Anwaltsverband Baden-Württemberg
im Deutschen **Anwalt**Verein e. V.

Anwaltsverband Baden-Württemberg – Postfach 1221 – 70808 Korntal-Münchingen

Ministerium für Inneres, Digitalisierung und Migration BW
Herrn Ministerialdirigent Herbert Hellstern
Frau Dr. Maximiliane Friederich
Willy-Brandt-Str. 41
70173 Stuttgart

Hasenbergsteige 5
70178 Stuttgart

Geschäftsstelle:
Johannes-Daur-Straße 10
70825 Korntal-Münchingen

Postfach 1221
70808 Korntal-Münchingen

Telefon 0711 / 2 36 59 63
Telefax 0711 / 2 55 26 55

www.av-bw.de
info@av-bw.de

14. August 2017

Per E-Mail (poststelle@im.bwl.de)!

Az. 4-1080/194-1
Änderung des Landesverfassungsschutzgesetzes (LVSG) und des Ausführungsgesetzes zum Artikel 10-Gesetz (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses nach Art. 10 GG)
- Stellungnahme des Anwaltsverbandes BW im DAV e. V.

Sehr geehrter Herr Ministerialdirigent Hellstern,
sehr geehrte Frau Doktor Friederich,

vielen Dank für die Übermittlung der Anhörungsunterlagen zum Entwurf eines Gesetzes zur Änderung des Landesverfassungsschutzgesetzes und des Ausführungsgesetzes zum Artikel 10-Gesetz (Abhörgesetz von 1968 bzw. 2001) nebst Anlagen mit Schreiben vom 27. Juni 2017. Nach Beteiligung seiner fünfundzwanzig Mitgliedsvereine nimmt der Anwaltsverband die Gelegenheit zur Stellungnahme gern wahr.

Der Anwaltsverband Baden-Württemberg e. V. ist der freiwillige Zusammenschluss der Rechtsanwältinnen und Rechtsanwälte im Land Baden-Württemberg. Er repräsentiert mehr als die Hälfte aller Kolleginnen und Kollegen in Baden-Württemberg und vertritt als größte Anwaltsorganisation dieses Bundeslandes die Interessen der Anwaltschaft in unserem Bundesland und – in Zusammenarbeit mit dem Deutschen Anwaltverein (DAV) – auch auf nationaler und internationaler Ebene.

1. Allgemeine Bewertung

Der Anwaltsverband teilt die Einschätzung der Sicherheitsbehörden, dass aufgrund der bekannt gewordenen Vorkommnisse mit einer hohen abstrakten Gefahr terroristischer Anschläge in Baden-Württemberg zu rechnen ist. Allerdings meint er, dass mögliche Anschläge nicht nur aus einem extremen islamischen Spektrum drohen, sondern auch aus anderen Kreisen, wie rechts- oder linksextremen oder von aus anderen Gründen (beispielsweise familiären, schulischen oder finanziellen) fanatisierten Einzeltätern.

Zwar gingen die Vorfälle beim Festival in Ansbach (Juli 2016) und in der Regionalbahn bei Würzburg (Juli 2016), im Olympiacenter in München (Juli 2016) oder auf dem Weihnachtsmarkt in Berlin (Dezember 2016) von islamisch geprägten Tätern aus. Es darf aber nicht vergessen werden, dass beispielsweise die jahrelange Anschlagserie des Nationalsozialistischen Untergrunds (NSU) oder zahlreiche Angriffe auf Flüchtlinge von deutschen rechtsextremen Kreisen verübt wurden bzw. werden und damit gleichsam „hausgemacht" waren und sind. Die letzten Taten der RAF reichten wohl bis ins Jahr 1991. Beim aktuellen G20-Gipfel in Hamburg traten wohl wieder vermehrt Linksextreme als Gewalttäter auf. Der Anschlag auf die Fußballmannschaft von Borussia Dortmund, der Amoklauf in Winnenden und die aktuellen Berichte aus Esslingen über eine versuchte Amoktat in einer Schule weisen auf aus anderen Gründen radikalisierte Einzeltäter hin. Entsprechendes kann wohl in Bezug auf die aktuell verstärkt ins Visier geratene sog. Reichsbürgerbewegung festgestellt werden.

Aufgrund dieser Überlegungen greift nach Auffassung des Anwaltsverbandes eine Begründung des Gesetzentwurfs und der darin vorgesehenen Maßnahmen vor allem mit der Gefahr des international agierenden islamischen Terrorismus zu kurz. Es mag sein, dass das Bundesverfassungsgericht in seiner Entscheidung vom 20.04.2016 zum BKA-Gesetz speziell zur Bekämpfung solcher Gruppierungen eine weitere Ausdehnung der Grundrechtseingriffsmöglichkeiten und Absenkung der Gefahrschwellen bejaht hat, dies sollte aber nicht dazu verleiten, den Blickwinkel zu verengen und die Erfordernisse der Gefahrenabwehr nicht in ihrer gesamten Bandbreite wahrzunehmen.

Bemerkenswert ist, dass bei Anschlägen, die in anderen Bundesländern stattfanden, oft eine Verbindung nach Baden-Württemberg gegeben zu sein schien. Dies mag es notwendig erscheinen lassen, über die Praktikabilität der Gefahrenabwehrvorschriften, insbesondere auch des Polizeigesetzes, nachzudenken und bei angenommener Notwendigkeit den Sicherheitsbehörden weitergehende Befugnisse einzuräumen. Nichtsdestotrotz ist hierbei zwingend zu hinterfragen, ob Verschärfungen, die tief in mehrere Grundrechte aller Bürger eingreifen, überhaupt zielführend von den ausführenden Personen angewandt und durchgesetzt werden können. Wenn mangelnde Professionalität, Konkurrenzdenken der Sicherheitsbehörden, unzureichende Ausstattung mit Personal und Sachmitteln oder ungenügende Kommunikation den Erfolg präventiv-polizeilicher Maßnahmen vereiteln, nützen auch gut gemeinte Gesetzesänderungen nichts. Die offenbar

wohl unbemerkt gebliebene Zusammenhang der Taten des NSU oder der Fall Amri zeichnen da kein gutes Bild. Diese Vorgänge legen vielmehr offen, an welchen Stellen tatsächlicher Verbesserungsbedarf besteht.

Aus diesem Grund sind jeweils die tatsächliche Machbarkeit, die Erfolgsaussichten und vor allem die Verhältnismäßigkeit besonders zu prüfen. Vor gesetzgeberischen Aktionismus mit Placebo-Effekt ist dringend zu warnen.

Unverzichtbar ist ein wehrhafter Rechtsstaat, der sich etwa für die Wahrung der Grundrechte auf körperliche Unversehrtheit und Freiheit seiner Bürgerinnen und Bürger einsetzt und diese auch verteidigt. Dazu gehört aber auch, die Persönlichkeitsrechte aller Bürgerinnen und Bürger zu wahren.

Trotz der bestürzenden Terrorereignisse darf es keinen die rechtsstaatlichen Vorgaben den Augen verlierenden Überbietungswettbewerb um die härtesten Gesetzesverschärfungen geben. Beinahe täglich gelangen neue Ideen an die Öffentlichkeit, etwa die Diskussion, wie weit die Voraussetzungen für die Aberkennung des Aufenthaltsrechts von Asylbewerbern bei einer rechtskräftigen Verurteilung abgesenkt werden können. Vorschläge zur verschärften Videoüberwachung und verdachtsunabhängigen Personenkontrolle lassen befürchten, dass die Politik keinen kühlen Kopf behält. Dies ist aber trotz der jetzigen Situation dringend geboten, denn der Gesetzgeber hat einen angemessenen Ausgleich zwischen der Schwere der Grundrechtseingriffe potentiell Betroffener und der Pflicht zum Schutz der Grundrechte zu finden.

Im weitesten Sinne sind die geplanten Möglichkeiten für Grundrechtseingriffe am Verhältnismäßigkeitsgrundsatz zu messen. Dort, wo beispielsweise mehrere schwerwiegende Überwachungsmaßnahmen, wie längerfristige heimliche Wohnraumüberwachung und verdeckter Zugriff auf informationstechnische Systeme, bei einer Person und ihrem Umfeld zusammentreffen, so dass geradezu die Erstellung eines Persönlichkeitsprofils möglich wäre, setzt die Menschenwürde eigene verfassungsrechtliche Grenzen,

vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 130).

Weitere eigene verfassungsrechtliche Grenzen heimlicher Überwachungsmaßnahmen ergeben sich aus Verhältnismäßigkeitsgesichtspunkten gegenüber bestimmten Berufsgruppen, wie Geistlichen, Rechtsanwälten, Journalisten oder Abgeordneten, deren verfassungsrechtlich garantierte Tätigkeit eine besondere Vertraulichkeit voraussetzt. Der Gesetzgeber muss gewährleisten, dass die Behörden bei der Anordnung und Durchführung von Überwachungsmaßnahmen diese Grenzen beachten

vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 131).

Der Anwaltsverband begrüßt daher ausdrücklich die Regelung in § 5c Abs. 3 LVSG-BW - neu -, der zufolge

> „§ 3b des Artikel-10-Gesetzes mit der Maßgabe anzuwenden ist, dass sich Absatz 1 auch auf Rechtsanwälte erstreckt, die in anderen Mandatsverhältnissen als der Strafverteidigung tätig sind".

Der Anwaltsverband hat die künstliche Unterscheidung zwischen Strafverteidigern und anderen Rechtsanwälten stets abgelehnt. Zum einen aus grundsätzlichen Erwägungen, zum anderen aber auch aus Gründen der Praktikabilität, denn – erstens – kann jedes Mandat im Laufe der Zeit eine zu Beginn nicht erkennbare strafrechtliche Implikation entwickeln und – zweitens – ist im Vorfeld der Legitimation gegenüber den Strafverfolgungsbehörden nicht erkennbar, ob ein Rechtsanwalt bereits als Strafverteidiger tätig ist oder (noch) nicht. Der Anwaltsverband hatte sich deshalb stets gegen eine solche Differenzierung ausgesprochen wie sie etwa in § 9a PolG BW 2008 enthalten war.

Der gewählte Weg, den noch problematischen § 3b Abs. 1 G-10-Gesetz betreffend den Schutz zeugnisverweigerungsberechtigter Personen, in dem die Erwähnung von § 53 Abs. 1 Nr. 3 StPO (andere Rechtsanwälte als Strafverteidiger) fehlt, auf diese Weise „zu reparieren", erscheint dringend geboten, solange der Bundesgesetzgeber insoweit untätig bleibt. Damit wird der Sichtweise des Bundesverfassungsgerichts entsprochen. Im Bereich der Gefahrenabwehr nach Polizeirecht oder wie hier noch weiter vorgelagert im reinen Beobachtungsspektrum, kann ein Strafverteidiger als solcher noch gar nicht bestellt sein. Ein Bürger kann wegen des Rechts auf freie Anwaltswahl auch nicht darauf verwiesen werden, sich - um Rechtsrat zu erhalten - lediglich an Fachanwälte für Strafrecht zu wenden oder gleichsam vorbeugend einen Strafverteidiger zu bestellen. Dies zwänge dazu jede Vollmacht prophylaktisch auf Strafverteidigungen zu erstrecken. Der Berufsgeheimnisschutz dient nicht den Berufsträgern, sondern dem rechtssuchenden Bürger als Vertrauensgarantie im Rechtsstaat.

Wenig Verständnis hat der Anwaltsverband allerdings für den geplanten Einsatz von sog. „Staatstrojanern" zur Ausspähung auch verschlüsselter Internet-Kommunikation (vgl. § 5c LVSG - neu) wegen der hier wohl kaum zu beherrschenden technischen Auswirkungen und praktischen Schwierigkeiten gerade dann, wenn es um möglicherweise ausländische islamistische Terrorverdächtige geht, deren Sprache schon gar nicht verstanden wird oder deren Telekommunikationsanbieter man von deutschem Boden aus gar nicht erreichen kann. Es kann nicht sein, dass hier einzelne Betroffene – an einer Kommunikation harmlos Beteiligte - gleichsam gläsern gemacht werden, dauerhafte Schäden an ihren jeweiligen informationstechnischen Systemen verbleiben und kriminellen Dritten, die die vom Staat geschaffenen Sicherheitslücken ausnutzen, möglicherweise noch in die Hand gespielt wird. Anstelle der in der Gesetzesbegründung auf S. 23 vorgesehenen „lediglich in allgemeinen Angaben gehaltenen Information" über das eingesetzte technische Mittel (Spähsoftware), fordert der Anwaltsverband eine möglichst präzise Protokollierung, welche Software genau mit welchen Spezifikationen eingesetzt wurde. Nur so kann es einem Geschädigten möglich sein, seine vielleicht nachhaltig gestörten informationstechnischen Systeme wieder vernünftig in Betrieb zu nehmen.

Die vorgeschlagenen Maßnahmen scheinen recht kostenintensiv dabei im Einzelfall wenig erfolgversprechend zu sein. Der Anwaltsverband regt an, die finanziellen Mittel besser für die effektivere Handhabung der bisher zur Verfügung stehenden Maßnahmen einzusetzen.

2. Im Einzelnen

a) § 3 Abs. 3 Satz 1 Nr. 10 und 11 und Abs. 4 LVSG BW - neu -

Der Katalog der Mitwirkungsaufgaben soll um die Befugnis ergänzt werden, bei weiteren Zuverlässigkeitsüberprüfungen mitzuwirken. Insbesondere soll es um die Zuverlässigkeit bei Bewachungsunternehmen (mit Blick auf die Bewachung von Flüchtlingsunterkünften gehen (§ 34a GewO). Ebenso steht der gewerbliche oder ehrenamtliche Zugang in nicht allgemein zugängliche Bereiche (wie Backstage-Bereiche) bei Großveranstaltungen im Blickpunkt.

Bedenklich erscheint zunächst die Formulierung der Begründung, weshalb Befugnis zur Zuverlässigkeitsüberprüfung Personen auf Personen beschränkt werden soll, denen wegen ihrer Tätigkeit Zugang zu nicht allgemein zugänglichen Bereichen gewährt werden soll. Das Argument, sie seien wegen des Zugangs zu sensiblen Bereichen in der Lage, erheblichen Schaden anzurichten, vermag nicht zu überzeugen. So richtete sich die Angriffsserie des Islamischen Staats am 13.11.2015 in Paris u. a. gegen die Zuschauer eines Fußballspiels im Stade de France und gegen die Besucher eines Rockkonzerts im Bataclan-Theater. Der Bombenanschlag beim Musikfestival in Ansbach war wohl auch eher gegen Zuschauer gerichtet. Dass derartige Anschläge eher aus „nicht allgemein zugänglichen Bereichen“ verübt werden als aus allgemein zugänglichen, ist nicht belegt und wohl auch nicht belegbar. Als treffender erweist sich das Argument, dass von Personen, die sich auf dem gesamten Gelände einer Großveranstaltung einschließlich der sensiblen Bereiche frei bewegen können, ein höheres Risiko ausgeht als von Zuschauern. Wenn dies der Ansatz ist, sollte dies auch in der Begründung so ausgeführt werden. Dieser Ansatz, der zur Konkretisierung der zu überprüfenden Personen – und nicht zur Beschreibung schutzwürdiger Bereiche – diente, fände die Zustimmung des Anwaltsverbandes.

Bei dem jetzigen Wortlaut der Begründung entsteht jedoch der Eindruck, als seien die „nicht allgemein zugänglichen Bereiche“ und die sich dort aufhaltenden Personen schutzwürdiger als „einfache Zuschauer“. Eine Differenzierung des Schutzniveaus in einem solchen Sinne würde vom Anwaltsverband abgelehnt.

In rechtlicher Hinsicht begegnet § 3 Abs. 4 LVSG, der um eine Regelung ergänzt wird, der zufolge die Übermittlung personenbezogener Daten an das LfV von der Einwilligung des Betroffenen abhängig gemacht wird, anderweitigen Bedenken. Wenn der Betreffende die Einwilligung verweigert, soll er in den sensiblen Bereichen bei Großveranstaltungen nicht tätig werden dürfen.

Der Zwang zur Einwilligung in eine Zuverlässigkeitsüberprüfung greift bei den Betroffenen in Art. 12 GG (und bei den Unternehmen, die die betreffenden Personen dann nicht beschäftigen können, in Art. 12, 14 GG) ein. Ein solcher Eingriff kann nur mit dem Schutz wichtiger Gemeinschaftsgüter gerechtfertigt werden. Der Schutz von Leib und Leben, beispielsweise prominenter Personen, ist sicherlich ein solches Gemeinschaftsgut. Gleichwohl stellt sich die Frage, ob die Regelung verhältnismäßig ist.

Zum einen vermisst der Anwaltsverband eine Konkretisierung des Inhalts, dass nur Daten erhoben und geprüft werden, die in einem Zusammenhang mit der Tätigkeit bei derartigen Veranstaltungen stehen bzw. für eine solche Tätigkeit von Bedeutung sein können; dazu zählen etwa nicht Gesundheitsdaten. Dementsprechend wird die einzuholende Zustimmung zur Überprüfung auf relevante Daten zu beschränken sein; dies muss dem Betroffenen ebenso erläutert werden wie die Folgen einer Verweigerung der Einwilligung. Nur auf diese Weise lässt sich verhindern, dass die Einwilligung nicht irrigerweise aus Gründen versagt wird, die mit dem Zweck der Sicherheitsüberprüfung in keinem Zusammenhang stehen.

Zum anderen erfasst die Regelung – angesichts der heutigen zahlreichen Großveranstaltungen - einen sehr großen Adressatenkreis. Viele der Personen, die in sog. sensible Bereiche betreten, führen nur untergeordnete Dienstleistungen, wie Getränkelieferung oder Reinigungsarbeiten, aus. Die entsprechenden Dienstleister arbeiten oft mit Aushilfen. Denkbar ist auch, dass ein Dienstleister kurzfristig auf Vertretungskräfte ausweichen muss, weil die vorgesehene Person arbeitsunfähig erkrankt oder sonst kurzfristig verhindert ist. Jeden einzelnen Angehörigen dieses Adressatenkreises vor einer Großveranstaltung überprüfen zu wollen, erfordert deshalb massenhaften Kontrollen. Hierfür müsste das LfV über die erforderlichen Kapazitäten verfügen, was angesichts der Personalstärke der Behörde ungewiss erscheint. Diese Frage nach der praktischen Umsetzbarkeit des Unterfangens lässt zugleich an der Geeignetheit der Regelung zweifeln.

b) § 5a LVSG BW – neu –

aa) § 5a Abs. 1 LVSG BW – neu –

Gegen die geplanten redaktionellen Änderungen sowie die Erweiterung der Befugnis, bei tatsächlichen Anhaltspunkten für schwerwiegende Gefahren für erhebliche Schutzgüter, Auskünfte auch von Flugreservierungssystemen verlangen zu können, bestehen keine Bedenken.

bb) § 5a Abs. 3 LVSG BW – neu –

Gegen die geplanten, vor allem redaktionellen, Änderungen bestehen keine Bedenken.

cc) § 5a Abs. 7 LVSG BW – neu –

Die Aufnahme des Benachteiligungsverbots wird ausdrücklich begrüßt. Es soll dazu dienen, dass auskunftspflichtige nicht-öffentliche Stellen, wie Kreditinstitute, Fluggesellschaften, Post- und Telekommunikationsdienstleistern, allein aufgrund des Umstands einer Anfrage des LfV nach § 5a LVSG BW nicht dazu veranlasst werden, bestehende Verträge mit Personen, um die es bei der Anfrage ging, zu beenden oder die Person sonst zu benachteiligen.

Misslich erscheint allerdings die Formulierung, der zufolge in Satz 1 von dem Auskunftgeber und in Satz 2 von dem Verpflichteten gesprochen wird. Dies lenkt den Blick darauf, dass im LVSG – anders als im Art. 10-Gesetz – nicht ausdrücklich eine Verpflichtung zur Auskunft geregelt ist. Sie ergibt sich allenfalls mittelbar aus der Befugnis des LfV, Auskünfte einzuholen; eine damit korrespondierende Pflicht derjenigen, die über die Informationen verfügen, auch entsprechende Auskünfte zu erteilen, findet sich hingegen nicht im Gesetz.

c) § 5c LVSG BW – neu -

aa) Allgemein zur Quellen-TKÜ

Die neue Vorschrift soll die verdeckte Telekommunikationsüberwachung im Einzelfall durch Zugriff **mit technischen Mitteln** auf informationstechnische Systeme ermöglichen. Ermöglicht werden soll der Einsatz der bereits viel in der Öffentlichkeit diskutierten sog.

staatlichen Spähsoftware im Internet, gerade auch um möglicherweise verschlüsselte Informationen international agierender Extremisten verstehen zu können.

Bei der sog. Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) soll auf dem Computer, mit dem die zu überwachende Kommunikation getätigt wird, ein Programm installiert werden, das die Kommunikation vor der Verschlüsselung mitschneidet und an die Ermittlungsbehörde übermittelt. Die technische Umsetzung ähnelt dabei derjenigen des sog. Bundestrojaners, allerdings wird – laut Mitteilung der Bundesregierung – nur die Kommunikation überwacht und es werden keine weiteren Daten erhoben.

Der Einsatz von technischen Mitteln durch den Landesverfassungsschutz, um in IT-Systeme der Betroffenen zwecks Telekommunikationsüberwachung einzudringen, um z. B. auch verschlüsselte Nachrichten lesen zu können, erscheint aus mehreren Gründen verfassungswidrig.

Dies betrifft zunächst den Einsatz technischer Mittel, um in IT-Systeme der Betroffenen zwecks Telekommunikationsüberwachung einzudringen, um z. B. auch verschlüsselte Nachrichten lesen zu können. Der Staat würde dabei selbst Sicherheitslücken ausnutzen, deren Existenz er eigentlich verhindern sollte. Das Bundesverfassungsgericht hat in seiner Entscheidung

BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07 –, BVerfGE 120, 274,

in diesem Zusammenhang das Grundrecht „auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ herausgearbeitet. Die vorgesehenen Regelungen im Gesetzentwurf schaffen nun aber geradezu einen Anreiz für staatliche Stellen, IT-Sicherheitslücken auszunutzen oder gar aufrecht zu erhalten.

Soweit der Staat Sicherheitslücken in informationstechnischen Systemen ausnutzen will, um möglichen Terrorverdächtigen auf die Spur zu kommen, bestehen Bedenken an dem vom Bundesverfassungsgericht geforderten legitimen Ziel für die Maßnahmen. Es gehört auch zu den staatlichen Aufgaben, das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für alle Bürgerinnen und Bürger, aber auch von Inhabern von Wirtschaftsunternehmen (Art. 14 GG), zu schützen. Dafür wurde z. B. mit Steuermitteln das Bundesamt für Sicherheit in der Informationstechnik (BSI) eingerichtet. Zur erfolgreichen Gefahrenabwehr müsste der Staat aber geradezu ein Interesse am Bestehen von Sicherheitslücken in IT-Systemen haben. Der Zielkonflikt ist offensichtlich.

2010 wurde bekannt, dass der deutsche Zollfahndungsdienst die Quellen-TKÜ nach richterlicher Anordnung benutzt, um mittels einer speziell entwickelten Software Inhalte von Gesprächen über Skype, noch bevor sie verschlüsselt werden, auf einen bestimmten Server auszuleiten.

Am 8.10.2011 veröffentlichte der Chaos Computer Club (CCC) eine Analyse eines Programmes zur Quellen-TKÜ und deckte dabei auf, dass die Fähigkeiten des Programmes die Überwachung der Telefonie übersteigen. Das untersuchte Programm ermöglichte nebenher ein Nachladen von beliebigen Programmen aus dem Internet, das Erstellen von Bildschirmfotos (Screenshots) und enthielt ein Modul, welches eine Aufzeichnung der Tastaturanschläge ermöglicht. Des Weiteren können durch den Trojaner auch einfache Daten, wie z. B. Bilder, auf den Computer aufgespielt werden, mithin auch etwaige manipulierte Beweise oder sonstiges kompromittierendes Material. Die vom CCC analysierte Software wurde von der hessischen Firma *Digi Task GmbH – Gesellschaft für besondere Telekommunikationssysteme* u. a. im Auftrag der Bayerischen Staatsregierung entwickelt.

Neben den verfassungsrechtlich bedenklichen Zusatzfunktionen kritisierte der CCC die Sicherheitsfunktionen des Trojaners. Verschlüsselt wurde lediglich der Upload der zu exfiltrierenden Daten, wobei in allen Fällen derselbe Schlüssel verwendet wurde. Die Steuerung des Trojaners erfolgte unverschlüsselt und ohne Authentifizierung, so dass eine Sicherheitslücke auf den Computern der Betroffenen geöffnet wurde.

Das Bundesverfassungsgericht hat in seiner Entscheidung

BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07 –, BVerfGE 120, 274,

auf die besonderen Risiken hingewiesen, die mit einer Quellen-TKÜ verbunden sind. Mit der Infiltration eines IT-Systems sei die entscheidende Hürde gefallen, das **System insgesamt auszuspähen**. Daraus resultiere eine **größere Eingriffstiefe als bei herkömmlichen TKÜ-Maßnahmen**. Die Einsatzmöglichkeit kann daher nur zur Abwendung von Gefahren für ein „**überragend wichtiges Rechtsgut**“ bestehen. Hierzu zählen Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

Von Experten wird u. a. die technische Umsetzbarkeit einer Quellen-TKÜ bezweifelt: Antivirenprogramme würden alle Schadprogramme gleich behandeln. Tjark Auerbach, Ge-

schäftsführer von Avira sagte: „Ein Trojaner ist und bleibt eine Spionage-Software". Sobald die Struktur den Software-Herstellern bekannt wird, würde sie in ein Verzeichnis bekannter Viren aufgenommen und von den Programmen blockiert werden.

Andreas Lamm, Geschäftsführer von Kaspersky Lab, sagte zu der Möglichkeit einer Zusammenarbeit mit staatlichen Behörden, „es würde sich dabei um einen massiven Eingriff in die gesamte IT-Sicherheitsindustrie handeln, der aus unserer Sicht nicht vorstell- und durchführbar wäre".

Zusätzlich ist zu bedenken, dass von Seiten der überwachenden Behörde nicht überprüfbar ist, ob ein staatlicher Trojaner von einem technisch begabten Kriminellen erkannt und manipuliert wird. In diesem Fall könnte dieser gefälschte Daten an die Behörde übermitteln, um Dritte zu belasten. Im Gegensatz zur herkömmlichen Telefonüberwachung wäre dieser Eingriff nicht einmal im Nachhinein nachweisbar. Der Einsatz zur Gewinnung weiterer Ansätze zur Gefahrenabwehr ist daher fragwürdig.

Auch ist die Verhältnismäßigkeit zu bezweifeln, da ein staatlicher Trojaner nur bei technisch minderbegabten Terroristen funktionieren würde. Bei solchen dürften aber auch herkömmliche Ermittlungsmethoden genügen.

Ein nicht zu unterschätzendes Risiko sieht der Anwaltsverband darin, dass durch das Aufspielen sog. Staatstrojaner die beim Betroffenen vorhandene Computertechnik nachhaltig gestört wird. Der bisherige Gesetzentwurf sieht hier keinerlei Schutzmechanismen vor. So ist weder eine Zertifizierung der eingesetzten Software noch ein Ausschluss der Produkte privater Anbieter vorgesehen.

Einen Betroffenen auf die Entschädigung oder Ansprüche aus Aufopferung, enteignendem und – bei rechtswidrigen Handeln – enteignungsgleichem Eingriff, Amtshaftung oder auf Folgenbeseitigung zu verweisen, könnte die Folge sein. Gerade aber bei Störungen der Computertechnik kann der Nachweis der Verursachung durch heimliche staatliche Manipulation für den Betroffenen sehr kostenaufwändig und schwierig sein. Die ihm durch eine Systemstörung entstehenden Schäden können enorm sein.

Das große Schadenspotential beim heimlichen Eingreifen von unbefugten Dritten spricht ebenfalls für die besondere Eingriffstiefe solcher informationstechnischen Überwachungsmaßnahmen. Es wird bezweifelt, dass der Staat es sicherstellen kann, dass nicht genau die Sicherheitslücke, die er durch das Einschleusen eines Trojaners o. ä. beim Betroffenen geschaffen hat, wiederum von anderen Widersachern des Betroffenen ausgenutzt wird.

Dann aber wäre der Staat eine fördernde Kraft in einem „Cyber-Krieg". Dafür ist die Aufgabe des Verfassungsschutzes und der Gefahrenabwehr aber nicht gedacht.

Die mögliche materielle (Kollateral-)Schädigung eines Betroffenen durch den Eingriff in Art. 2, 12 und 14 GG ist so erheblich, dass bei Abwägung der betroffenen Rechtsgüter eine gesetzliche Regelung nur dann als verhältnismäßig und damit verfassungsgemäß erachtet werden kann, wenn im Gesetz selbst eine entsprechende Anspruchsgrundlage für den Ersatz materieller Schäden, wie Kosten eines IT-Technikers zur Störungsfindung, Kosten der Ersatzbeschaffung von Soft- und Hardware, Datenwiederherstellung, Sachverständigen-/Gutachter- und Rechtsverfolgungskosten, aufgenommen würde.

Aus den vorgenannten Gründen hat der Anwaltsverband erhebliche verfassungsrechtliche Bedenken gegen die Ermöglichung des heimlichen Einsatzes technischer Mittel bei vorhandenen informationstechnischen Systemen.

Das Bundesverfassungsgericht hat in seiner Entscheidung

BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220,

bezogen auf Maßnahmen wie heimlicher **Wohnraumüberwachung**, **Telekommunikationsüberwachung (TKÜ)**, **Telekomunikations-Verkehrsdatenüberwachung**, **Online-Durchsuchung oder Quellen-TKÜ**, zahlreiche Hinweise gegeben, wie präventiv-polizeiliche Befugnisse ausgestaltet sein müssen, um verfassungsgemäß – und damit ausreichend grundrechtsrespektierend - zu sein. Es hat dabei berücksichtigt, dass die Entwicklung der Informationstechnik die Reichweite von solchen Überwachungsmaßnahmen ausdehnt, ihre Durchführbarkeit erleichtert und Verknüpfungen erlaubt, die bis hin zur Erstellung von Persönlichkeitsprofilen reichen. Solche Eingriffsbefugnisse erhalten daher ein besonderes Gewicht.

So müssen die Eingriffe in Grundrechte wie das **Telekommunikationsgeheimnis (Art. 10 GG**, **die Unverletzlichkeit der Wohnung (Art. 13 GG)**, **das Recht auf informationelle Selbstbestimmung und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnisches Systeme (Ausprägungen von Art. 2 und 1 GG)**, einem legitimen Ziel dienen.

Im Grundsatz ist sicherlich davon auszugehen, dass der hiesige Gesetzentwurf mit den verbesserten Möglichkeiten zur Erkennung und damit Abwehr terroristischer Gefahren legitime Ziele verfolgt.

Allerdings ist die Verhältnismäßigkeit zu bezweifeln, da ein staatlicher Trojaner voraussichtlich nur bei technisch minderbegabten Terroristen funktionieren würde. Bei solchen dürften aber auch herkömmliche Ermittlungsmethoden genügen.

Die heimliche Infiltration eines informationstechnischen Systems ist laut dem Bundesverfassungsgericht grundsätzlich unter den **Vorbehalt richterlicher Anordnung** zu stellen. Ein Gesetz, das zu einem solchen Eingriff ermächtige, müsse Vorkehrungen enthalten, um den **Kernbereich privater Lebensgestaltung** zu schützen. Beiden Anforderungen wird **nicht hinreichend** Rechnung getragen. Mit der in der hiesigen Gesetzesbegründung zitierten Entscheidung vom 20.04.2016 hat das Bundesverfassungsgericht seine Rechtsprechung, insbesondere zur Datenweitergabe, weiterentwickelt.

bb) § 5c Abs. 1 LVSG BW - neu – (Verweis auf § 3 Artikel-10-Gesetz)

Die heimliche Infiltration eines informationstechnischen Systems ist nach der Entscheidung

> BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07 –, BVerfGE 120, 274,

grundsätzlich unter den **Vorbehalt richterlicher Anordnung** zu stellen.

Das Bundesverfassungsgericht hat auch 2016 in verfahrensrechtlicher Hinsicht – als Ausfluss des Verhältnismäßigkeitsgrundsatzes – bei eingriffsintensiven heimlichen Überwachungsmaßnahmen einen **Richtervorbehalt** gefordert

> vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 117).

Ein entsprechender **Antrag** auf richterliche Anordnung muss – um eine effektive vorbeugende unabhängige Kontrolle zu gewährleisten – in spezifischer und normenklarer Form abgefasst sein.

Auf diese Weise will das Bundesverfassungsgericht gewährleistet wissen, dass den besonderen Risiken Rechnung getragen wird, die mit einer Quellen-TKÜ verbunden sind. Mit der Infiltration eines IT-Systems sei die entscheidende Hürde gefallen, das **System insgesamt auszuspähen**. Daraus resultiere eine **größere Eingriffstiefe als bei herkömmlichen TKÜ-Maßnahmen**. Die Einsatzmöglichkeit darf daher nur zur Abwendung von Ge-

fahren für ein „*überragend wichtiges Rechtsgut*" bestehen. Um dem Verhältnismäßigkeitsgrundsatz zu genügen, müssen derart **weit reichende Grundrechtseingriffe** dem Schutz **hinreichend gewichtiger Rechtsgüter** gegen **hinreichend konkrete Gefahren** dienen.

Schutzgüter von besonders hohem verfassungsrechtlichem Gewicht sind die verfassungsmäßige Ordnung, der Bestand und die Sicherheit des Bundes und der Länder sowie Leib, Leben und Freiheit der Person,

> vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 100, 108).

Ein uneingeschränkter Sachwertschutz ist hingegen nicht ausreichend gewichtig für heimliche TKÜ-Maßnahmen. Online-Durchsuchungen sollen auch bei einer Gefahr für Güter der Allgemeinheit, die die Existenz der Menschen berühren, möglich sein,

> vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 108).

Die Eingriffsbefugnisse müssen für die gewünschte Zielerreichung, z. B. Abwehr internationaler Terrorismustaten, generell geeignet und erforderlich sein. Diese beiden Voraussetzungen hat das BVerfG in seiner Entscheidung vom 20.04.2016 bejaht. Im Rahmen der Prüfung der Verhältnismäßigkeit im engeren Sinne ist abzuwägen, ob die - durch die Heimlichkeit - besonders tiefgehenden Grundrechtseingriffe auch im Einzelfall erforderlich sind oder ob da nicht auch mildere Mittel, wie z. B. eine herkömmliche Observation, in Frage kommen.

cc) Erforderlicher Gefahrengrad

Die Rechtmäßigkeit der heimlichen schweren Grundrechtseingriffe bei einer Person setzt im Einzelfall belastbare tatsächliche Anhaltspunkte für das Vorliegen einer Gefahrensituation voraus. Eine vorwiegend auf Intuition der Sicherheitsbehörden beruhende bloße Möglichkeit weiterführender Erkenntnisse reicht dafür nicht aus,

> vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 112).

Die Verfassung setzt der Absenkung der Eingriffsschwellen für heimliche Maßnahmen der Straftatenverhütung damit deutliche Grenzen.

Zwar soll zur Verhinderung terroristischer Straftaten eine Überwachung auch dann möglich sein, wenn das **individuelle Verhalten** einer Person eine konkrete Wahrscheinlichkeit

begründet, dass sie solche Taten in überschaubarer Zukunft begehen wird. Dies soll z. B. bei einem Rückkehrer aus einem terroristischen Ausbildungslager im Ausland der Fall sein

> vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 112).

Die bloße Erkenntnis, dass sich eine Person zu einem fundamentalistischen Religionsverständnis hingezogen fühlt, sei noch nicht ausreichend

> vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 113)

Das BVerfG hat bei „individuellem Verhalten" lediglich beispielhaft angeführt, dass dies etwa denkbar sei, „wenn eine Person aus einem Ausbildungslager für Terroristen im Ausland in die Bundesrepublik Deutschland einreist"

> vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 112.).

Welches „individuelle Verhalten" aber darüber hinaus die tatbestandlichen Voraussetzungen erfüllen soll, bleibt dunkel.

dd) Richtiger Adressatenkreis

§ 5c Abs. 1 LVSG BW - neu – wird den vom Bundesverfassungsgericht in der zitierten Entscheidung vom 20.04.2016 herausgearbeiteten Anforderungen an den Adressatenkreis gerecht, indem auf den nach § 3 G-10-Gesetz Verdächtigen und seine Unterstützer (u. a. Nachrichtenmittler) verwiesen wird. Sinnvoll kann eine Kommunikationsüberwachungsmaßnahme nur sein, wenn damit die Geräte erfasst werden, von denen aus die Kommunikation stattfindet. Damit erscheint die Ausweitung des Anwendungsbereichs auf „harmlosere" Nachrichtenvermittler oder Gerätebereitsteller sinnvoll und rechtmäßig.

Nur unter eingeschränkten Voraussetzungen dürfen solche präventiven Maßnahmen auch Unbeteiligte einbeziehen. Sie müssen aus der Sicht eines verständigen Dritten den objektiven Umständen nach in eine Gefährdungssituation verfangen sein

> vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 109, 115).

Der Zugriff auf informationstechnische Systeme und die Wohnraumüberwachung dürfen sich nur unmittelbar gegen die Zielperson richten. Wenn dadurch Dritte **unvermeidbar** miterfasst würden, sei das tragbar

> vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 115).

Deswegen könne sogar die Wohnung des Dritten überwacht werden, wenn die Zielperson sich dort zu einem relevanten Zeitpunkt aufhalten werde. Ebenso könne die Online-Durchsuchung auf die Geräte Dritter erstreckt werden, wenn sie eine **spezifische** individuelle Nähe zur Zielperson aufweisen. Bei einfachen Kontaktpersonen müssen weniger eingriffsintensive Überwachungsmaßnahmen eingesetzt werden.

Die in § 5c LVSG BW – neu - gefundenen Regelungen erfüllen die verfassungsrechtlichen Vorgaben hinsichtlich des Adressatenkreises und der zu schützenden Rechtsgüter. Insbesondere § 3 G-10-Gesetz, auf den verwiesen wird, enthält in Abs. 2 mit den Tatbestandsmerkmalen „sonst aussichtslos oder wesentlich erschwert" eine begrüßenswerte Konkretisierung des Verhältnismäßigkeitsgebotes.

ee) § 5c Abs. 1 Nr. 1 und 2 LVSG BW - neu -

Soweit sich eine Ermächtigung auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der **laufenden** Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff nach dem Bundesverfassungsgericht an **Art. 10 Abs. 1 GG** zu messen. Verschafft sich der Staat Kenntnis von Inhalten der Internetkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin nur dann ein Eingriff in Art. 10 Abs. 1 GG, wenn die staatliche Stelle **nicht** durch Kommunikationsbeteiligte zur Kenntnisnahme **autorisiert** ist.

§ 5c Abs. 1 Nr. 1 LVSG BW-neu zielt darauf ab, nur die laufende Telekommunikation zu erfassen. Der Anwaltsverband hat aber Zweifel, ob es tatsächlich gelingen kann, einen „Staatstrojaner" so auszugestalten, dass er auch wirklich nur diese Informationen erfasst. Wie zuvor ausgeführt, hat der CCC schon festgestellt, dass die bisher verwendete Software deutlich mehr kann. Ein geschickter Krimineller könnte die Software so verändern, dass sie tatsächlich auch mehr als die laufende Kommunikation – zu seinen Gunsten – ausspäht. Wenn die staatlichen Behörden aber nicht wirklich zuverlässig sicherstellen können, dass ausschließlich die laufende Kommunikation erfasst wird, ist der Einsatz einer solchen Software zu unterlassen.

ff) Zu § 5c Abs. 2 LVSG BW - neu –

Richtig ist es, den Eingriff in ein informationstechnisches System so gering wie möglich zu gestalten und auch Zurückversetzung in den Zustand vor der Manipulation vorzusehen.

Es erscheint aber angesichts der rasanten IT-Entwicklung kaum vorstellbar, dass der Landesverfassungsschutz eine Spähsoftware einsetzen kann, die die in § 5c Abs. 2 LVSG BW - neu - unerwünschten Nebeneffekte, wie dauerhafte Veränderung eines informationstechnischen Systems oder unbefugte Nutzung durch Dritte, ausschließt.

gg) Zu § 5c Abs. 3 LVSG BW - neu –

Aufgrund der zitierten Entscheidung des Bundesverfassungsgerichts vom 20.04.2016 sind - wie ausgeführt - an die Verfassungsmäßigkeit der Quellen-TKÜ und deren Ausgestaltung zahlreiche Anforderungen zu stellen. Mit dem Verweis auf den im G-10-Gesetz geregelten Kernbereichsschutz für die private Lebensführung (dort § 3a), den Zeugnisverweigerungsschutz (§ 3b), die Prüf-, Kennzeichnungs- und Löschungspflichten, aber auch die Vorschriften zur Datenübermittlung und Zweckbindung wird diesen Anforderungen weitgehend Genüge getan.

Der Anwaltsverband begrüßt daher ausdrücklich die Regelung in § 5c Abs. 3 LVSG-BW – neu -, der zufolge „§ 3b des Artikel-10-Gesetzes mit der Maßgabe anzuwenden ist, dass sich Absatz 1 auch auf Rechtsanwälte erstreckt, die in anderen Mandatsverhältnissen als der Strafverteidigung tätig sind“.

Der Anwaltsverband hat die künstliche Unterscheidung zwischen Strafverteidigern und anderen Rechtsanwälten stets abgelehnt. Zum einen aus grundsätzlichen Erwägungen, zum anderen aber auch aus Gründen der Praktikabilität, denn – erstens – kann jedes Mandat im Laufe der Zeit eine zu Beginn nicht erkennbare strafrechtliche Implikation entwickeln und – zweitens – ist im Vorfeld der Legitimation gegenüber den Strafverfolgungsbehörden nicht erkennbar, ob ein Rechtsanwalt bereits als Strafverteidiger tätig ist oder (noch) nicht. Der Anwaltsverband hatte sich deshalb stets gegen eine solche Differenzierung ausgesprochen wie sie etwa in § 9a PolG BW 2008 enthalten war.

Der gewählte Weg, den noch problematischen § 3b Abs. 1 G-10-Gesetz betreffend den Schutz zeugnisverweigerungsberechtigter Personen, in dem die Erwähnung von § 53 Abs. 1 Nr. 3 StPO (andere Rechtsanwälte als Strafverteidiger) fehlt, auf diese Weise „zu reparieren“, erscheint dringend geboten, solange der Bundesgesetzgeber insoweit untätig

bleibt. Damit wird der Sichtweise des Bundesverfassungsgerichts entsprochen. Im Bereich der Gefahrenabwehr nach Polizeirecht oder wie hier noch weiter vorgelagert im reinen Beobachtungsspektrum, kann ein Strafverteidiger als solcher noch gar nicht bestellt sein. Ein Bürger kann wegen des Rechts auf freie Anwaltswahl auch nicht darauf verwiesen werden, sich - um Rechtsrat zu erhalten - lediglich an Fachanwälte für Strafrecht zu wenden oder gleichsam vorbeugend einen Strafverteidiger zu bestellen. Dies zwänge dazu jede Vollmacht prophylaktisch auf Strafverteidigungen zu erstrecken. Der Berufsgeheimnisschutz dient nicht den Berufsträgern, sondern dem rechtssuchenden Bürger als Vertrauensgarantie im Rechtsstaat.

Das Bundesverfassungsgericht hat in seiner Entscheidung

> BVerfG, Urteil vom 15.12.1970 – 2 BvF 1/69 –, BVerfGE 30, 1,

ausgeführt, dass das Prinzip der Gewaltenteilung es erlaube, dass Rechtsschutz gegenüber Maßnahmen der Exekutive ausnahmsweise nicht durch Gerichte, sondern durch vom Parlament bestellte oder gebildete unabhängige Institutionen innerhalb des Funktionsbereichs der Exekutive gewährt wird. Diese Ausnahme vom Richtervorbehalt ist demgemäß nach Art. 10 Abs. 2 GG zum „Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes“ zulässig. Unter dieser Voraussetzung ist der Verweis in § 5c Abs. 3 LVSG BW - neu - hinsichtlich des Antragsverfahrens für die Anordnung einer verdeckten Telekommunikationsüberwachung, der Anordnungserfordernisse und der nachträglichen Mitteilungspflichten auf §§ 9 – 13 des Artikel-10-Gesetzes nicht zu beanstanden.

hh) Zu § 5c Abs. 4 LVSG BW - neu –

Abs. 4 sieht eine umfassende Protokollierungspflicht bei der Datenerhebung mittels Spähsoftware vor und versucht die Vorgaben der Entscheidung

> vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 115).

umzusetzen. Anders als in der Gesetzesbegründung auf S. 24 vorgesehen ist es jedoch geboten, dass den Typ der eingesetzten Software so genau wie möglich zu protokollieren, damit im Nachhinein dennoch aufgetretene Schäden am informationstechnischen System möglichst effektiv repariert werden können.

d) § 10 LVSG BW - neu –

Mit der beabsichtigten Neuregelung wird der bisherige § 10 Abs. 1 LVSG vollständig neu gestaltet. Die Gesetzesbegründung führt auf S. 25 f. an, dass damit die Vorgaben des Bundesverfassungsgerichts zur sog. Antiterrordatei umgesetzt werden sollen,

> BVerfG, Urteil vom 24.04.2013 – 1 BvR 1215/07 –, BVerfGE 133, 277.

Die neue Regelung soll sich an den schon in 2015 verabschiedeten § 19 BVerfSchG anlehnen.

Erfreulich ist zunächst, dass die Behörden, an die - mit nachrichtendienstlichen Mitteln erhobenen - personenbezogenen Daten übermittelt werden dürfen, nun konkret benannt sind, wie Staatsanwaltschaften, Finanzbehörden, Polizei, Steuer- und Zollfahndungsbehörden.

Des Weiteren zu begrüßen ist die Konkretisierung der Erforderlichkeit (als Ausprägung der Verhältnismäßigkeit) durch die Begrenzung der Übermittlungsbefugnis auf die eigene Aufgabenerfüllung des LfV, der Gefahrenabwehr bei entsprechendem öffentlichen Interesse, der Verhinderung von Straftaten mit erheblicher Bedeutung sowie der Verfolgung von Straftaten mit erheblicher Bedeutung.

Der Anwaltsverband versteht die einschlägigen Entscheidungen des Bundesverfassungsgerichts

> BVerfG, Urteil vom 24.04.2013 – 1 BvR 1215/07 –, BVerfGE 133, 277; BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220,

jedoch dahin, dass aufgrund der darin entwickelten Grundsätze zur Zweckbindung und Zweckänderung – entsprechend dem Grundsatz von der hypothetischen Datenneuerhebung – eine Weitergabe von erhobenen Daten nur zum **Schutz genau solcher Rechtsgüter** und bei **Vorliegen eines ebensolchen Gefahrengrades** möglich ist, die auch die Datenerhebung gestattet haben.

Dies würde im Falle von durch heimliche Wohnraumüberwachung (Art. 13 GG) oder Telekommunikationsüberwachung (Art. 10, 2 GG) erlangten Daten bedeuten, dass sie nur zum Schutz besonders gewichtiger Verfassungsgüter, wie beispielsweise in § 3 Abs. 1 G-10-Gesetz, § 129a StGB oder § 100a StPO angeführt, und bei Vorliegen eines konkreten Ermittlungsansatzes weitergegeben werden dürften,

> vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220.

Der neue § 10 Abs. 1 LVSG würde aber schon „erhebliche“ Gefahren, Schutzgüter oder Straftaten erfassen. Erheblich sein sollen nach der Gesetzesbegründung (und z. B. auch § 22 Abs. 5 PolG BW), Verbrechen nach § 12 StGB und Straftaten, die lediglich dem Bereich der mittleren Kriminalität zuzurechnen sind.

Das Beispiel der mit diesem Gesetzentwurf in § 5c vorgesehenen Befugnis zur verdeckten Telekommunikationsüberwachung durch Eingriffe in informationstechnische Systeme mit Hilfe von „technischen Mitteln“ zeigt, dass die Voraussetzungen zur Datenerhebung nach dem G-10-Gesetz und zur Datenübermittlung nach dem LVSG deckungsgleich sein müssen. Das Bundesverfassungsgericht hat in seiner Entscheidung vom 20.04.2016 mehrfach betont, dass speziell für verdeckte Wohnraumüberwachungen und dem verdeckten Zugriff auf informationstechnische Systeme besonders hohe Anforderungen an die Datenerhebung und Datenweiternutzung zu stellen sind,

> vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 275, 294, 302).

Begründet wird die Absenkung der Eingriffsschwelle für die Übermittlung von Daten durch das LfV im hiesigen Gesetzentwurf damit, dass es nach der Datenerhebung erst noch eine Filterung vornehme, bevor es „Erkenntnisse“ (nicht unbedingt alle erhobenen Daten) an die berechtigten Behörden weitergeben würde. Es seien an eine solche Datenweitergabe nicht so hohe Anforderungen zu stellen, weil sie nicht die gleiche Grundrechtseingriffsintensität hätte. Dabei wird auf die Gesetzesbegründung vom 20.04.2015 (BT-Drucks. 18/4654, S. 33) Bezug genommen. Dass die Erwägungen des Bundesverfassungsgerichts

> BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220,

in diese schlechterdings noch nicht eingeflossen sein können, bedarf keiner Vertiefung. Zum einen hat ein Betroffener nur sehr beschränkte Rechte zu erfahren, woher die über ihn erhobenen Daten stammen und wohin sie übermittelt wurden (§ 13 LVSG BW), weshalb sich für ihn die Datenweitergabe an etwa eine Polizeidienststelle, die dann über diese Informationen verfügt, als genauso schwerwiegend darstellt, als hätte die Polizei die Daten selbst erhoben. Ferner ist nicht auszuschließen, dass die vom LfV möglicherweise aus verschiedenen Datenerhebungen zusammengestellten „Erkenntnisse“, die es weitergibt, sogar noch schwerwiegender wirken als hätte es nur die „Rohdaten“ weitergegeben. Die Argumentation der Gesetzesbegründung vermag deshalb nicht zu überzeugen. Vielmehr ist eine Zweckänderung von der Datenerhebung zu Datenweitergabe zu unterbinden.

Auch wenn mit Blick auf die Besonderheiten der Quellen-TKÜ in § 5c Abs. LVSG BW – neu - den Besonderheiten durch Verweis auf das G-10-Gesetz Rechnung getragen wurde, bleibt festzuhalten, dass § 10 Abs. 1 LVSG BW – neu - mit Blick auf die verfassungsgerichtliche Rechtsprechung zu wenig differenziert ist und dringend der Nachbesserung bedarf.

e) § 13 LVSG BW - neu –

Mit der beabsichtigten Gesetzesänderung soll der ohnehin schon stark einschränkte Auskunftsanspruch eines Betroffenen weiteren Restriktionen unterworfen werden, indem er Auskünfte aus Akten nur erhält, wenn diese in gemeinsamen Dateien im automatisierten Verfahren, z. B. im nachrichtendienstlichen Informationssystem-Wissensnetz (NADIS-WN) auffindbar sind.

Die Gesetzesbegründung führt auf S. 29 aus, dass der Auskunftsanspruch eines Betroffenen im Zusammenhang mit dem BVerfSchG beschränkt werden müsse, um einem unverhältnismäßig hohen Verwaltungsaufwand des LfV zu begegnen. Dies vermag nicht zu überzeugen.

Der Auskunftsanspruch des Betroffenen dient der Verwirklichung seiner Grundrechte auf informationelle Selbstbestimmung und auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme; mit diesem Auskunftsanspruch soll der Betroffene in die Lage versetzt werden im Nachhinein Rechtsschutz zu erlangen. Die Effektivität seines Rechtsschutzes wird durch die erst nachträgliche Gewährung ohnehin zugunsten der Aufgabenwahrnehmung des LfV zurückgedrängt. Diesen Auskunftsanspruch mit dem Hinweis auf den Verwaltungsaufwand für das LfV zusätzlich einzuschränken ist unvertretbar und findet im Rahmen einer Abwägung des Grundrechtsschutzes des Betroffenen gegen den Gefahrenabwehrauftrag des LfV keine Stütze.

Soweit damit argumentiert wird, dass das LfV Informationen, die nicht in gemeinsamen Dateien automatisiert seien, ohnehin nicht nutzen könne und dürfe, ist dies anhand der dazu gegebenen Informationen nur schwer vorstellbar. Weshalb sollte das LfV eine Information, die beispielsweise handschriftlich in einer Papierakte hinterlegt wurde, ihm auf einem Datenträger oder in anderer Weise übergeben wurde, nicht für weitere Ermittlungen nutzen können oder dürfen? Gerade daran, ob solche „Beiakten“ mit weiteren Informationen bestehen, kann ein Betroffener doch ein berechtigtes Auskunftsinteresse haben.

Bemerkenswert ist, dass in diesem Zusammenhang mit einem erhöhten Verwaltungsaufwand argumentiert wird, der im Zusammenhang mit Sicherheitsüberprüfungen bei Großveranstaltungen offenbar nicht gesehen wird, obwohl er dort aufgrund der Massenverfahren in weit größerem Maße bestehen dürfte.

Die vorgesehene Einschränkung des Auskunftsanspruchs ist abzulehnen. Bezogen auf Daten, die dem LfV gleich in welcher Form zur Verfügung stehen, muss ein Auskunftsanspruch aus Gründen effektiven Grundrechtsschutzes bestehen.

f) § 15 LVSG BW - neu –

Sollte sich der Landesgesetzgeber – trotz der offensichtlichen Verfassungswidrigkeit – zur Zulassung einer verdeckten Quellen-TKÜ entschließen, erscheint es unverzichtbar, wenn die speziellen Berichtspflichten des Innenministeriums gegenüber dem Parlamentarischen Kontrollgremium und der G-10-Kommision auf die Maßnahmen nach dem neuen § 5c LVSG BW zu erstrecken.

Wir würden uns freuen, wenn unsere Hinweise und Vorschläge Berücksichtigung fänden. Für etwaige Rückfragen oder auch Gespräche stehen wir selbstverständlich gerne zur Verfügung. Sollte im Laufe des weiteren Verfahrens eine weitere Anhörung durchgeführt werden, bitten wir um eine Unterrichtung und die Gelegenheit zur Äußerung.

Mit freundlichen Grüßen

Prof. Dr. Peter Kothe
Präsident