um einen Bereich schwerwiegender Kriminalität, deren (präventive und repressive) Bekämpfung zu den **klassischen Aufgaben der Polizei- und Strafverfolgungsbehörden** gehört.

Im Sonderfall des Freistaates Sachsen - nach Art. 83 Abs. 3 Satz 1 der Sächsischen Verfassung unterhält der Freistaat explizit „keinen Geheimdienst mit polizeilichen Befugnissen" - hat der Sächsische Verfassungsgerichtshof eine Zuständigkeit der Verfassungsschutzbehörden in diesem Bereich sogar für verfassungswidrig erklärt.[4] Das Urteil ist mangels vergleichbarer Regelung in der Hessischen Verfassung nicht direkt übertragbar. Die durch das Gericht geäußerten Bedenken zu einem Verschwimmen zwischen Verfassungsschutz- und Polizeibehörden sind allerdings auch für das Grundgesetz und die Hessische Verfassung valide. In der grundlegenden **Aufgabenbeschreibung des Bundesverfassungsgerichts für die Nachrichtendienste** im ATDG-Urteil von 2013 hat das Gericht betont, diesen komme „die Aufgabe zu, Aufklärung bereits im Vorfeld von Gefährdungslagen zu betreiben".[5] Unbeschadet näherer Differenzierungen zwischen den verschiedenen Diensten beschränke sich deren Aufgabe im Wesentlichen darauf, fundamentale Gefährdungen, die das Gemeinwesen als Ganzes destabilisieren können, zu beobachten und hierüber zu berichten, um eine politische Einschätzung der Sicherheitslage zu ermöglichen. Ziel sei „**nicht die operative Gefahrenabwehr, sondern die politische Information**".[6]

---

[4] SächsVerfGH, NVwZ 2005, 1310, 1311 f.; dies gilt, solange der Verfassungsschutz „nicht gleichzeitig dem Schutz der freiheitlichen demokratischen Grundordnung oder des Bestands oder der Sicherheit des Bundes oder der Länder oder vor Bestrebungen im Geltungsbereich des Grundgesetzes, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden, dienen soll".

[5] BVerfGE 133, 277 (325).

[6] BVerfGE 133, 277 (326).

Die Aufgabenzuweisung in § 2 Abs. 2 Nr. 5 HVSG-E ist dementsprechend systemfremd. Hinzu kommen praktische Probleme der Parallelzuständigkeit mit den Polizei- und Strafverfolgungsbehörden. Schließlich **wiederspricht die Zuständigkeit dem selbstgesetzten Ziel der Novelle, „ein größtmögliches Maß an Harmonisierung" auf dem Gebiet des Verfassungsschutzes zu erreichen.**[7] Weder im Bund noch in fast allen anderen Bundesländern besteht nämlich eine Zuständigkeit der Verfassungsschutzbehörden für den Bereich der Organisierten Kriminalität.[8]

In der Folge kann das Landesamt in dieser Sache de facto nur mit den Strafverfolgungsbehörden zusammenarbeiten, was aber rechtlich nur sehr eingeschränkt möglich ist. Im Ergebnis sollte deshalb **erwogen werden, § 2 Abs. 2 Nr. 5 HVSG-E zu streichen.** Als Minimum wäre zu evaluieren, ob die hessische Regelung bei der Bekämpfung der Organisierten Kriminalität dem Land Hessen einen Vorteil gegenüber den Strategien anderer Bundesländer verschafft hat.

3. Technische Erhebungs- und Auswertungsbefugnisse

3.1 Verfassungsrechtliche Problematik

§ 7 HVS-E normiert Regelungen zum **verdeckten Einsatz technischer Mittel zur Wohnraumüberwachung.** Hierzu hat das Bundesverfassungsgericht hervorgehoben, dass Eingriffe in diesen Bereich von ganz erheblicher Grundrechtsrelevanz sind. Die Wohnraumüberwachung erlaubt dem Staat auch in Räume einzudringen, die privater Rückzugsort des Einzelnen sind und einen engen Bezug zur Menschenwürde haben.[9]

Der Entwurf enthält mit der Befugnis zur sogenannten Quellen-Telekommunikationsüberwachung (§ 6 Abs. 2-4 HVSG-E) sowie zur sogenannten Online-Durchsuchung (§ 8 HVSG-E) darüber hinaus zwei neue Maßnahmen, die das Bundesverfassungsgericht zwar im Grundsatz gebilligt hat, die **ihre verfassungsrechtliche und politische Problematik** deshalb aber keineswegs eingebüßt haben. **Der Inhalt informationstechnischer Systeme ist in der heutigen Zeit die sensibelste Datensammlung vieler Menschen.** Auch aus anderen Gründen sind Bürgerinnen und Bürger darauf angewiesen, sich auf die Vertraulichkeit und Funktionsfähigkeit ihrer IT-Systeme verlassen zu können. Quellen-Telekommunikationsüberwachung und Online-Durchsuchung müssen Lücken in der IT-Sicherheit der Systeme ausnutzen oder sogar erst schaffen. Dies ist nicht nur ein strukturelles Problem staatlichen Handelns (da der Staat in der heutigen Zeit eine Infrastrukturverantwortung für die IT Sicherheit innehat und diese schützen muss), sondern auch ein grundrechtliches Problem. Letzteres hat das Bundesverfassungsgericht im Jahre 2008 dazu bewogen, das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus dem Grundgesetz abzuleiten.[10] Es hat zugleich sehr hohe verfassungsrechtliche Anforderungen an Eingriffe in dieses Grundrecht aufgestellt und diese in der Folge mehrfach bekräftigt.[11]

---

[7] S. Drucks. 19/5412, S. 29.

[8] Die einzigen Ausnahmen bilden Bayern (Art. 3 Satz 2 BayVSG) und das Saarland (§ 3 Abs. 1 Satz 1 Nr. 4 SaarlVSG).

[9] BVerfGE 109, 279 (313 f.).

[10] BVerfGE 120, 274.

[11] Zuerst in BVerfGE 120, 274 (315 ff.); später z.B. im Urteil zum ATD-Gesetz, BVerfGE 133, 277 (373 f.) sowie zum BKA-Gesetz, BVerfGE 141, 220 (Rn. 208 ff.).

3.2 Quellen-Telekommunikationsüberwachung (§ 6 Abs. 2-4 HVSG-E)

Die Quellen-Telekommunikationsüberwachung greift demgegenüber in ihrer „reinen" Form (die in § 6 Abs. 2 HVSG-E ganz offenbar bezweckt wird) nicht in dieses Grundrecht, sondern „nur" in das Fernmeldegeheimnis des Art. 10 GG und Art. 12 HV ein. Der Entwurf **hält insoweit die Anforderungen ein, die das Bundesverfassungsgericht** an eine Quellen-Telekommunikationsüberwachung anlegt.[12]

Es ist allerdings darauf hinzuweisen, dass gerade wegen dieser in § 6 Abs. 2 HSVS-E aufgestellten Anforderungen der **Einsatz in der Praxis vor große und ggf. sogar nicht lösbare Aufgaben** gestellt werden wird. Der Ausschluss des Anwendungsbereichs des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gilt nämlich nur unter der Maßgabe, dass tatsächlich die in § 6 Abs. 2 Nr. 1 HVSG-E aufgestellte Anforderung eingehalten wird, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird.[13] Dies ist in der Praxis offenbar ein ganz erhebliches Problem und wurde in der Vergangenheit mehrfach nicht eingehalten.[14]

Eine allgemeinverständliche Herausforderung ist, dass die Quellen-Telekommunikationsüberwachung gerade darauf abzielt, vor einer etwaigen Verschlüsselung der Kommunikationsinhalte zuzugreifen (da dies im Anschluss nicht oder nur noch sehr schwer möglich ist). Aus technischer Sicht wird also - notwendigerweise - gerade nicht die „laufende Telekommunikation" überwacht, wie es § 6 Abs. 2 Nr. 1 HVSG-E vorschreibt, sondern Entwürfe für diese, die mehr oder weniger kurz vor dem Absenden erstellt wurden (oder ggf. dann sogar nicht mehr abgesendet wurden). Man kann also **mit guten Gründen davon ausgehen, dass § 6 Abs. 2 Nr. 1 HVSG-E de facto unerfüllbare Anforderungen enthält**, die der Gesetzgeber dennoch gewählt hat, um „nur" den verfassungsrechtlichen Anforderungen des Art. 10 GG (bzw. Art. 12 HV), nicht aber den höheren Anforderungen des Eingriffs in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme genügen zu müssen.

Das Bundesverfassungsgericht hat derartige praktische Probleme der Einhaltung der Begrenzung auf laufende Telekommunikation für § 20l Abs. 2 BKAG explizit für nicht entscheidungserheblich erklärt und gefolgert, wenn die technischen Vorgaben zur Überwachung nicht einhaltbar seien, dürfe die Vorschrift nicht vollzogen werden und **laufe „folglich bis auf weiteres leer"**.[15] Es handelt

---

[12] BVerfGE 141, 220 (Rn. 228 ff.); die für die weitgehend parallele Regelung in § 20l BKA-Gesetz dort beanstandete zu knappe Aufbewahrungsfrist der Löschungsprotokolle gemäß § 20l Abs. 6 Satz 10 BKAG wird durch § 6 Abs. 3 Satz 2 HVSG-E behoben.

[13] S. die Formulierung in BVerfGE 120, 274 (309): „Art. 10 Abs. 1 GG ist hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer "Quellen-Telekommunikationsüberwachung", wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein". S.a. BVerfGE 141, 220 (Rn. 228 ff.).

[14] S. z.B. *Der Bayerische Landesbeauftragte für den Datenschutz*, Prüfbericht Quellen-TKÜ, 2012, https://www.datenschutz-bayern.de/0/bericht-qtkue.pdf.

[15] BVerfGE 141, 220 (Rn. 234).

sich also um eine verbindliche und anspruchsvolle Aufgabe für die Vollzugspraxis des vorgeschlagenen Gesetzes.

3.3 Online-Durchsuchung (§ 8 HVSG-E)

Lässt sich die Quellen-Telekommunikationsüberwachung noch als Reaktion auf die zunehmende Ende-zu-Ende Verschlüsselung der Telekommunikation verstehen (inzwischen teilweise auch flächendeckend, beispielsweise bei der Messenger-Anwendung WhatsApp), so handelt es sich bei der in § 8 HVSG-E vorgesehenen Online-Durchsuchung um eine **sehr eingriffsintensive zusätzliche Maßnahme.** Sie darf nach § 8 Abs. 1 Nr. 1, 2. Alt. HVSG-E das Ziel verfolgen, auf diesem System „verarbeitete Daten zu erheben" - im Grundsatz also sämtliche Daten auch intimster Art (elektronisch gespeicherte Korrespondenz, Tagebücher, höchstpersönliche Fotos und Videos, lange zurückliegende Kommunikation mit früheren Sexualpartnern, umfassende Backupdateien aktueller und früherer E-Mail-Accounts, Browser-Verläufe über besuchte Webseiten, Gesundheitsinformationen etc.).

Diese Eingriffsintensität versucht der Gesetzentwurf - in Übernahme des weitgehend wortgleichen Art. 9 BayVSG - durch eine Rückbindung an die Regeln zum verdeckten Einsatz technischer Mittel zur Wohnraumüberwachung in § 7 HVSG-E rechtsstaatlich einzuhegen. Dies ist im Grundsatz ein nachvollziehbarer Ansatz, da das Bundesverfassungsgericht selbst betont, die Eingriffsintensität der Online-Durchsuchung sei mit der der akustischen Wohnraumüberwachung vergleichbar.[16] Dies bedeutet aber nicht, dass man unbesehen dieselben Maßnahmen zur Sicherung der Verhältnismäßigkeit anwenden kann. Die vorgeschlagene Regelung hält deshalb an **mehreren Stellen die verfassungsrechtlichen Anforderungen des Bundesverfassungsgerichts nicht ein.**

Hinreichend ist die durch den Verweis auf § 7 Satz 1 HVSG-E geltende **Eingriffsschwelle** der tatsächlichen Anhaltspunkte für eine dringende Gefahr. Das Bundesverfassungsgericht hat in der Entscheidung zur Online-Durchsuchung sogar eine etwas weniger qualifizierte Schwelle, nämlich „„tatsächliche Anhaltspunkte einer konkreten Gefahr" gebilligt.[17] Das Gericht hat explizit betont, dass dies auch für die Verfassungsschutzbehörden gilt.[18] Begrüßenswert sind daneben die **Regelungen in § 8 Abs. 2 und Abs. 3 HVSG-E**, die direkt bzw. über § 6 Abs. 4 HVSG-E einen Gleichlauf mit § 20k Abs. 2 und Abs. 3 BKAG herstellen.[19]

Die Rechtsgüter in § 7 Satz 1 HVSG-E entsprechen demgegenüber nicht den Vorgaben des Bundesverfassungsgerichts. Dieses hatte neben „Leib, Leben und Freiheit der Person" (§ 7 Satz 1 Nr. 2 HVSG-E) nur „solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt" als hinreichende Legitimation angesehen.[20] Darunter lässt sich § 7 Satz 1 Nr. 3 HVSG-E (Sachen von bedeutendem Wert) nicht subsummieren, selbst wenn die Erhaltung dieser Sachen, wie es die Norm verlang, im öffentlichen Interesse geboten ist. Der Gesetzentwurf weicht in Nr. 3 auch ohne Not von der bundesgesetzlichen Regelung in § 20k Abs. 1 BKAG ab. **Der Verweis in § 8 HVSG-E auf § 7 Satz 1 Nr. 3 HVSG-E**

[16] BVerfGE 141, 220 (Rn. 210).
[17] BVerfGE 120, 274 (328 f.).
[18] BVerfGE 120, 274 (329 f.).
[19] Diese hat das Bundesverfassungsgericht für erforderlich gehalten, s. BVerfGE 141, 220 (Rn. 215).
[20] BVerfGE 120, 274 (328).

ist deshalb verfassungswidrig. Nr. 3 ist jedenfalls für die Online-Durchsuchung, unter Verhältnismäßigkeitsgesichtspunkten aber auch für die Wohnraumüberwachung zu streichen.

Der Gleichlauf mit § 7 HVSG-E ist auch im Übrigen zwar eine nachvollziehbare Regelungsstrategie des Gesetzgebers, führt aber dennoch zu problematischen Ergebnissen. Wenn **tatsächlich eine dringende Gefahr** für die in § 7 Nr. 1-3 HVSG-E genannten Rechtsgüter vorliegt, so ist es im Grundsatz **Aufgabe der Polizeibehörden** des Bundes und der Länder, diese abzuwehren. Wieso (alternativ oder zusätzlich) das Landesamt für Verfassungsschutz zu diesem Zweck eine Online-Durchsuchung durchführen dürfen soll, ist nicht ersichtlich. Die Begründung des Gesetzentwurfs betont selbst, dass die Nachrichtendienste im Gefahrenvorfeld tätig sein sollen, während die Polizeibehörden konkrete Gefahren abwehren.[21]

Über die **Verweisung auf § 7 HVSG-E** finden über dessen Satz 2 die Regelungen des Artikel 10-Gesetzes zu den Adressaten (§ 3 Abs. 2 Artikel 10-Gesetz), zum Schutz des Kernbereichs privater Lebensgestaltung (§ 3a Artikel 10-Gesetz) und zeugnisverweigerungsberechtigter Personen (§ 3b Artikel 10-Gesetz) Anwendung. **Alle drei Verweise sind verfassungsrechtlich unzulässig.**

§ 3 Abs. 2 Artikel 10-Gesetz gestattet Maßnahmen nicht nur gegen Verdächtige, sondern auch gegen sog. Nachrichtenmittler. Diese Erstreckung hat das Bundesverfassungsgericht für die Telekommunikationsüberwachung als noch verhältnismäßig bewertet.[22] Für die Online-Durchsuchung musste das Gericht die Frage nicht beantworten, weil § 20k Abs. 4 BKA-Gesetz Nachrichtenmittler gerade nicht erfasst. Für die Wohnraumüberwachung bestehen jedoch gesteigerte Anforderungen. Eine Überwachung Dritter ist verfassungsrechtlich nur insoweit zulässig, als diese durch eine Überwachung unvermeidbar mitbetroffen werden.[23] Bei Wohnraumüberwachungen kann die Überwachung der Wohnung eines Dritten nur erlaubt werden, wenn anzunehmen ist, dass die Zielperson sich dort zur Zeit der Maßnahme aufhält, sie dort für die Ermittlungen relevante Gespräche führen wird und eine Überwachung ihrer Wohnung allein zur Erforschung des Sachverhalts nicht ausreicht. Vergleichbare Anforderungen sind auch für die Online-Durchsuchung zu stellen. Der **Verweis auf § 3 Abs. 2 Artikel 10-Gesetz ist insoweit verfassungswidrig.**

Der Verweis auf § 3a Artikel 10-Gesetz ist überdies problematisch, weil dieser auf die Überwachung der Telekommunikation gerichtet ist. Durch die Verweistechnik werden die Vorgaben des Bundesverfassungsgerichts für die Online-Durchsuchung in wichtigen Punkten nicht eingehalten. § 8 HVSG-E ist in der vorliegenden Form auch **aufgrund fehlender hinreichender Regelungen zum Kernbereichsschutz verfassungswidrig**:

- Eine Überwachung der Telekommunikation kann unmittelbar (Mithören) oder automatisiert (Aufzeichnen) erfolgen, weshalb § 3a Artikel 10-Gesetz für diese Varianten unterschiedliche Regelungen enthält. Diese Differenzierung ist bei der Online-Durchsuchung nicht möglich, weil hier eine unmittelbare Wahrnehmung der aus dem System ausgeleiteten Daten nicht möglich ist und dementsprechend stets automatisiert vorgegangen wird. Dementsprechend ist unklar, unter welchen Voraussetzungen die in § 7 Satz 2 HVSG-E geregelte richterliche Entscheidung über die Verwertbarkeit erforderlich ist. Die entsprechende

[21] Drucks. 19/5412, S. 31.

[22] BVerfGE 141, 220 (Rn. 233).

[23] BVerfGE 141, 220 (115, 191 ff.).

Regelung in **§ 3a Satz 4 Artikel 10-Gesetz hat Tatbestandsvoraussetzungen, die bei der Online-Durchsuchung schlicht keinen Sinn ergeben.**

- Im Übrigen hat das Bundesverfassungsgericht für die Online-Durchsuchung die besondere Relevanz der Aus- und Verwertungsebene hervorgehoben: „Entscheidende Bedeutung hierfür kommt dabei einer Sichtung durch eine unabhängige Stelle zu, die kernbereichsrelevante Informationen vor ihrer Kenntnisnahme und Nutzung [...] herausfiltert".[24] Dies erfordert - wie es sogar derzeit der durch das Bundesverfassungsgericht für nicht hinreichend bewertete § 20k Abs. 7 BKAG regelt - eine **Durchsicht aller erhobenen Informationen, nicht nur eine solche „bei Zweifeln über die Verwertbarkeit"**, wie es § 7 Satz 2 HVSG-E formuliert.[25]
- Außerdem **fehlt es** an der durch das Bundesverfassungsgericht für die Online-Durchsuchung explizit geforderten **Regelung, dass verfügbare informationstechnische Sicherungen einzusetzen sind.** Die Ermächtigungsgrundlage muss vorsehen, dass die Erhebung von Informationen, die dem Kernbereich zuzuordnen sind, soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt.[26] Da § 3a Artikel 10-Gesetz, auf den § 8 HVSG-E über § 7 Satz 2 HVSG-E verweist, eine solche Regelung nicht enthält, sind die verfahrensrechtlichen Sicherungen insoweit unzureichend.

Der Verweis auf § 3b BVerfSchG berücksichtigt grundsätzlich in zulässiger Weise den Schutz von Berufsgeheimnisträgern. Die Norm differenziert jedoch zwischen Strafverteidigern und sonstigen Rechtsanwälten. Dies ist nach der Entscheidung des Bundesverfassungsgericht zu dem parallel formulierten § 20u BKA-Gesetz aus Gleichbehandlungsgründen unzulässig und im - hier vorliegenden - präventiven Bereich auch deshalb zweckwidrig, weil die in Frage stehenden Überwachungsmaßnahmen nicht der Strafverfolgung, sondern der Gefahrenabwehr dienen, die Strafverteidigung also hier gerade nicht entscheidend ist.[27] Auch der **Verweis auf § 3b BVerfSchG ist damit (teilweise) verfassungswidrig.**

Neben den genannten Verweisungen auf § 7 HVSG-E sind zwei verfahrensrechtliche Regelungen aus verfassungsrechtlicher Sicht problematisch.

- § 9 Abs. 1 Satz 2 HVSG-E enthält eine **Ausnahme vom Richtervorbehalt** für Eilfälle. Auf diese sollte **für die Online-Durchsuchung verzichtet werden.** Diese wird typischerweise ohnehin einen relativ langen technischen Vorbereitungsaufwand erfordern, sodass es kaum jemals dazu kommen wird, dass eine richterliche Anordnung nicht rechtzeitig zu erlangen

---

[24] BVerfGE 120, 274 (338 f.); BVerfGE 141, 220 (Rn. 220).

[25] Das Bundesverfassungsgericht hat den Unterschied sogar explizit hervorgehoben und formuliert, anders als bei der Online-Durchsuchung sei es bei der Telekommunikationsüberwachung nicht erforderlich, in jedem Fall auch die Sichtung durch eine unabhängige Stelle vorzugeben, s. BVerfGE 129, 208 (249); BVerfGE 141, 220 (Rn. 240).

[26] BVerfGE 120, 274 (338); BVerfGE 141, 220 (Rn. 219); demgegenüber hält der insoweit modifizierte Verweis in § 7 Satz 2 HVSG-E auf § 3a Artikel 10 Gesetz die durch das Bundesverfassungsgericht zu § 20k Abs. 7 BKAG formulierte Vorgabe ein, dass eine solche Entscheidung „maßgeblich in den Händen von dem Bundeskriminalamt gegenüber unabhängigen Personen liegen" muss. Über den Verweis greift insoweit § 3a Satz 4 Artikel 10 Gesetz mit der Maßgabe des § 7 Satz 2 HVSG-E, dass an die Stelle der Entscheidung durch ein Mitglied der G10-Kommission die Anordnung des zuständigen Gerichts tritt.

[27] BVerfGE 141, 220 (Rn. 257).

ist. Dementsprechend enthält die Parallelregelung in § 20k Abs. 6 BKAG keine derartige Ausnahme.[28]

- § 9 Abs. 4 HVSG-E stellt geringere verfahrensrechtliche Anforderungen an den Einsatz technischer Mittel, wenn diese ausschließlich dem Schutz der für den Verfassungsschutz tätigen Personen bei einem Einsatz in Wohnungen dienen. Dieser Fall passt nicht auf den Fall von § 8 HVSG-E, weil **nicht erkennbar ist, in welcher Weise eine Online-Durchsuchung ausschließlich dem Schutz eines Einsatzes von für den Verfassungsschutz tätigen Personen in einer Wohnung** dienen sollte.

Angesichts der grundlegenden Probleme der Maßnahme, der Schwierigkeiten, ihre technischen und rechtlichen Wirkungen zu begrenzen sowie der grundsätzlichen Zuständigkeit der Polizeibehörden für die genannten Aufgaben, denen die Maßnahme dienen soll, **sollte § 8 HVSG-E gestrichen werden**. Hierfür spricht auch, dass es eine Befugnis zur Online-Durchsuchung im Verfassungsschutzbereich bisher weder auf Bundesebene noch in praktisch allen Bundesländern gibt.[29] Es ist nicht erkennbar, dass das Fehlen dieses Instruments die Arbeit der Verfassungsschutzbehörden bisher merkbar behindert hätte.

3.4 Verdeckter Einsatz technischer Mittel zur Wohnraumüberwachung (§ 7 HVSG-E)

Die Neuregelung in § 7 HVSG-E **entspricht im Grundsatz den Vorgaben, die das Bundesverfassungsgericht** zuletzt in der Entscheidung zum BKA-Gesetz an derartige Maßnahmen aufgestellt hat.[30] Insbesondere hat das Gericht die Schutzgüter und die Schwelle der dringenden Gefahr[31] aus § 7 Satz 1 HVSG-E für den im Wesentlichen gleichlautenden § 20h Abs. 1 BKA-Gesetz gebilligt. Dasselbe gilt für die Formulierung „verdeckter Einsatz technischer Mittel" als Oberbegriff für die sowohl akustische als auch optische Wohnraumüberwachung. Insoweit muss allerdings bei der Gesetzesanwendung beachtet werden, dass die Verbindung von akustischer und optischer Überwachung ein wesentlich größeres Eingriffsgewicht als etwa nur eine akustische Überwachung hat und deshalb besonderer Rechtfertigung bedarf. Es reicht für die zusätzliche Anordnung einer optischen Überwachung folglich regelmäßig nicht, auf bloße Erleichterungen für die Zuordnung von Stimmen zu verweisen, sondern es bedarf gewichtiger, für den Erfolg der Überwachung maßgeblicher eigener Gründe.[32] Schließlich hat der Entwurf beachtet, dass das Bundesverfassungsgericht in derselben Entscheidung die zu kurze Aufbewahrung von Protokollierungsdaten für verfassungswidrig erklärt hat. Statt insoweit vollständig auf die §§ 3a, 3b § 3a Artikel 10-Gesetz zu verweisen, löst der Entwurf dies in verfassungskonformer Weise, indem er die Bestimmung in § 7 Satz 3 i.V.m. § 6 Abs. 3 Satz 2 HVSG-E an ihre Stelle setzt.

Demgegenüber sind die **Regelungen zu den Adressaten, zum Kernbereichsschutz und zum Schutz von Berufsgeheimnisträgern** auch für die technische Wohnraumüberwachung **nicht im Einklang mit den Vorgaben des Bundesverfassungsgerichts**.

---

[28] S. BVerfGE 141, 220 (Rn. 216).

[29] Die einzige Ausnahme ist Bayern (Art. 10 BayVSG).

[30] BVerfGE 141, 220 (Rn. 179 ff.).

[31] Die oben für die Online-Durchsuchung angeführte Problematik dieser Gefahrenschwelle und der daraus folgenden Parallelzuständigkeit mit den Polizeibehörden besteht freilich auch hier.

[32] BVerfGE 141, 220 (Rn. 185).

- Die Adressatenregelung in § 7 Satz 2 HVSG-E verweist auf § 3 Abs. 2 Artikel 10-Gesetz. Es wurde bereits ausgeführt, dass die **Erstreckung der Wohnraumüberwachung auf Nachrichtenmittler verfassungsrechtlich unzulässig** ist.[33]
- Für den **Kernbereichsschutz** verweist der Entwurf in § 7 Satz 2 HVSG-E auf § 3a Artikel 10-Gesetz. Dieser entspricht der Sache nach im Wesentlichen § 20h Abs. 5 BKA-Gesetz. Diese Regelung ist hingegen durch das Bundesverfassungsgericht für verfassungswidrig erklärt worden. Das Gericht hat den Schutz auf Erhebungsebene für hinreichend bewertet, jedoch nicht den auf der Durchsichtsebene. **Die unabhängige Kontrolle lediglich in Zweifelsfällen ist danach nicht ausreichend.** Vielmehr bedarf es - ebenso wie bei der Online-Durchsuchung (s.o.) - einer umfassenden Sichtung, deren Ziel nicht allein in dem Herausfiltern von Zweifelsfällen liegen darf, „sondern auch in der Gewährleistung einer unabhängigen Kontrolle der dem Kernbereichsschutz dienenden Anforderungen insgesamt".[34]
- Der Verweis auf § 3b BVerfSchG ist grundsätzlich angemessen, bezieht jedoch dessen - jedenfalls im präventiven Bereich - **verfassungswidrige Ungleichbehandlung zwischen Strafverteidigern und sonstigen Rechtsanwälten** ein (s.o.).[35]

Dementsprechend ist der Verweis aus § 7 Satz 2 HVSG-E auf § 3 Abs. 2, § 3a und § 3b Artikel 10-Gesetz nicht hinreichend; die Regelung ist insoweit verfassungswidrig.

4. Automatisierte Datenanalyse (§ 25a HSOG-E in der Fassung des Änderungsantrags)

Der vorgeschlagene § 25a HVSG-E regelt einen Bereich der Informationsverarbeitung der Sicherheitsbehörden, der bisher in rechtsstaatlich problematischer Weise unterreguliert ist. Während die Gesetzgeber des Bundes und der Länder - nicht zuletzt aufgrund entsprechender Vorgaben des Bundesverfassungsgerichts - seit vielen Jahren detaillierte gesetzliche Vorgaben für die Datenerhebung sowie die Übermittlung an andere Stellen schaffen, ist der nachfolgende Bereich der internen Datenanalyse weitgehend unreguliert. Da die Zusammenführung und Auswertung großer Mengen personenbezogener Daten in Zeiten elaborierter Big Data-Algorithmen selbstständige und erhebliche zusätzliche Eingriffe in das Recht auf informationelle Selbstbestimmung mit sich bringen kann, ist dies rechtsstaatlich problematisch und wird auf Dauer kaum zu halten sein. Der **Regelungszweck der Norm verdient deshalb große Unterstützung.**

Die vorgeschlagene Regelung enthält durch die Anbindung an § 100a Abs. 2 StPO bzw. Gefahren für die in § 25a Abs. 1 HSOG-E genannten Rechtsgüter relativ hohe materiellrechtliche Anforderungen. Demgegenüber **fehlt es außer der Anordnungsbefugnis in Abs. 3 an allen verfahrensrechtlichen Sicherungen.** Es wird weder geregelt, wie mit den gewonnenen Erkenntnissen umgegangen wird, noch wie lange diese aufbewahrt und wann sie gelöscht werden müssen. Vorgaben zu Erkenntnissen über Unbeteiligte oder sensible Informationen (Bewegungs- oder sogar umfassende Verhaltensprofile) fehlen. Überdies bedürfte es gerade dann, wenn die Maßnahme - wie

---

[33] BVerfGE 141, 220 (115, 191 ff.).
[34] BVerfGE 141, 220 (Rn. 204).
[35] BVerfGE 141, 220 (Rn. 257).

erhofft – zu wichtigen neuen Erkenntnissen über konkrete Personen führt, die in den bisher verstreut gespeicherten Daten nicht erkennbar waren, einer Benachrichtigung der betroffenen Personen.

5. Einsatz von Vertrauensleuten (§ 14 HVSG-E)

Die grundsätzliche Sinnhaftigkeit und Problematik des Einsatzes von Vertrauensleuten soll an dieser Stelle nicht thematisiert werden. Das Bundesverfassungsgericht hat den Einsatz von Vertrauensleuten durch Verfassungsschutz- und Polizeibehörden im Grundsatz gebilligt.[36]

§ 14 HVSG-E lehnt sich **eng an die im Jahre 2015 verabschiedete Neuregelung auf Bundesebene** (§ 9b BVerfSchG an). Abweichend ist zum einen die Bestimmung in § 14 Abs. 2 S. 2 HVSG-E zur persönlichen und charakterlichen Eignung, die es auf Bundesebene nicht gibt. Zum anderen erweitert § 14 Abs. 2 Satz 5 HVSG-E die Ausnahmen von der Einschränkung in Satz 4 Nr. 5 über das Ziel einer Aufklärung von Bestrebungen zur Begehung von Straftaten nach § 3 Abs. 1 Artikel 10-Gesetz hinaus auch auf solche Straftaten nach § 100b Abs. 2 StPO. Diese Ausweitung ist angesichts der hohen Hürden von § 100b Abs. 2 StPO (der die Katalogstraftaten für eine Online-Durchsuchung nach der StPO regelt) vertretbar.

Die Übernahme **wesentlicher Sicherungen aus den §§ 9a, 9b BVerfSchG ist zu begrüßen.** Insbesondere dürfen weder verdeckte Mitarbeiter noch Vertrauensleute an Bestrebungen teilnehmen, die in Individualrechte eingreifen (§ 13 Abs. 2 Satz 3 Nr. 1 HVSG-E; hier i.V.m. § 14 Abs. 1 HVSG-E).

Dennoch sollte erwogen werden, die Regelung **in mehreren Punkten weiter zu verbessern**:

- Der Ausschlussgrund in **§ 14 Abs. 2 Satz 4 Nr. 2 HVSG-E** entspricht zwar § 9b Abs. 2 Satz 1 Nr. 2 BVerfSchG, ist jedoch ebenso wie letzterer **zu eng gefasst.** Es ist faktisch ausgeschlossen, dass Geld- oder Sachzuwendungen die „alleinige" Lebensgrundlage einer Vertrauensperson darstellen, weil praktisch immer weitere Finanzierungsquellen vorhanden sind – und seien es nur staatliche Sozialleistungen. Stattdessen sollte die Zusammenarbeit ausgeschlossen werden, wenn die Zuwendungen auf Dauer als „wesentliche" Lebensgrundlage dienen.
- Es sollte erwogen werden, verfahrensrechtliche Vorgaben für die Anwerbung sowie insbesondere für die **begrenzte Dauer des „Führens" durch denselben Mitarbeiter** innerhalb der Verfassungsschutzbehörde vorzusehen.
- Rechtsstaatlich vorzugswürdig wäre es, anstelle der globalen Regelung zur Begehung von Straftaten in § 13 Abs. 2 (hier i.V.m. § 14 Abs. 1) HVSG-E einen **konkreten Katalog mit Straftaten** vorzusehen, den verdeckte Mitarbeiterinnen und Mitarbeiter sowie Vertrauensleute begehen dürfen. Dies wäre auch in deren Interesse, weil sie so eine erheblich präzisere Vorstellung darüber vermittelt bekämen, welche Handlungen zulässig sind.

[36] BVerfGE 57, 250 (284); 109, 13 (Rn. 71 f.); s.a. BVerfG, NVwZ 2017, 1364 (Rn. 109 ff.).

6. Datenschutzrechtliche Fragen

Auf eine detaillierte Analyse der Informationsübermittlungsmaßnahmen in den §§ 19 ff. HVSG-E wird an dieser Stelle verzichtet. Die grundsätzliche Zielrichtung, entsprechend den Vorgaben des Bundesverfassungsgerichts sowohl die Befugnisse der datenübermittelnden als auch die der datenempfangenden Stelle spezifisch zu regulieren („Doppeltür-Modell"),[37] ist begrüßenswert. Dasselbe gilt für das Bemühen um eine einheitliche Regelung mit den Übermittlungsvorschriften auf Bundesebene.

Handlungsbedarf besteht hinsichtlich der Geltung des allgemeinen Datenschutzrechts (§ 16 HVSG-E) sowie der Betroffenenrechte (§ 27 HVSG-E).

6.1. Geltung des allgemeinen Datenschutzrechts (§ 16 HVSG-E)

§ 16 Satz 1 HVSG-E enthält im Grundsatz **nur die Klarstellung**, dass das hessische Datenschutzgesetz subsidiär Anwendung findet, soweit das HVSG-E keine spezielle Regelung enthält. Dieselbe Rechtsfolge ordnet bereits § 3 HessDSG an. Nach dessen Abs. 1 gilt das Gesetz für Behörden des Landes (also auch für das Landesamt für Verfassungsschutz). Abs. 3 bestimmt die vorrangige Geltung spezieller Regelungen wie die des vorliegenden Gesetzentwurfs.

Dennoch führt die Verweisung in § 16 HVSG-E zu einem gesetzgeberischen Handlungsbedarf, nämlich der **Abstimmung hinsichtlich der Anpassung des Hessischen Datenschutzgesetzes an die Datenschutz-Grundverordnung[38] und die JI-Richtlinie für den Datenschutz.**[39] Da die Reform auch für den Bereich der staatlichen Verwaltung gilt, wird das hessische Datenschutzgesetz aufgrund des Vorrangs des Europarechts in weiten Teilen ab dem 25. Mai 2018 nicht mehr anwendbar sein. Sollte der hessische Gesetzgeber – was naheliegend ist – eine Anpassung des hessischen Datenschutzgesetzes an die Datenschutz-Grundverordnung und die JI-Richtlinie vornehmen und dabei größere Teile des Gesetzes aufheben, so ist zu beachten, dass die datenschutzrechtliche „Grundregulierung" der europäischen Verordnung gemäß Art. 2 Abs. 2 lit. a, d DSGVO den Bereich des Verfassungsschutzes nicht umfasst. Dementsprechend ist entweder eine selbstständige Regelung im Verfassungsschutzgesetz erforderlich oder eine Regelung wie in § 1 Abs. 8 HDSIG-E.[40]

6.2 Auskunftsanspruch (§ 27 HVSG-E)

Die Neuregelung zum Auskunftsanspruch der betroffenen Person in § 27 HSVG-E orientiert sich zwar in weiten Teilen an Art. 23 BayVSG bzw. der Parallelvorschrift in § 15 BVerfSchG. Sie ist jedoch

---

[37] S. BVerfGE 130, 151 (184); 141, 220 (Rn. 305).

[38] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. 2016 L 119, 1.

[39] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. 2016 L 119, 89.

[40] Drucks. 19/5728.

zugleich in Teilen eine erhebliche **Einengung gegenüber der Vorläufervorschrift in § 18**, die nicht in das Gesetz übernommen werden sollte.

Bisher war der Auskunftsanspruch nicht mit einer besonderen Darlegungslast verbunden. Die neue Regelung klingt dies gleich zweifach ein. Die betroffene Person muss „auf einen konkreten Sachverhalt" hinweisen sowie zusätzlich ein „besonderes Interesse an einer Auskunft" darlegen. **Beide Anforderungen sollten gestrichen werden.** Die Arbeit des Landesamts für Verfassungsschutz bringt es gerade mit sich, dass eine betroffene Person Adressat von Informationserhebungsmaßnahmen wird, ohne dies anhand eines konkreten Sachverhalts feststellen zu können. Das Erfordernis eines besonderen Interesses ist überdies eine unzulässige Einengung der verfassungsrechtlichen Vorgaben. Bürgerinnen und Bürger haben als Träger des Rechts auf informationelle Selbstbestimmung ein prinzipielles Recht zu wissen, „wer was wann und bei welcher Gelegenheit über sie weiß".[41] Dieses Recht kann im Einzelfall beschränkt werden, es ist aber nicht begründungspflichtig.[42] Die Regelung ist auch deshalb problematisch, weil die Anforderungen des besonderen Interesses und des konkreten Sachverhalts **im Extremfall dazu führen können, dass Antragsteller sich selbst belasten, indem sie auf Gesichtspunkte hinweisen (müssen), die dem Landesamt noch gar nicht bekannt sind.**

Die Auskunft soll sich nach § 27 Abs. 1 Satz 3 HSVG-E **nicht auf die Herkunft der Daten und die Empfänger von Übermittlungen erstrecken** (Nr. 1, s. bisher § 18 Abs. 3 sowie § 15 Abs. 3 BVerfSchG), sowie – von Ausnahmefällen abgesehen – nicht auf Daten, die „nicht strukturiert in automatisierten Dateien gespeichert sind" (Nr. 2, keine Entsprechung im BVerfSchG). Beide Ausnahmen sind abzulehnen und sollten gestrichen werden:

- Zwar können bestimmte Gründe, die in der Herkunft der Daten und den Empfängern liegen, eine Beschränkung des Auskunftsrechts rechtfertigen. Genauso sind jedoch Fälle denkbar, in denen beides rechtlich unproblematisch ist. So mögen die Daten aus einer öffentlich zugänglichen Quelle stammen (§ 4 Abs. 2 HSVG-E) oder im Rahmen von Sicherheitsüberprüfungsverfahren an öffentliche Stellen übermittelt werden (§ 21 Abs. 1 Nr. 2 HSVG-E). Es ist **nicht erkennbar, wieso in diesen Fällen die Auskunft kategorisch unterbleiben sollte.** Ein entsprechender Ausnahmetatbestand ist hinreichend. Diese ergibt sich freilich für die relevanten Fälle bereits aus § 27 Abs. 2 HSVG-E.
- Der Ausschluss von Daten, die nicht strukturiert in automatisierten Dateien gespeichert sind, ist zum einen sprachlich missverständlich, zum anderen inhaltlich nicht erforderlich. Prima facie schließt die Regelung alle Daten aus, die nicht (kumulativ) zum einen strukturiert, zum anderen in automatisierten Dateien gespeichert sind. Damit **wären alle nicht automatisierte Dateien (§ 2 Abs. 8 Nr. 2 HessDSG) und aktenmäßig verwahrte Informationen (§ 2 Abs. 7 HessDSG) ausgeschlossen.** Dies ließe sich **in keiner Weise rechtfertigen**, zumal derartige Speicherungsformen schon aus Eigeninteresse des Landesamts in einer Art

[41] BVerfGE 65, 1 (43); zu den verfassungsrechtlichen Vorgaben für Auskunftsanspruche s. BVerfGE 120, 351; 133, 277 (367 ff.).

[42] Die Regelung in § 27 Abs. 1 Satz 2 HSVG-E, wonach bei Fehlen einer entsprechenden Darlegung eines besonderen Interesses eine Entscheidung nach pflichtgemäßem Ermessen erfolgen soll und dieses Ermessen maßgeblich darin besteht, einen unverhältnismäßigen Verwaltungsaufwand und Ausforschungen zu verhindern (Drucks. 19/5412, S. 61) kann dieses Problem nur abmildern, nicht aber beseitigen.

und Weise aufbewahrt werden dürften, die ein Auffinden der relevanten Informationen ermöglicht. **Auch mit Blick auf das gesetzgeberische Ziel ist die Formulierung zu weit geraten.** Ausweislich der Begründung ist gerade nicht beabsichtigt, (alle) Daten von der Auskunft auszunehmen, die nicht in automatisierten Dateien gespeichert sind. Vielmehr sollen Fälle ausgeschlossen werden in denen die betroffene Person nicht das Strukturmerkmal der jeweiligen Datei ist. Es geht mit anderen Worten nicht darum, in welcher Weise die Daten gespeichert sind, sondern, ob sie durch eine Abfrage zu der antragstellenden Personen auffindbar sind, ohne den gesamten Datenbestand des Landesamts zu rastern. Dies kommt in der Formulierung nicht zum Ausdruck.

§ 27 Abs. 1 Satz 4 HSVG-E überlässt das Verfahren dem pflichtgemäßen Ermessen des Landesamts. Der Verzicht auf jede gesetzliche Vorgabe ist schwer verständlich. Zumindest sollten eine im Grundsatz **schriftliche Auskunft sowie eine regelmäßige Frist** für die Beantwortung des Antrags vorgegeben werden.

Gemäß § 27 Abs. 3 Satz 1 HSVG-E bedarf die **Ablehnung der Auskunftserteilung keiner Begründung.** Dies ist eine Einschränkung sowohl gegenüber dem bisherigen § 18 Abs. 4 Satz 1 als auch gegenüber § 15 Abs. 4 Satz 1 BVerfSchG und ist in der Sache **nicht zu rechtfertigen.** Beide Normen binden das Entfallen der Begründungspflicht daran, dass durch eine Begründung der Zweck der Auskunftsverweigerung gefährdet würde. Diese Ausnahme lässt sich aufgrund einer Einzelfallprüfung rechtfertigen, weil beispielsweise eine Begründung durch die Gefährdung des Nachrichtenzugangs (§ 27 Abs. 2 Satz 1 Nr. 2 HSVG-E) die betroffene Person darauf aufmerksam machen könnte, dass in ihrem persönlichen Umfeld Informationen erhoben wurden. Es ist jedoch nicht ersichtlich, wieso die Ablehnung der Auskunftserteilung niemals begründungspflichtig sein sollte.

7. Parlamentarische Kontrolle (Verfassungsschutzkontrollgesetz)

Die Neustrukturierung der parlamentarischen Kontrolle durch den Entwurf eines Verfassungsschutzkontrollgesetzes ist **überaus begrüßenswert.** Die bisherigen Normen (§§ 20-22) entsprechen weder den jüngeren Vorgaben des Bundesverfassungsgerichts zur parlamentarischen Kontrolle der Exekutive[43] noch den Fortentwicklungen der Rechtsgrundlagen und der parlamentarischen Kontrollpraxis auf Bundesebene.[44]

Im Grundsatz sind sowohl die Struktur des Gesetzes als auch die wesentlichen Inhalte der Neuregelung **sinnvoll** und **werden die parlamentarische Kontrolle** des Landesamts für Verfassungsschutz **wesentlich stärken.** Dies gilt sowohl für die Wahl der Mitglieder (§ 1 Verfassungsschutzkontrollgesetz-E), als auch für die detaillierteren Unterrichtungspflichten der Landesregierung (§ 3 Verfassungsschutzkontrollgesetz-E), die erweiterten Einsichts- und Kontrollbefugnisse (§ 4 Verfassungsschutzkontrollgesetz-E, vor allem das selbstständige Akteneinsichtsrecht jedes Mitglieds,

---

[43] S. z.B. BVerfGE 124, 161 (187ff.) 137, 185 (230f.), 139, 194 (223); BVerfG, NVwZ 2018, 51.

[44] Das Kontrollgremiumgesetz des Bundes ist im Jahre 2009 zusammen mit der Einführung von Art. 45d GG grundsätzlich umgestaltet worden (Gesetz zur Fortentwicklung der parlamentarischen Kontrolle der Nachrichtendienste des Bundes v. 29.7.2009, BGBl. I S. 2346); im Jahre 2016 wurden die Regelungen zum Ständigen Bevollmächtigten in §§ 5a, 5b PKGrG ergänzt und die Rechte des Gremiums weiter ausgebaut (Gesetz zur weiteren Fortentwicklung der parlamentarischen Kontrolle der Nachrichtendienste des Bundes, BGBl. I S. 2746).

das es bisher nicht gab) und die Pflicht zur Berichterstattung (§ 6 Verfassungsschutzkontrollgesetz-E). Angesichts der erweiterten Aufgaben des Landesamts sowie seiner erheblichen personellen Aufstockung ist es daneben von besonderer Bedeutung, dass die Mitglieder der parlamentarischen Kontrollkommission gemäß § 5 Verfassungsschutzkontrollgesetz-E die Befugnis erhalten, je eine Mitarbeiterin oder einen Mitarbeiter in die Arbeit einzubeziehen.

Trotz dieser grundsätzlich positiven Bewertung gibt es an einigen Stellen der Regelung **Verbesserungsbedarf.**

Dies betrifft an mehreren Stellen die **Stellung der Opposition** im Hessischen Landtag sowie die Verfahrensrechte der ihr angehörenden Mitglieder der Kontrollkommission. Die parlamentarische Kontrolle leidet im modernen parlamentarischen System ohnehin daran, dass die Regierung von einem Parlament kontrolliert wird, dessen Mehrheit sie ins Amt gewählt hat und deshalb typischerweise politisch unterstützt. Eine effektive Kontrolle der Exekutive muss deshalb zwingend bestimmte Rechte der Opposition vorsehen. Hier bestehen mehrere offene Fragen des Entwurfs:

- Bei der Regelung zur Wahl der Mitglieder (§ 1 Abs. 3 und Abs. 4 Verfassungsschutzkontrollgesetz-E) sollte eine Ergänzung vorgenommen werden, dass **die Oppositionsfraktionen angemessen zu beteiligen sind.** Dies könnte unter Verwendung des Grundsatzes der Spiegelbildlichkeit erfolgen, der in der Ausschuss- und Gremienarbeit der parlamentarischen Demokratie anerkannt ist.[45]
- Positiv ist, dass jedes Mitglied nach § 4 Abs. 1 Satz 1 Verfassungsschutzkontrollgesetz-E nicht nur die Einberufung einer Sitzung, sondern auch die Unterrichtung der Kontrollkommission verlangen kann. Das **Mehrheitserfordernis von zwei Dritteln für die Beauftragung einer Sachverständigenperson** mit der Durchführung von Untersuchungen in § 4 Abs. 3 Satz 1 Verfassungsschutzkontrollgesetz-E entspricht demgegenüber zwar dem Quorum in § 7 Abs. 1 PKGrG, ist aber dennoch **unangemessen hoch.**[46] Statt über eine Mitgliedermehrheit in derartigen Fragen noch hinauszugehen und die Rechte der Opposition so zusätzlich zu beschränken, wäre umgekehrt zu erwägen, einer qualifizierten Oppositionsminderheit derartige verfahrensrechtliche Positionen zuzuerkennen.
- Aus demselben Grund sollte § 6 Verfassungsschutzkontrollgesetz-E um die Möglichkeit ergänzt werden, dass einzelne Mitglieder der Kontrollkommission dem Bericht an den Landtag ein **Sondervotum** beifügen.[47]

Daneben bestehen mehrere Fragen, in denen eine Änderung des Entwurfs zu einer Verbesserung der Arbeitsfähigkeit der Kontrollkommission und der parlamentarischen Kontrolle insgesamt führen würde:

- Es fehlt an einer Regelung für die Zeit zwischen dem Ende einer Wahlperiode und der Wahl eines Kontrollgremiums zu Beginn der nächsten Wahlperiode. § 3 Abs. 4 PKGrG bestimmt für diesen Fall, dass die bereits gewählten Mitglieder ihre **Tätigkeit auch über das Ende der**

---

[45] S. BVerfGE 80, 188 (222); 84, 304 (323); 112, 118 (133); 130, 318 (353 f.); 135, 317 (396).

[46] S. Nomos-BR/*Hornung*, § 7 PKGrG Rn. 4 m.w.N.

[47] Mit der entsprechenden Regelung in § 10 Abs. 2 Satz 2 PKGrG wollte der Gesetzgeber im Jahre 2009 die Transparenz erhöhen, weil dadurch mögliche Bewertungsdifferenzen innerhalb des PKGr erkennbar werden, s. die Begründung, BT-Drucks. 16/12411, 7.

Wahlperiode hinaus ausüben. Diese Regelung ist als begrenzte gesetzliche Legitimation eine zulässige Ausnahme vom Prinzip der Diskontinuität,[48] die für eine effektive Tätigkeit der parlamentarischen Kontrolle geboten ist.

- Es ist zu begrüßen, dass der oder die Vorsitzende der Kontrollkommission eine **Geschäftsstelle** zur Unterstützung erhalten wird (§ 1 Abs. 6 Verfassungsschutzkontrollgesetz-E). Es fehlt aber - auch in der Begründung - an jedem Hinweis, **welche Aufgaben** diese erfüllen und wie sie zusammengesetzt sein soll. Da es insbesondere an einer Regelung zum Umgang mit Verschlusssachen fehlt (s. für Mitarbeiterinnen und Mitarbeiter der Fraktionen § 5 Abs. 1 S. 2 Verfassungsschutzkontrollgesetz-E), dürfte die Regelung so gemeint sein, dass es sich um eine rein administrative, d.h. in keiner Weise inhaltliche Unterstützung handelt. Die effektive Arbeit der Kontrollkommission würde dagegen durch **„echte" Beschäftigte analog § 12 PKGrG** erheblich verbessert werden.[49]
- § 3 Verfassungsschutzkontrollgesetz-E regelt detailliert die regelmäßigen proaktiven Unterrichtungspflichten der Landesregierung. Demgegenüber ist die Regelung zu **Zeit, Art und Umfang der Unterrichtung** in § 3 Abs. 2 Verfassungsschutzkontrollgesetz-E **sehr vage.** Weder kommt hier eine grundsätzliche Pflicht zur Unterrichtung zum Ausdruck, noch etwaige Verweigerungsrechte der Landesregierung. Dass diese beispielsweise nach der Rechtsprechung des Bundesverfassungsgerichts[50] befugt ist, im Kernbereich exekutiven Eigenverantwortung Informationen zu verweigern (s. § 6 Abs. 2 PKGrG), kommt in der Regelung in keiner Weise zum Ausdruck. Dies sollte explizit geregelt werden.
- Die Befugnis in § 4 Abs. 2 Satz 1 Verfassungsschutzkontrollgesetz-E beschränkt sich auf die Akteneinsicht. Demgegenüber sieht § 5 Abs. 1 Satz 1 PKGrG auch eine Befugnis vor, sich **Akten und Schriftstücke**, gegebenenfalls auch im Original, **herausgeben** und in Dateien gespeicherte Daten übermitteln zu lassen. Dies wäre eine erhebliche Arbeitserleichterung auch für das Hessische Kontrollgremium.
- Die Befugnis zum Betreten der Dienststellen des Landesamts in § 4 Abs. 2 Satz 3 Verfassungsschutzkontrollgesetz-E ist explizit darauf beschränkt, dort Akten einzusehen. Es ist **weder vorgesehen, die Dienststellen zu allgemeinen Kontrollzwecken zu besichtigen, noch sind die Mitglieder der Kontrollkommission befugt, mit den Beschäftigten zu sprechen.** Beides sind jedoch essenzielle Elemente einer wirksamen Kontrolle, die auch in § 5 Abs. 1 Satz 2, Abs. 2 PKGrG enthalten sind.
- Aus demselben Grund sollte in das Gesetz eine explizite Regelung zum **Umgang mit Eingaben** durch Beschäftigte des Landesamts analog § 8 PKGrG aufgenommen werden.

---

[48] S. Nomos-BR/*Hornung*, § 3 PKGrG Rn. 4 m.w.N.

[49] Dass in dem Gesetzentwurf eine Regelung für einen ständigen Bevollmächtigten der parlamentarischen Kontrollkommission fehlt (s. auf Bundesebene §§ 5a, 5b PKGrG), ist demgegenüber sachgerecht, weil die Aufgaben des parlamentarischen Kontrollgremiums auf Bundesebene erheblich umfangreicher und komplexer sind.

[50] S. BVerfGE 67, 100 (139); 110, 199 (214 ff.); 124, 78 (120 ff.); 131, 152 (210) 137, 185 (233 ff.).

Forum InformatikerInnen
für Frieden
und gesellschaftliche
Verantwortung e. V.

Technische und gesellschaftliche Kosten des verdeckten Zugriffs auf die Grundlagen der vernetzten Gesellschaft

Sachverständigenauskunft zu dem Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen – Drucksache 19/5412

Dipl. Inf. Rainer Rehak für das FIfF
rainer.rehak@fiff.de
0D66 63E5 70A3 964A EE60D927 4427 CFE5 8C19 AE19

Dienstag, 6.2.2018
Version 1.3

Inhaltsverzeichnis

„Gegeben die technische Entwicklung, wird Freiheit und Unbeobachtbarkeit des Denkens (etwa beim Erwägen von Äußerungen oder Handlungen) künftig untrennbar mit dem Schutz persönlichster Rechner, ihrer Anwendung und auch der Daten auf ihnen verknüpft sein. [...] Der Zugriff auf gespeicherte Computerdaten auf persönlichsten Rechnern entgegen des Willens des Eigennutzers ist daher künftig weniger mit einer klassischen Hausdurchsuchung vergleichbar, als vielmehr mit der Verabreichung bewusstseinsverändernder Drogen zum Zwecke des Erlangens von Aussagen."

Prof. Dr. Andreas Pfitzmann[1]

1 Prof. Dr. Andreas Pfitzmann, Rede vor dem Bundesverfassungsgericht als Sachverständiger zur Online-Durchsuchung, 10.10.2007, Seiten 3 und 4. Pfitzmann hatte den Lehrstuhl für Datenschutz und Datensicherheit an der Technischen Universität Dresden inne.

1 Zusammenfassung und Änderungsvorschläge

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung nimmt gern zum vorliegenden Gesetzesentwurf DS-19/5412 Stellung.

Speziell die Paragraphen §6 (Quellen-TKÜ) und §8 (Online-Durchsuchung) beziehen sich auf eine technische Ermächtigung, mit der ein informationstechnisches System infiltriert werden kann. Welche Daten letztendlich ausgeleitet werden – Kommunikation oder nicht – ist technisch nicht automatisiert unterscheidbar und dementsprechend auch nicht sinnvoll einzuhegen. *QTKÜ und OD müssen daher die gleichen Eingriffshürden haben.*

Des weiteren gibt es technisch begründet wesentliche Zweifel an einer vertrauenswürdigen Protokollierbarkeit der Aktivitäten und Funde einer QTKÜ/OD auf einem infiltrierten Zielsystem. Die technischen Grundvoraussetzungen für verlässliches Logging und Signierung sind auf einem fremden System nicht gegeben. *Eine detaillierte Dokumentation jedes Zugriffs, mindestens in Form von kompletter Quellcodevorlage und -Auditierung, ist ebenso nötig, wie die rechtliche Eingrenzung auf bestimmte Zielsystemarten.*

Die heimliche Installation einer QTKÜ/OD-Software verlangt die Nutzung von Sicherheitslücken. Die dadurch entstehenden Anreize für Dritte, Sicherheitslücken nicht mehr zu melden, sondern zu verkaufen oder derartige Dienste anzubieten, schadet der allgemeinen IT-Sicherheit weltweit. Das greift langfristig die Grundlagen der vernetzten Gesellschaft an und korrodiert die digitale Infrastruktur. Zusätzlich vertreiben diese Dritten die gleichen Sicherheitslücken üblicherweise auch an Diktaturen weltweit, die damit ihre BürgerInnen kontrollieren, DissidentInnen/MenschenrechtsverteidigerInnen ausspähen und verfolgen. *Um auf eine sichere und menschenfreundliche IT-Landschaft hinzuwirken, dürfen keine Sicherheitslücken verwendet, gehandelt oder zurückgehalten werden – insbesondere keine bislang unbekannten Lücken (zerodays).*

Die These eines „Blindwerdens von Behörden“ durch Kryptographienutzung („Going-dark“) lässt sich nicht erhärten, physische Interaktionen von Kriminellen und allgemeine Effekte der Digitalisierung bieten nach wie vor hinreichende Ansatzpunkte für eine effektive Gefahrenabwehr.

Der Verfassungsschutz ist ein Geheimdienst und per definitionem ungleich intransparenter und schwerer demokratisch zu kontrollieren als etwa Polizeien. *Derartig eingriffstiefe und folgenschwere Ermächtigungen wie §6 und §8 dürfen ihm demnach grundsätzlich nicht erteilt werden.*

In der Konsequenz raten wir nachdrücklich dazu, die Paragraphen §6 (Quellen-TKÜ) und §8 (Online-Durchsuchung) ersatzlos zu streichen.

2 Vertrauen in die digitale Welt

In einer vernetzten Informationsgesellschaft,[2] die sich mehr und mehr auf digitale Infrastrukturen verlässt – vom Laptop bis zum Stromnetz – verlangt die enorme und immer größer werdende Komplexität dieser Zusammenhänge nach einem Kit, um überhaupt funktionsfähig zu bleiben. Dieser Kit ist Vertrauen, Vertrauen in technische Systeme, in deren Hersteller, in die Nutzerinnen und Nutzer und auch in staatliche Organe dahingehend, diesen neuen Umstand der Digitalisierung in der Breite sinnvoll zu nutzen, mit zu gestalten und auch, wo nötig, rechtlich einzuhegen. Dieses Vertrauen – gerade in üblicherweise als verlässlich empfundene behördliche Stellen – hat jedoch in jüngerer Vergangenheit wiederholt auf diverse Arten Schaden genommen. Dabei muss nicht über den Atlantik zur National Security Agency (NSA) geblickt werden, sondern ganz konkret auf deutsche Behörden des Sicherheitsbereichs.[3]

Angefangen bei den politischen Enthüllungen um die Operationen Glotaic[4] oder Eikonal[5], über die Nutzung der NSA-Programms XKEYSCORE durch den Verfassungsschutz[6] bis hin zum bundesweiten *Digitask*-Trojaner-Debakel[7] ist offensichtlich, dass ein erneuter Vertrauensaufbau dringend geboten ist. Und Projekte wie der gehackte „Hamburger Wahlstift", das gescheiterte „De-Mail" oder kürzlich das „besondere elektronische Anwaltspostfach" (beA) zeigen, wie kompliziert es tatsächlich ist, sensible IT-Projekte zu stemmen und Vertrauen aufzubauen. Dafür sind behutsamer Technikeinsatz, reflektiertes Vorgehen und kontinuierliche Transparenz unablässig.[8]

3 Vertraulichkeits- und Integritätserwartung

Genau diese Aspekte hatte das Bundesverfassungsgericht im Blick, als es 2008 das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) formulierte. Es ist dabei kein Grundrecht auf die zwei Schutzziele der IT-Sicherheit „Vertraulichkeit" und „Integrität", sondern ein Grundrecht auf die *Gewährleistung* der beiden, also eine wesent-

2 Nach Prof. Wolfgang Coy in Anlehnung an die McLuhansche Gutenberg-Galaxis auch „Turing-Galaxis" genannt.
3 Siehe Konferenzbeiträge der FIfFKon2014 „Der Fall des Geheimen – ein Blick unter den eigenen Teppich." 2014, TU-Berlin, https://2014.fiffkon.de.
4 Greis , Friedhelm: BND griff Daten offenbar über Tarnfirma ab, Golem.de, 24.2.2015, https://www.golem.de/news/operation-glotaic-bnd-griff-daten-offenbar-ueber-tarnfirma-ab-1502-112571.html.
5 Kehrhahn , Jobst-H.: Operation Eikonal: BND soll jahrelang Daten deutscher Bürger an NSA übermittelt haben, Heise.de, 05.10.2014, https://www.heise.de/newsticker/meldung/Operation-Eikonal-BND-soll-jahrelang-Daten-deutscher-Buerger-an-NSA-uebermittelt-haben-2411680.html.
6 Biermann , Kai: Wozu braucht der Verfassungsschutz Xkeyscore?, Zeit.de, 12.2.2016, http://www.zeit.de/digital/datenschutz/2016-02/verfassungsschutz-bfv-nsa-xkeyscore.
7 CCC: Chaos Computer Club analysiert aktuelle Version des Staatstrojaners, ccc.de, 26.10.2011, https://www.ccc.de/de/updates/2011/analysiert-aktueller-staatstrojaner.
8 Bundesamt für Sicherheit in der Informationstechnik (BSI, Hrsg): Broschüre Digitale Gesellschaft: smart & sicher, IT-Sicherheit aus Nutzer- und Expertensicht, 2017, S. 50.

liche Vorverlagerung des Schutzes. Um die zugrundeliegenden Überlegungen zu beschreiben, legte das Gericht in seiner Urteilsbegründung dar, dass der Wesensgehalt des Grundrechts der „Schutz der Vertraulichkeits- und Integritätserwartung“[9] an informationstechnische Systeme ist. Daraus lässt sich nach unserer Lesart eine klare präventive Handlungspflicht staatlicher Stellen – inklusive der gesetzgebenden – zum Schutze informationstechnischer Systeme ableiten.

3.1 Digitale Infrastrukturen

Dabei darf auch nicht nur die Privatsphäre der einzelnen Person[10] maßgeblich sein, sondern es muss immer auch die digitale Infrastruktur der vernetzten Gesellschaft mit in den Blick genommen werden, und das Vertrauen hierin. Der Begriff der „Vernetzung“ verweist hier hier keinesfalls nur auf direkte, technische Netzwerkverbindungen zwischen Geräten, sondern auch auf die vielgestaltigen Abhängigkeiten der verschiedenen Systeme und Akteure voneinander. Dies können gemeinsame Softwarehersteller sein oder aber der Einsatz bestimmter Softwarekomponenten oder Betriebssysteme an ganz verschiedenen Stellen der digitalen Landschaft. Wird also ein Hersteller oder Softwareprodukt durch bestimmte Maßnahmen und Regelungen geschützt, werden parallel dazu auch die anderswo eingesetzten Systeme, NutzerInnen und Nutzungsweisen mitgeschützt. Im Gegenzug bedeutet dies jedoch auch, dass Schädigungen oder Schwächungen von bestimmten Softwarekomponenten gleichermaßen auch alle anderen Einsatzweisen schwächt und unsicherer macht. Aus diesem Grunde war es beispielsweise möglich, dass die Schadsoftware „Wannacry“ sowohl private Laptops, als auch Krankenhaus- Eisenbahn- und Providersysteme[11] lahmlegen konnte: Millionen Systeme hatten ähnliche Softwarekomponenten – in diesem Falle das Betriebssystem Microsoft Windows – und waren damit gleichermaßen verwundbar.

Wenn wir also von einer vernetzten Gesellschaft mit „Cloud“, „Industrie 4.0“ und „smarten“ Infrastrukturen sprechen, muss immer auch die damit einhergehende gegenseitig Abhängigkeit und Verwundbarkeit mitgedacht werden.

4 Gegenstand der Stellungnahme

Wie kann eingangs beschriebene Vertrauen aufgebaut bzw. erhalten bleiben, wie können informationstechnische Systeme sicher gemacht und die Vertraulichkeits- und Integritätserwartung der BürgerInnen tatsächlich geschützt

9 Bundesverfassungsgericht: Bundesverfassungsgerichtsurteil zur Online-Durchsuchung, BverfG, 1 BvR 370/07, 27.2.2008, Abs. 206, http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.

10 Seite 40 des Gesetzesentwurfes, Drucksache 19/5412.

11 Holland, Martin und Kannenberg, Axel: WannaCry – Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm, heise.de, 12.5.2017, https://www.heise.de/newsticker/meldung/WannaCry-Angriff-mit-Ransomware-legt-weltweit-Zehntausende-Rechner-lahm-3713235.html.

werden? Diese sehr grundsätzlichen Fragen sollen hier in Bezug auf den anlassgebenden Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen angegangen werden.

Geheimdienste, also staatliche Behörden, die wesentlich auf verdeckte Maßnahmen, Tarnoperationen, „Vertrauensleute" oder verdeckte MitarbeiterInnen setzen – sind inhärent auf Intransparenz angelegt und angewiesen, da Heimlichkeit das primäre Mittel ist, die ihnen übertragenen Aufgaben auszufüllen. Ermächtigungen derartiger Dienste müssen folglich besonders kritisch analysiert werden, da einmal freigegebene Maßnahmen und ermöglichte Methoden meist nur nach Skandalen erneut zur breiten Diskussion gestellt werden (können). Auch wenn laut dem flankierenden Entwurf eines neuen Verfassungsschutzkontrollgesetzes (VSKG) nun beispielsweise jedes einzelne Mitglied der Kontrollkommission gemäß VSKG §4 Abs. 2 Akteneinsicht bekommen kann und zudem eigene MitarbeiterInnen zur Seite gestellt bekommt, besteht naturgemäß dennoch die übliche Geheimhaltungspflicht der Kommission nach VSKG §2.

Besonderheit von Geheimdiensten

In der Stellungnahme werden wir uns unserer Expertise entsprechend vordringlich den im Gesetzesentwurf angesprochenen verdeckten technischen Maßnahmen und ihren gesellschaftlichen Implikationen zuwenden – konkret der sogenannten Quellen-Telekommunikationsüberwachung (QTKÜ) und der heimlichen Online-Durchsuchung (OD)[12]. Dabei ist hervorzuheben, dass diese Maßnahmen zwei Besonderheiten aufweisen, die sie gerade in den Händen von Geheimdiensten zusätzlich problematisch erscheinen lassen: Erstens sind es aktive Maßnahmen von immenser Eingriffstiefe für die Betroffenen und zweitens sind die langfristigen Konsequenzen des Einsatzes sehr schwer abzuschätzen, weil sich die Anreizstrukturen bestimmter IT-sicherheitsrelevanter Märkte dadurch ändern können.

Eine Evaluation und Diskussion der genauen Auswirkungen solcher Maßnahmen wird beim Einsatz durch Geheimdienste wesentlich erschwert oder sogar unmöglich gemacht. Auch wenn sich die Aufgabenbereiche von Polizeien und Geheimdiensten mittlerweile gefährlich überlappen, sind dennoch die Berichts- und Transparenzpflichen von polizeilichen Behörden – im Gegensatz zu verdeckt tätigen Organisationen – immer noch grundsätzlich auf Offenheit angelegt. Wegen dieses gewichtigen Unterschieds gehen die rechtfertigenden Referenzen auf die BKAG-Entscheidung des Bundesverfassungsgerichts, wie etwa auf Seite 40 des vorliegenden Gesetzentwurfs

12 Im Text werden auch die Begriffe verdeckte Online-Datenerhebung bzw. verdeckte Online(-)Überwachung verwendet.

(Drucksache 19/5412), grundsätzlich fehl. Ein Geheimdienst ist keine Polizei und eine Polizei ist kein Geheimdienst.

Struktur der Stellungnahme

Zunächst werden einige technische Sachverhalte der Maßnahmen kommentiert und diskutiert, danach werden indirekte Auswirkungen des Einsatzes derartiger Maßnahmen auf die öffentliche Sicherheit erläutert sowie diskutiert und dann folgen resultierende Vorschläge, alternative Herangehensweisen und abschließende Überlegungen.

Ziel dieser Sachverständigenauskunft ist es, in Anlehnung an HVSG §15 Abs. 2 (Verhältnismäßigkeit) erkennbar zu machen, wie sehr die Nachteile außer Verhältnis zu etwaigen Erfolgen der angesprochenen Maßnahmen stehen.

5 Direkte Auswirkungen technischer Eigenschaften

Im ersten Abschnitt soll es um die technischen Unterschiede und Gemeinsamkeiten der Maßnahmen QTKÜ und OD gehen, wonach eine Betrachtung der Protokollierungsmöglichkeiten sowie Vertrauenswürdigkeit der Funde solcher Maßnahmen erfolgt. In dieser Stellungnahme findet sich jedoch keine vollständige Diskussion des Lebenszyklus' einer QTKÜ- bzw. OD-Software und aller vorhandenen Risiken, da dies an anderer Stelle schon ausführlich beschrieben worden ist.[13]

5.1 Die technische Natur von QTKÜ und OD

Dieser Gesetzesentwurf geht, wie andere vor ihm auch, fälschlicherweise davon aus, dass QTKÜ (§6) und OD (§8) gänzlich verschiedene Maßnahmen sind, die demnach auch getrennt voneinander betrachtet und geregelt werden können. So wird die QTKÜ im Entwurf auf Seite 37 als spezielle Form der grundrechtlich vergleichsweise „leichtgewichtigen" Telekommunikationsüberwachung beschrieben, die OD jedoch als „Sonderform" einer eingriffsintensiven Wohnraumüberwachung. Dies zeigt sich u. a.daran, dass die OD in §8 „nach Maßgabe des §7" ermöglicht wird und in §9 das Verfahren bei Maßnahmen nach den §§ 7 und 8 in einem Rutsch geregelt wird.

Auch im Verfassungsschutzkontrollgesetz (VSKG) wird derartig unterschieden: So muss nach VSKG §3 Abs. 3 Satz 2. ein jährlicher Lagebericht zur OD-Maßnahmen erstellt werden und auch dem Landtag muss laut VSKG §6 über OD-Maßnahmen berichtet werden, all dies gilt für QTKÜ-Maßnahmen nicht. Weiterhin kann eine QTKÜ nach unserer Lesart auch schon zur Quellengewinnung nach HVSG §5 Abs. 1 Satz 2 verwendet werden.

13 Rehak, Rainer: Angezapft – Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung, MV-Verlag Editon Wissenschaft, 2013.

Das ist juristisch betrachtet nachvollziehbar, doch technisch absolut nicht haltbar – mit schwerwiegenden Implikationen, denn im Entwurf wird betrachtet, was der gewünschte Zweck einer Maßnahme ist, aber ignoriert, was die tatsächliche Realisierung nach sich zieht: Alle Schritte – von der Aufbringung der Software auf das Zielsystem – also die Infiltration – über das versteckte Agieren darin, das Aktualisieren und Nachladen von Funktionalität bis hin zur Löschung – sind identisch.[14] Allein die Datensuche ist geringfügig unterschiedlich; sie ist jedoch nur abhängig von wenigen Konfigurationsparametern und selbst dieser Unterschied taugt nicht für eine Reduzierung der Eingriffstiefe, wie in 5.3 weiter ausgeführt wird. Die jeweils für die verschiedenen Maßnahmen eingesetzte Software ist also gleich mächtig und jederzeit gleichermaßen anpass- und erweiterbar. Nur ein kleiner Schalter macht aus einer QTKÜ eine OD, weil beide nach Aktivierung bereits tief im System verankert sind.

Diese Dynamik ist bei üblichen technischen Geräten nicht zu finden. Mit einem Fernseher kann man keinen Brief schreiben und mit einer Schreibmaschine kann man nicht fernsehen; die Nutzungsarten sind streng getrennt, weil sie mit unterschiedlichen Geräten realisiert werden. Ein Digitalcomputer jedoch ist eine sogenannte „Universalmaschine", die allein durch die aktuell laufende Software bestimmt jegliche (berechenbare) Funktion ausführen kann. Im Gegensatz zu physischen Maschinen lässt sich Software jedoch sehr leicht verändern und bei so ähnlichen Funktionen wie sie QTKÜ und OD erfüllen, besteht der Unterschied tatsächlich nur in einer anderen Konfigurationsdatei.

Die grundlegende Unterscheidung zwischen QTKÜ und OD ist also juristisch gewünscht, aber technisch nicht abbildbar. In der Folge müssten die beiden Maßnahmen jedoch auch grundrechtlich ähnlich behandelt werden und nicht wie im aktuellen Entwurf fundamental unterschiedlich.

Eine erhellende Analogie

Das konzeptionelle Problem lässt sich gut mit einer Analogie beschreiben. Angenommen es gäbe eine sehr günstige, leichte, kleine, genaue Maschinenpistole, die nur mit einem kleinen Schalter zwischen langsamen Einzelschuss und Automatik umgeschaltet werden könnte. Nun ist die entscheidende Frage, warum nicht normale Polizeistreifen und Spezialkommandos einfach diese gleiche Waffen bekommen sollten; die ersteren mit dem Schalter auf „leicht bewaffnet" und die letzteren mit dem Schalter auf „schwer bewaffnet"? Die Verneinung liegt in struktureller, staatlicher Selbstbeschränkung begründet. Staatliche Stellen sollen nur gerade so viel Macht zugewiesen bekommen, um

14 Ebd. Seite 16.

ihre Aufgaben zu erledigen; eine normale Polizeistreife hat eben keine Maschinenpistole.

Genau diese rechtsstaatlich gebotene Beschränkung ist mit einer QTKÜ technisch bedingt nicht umsetzbar, denn sie ist einer OD baugleich und somit gleichmächtig.

5.2 Die entscheidende Hürde

Diese „Unbeschränkbarkeit" hat auch das Bundesverfassungsgericht 2008 in seinem Urteil zur heimlichen Online-Durchsuchung ausgeführt: „Wird ein komplexes informationstechnisches System zum Zweck der Telekommunikationsüberwachung technisch infiltriert („Quellen-Telekommunikationsüberwachung"), so ist mit der Infiltration die entscheidende Hürde genommen, um das System insgesamt auszuspähen. Die dadurch bedingte Gefährdung geht weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist."[15]

Es ist demnach gänzlich unverständlich und entbehrt jeder technischen Grundlage, warum eine QTKÜ mit geringeren Eingriffshürden als die OD zur Anwendung kommen können soll. Die gleiche technische Fehleinschätzung liegt auch der StPO-Änderung von 22. Juni 2017 zugrunde, bei der die Möglichkeiten für Anwendung von QTKÜ und OD – mittels einer Formulierungshilfe – stark ausgeweitet worden sind.[16] Auch in der dortigen Anhörung hatten die technischen Sachverständigen auf dieses gravierende Problem hingewiesen – vergeblich.[17] Auch bei der Entscheidung zur Verfassungsbeschwerden gegen die Ermittlungsbefugnisse des BKA zur Terrorismusbekämpfung wurde dieser Umstand übersehen.[18]

Der Trojaner des Bundesverfassungsgerichts

Diese aus technischer Sicht rechtliche Fehlentwicklung ist in einem juristischen Winkelzug des Bundesverfassungsgerichts begründet. In einer abstrakten „Wenn-dann"-Formulierung platzierte es selbst einen Trojaner im eigenen Urteil: „Art. 10 Abs. 1 GG ist hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer „Quellen-Telekommunikationsüberwachung", wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt

15 Bundesverfassungsgericht: Bundesverfassungsgerichtsurteil zur Online-Durchsuchung, BverfG, 1 BvR 370/07, 27.2.2008, Abs. 188.

16 FIfF-Pressemitteilung vom 23. Juni 2017: Entfesselter Staatstrojaner: Große Koalition verhöhnt IT-Sicherheit und Demokratie, https://www.fiff.de/presse/pressemitteilungen/entfesselter-trojaner-grosse-koalition-verhoehnt-it-sicherheit-und-demokratie.

17 Anhörung des Rechtsausschusses, Mittwoch, 31. Mai 2017 „Änderung StGB, JGG, StPO". https://www.bundestag.de/ausschuesse/ausschuesse18/a06/anhoerungen/aenderung-stgb--jgg--stpo-2/507628

18 Gemeinsame Erklärung vom 20. April 2016, https://www.fiff.de/presse/pressemitteilungen/urteil-zum-bka-gesetz.

sein."[19] Dieser Passus ist technisch unbegründbar und inkonsistent mit dem Rest des Urteils; entweder wurde das System unter Verletzung des IT-Gewährleistungsgrundrechts infiltriert oder aber nicht. Aus Sicht der IT-Sicherheit ist Datenauswahl nach einer gelungenen Infiltration zweitrangig, das System ist kompromittiert – und außer Kontrolle.

Nun stellt aber HVSG §6 (Abs. 2) 1. genau auf diese Hintertür ab, wonach die QTKÜ anwendbar wird, wenn „sichergestellt ist, dass ausschließlich laufende Kommunikation überwacht und aufgezeichnet wird". Ignorieren wir für einem Moment alle Konzepte und Erkenntnisse der IT-Sicherheit und folgen dem Bundesverfassungsgericht ist seiner Ausnahmeregelung: Das neue konkrete Problem besteht nun darin, dass diese Beschränkung auf laufende Kommunikation prinzipiell technisch nicht sichergestellt werden kann, die Bedingung also nie erfüllt wird und dieser Passus folglich immer nur abstrakt bleiben muss.

5.3 Beschränkung auf laufende Kommunikation

Eine QTKÜ soll die Klartextdaten einer verschlüsselt ablaufenden Kommunikation erlangen, welche einer normalen Telekommunikationsüberwachung (TKÜ) nur verschlüsselt zugänglich sind. Zusätzlich dürfen nur genau die Daten der aktuell laufende Kommunikation überwacht und aufgezeichnet werden – nichts weiter.

Zu diesem Zweck müssten die Kommunikationsdaten also direkt auf dem Endgeräten vor der Verschlüsselung (beim Versand) bzw. direkt nach der Entschlüsselung (beim Empfang) auf dem Endgeräten abgegriffen werden. Auf weitere Daten – etwa Daten aus vorherigen Kommunikationsvorgängen – darf nicht zugegriffen werden.

Eine gleichzeitige Umsetzung beider Anforderungen ist praktisch nicht leistbar, wie in der technischen Literatur bereits detailliert beschrieben worden ist.[20] Exemplarisch sollen hier nur einige wesentliche Probleme erläutert werden.

Transport- und normale Datenverschlüsselung

Technisch kann zwischen Transport- und normaler Datenverschlüsselung unterschieden werden. Im ersten Fall ist die Verschlüsselung Teil des Transport-, also Versendevorgangs; beispielhaft sei dafür die HTTPS-Verschlüsselung beim Webseitenzugriff genannt. Im zweiten Fall findet die

19 Bundesverfassungsgericht: Bundesverfassungsgerichtsurteil zur Online-Durchsuchung, BverfG, 1 BvR 370/07, 27.2.2008, Absatz 190.

20 Rehak, Rainer: Angezapft – Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung, MV-Verlag Editon Wissenschaft, 2013, Seite 44 ff.

Verschlüsselung direkt auf den lagernden Daten des Systems statt; beispielhaft seien hier passwortgeschützte ZIP-Dateien genannt.

Bei den am weitesten verbreiteten Standards für E-Mailverschlüsselung (PGP[21] und S/MIME[22]) und bei jeglichen Instant-Messenger-Anwendungen (Signal[23], Whatsapp, etc) wird normale Datenverschlüsselung verwendet. Dies leuchtet ein, da die Nachrichten zunächst zum Versenden vorbereitet werden und gegebenenfalls erst später, wenn eine Verbindung mit dem Internet besteht, tatsächlich versendet werden.

Der Prozess des Versendens einer verschlüsselten Nachricht gleicht also strukturell eher dem Schützen einer ZIP-Datei mit einem Passwort und dem späteren, eventuellen Verschicken. „Eventuell" deshalb, weil etwa die meisten für Verschlüsselung konfigurierten E-Mailprogramme auch Entwürfe verschlüsselt speichern. Diese können dann später verschickt werden; oder auch nicht. Gleiches gilt für den Postausgang, aus dem noch nicht verschickte E-Mails wieder gelöscht werden können. Auch der normale Versendevorgang einer Nachricht kann abgebrochen werden, sei es weil etwas Wichtiges vergessen wurde oder weil man es sich einfach anders überlegt hat. In all diesen Fällen hat eine QTKÜ, die die Daten vor der Verschlüsselung kopieren muss, Daten überwacht und gespeichert, die nicht zu laufender Kommunikation gehören.

Ein weiteres, wesentliches Problem gerade bei mobilen Instant-Messengern ist der Zugriff auf eingehende und gespeicherte Nachrichten, denn dafür ist ein Vollzugriff auf die innerhalb der App gespeicherten Nachrichten nötig. Wenn allerdings dieser Zugriff erfolgreich ist, müssen die Daten beispielsweise nach Datum sortiert werden, was einen Zugriff auf alle Nachrichten impliziert. Wieder werden Daten überwacht, die nicht zu laufender Kommunikation gehören.

Ein Extremszenario muss noch erwähnt werden, weil es die grundrechtliche, immense Gefährdung der QTKÜ gut illustrieren kann. Um verschlüsselte Videotelefonie (Skype, etc) auszuleiten, wird von einer QTKÜ üblicherweise das Mikrofon und die Kamera angezapft, um dann anhand des System- und Softwareverhaltens zu detektieren, wann ein Gespräch stattfindet. Da die Kommunikationssoftware nicht kooperiert – der Zugriff soll ja heimlich stattfinden – ist die Erkennung laufender Kommunikation technisch nicht trivial umzusetzen. Schlägt sie fehl und es wird aufgezeichnet, obwohl keine Kommunikation stattfindet – weil etwa das Mikrofon softwareseitig stumm geschaltet ist oder ausschließlich Screensharing aktiviert ist, so ist aus der

21 OpenPGP Message Format, https://tools.ietf.org/html/rfc4880.
22 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, https://tools.ietf.org/html/rfc5751.
23 Signal protocol family, Technical Specifications, https://signal.org/docs/.

„leichtfüßigen" QTKÜ kurzerhand eine volle Wohnraumüberwachung mit Bild und Ton geworden.

Und all diese Funktionalität muss verdeckt gegen alle Abwehrmechanismen des Systems, sowie der einzelnen Softwarekomponenten durchgesetzt werden, sowie ohne selbst weitere Sicherheitslöcher im System zu erzeugen.

5.4 Detailgrad und Vertrauenswürdigkeit der Protokollierung

Der vertrauenswürdigen Protokollierung der Aktivitäten einer QTKÜ/OD kommt nicht nur wegen der Einschätzung und Verwertbarkeit der Ergebnisse eine große Bedeutung zu, sondern auch für den Schutz der Betroffenen, also der Wahrung ihrer Interessen und Rechte während der verdeckten Maßnahme.

Einerseits sollen die vorgenommenen Änderungen am System der Betroffenen detailliert protokolliert werden, sodass belegbar ist, dass diese Änderungen nach HVSG §8 (Abs. 2) möglichst minimal waren und dass sie nach Beendigung der Maßnahme automatisiert rückgängig gemacht werden können. Andererseits muss daraus hervorgehen, dass die erlangten Daten und Hinweise tatsächlich auf dem System gefunden worden sind und nicht durch Softwarefehler der QTKÜ/OD selbst erzeugt worden, von dritten platziert oder gar ein falsches System infiltriert worden ist.

Ein objektives Mindestmaß an Detailgrad und Vertrauenswürdigkeit der Protokollierung sind daher essentiell für eine derartig eingriffsintensiven Maßnahme. Es verwundert daher sehr, dass die Protokollpflicht in HVSG§ 6 (Abs. 4) für QTKÜ/OD so unbestimmt formuliert ist. Festzuhalten ist nur „das zur Datenerhebung eingesetzte Mittel" und „Angaben, die die Feststellung der erhobenen Daten ermöglichen", doch was bedeutet dies? Alles ist denkbar von der Nennung des Firmen-/Produktnamens bis hin zur Dokumentation des Quellcodes der eingesetzten Software und der ausgenutzten Sicherheitslücken auf dem Zielsystem.

Die Vergangenheit hat gezeigt, dass sich Behörden durch den unvorbereiteten externen Einkauf von QTKÜ/OD-Software gänzlich von den Bedingungen der Hersteller abhängig machen.[24] Die Verweigerung der Einsichtnahme in den Quellcode oder zurückgehaltene Informationen zu ausgenutzten Sicherheitslücken beispielsweise sind ein unhaltbarer Zustand bei derartigen Maßnahmen und müssen von Anfang an rechtlich als Mindestforderung detailliert verhindert werden. Nur so können auch unabhängige Audits zur Sicherstellung der Funktion ermöglicht werden.

24 Meister, Andre: Staatstrojaner: DigiTask verweigert Datenschutzbeauftragten Einblick in Quellcode, netzpolitik.org, 11.9.2012, https://netzpolitik.org/2012/staatstrojaner-digitask-verweigert-datenschutzbeauftragten-einblick-in-quellcode/.

Wenn es keine kommerziellen Anbieter gibt, die den rechtsstaatlichen Anforderungen entsprechen, so bliebe vor diesem Hintergrund nur die Eigenentwicklung oder Unterlassung.

Vertrauenswürdigkeit

Der zweite relevante Aspekt ist die Vertrauenswürdigkeit der Protokollierung von Softwareaktivitäten. Dabei gibt es grundsätzliche Probleme, denn die Software legt die Protokolle an, während sie auf einem „fremden" - dem infiltrierten - System agiert. Die Protokolle sind demnach stets mit Vorsicht zu interpretieren. Auch eine kryptographische Absicherung der Protokolle kommt nicht ernsthaft in Frage, da jegliches dafür nötige Schlüsselmaterial wiederum dem fremden System auch zugreifbar wäre.[25] Sobald also das fremde System die QTKÜ/OD-Software entdecken würde, könnte sie anfangen, gefälschte Protokolle zu erzeugen und kryptographisch korrekt abgesichert an die Behörden zu senden. Diese Fälschung ist im Betrieb praktisch unentdeckbar und kann auch durch nachträgliche forensische Untersuchungen kaum bemerkt werden. Diese auch nachträglich nicht aufzulösende Unkontrollierbarkeit der ohnehin schon verdeckten Maßnahme stellt eine derartig gravierende grundrechtliche Gefährdung der Betroffenen dar und sollte daher einem Geheimdienst nicht zur Verfügung stehen.

6 Auswirkungen auf die öffentliche Sicherheit

Jedes informationstechnische System enthält eine Reihe von Sicherheitsmaßnahmen, um die IT-Sicherheit des Systems zu gewährleisten, etwa dass nur Befugte Zugriff auf die dortigen Informationen haben; diese also lesen (Informationsvertraulichkeit) oder verändern (Datenintegrität) können. Wer befugt ist, entscheiden die BesitzerInnen der Systeme, und jegliche Software - vom Betriebssystem bis zum Browser - unterstützen sie bei der Durchsetzung dieser Entscheidung.

Externe Zugriffsversuche durch staatliche Akteure sind folglich aus Sicht des Systems die gleichen Angriffe, wie sie beispielsweise auch von Schadsoftware - Viren, Würmern und Trojanern - der (organisierten) Kriminalität kontinuierlich versucht werden.

Soll also ein externer Zugriff für eine QTKÜ oder OD durchgeführt werden, so müssen die systemeigenen Sicherheitsmechanismen umgangen werden, was alle Softwarehersteller wiederum nach Kräften zu verhindern suchen. Jedes hinreichend komplexe System hat jedoch auch Fehler, die, wenn sie Auswirkungen auf die Sicherheitsfunktionen des Systems haben, Sicherheits-

25 Rehak, Rainer: Angezapft – Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung, MV-Verlag Editon Wissenschaft, 2013, Seite 38 ff.

lücken genannt werden.[26] Kleine Softwareteile, die diese Lücken praktisch ausnutzen, um unbefugt Kontrolle über ein fremdes System zu erlangen, werden Expoits[27] genannt.

Sicherheit versus Sicherheit

Damit nun extern auf ein Zielsystem zugegriffen werden kann, so muss die QTKÜ/OD-Software solche Expoits nutzen, wodurch ein folgenreicher und gesellschaftlich hoch relevanter Zielkonflikt entsteht: staatliche Behörden brauchen funktionierende Exploits für Maßnahmen wie die QTKÜ und OD, doch die Sicherheit unserer IT-Infrastruktur hängt gerade davon ab, jegliche Sicherheitslücken schnellstens zu schließen. Alle informationstechnischen Systeme, von Privatgeräten, über Krankenhaus-, Eisenbahn-, Verkehrsleitsysteme bis hin zu Kraftwerkssteuerungen nutzen mittlerweile ähnliche vernetzte Softwarekomponenten, und diese müssen so sicher wie möglich gehalten werden, oder eben nicht.

Wenn der Verfassungsschutz auch im digitalen Zeitalter die „Sicherheit des Einzelnen" effektiv und auch glaubwürdig schützen möchten, wie auf der ersten Seite des Gesetzesentwurfes zu lesen ist, so muss auch er sich uneingeschränkt für die Schließung von Sicherheitslücken einsetzen. Dazu gibt es keine Alternative, will man Konzepte wie „Cloudcomputing", Datenschutz, „smart city", „Internet of things" oder „Industrie 4.0" tatsächlich ernst nehmen. Diese Erkenntnis ist Konsens in der wissenschaftlichen und praktischen IT-Sicherheit.

Globaler Schwarzmarkt von Sicherheitslücken

Doch diese Frage hat noch weitreichendere gesellschaftliche Implikationen, denn woher kommen die für eine QTKÜ/OD nötigen, noch unentdeckten Sicherheitslücken – die sogenannten Zerodays? Diese Lücken können aufwändig selbst gesucht werden, was sehr viel behördeninterne IT-Kompetenz erfordert. Wenn dann Lücken gefunden werden, so ist das ein Beleg dafür, dass auch andere diese Lücken haben finden können und sie womöglich schon ausnutzen. Eine sofortige Übermittlung an den Hersteller und ggf. das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist im Sinne der (öffentlichen) Sicherheit dringend geraten. Gleiches gilt für schon bekannte Sicherheitslücken: diese dürfen nicht genutzt, sondern müssen so schnell wie möglich geschlossen werden. Das wohl bekannteste Beispiel für den Irrweg, Lücken zu behalten, war sicherlich der oben schon erwähnte Erpresserwurm „Wannacry", der weltweit zehntausende Systeme infiltrierte und Sicherheitslücken nutze, die der US-Geheimdienst NSA seit Jahren für eine

26 Eckert, Claudia: IT-Sicherheit: Konzepte - Verfahren – Protokolle, De Gruyter Oldenbourg, 2014, Einführung.
27 Engl. für ausnutzen, ausbeuten, instrumentalisieren.

spätere Verwendung aufgehoben hatte – trotz diesbezüglicher interner Risikoabwägungsmechanismen.[28]

Die zweite Möglichkeit besteht darin Sicherheitslücken/Exploits auf dem globalen Schwarzmarkt zu kaufen und in eigene QTKÜ/OD-Software zu integrieren oder aber schon fertige Infiltrationssoftware von spezialisierten Firmen zu „mieten". Der externe Kauf bzw. das Mieten derartiger Software haben jedoch gravierende Nebeneffekte, und das nicht nur auf die IT-Sicherheit. Gerade staatliche Akteure im Sicherheitsbereich sind oft finanziell gut ausgestattet, wodurch diese Exploit-Märkte ganz wesentlich erzeugt und auch erst legitimiert werden. In der Folge wird die gesamte IT-Infrastruktur unsicherer, weil Lücken zunehmend nicht mehr an Hersteller gemeldet, sondern auf den Märkten an die Meistbietenden versteigert werden.

Sowohl beim Lückenankauf, als auch beim externen „Mieten" bleibt stets unklar, an wen die Lücken sonst noch verkauft werden. Auch wenn derartige IT-Firmen wie *Hacking Team*, zu deren Kunden beispielsweise spanische und US-amerikanische Behörden (CNI, FBI, DEA) gehören, stets bestreiten, mit Diktaturen zusammenzuarbeiten, kommt dennoch immer wieder das Gegenteil ans Licht. So verkaufte *Hacking Team* nachweislich an Behörden in Ägypten, Libanon, Aserbaidschan, Kasachstan, Sudan und Äthiopien. In veröffentlichten E-Mails an die Firma *Hacking Team* bedankten sich die staatlichen Stellen der Diktaturen dafür, „oppositionelle Ziele [nun] schnell identifizieren zu können".[29]

Gleiches lässt sich über die aktuell vom Bundeskriminalamt (BKA) beauftragte[30] deutsche Firma Gamma/FinFisher berichten, die u. a. den *FinSpy-QTKÜ*-Trojaner herstellt, der nun eingesetzt werden soll.[31] FinSpy wurde damals auch von bahrainischen Behörden genutzt, um DissidentInnen zu verfolgen und den Arabischen Frühling niederzuschlagen.[32] Weitere Kunden der Firma sind Behörden in Diktaturen wie Dubai oder Katar, aber auch die Mongolei und Indonesien.[33] Dabei werden auch diese Firmen immer

28 Hay Newman, Lily: Feds Explain Their Software Bug Stash—But Don't Erase Concerns, wired.com, 15.11.2017, https://www.wired.com/story/vulnerability-equity-process-charter-transparency-concerns/.

29 Borchers, Detlef: Überwachungssoftware: Aus Hacking Team wurde Hacked Team, heise.de 6.7.2015, https://www.heise.de/security/meldung/Ueberwachungssoftware-Aus-Hacking-Team-wurde-Hacked-Team-2736160.html.

30 Meister, Andre: Geheimes Dokument: Das BKA will schon dieses Jahr Messenger-Apps wie WhatsApp hacken, netzpolitik.org, 20.7.2017, https://netzpolitik.org/2017/geheimes-dokument-das-bka-will-schon-dieses-jahr-messenger-apps-wie-whatsapp-hacken/.

31 dpa/pbe: Grünes Licht für den gekauften Staatstrojaner, spiegel.de, 2.2.2018, http://www.spiegel.de/netzwelt/netzpolitik/smartphone-ueberwachung-bka-darf-gekauften-staatstrojaner-jetzt-einsetzen-a-1191112.html.

32 Meister, Andre: Gamma FinFisher: Überwachungstechnologie „made in Germany" gegen Arabischen Frühling in Bahrain eingesetzt, netzpoltik.org, 8.8.2014, https://netzpolitik.org/2014/gamma-finfisher-ueberwachungstechnologie-made-in-germany-gegen-arabischen-fruehling-in-bahrain-eingesetzt/.

33 Meister, Andre: Gamma FinFisher: Neue Analyse des Staatstrojaners deutet auf weitere Kunden hin, Netzpoltiik.org, 9.8.2012, https://netzpolitik.org/2012/gamma-finfisher-neue-analyse-des-staatstrojaners-deutet-auf-weitere-kunden-hin/.

wieder gehackt und dann die Software, Sicherheitslücken und interne Dokumente veröffentlicht.[34]

Das ist der aktuelle, katastrophale Zustand der weltweiten IT-Sicherheit, und deutsche Behörden helfen mit, diesen status quo aufrecht zu erhalten. Wir halten das wir für inakzeptabel.

In der wohlwollenden Interpretation unterstützen deutsche Behörden mit Steuergeldern nur derartig schäbige Geschäftsmodelle, im der besorgniserregenderen Deutung finanziert Deutschland Firmen, die direkt oder indirekt an der Verfolgung von DissidentInnen und MenschenrechtsverteidigerInnen in Diktaturen beteiligt sind.[35] Dies ist neben dem eigentlichen Skandal zudem eine denkbar schlechte Position, um auf eine Lösung des dringenden Problems der globalen IT-Sicherheit hinzuarbeiten

Es kann nicht im Interesse Deutschlands sein, international wirksame Anreize zu schaffen und zu stützen, die diametral dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entgegenstehen, deswegen darf auch der Verfassungsschutz derartige Aktivitäten nicht unterstützen.

Wenn es tatsächlich um Sicherheit gehen soll, so muss die Suche nach Sicherheitslücken strukturiert, koordiniert und konsequent angegangen werden, ohne Ausnahme. Die globalisiert-vernetzte Informationsgesellschaft bedeutet mittlerweile eben auch: es gibt keine öffentliche Sicherheit mehr ohne IT-Sicherheit.

7 Alternative Ansätze zu staatlichem Hacking

In den USA und auch in Deutschland findet sich die Argumentation, dass das Aufkommen von Ende-zu-Ende-verschlüsselten Kommunikationskanälen die Arbeit von Sicherheitsbehörden zunehmend erschwert. Der Zweck von QTKÜ und OD ist die Aufklärung und Informationsbeschaffung zur Gefahrenabwehr, weil dies scheinbar nicht mehr ohne Direktzugriff auf Endgeräte geht. Doch einer tieferen Analyse hält dieses Argument nicht stand, wie unter anderem in einem Report des Berkman Center for Internet & Society der Harvard University zu lesen ist.[36] Darin wird ausgeführt, wie sich durch die technische Weiterentwicklung auch immer neue Informationsquellen auftun, angefange bei der Analyse von Metadaten bis hin zu Firmen, deren Geschäftsmodelle gerade davon abhängen, keine Ende-zu-Ende-Verschlüsselung zu nutzen. Dabei

34 Meister, Andre: Gamma FinFisher gehackt: Werbe-Videos von Exploits und Quelltext von FinFly Web veröffentlicht, Netzpolitik.org, 6.8.2014, https://netzpolitik.org/2014/gamma-finfisher-gehackt-werbe-videos-von-exploits-und-quelltext-von-finfly-web-veroeffentlicht/.

35 Amnesty International: A year ago, Ahmed Mansoor's iPhone was targeted using elite spyware only sold to governments, amnesty.org, 2017, https://www.amnesty.org/en/get-involved/take-action/free-ahmed-mansoor/.

36 Schneier, Bruce, et al: Don't Panic: Making Progress on the „Going Dark" Debate, Berkman Center for Internet & Society, Harvard University, 1.2.2016, https://cyber.harvard.edu/pubrelease/dont-panic/.

geht es uns bestimmt nicht darum, gewissen datenschutzaversen Firmen das Wort zu reden, sondern zu überlegen, wie die stetige Digitalisierung in anderer Weise zur Gefahrenabwendung genutzt werden kann, ohne dabei die eigene Infrastruktur zu kompromittieren. Auch ohne Verschlüsselung haben Menschen mit der zunehmenden Verlagerung ins Digitale neue Alternativen, sich vor QTKÜ und OD von Behörden zu schützen.[37]

Die Motivation der Gesetzesänderung verdient ebenso einen Kommentar, auch wenn sich diese Stellungnahme speziell mit QTKÜ und OD beschäftigt. An vielen Stellen im Entwurf ist von Terror die Rede, insbesondere durch den NSU, aber auch auf andere Taten wird Bezug genommen. An dieser Stelle sei jedoch die Frage gestattet, wo QTKÜ oder OD tatsächlich die primäre Lösung hätten sein können, es also keine anderen Erfolgsansätze hätte geben können? Drei Beispiele aus der aktuellen Terror-und-Verschlüsselung-Debatte seien hier einmal kurz kommentiert:

1) Gerade im skandalösen Fall des NSU und seiner (Nicht-)Aufklärung waren fehlende QKTÜ/OD-Fähigkeiten sicherlich das kleinste Problem im ganzen Debakel.[38]

2) Im Fall der rechtsextremen „Oldschool Society" (OSS), weitläufig bekannt durch den höchst strittigen Telegram-Hack durch das BKA, waren die so erlangten Informationen vor dem Münchner Oberlandesgericht für die Verurteilung letztendlich gar nicht verwendet worden.[39]

3) Der weltweit berühmte Fall um die San-Bernadino-Bomber und ihr verschlüsseltes iPhone machte zwar gute Schlagzeilen für Apple, basierte jedoch auf einem Password-Reset-Fehler der Ermittler, der dann erst den extrem teuren Hack nötig machte. Das Öffnen des iPhones brachte im Übrigen gar keine nützlichen Informationen hervor.[40]

Insgesamt sehen wir die Begründung der neuen IT-Befugnisse in Bezug auf die im Entwurf benannten terroristischen Straftaten und Ereignisse also mit kritischer Vorsicht. Auch wenn der Zweck Terrorismusbekämpfung die volle Unterstützung verdient, scheinen uns die technischen Infiltrationsbefugnisse doch über das Ziel hinaus zu schießen. Gerade bei den im Entwurf genannten Ereignissen lohnt es sich, detailliert zu durchdenken, inwiefern eine QTKÜ/OD jeweils hilfreich und zwingend notwendig gewesen wäre, insbesondere weil in

37 Wood, Andrew Keane: Encryption Substitution, Hoover Institution, Stanford University, 18.7.2017, www.hoover.org/sites/default/files/research/docs/woods_encryption_substituteswebreadypdf.pdf.

38 Pichl, Maximilian: Von Aufklärung keine Spur: 20 Jahre NSU- Komplex, Blätter für deutsche und internationale Politik, 1/2018, https://www.blaetter.de/archiv/jahrgaenge/2018/januar/von-aufklaerung-keine-spur-20-jahre-nsu-komplex.

39 Braun, Sven: Bundeskriminalamt knackt Telegram-Accounts, netzpolitik.org, 26.08.2016, https://netzpolitik.org/2016/bundeskriminalamt-knackt-telegram-accounts/.

40 Ellen Nakashima: Comey defends FBI's purchase of iPhone hacking tool, washingtonpost.com, 11.5.2016, https://www.washingtonpost.com/world/national-security/comey-defends-fbis-purchase-of-iphone-hacking-tool/2016/05/11/ce7eae54-1616-11e6-924d-838753295f9a_story.html.

einigen Fällen die Täter schon vorher bekannt waren und etwa der Anschlag am Breitscheidtplatz in Berlin offenbar sogar mit Involvierung von V-Leuten durchgeführt worden ist.[41]

Dieser Kommentar ist an dieser Stelle wichtig, da insbesondere die hier diskutierten verdeckten Methoden der Informationstechnik sehr, sehr teuer sind und es muss reflektiert werden, ob diese Mittel nicht gesellschaftlich weitaus sinnvoller angelegt werden können – von Polizeipersonal[42] bis Schulangebote, als auf den Konten zwielichtiger Schwarzmarkthändler, deren Geschäftsmodell die Unsicherheit unserer IT-Infrastruktur, die Festigung von Diktaturen und das ungehinderte[43] Verfolgbarmachen von Menschenrechts-verteidigerInnen ist.

In der ganzen Debatte ist noch viel Bewegung über den richtigen Weg zum gleichen Ziel. Wir jedenfalls sehen nicht, dass die Geheimdienste blind werden, wenn sie keine Telefone infiltrieren können. Kriminalstatistiken sowie Aufklärungsraten geben uns glücklicherweise auch keinen Anlass zur Sorge, diese Diskussion übereilt abschließen zu müssen.

8 Offensive Unsicherheit

Der aktuelle Vorstoß, Geheimdiensten wie dem Verfassungsschutz die Ermächtigung zu geben, informationstechnische Systeme zu infiltrieren, ist in in einen stetigen, sehr beunruhigenden Trend einzuordnen: Der schrittweise Ausbau von informationstechnischen Offensivfähigkeiten der Behörden im Sicherheitsbereich.

Sowohl der Bundesnachrichtendienst (BND) hat mit seiner „Strategische Initiative Technik" die Fähigkeiten bekommen, technische Systeme verdeckt und offen angreifen können[44] als auch die Bundeswehr mit der „Strategische Leitlinie Cyber-Verteidigung", die explizit – anders als der Name impliziert – auch „offensive Cyber-Fähigkeiten" als „Wirkmittel" vorsieht.[45]

Wie erwartet war die Kritik aus den Kreisen der Informatik für eine derartige Offensivausrichtung bei einem gleichzeitig so desaströsen Zustand der

41 Goll, Jo und Adamek, Sascha: V-Mann soll Gruppe um Amri zu Anschlägen aufgehetzt haben, rbb, 19.10.17, https://www.rbb24.de/politik/beitrag/2017/10/amri-von-v-mann-angestachelt-anschlag-berlin-breitscheidplatz.html.

42 „Die Stadt wächst seit Jahren, unser Personalbestand aber nicht, das schafft jede Menge Tatgelegenheiten", aus Scheffer, Ulrike und Zawatka-Gerlach, Ulrich: Berlin ist die Hauptstadt des Verbrechens, tagesspiegel.de, 24.4.2017, http://www.tagesspiegel.de/politik/kriminalstatistik-2016-berlin-ist-die-hauptstadt-des-verbrechens/19711644.html.

43 Loll, Anna Catherin: Lieber ohne Menschenrechte exportieren, zeit.de, 17.9.2017, http://www.zeit.de/wirtschaft/2017-09/exporte-menschenrechte-dual-use-diktaturen/komplettansicht.

44 Meister, Andre: Strategische Initiative Technik: Wir enthüllen, wie der BND für 300 Millionen Euro seine Technik aufrüsten will, netzpolitik.org, 21.9.2015, https://netzpolitik.org/2015/strategische-initiative-technik-wir-enthuellen-wie-der-bnd-fuer-300-millionen-euro-seine-technik-aufruesten-will/.

45 Gebauer, Matthias: Von der Leyen rüstet an der Cyberfront auf, spiegel.de, 10.7.2015, http://www.spiegel.de/politik/deutschland/bundeswehr-ursula-von-der-leyen-ruestet-an-der-cyber-front-auf-a-1042985.html.

eigenen IT-Sicherheit immens.[46] Da werden viele hundert Millionen Euro in geheime IT-Angriffsstrategien investiert; und beispielsweise für das „Nationale Referenzprojekt zur IT-Sicherheit in Industrie 4.0"[47] - als Absicherung der Zukunft der deutschen Industrie - gibt es 33 Millionen Euro, ganze fünf Millionen Euro weniger, als für das krachend gescheiterte „besondere elektronische Anwaltspostfach" (BeA) ausgegeben worden ist.[48]

Spätestens an dieser Stelle wird klar, dass es keine digitale Gesamtstrategie gibt, doch das Resultat dieser Flucht nach vorn ist eine selbst initiierte Korrosion der Grundlagen unserer vernetzten Gesellschaft. Und genau in diese Kerbe schlägt auch dieses Gesetz mit seinen Ermächtigungen.

Mit dieser Fahrtrichtung wird es stetig schwieriger, langfristig auf eine globale Ächtung des Handels mit Sicherheitslücken oder sonstige Beschränkungen der strukturellen Verminderung der IT-Sicherheit hinzuarbeiten; und das wäre langfristig die einzig vernünftige Grundlagenstrategie einer Digitalisierung. Wenn diese Position aber glaubhaft vertreten werden soll, so müssen konsequent alle Ressourcen in die Verbesserung und Absicherung der Technik investiert werden, denn ist langfristig die beste Investition in öffentlich (IT-)Sicherheit überhaupt.[49]

In diesem Lichte muss nun auch HVSG § 15 Abs. 1 verstanden werden, wodurch die Erläuterung zu §6 Abs. 2, dass über technische Mittel gewonnene Informationen nicht die Problematik einer Mitarbeiter- bzw. Quellengefährdung bergen, wieder wesentlich relativiert wird: gefährdet wird dann eben die Allgemeinheit.

Differenzierungsmöglichkeiten

Dabei geht der Entwurf nicht einmal behutsam mit der Zielmaterie um. Es gibt keine Differenzierung nach Gerätearten, aktuell wäre die Ermächtigung gültig für PCs, Laptops, Tablets und Mobiltelefone, aber auch für Autos, Herzschrittmacher, Assistenzsysteme wie Alexa/Home/etc, Krankenhaussysteme, Hafenkrananlagen, Industriesteuerungen, „smarte" Fernseher, Türsteuerungen, Heizungsthermostate, Fitnessarmbänder, „smarte" Zahnbürsten bis hin zur vernetzten Spielzeugpuppe.[50] Immer nur theoretisch begrenzt vom abstrakten Verhältnismäßigkeitsparagraphen HVSG § 15, der jedoch bei QTKÜen in der aktuellen Ausgestaltung des Gesetzes gar nicht effektiv von

46 Meister, Andre, Geheime Cyber-Leitlinie: Verteidigungsministerium erlaubt Bundeswehr „Cyberwar" und offensive digitale Angriffe, netzpolitik.org, 30.7.2015, https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/.

47 Dipl.-Ing. Simon Duque Antón, Deutsches Forschungszentrum Künstliche Intelligenz (DFKI), https://www.dfki.de/web/forschung/projekte?pid=945.

48 Böck, Hanno: Noch mehr Sicherheitslücken im Anwaltspostfach, golem.de, 4.1.2018, https://www.golem.de/news/bea-noch-mehr-sicherheitsluecken-im-anwaltspostfach-1801-131942.html.

49 Siehe unsere Kampagne „Cyberpeace", https://cyberpeace.fiff.de.

50 Kühl, Eike: Vernichten Sie diese Puppe, zeit.de, 17.2.2017, http://www.zeit.de/digital/datenschutz/2017-02/my-friend-cayla-puppe-spion-bundesnetzagentur/komplettansicht.

der Kontrollkommission überprüft werden kann, weil es keine aktiven Lageberichte gibt.

Auch die Belehrung ausländischer Stellen über Zweckbindung der übermittelten Daten und ggf. zu verlangende Auskunft nach HVSG § 22 Abs. 3. klingen eher unbedacht. Zumindest der offizielle Fragekatalog der Bundesregierung an die USA nach den Snowden-Enthüllungen im Jahr 2013 ist bis dato unbeantwortet geblieben. Diese Möglichkeit muss vor einer Übermittlung an ausländische Stellen in Betracht gezogen und dann ggf. neu abgewogen werden.

8.1 Abschluss

Letztlich sind in diesem Entwurf bezüglich der QTKÜ und OD keinerlei wirksamen Grenzen zum Schutze des eigentlich „absolut geschützten Kernbereichs privater Lebensgestaltung" erkennbar und auch keine Ansätze, die langfristigen gesamtgesellschaftlichen Auswirkungen der Maßnahmen auf die öffentliche (IT-)Sicherheit entgegen zu wirken.

Auch die Vorgaben für das IT-Gewährleistungsgrundrecht wurden verwässert. So wurde die verfassungsrechtliche Vorgabe für eine Infiltration zum Schutz von „Güter[n] der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt"[51] umgewandelt in den Schutz von „Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist.[52] Diese neue Formulierung ist unserer Ansicht nach viel zu weit auslegbar.

Diese Gründe, zusammengenommen mit der prinzipiell geringen Transparenz eines Geheimdienstes, sorgen dafür, dass wir dringend zu einer ersatzlosen Streichung dieser beiden Ermächtigungen HVSG §6 und §8 raten.

Abschließend sei noch angemerkt, dass die vom Bundesverfassungsgericht formulierten Leitsätze und Überlegungen grundsätzlich nur den allerletzten verfassungsmäßigen Rahmen aufzeigen sollen, in welchem sich der Gesetzgeber unbedingt bewegen muss. Es besteht überhaupt keine Pflicht und Notwendigkeit, diesen Rahmen immer zwingend auszuschöpfen. Es zeugt unserer Ansicht nach eben nicht von Wertschätzung dieser Werte und Grenzen, wenn sie vom Gesetzgeber auffallend oft berührt und leider auch regelmäßig überschritten werden. Genau zu dieser Abgrenzungsthematik schrieb das Bundesverfassungsgericht 2004 im Urteil zum großen Lauschangriff: „Inzwischen scheint man sich an den Gedanken gewöhnt zu haben, dass mit den mittlerweile entwickelten technischen Möglichkeiten auch deren grenzenloser Einsatz hinzunehmen ist. Wenn aber selbst die

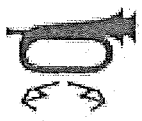
51 Bundesverfassungsgericht: Bundesverfassungsgerichtsurteil zur Online-Durchsuchung, BverfG, 1 BvR 370/07, 27.2.2008, 2. Leitsatz, http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.

52 HVSG §7 Satz 3.

persönliche Intimsphäre [...] kein Tabu mehr ist, vor dem das Sicherheitsbedürfnis Halt zu machen hat, stellt sich auch verfassungsrechtlich die Frage, ob das Menschenbild, das eine solche Vorgehensweise erzeugt, noch einer freiheitlich-rechtsstaatlichen Demokratie entspricht."[53] Im vorliegenden Fall ist eine Ablehnung der Befugnisse sogar im Namen der Sicherheit sinnvoll.

9 Über das FIfF

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V. ist ein deutschlandweiter Zusammenschluss von Menschen, die sich kritisch mit Auswirkungen des Einsatzes der Informatik und Informationstechnik auf die Gesellschaft auseinandersetzen. Unsere Mitglieder arbeiten überwiegend in informatiknahen Berufen, vom IT-Systemelektroniker bis hin zur Professorin für Theoretische Informatik. Das FIfF wirkt in vielen technischen und nichttechnischen Bereichen der Gesellschaft auf einen gesellschaftlich reflektierten Einsatz von informationstechnischen Systemen zum Wohle der Gesellschaft hin. Zu unseren Aufgaben zählen wir Öffentlichkeitsarbeit, sowie Beratung und das Erarbeiten fachlicher Studien. Zudem gibt das FIfF vierteljährlich die „FifF-Kommunikation – Zeitschrift für Informatik und Gesellschaft" heraus und arbeitet mit anderen Friedens- sowie Bürgerrechtsorganisationen zusammen.



53 Bundesverfassungsgericht: Bundesverfassungsgerichtsurteil zum großen Lauschangriff, BverfG, 1 BvR 2378/98, 3.3.2004, Absatz 373, http://www.bundesverfassungsgericht.de/entscheidungen/rs20040303_1bvr237898.html.

Für alle Links gilt: letzter Zugriff: 2.2.2018.

GESELLSCHAFT
FÜR INFORMATIK

STELLUNGNAHME ZU DEN DRUCKSACHEN 19/5412 UND 19/5782

Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen

Prof. Dr. Hannes Federrath
Universität Hamburg, Fachbereich Informatik
Präsident der Gesellschaft für Informatik e.V. (GI)

6. Februar 2018

Vorbemerkungen

Die Gesellschaft für Informatik beschränkt sich in dieser Stellungnahme auf Artikel 1 des Gesetzesentwurfs und dort insbesondere auf die Erweiterung der Befugnisse des Landesamts zur Quellen-Telekommunikationsüberwachung nach § 6 Abs. 2-4 Hessisches Verfassungsschutzgesetz (HVSG) und zum verdeckten Zugriff auf informationstechnische Systeme (§ 8 HVSG). Diese Befugniserweiterung berührt nicht nur die Grundrechte der betroffenen Personen, sondern auch die Sicherheit informationstechnischer Systeme und somit die Fundamente der digitalen Gesellschaft.

Beschaffung von Sicherheitslücken

Sowohl die Maßnahmen zur Telekommunikationsüberwachung (§ 6 Abs. 2-4 HVSG) als auch zum verdeckten Zugriff auf IT-Systeme (§ 8 HVSG) erfordern das Ausführen von Software auf dem System einer Zielperson. Damit Software dort ohne physischen Zugang zur Ausführung gebracht werden kann, muss sie entweder von der Zielperson selbst unbewusst gestartet werden (etwa durch das Klicken auf einen E-Mail-Anhang) oder durch die Ausnutzung einer Sicherheitslücke auf dem System der Zielperson eingespielt und gestartet werden. Eine solche Sicherheitslücke kann entweder in der Betriebssoftware (Firmware und/oder Betriebssystem) oder in einer Anwendungssoftware, die die Zielperson installiert hat, vorliegen. Das Einspielen der Software mittels einer Sicherheitslücke wird

GESELLSCHAFT
FÜR INFORMATIK

gewöhnlich ohne Zutun und Kenntnisnahme der Zielperson erfolgen und setzt somit nicht die Unachtsamkeit oder Fahrlässigkeit der Zielperson voraus, wodurch die Gefahr einer Entdeckung sinkt.

Damit der Eingriff über eine Sicherheitslücke im Betriebssystem oder in einer anderen Software erfolgreich sein kann, ist eine Sicherheitslücke erforderlich, die der Allgemeinheit, insbesondere aber den Herstellern der Betriebssoftware, der Anwendungssoftware und zusätzlich den Herstellern von Malware-Scannern bisher unbekannt ist. Bei bekannten Sicherheitslücken würde ein Einspielversuch auf Systemen mit aktuellen Sicherheitsupdates scheitern. Wird ein aktueller Malware-Scanner genutzt, kann der Versuch sogar entdeckt werden.

Die Kenntnis von bisher unbekannten Sicherheitslücken ist entweder durch eigene (hier: durch oder im Auftrag des Bedarfsträgers) Suche nach ausnutzbaren Softwarefehlern zu erlangen oder durch Ankauf von Informationen zu solchen Sicherheitslücken. Ein wesentlicher Anteil der Nachfrage auf dem gewerblichen Markt für Sicherheitslücken kommt von Cyber-Kriminellen, die unbekannte Sicherheitslücken beispielsweise als Grundlage für Erpressungssoftware (sog. Ransomware) benötigen.

Die auf solchen Märkten angebotenen Sicherheitslücken werden von ihren Entdeckern zunächst geheim gehalten. Der staatliche Ankauf von Sicherheitslücken stärkt solche geheimen Märkte und verringert die Motivation von Hackern, Sicherheitslücken in einer verantwortungsvollen Weise den Software-Herstellern zu melden, diesen genügend Zeit zum Schließen der Lücken einzuräumen, um ggf. anschließend die Lücke zu veröffentlichen.

Die Gesellschaft für Informatik fordert eine Melde- und Veröffentlichungspflicht von Sicherheitslücken, nachdem sie geschlossen sind, um Bürger, öffentliche Verwaltung und Unternehmen in die Lage zu versetzen, die IT-Sicherheitsrisiken realistisch einzuschätzen und frühzeitig geeignete Schutzmaßnahmen zu ergreifen.

Verbreitung von Sicherheitslücken

Damit der Zugriff auf das System einer Zielperson gelingt, werden zumeist Sicherheitslücken ausgenutzt, die in einer Vielzahl von Systemen existieren, weil sie dann mit hoher Wahrscheinlichkeit auch bei einer Zielperson ausgenutzt werden können. Solche der Öffentlichkeit bzw. den Soft-

GESELLSCHAFT
FÜR INFORMATIK

wareherstellern bisher unbekannte Sicherheitslücken (zumeist von IT-Sicherheitsexperten als Zero-Day-Exploits bezeichnet) stellen nicht nur eine Verwundbarkeit für einzelne, eingrenzbare Systeme von Zielpersonen dar, sondern setzen die Allgemeinheit der Gefahr aus, dass während einer Überwachungsmaßnahme auch Kriminelle diese Sicherheitslücken ausnutzen.

Die Geheimhaltung einer Sicherheitslücke durch Behörden ist kein geeigneter Schutz vor den Gefahren dieser Sicherheitslücke. Erstens werden Sicherheitslücken auf den o.a. geheimen Märkten nicht exklusiv angeboten. Zweitens kann eine existierende Lücke jederzeit erneut entdeckt und anderswo angeboten und ausgenutzt werden. Drittens werden die auf den geheimen Märkten angebotenen Sicherheitslücken üblicherweise auch nicht, nachdem die fragwürdige gewerbliche Nutzung abgeschlossen ist, auf verantwortungsvolle Weise den Software-Herstellern gemeldet, sondern bleiben weiterhin länger geheim, als dies für eine konkrete staatliche Maßnahme eigentlich erforderlich ist. Insbesondere hier leistet die staatliche Überwachung mit solchen Methoden nach Auffassung der Gesellschaft für Informatik der Unsicherheit und Schutzlosigkeit von Bürgern und Unternehmen unverantwortlichen Vorschub.

Schäden, die für die Allgemeinheit durch behördlich bekannte Sicherheitslücken entstehen, sind vermeidbare Schäden. Die Beseitigung der Sicherheitslücken zum Schutz der Allgemeinheit sollte Vorrang vor der Zugriffsmöglichkeit durch Behörden haben, gerade auch, weil das Ausmaß der Folgeschäden für Bürger und Unternehmen (insbesondere im Bereich der kritischen Infrastrukturen) gar nicht abschätzbar ist und somit eine Abwägung nicht vorgenommen werden kann.

Gefahr für kritische Infrastrukturen

Sicherheitslücken in Standardsoftware für Endanwender, wie sie für Eingriffe nach Maßgabe der vorliegenden Gesetzesänderung benötigt werden, stellen eine Gefahr für kritische Infrastrukturen dar. Standardsoftware wie etwa das Betriebssystem Windows wird ebenfalls in Behörden, bei Energieversorgern und in Krankenhäusern eingesetzt. Grundbausteine dieser Standardsoftware finden sich beispielsweise auch in Spezialsoftware für die Anlagensteuerung in Verkehrssystemen und Kernkraftwerken wieder, wodurch diese Systeme ebenfalls verwundbar werden bzw. bleiben.

GESELLSCHAFT
FÜR INFORMATIK

Teile der kritischen Infrastruktur sind nach Bekanntwerden einer Sicherheitslücke zudem länger verwundbar als Systeme von Endanwendern, da sie aufgrund notwendiger Stabilitätstests oder komplexerer Update-Prozesse weniger schnell auf das Bekanntwerden einer Sicherheitslücke und die Bereitstellung eines Sicherheitsupdates reagieren können. Umso mehr ist es für die Sicherheit kritischer Infrastrukturen erforderlich, dass Sicherheitslücken schnell, zuverlässig und kontrolliert geschlossen und anschließend mit ausreichender Vorwarnzeit veröffentlicht werden.

Unkontrollierbarkeit eines Eingriffs

Technische Mittel zum Eingriff in informationstechnische Systeme einer Zielperson haben unübersehbare Konsequenzen und gefährden die Integrität und Vertraulichkeit dieser Systeme. Eine Einschränkung der Funktionalität der technischen Mittel auf einen lediglich lesenden Zugriff oder auf ausgewählte Anwendungssoftware (z.B. verschlüsselnde Chat-Programme) unterliegt zwangsläufig immer dem Vorbehalt der Korrektheit dieser Mittel. In der Praxis ist es nicht auszuschließen, dass ein eingesetztes technisches Mittel aufgrund eines Fehlers von vorgesehenen Einschränkungen abweicht oder durch eigene Sicherheitslücken das System in einen durch Dritte verwundbaren Zustand versetzt. Dies kann Folgeschäden nach sich ziehen, für die der Verursacher – hier eine staatliche Stelle – verantwortlich ist.

Fazit und Forderungen

Die Gesellschaft für Informatik lehnt den vorliegenden Gesetzesentwurf für die Neuausrichtung des Verfassungsschutzes Hessen in dieser Form ab und sieht hinsichtlich der informationstechnischen Aspekte des Gesetzesentwurfs folgenden Handlungs- und Änderungsbedarf:

1. Ein Eingriff in informationstechnische Systeme unter Ausnutzung unbekannter Sicherheitslücken ist zu untersagen.

2. Bei Kenntnisnahme von bisher unbekannten Sicherheitslücken sind Behörden dazu zu verpflichten, diese unverzüglich an den Hersteller zu melden und kontrolliert zu veröffentlichen.

GESELLSCHAFT
FÜR INFORMATIK

3. Ein staatliches Förderprogramm zur Suche nach Sicherheitslücken in Software mit dem Ziel der Behebung der Schwachstellen ist einzurichten.

Danksagung

Für die fachliche Zuarbeit bei der Erstellung dieser Stellungnahme danke ich meinen wissenschaftlichen Mitarbeitern Christian Burkert und Matthias Marx.

Kontakt

Prof. Dr. Hannes Federrath
Präsident der Gesellschaft für Informatik e.V. (GI)
E-Mail: hannes.federrath@gi.de

Universität Hamburg, Fachbereich Informatik,
Arbeitsbereich Sicherheit in Verteilten Systemen (SVS)
Web: svs.informatik.uni-hamburg.de

Gesellschaft für Informatik e.V. (GI)

Geschäftsstelle Berlin
im Spreepalais am Dom
Anna-Louisa-Karsch-Str.2, 10178 Berlin
Tel.: +49 30 7261 566-15
Mobil: +49 163 8694216
Fax: +49 30 7261 566-19
E-Mail: berlin@gi.de

Geschäftsstelle Bonn
im Wissenschaftszentrum
Ahrstr. 45, 53175 Bonn
Tel.: +49 228 302-145
Fax: +49 228 302-167
E-Mail: bonn@gi.de

Web: www.gi.de