



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 Dr. Matthias Strohs
Herrn Marc-Christoph Rapp
Willy-Brandt-Str. 41

70173 Stuttgart

Sitz:
Hasenbergsteige 5
70178 Stuttgart

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

Postfach 1221
70808 Korntal-Münchingen

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

Internet: www.av-bw.de
E-Mail: info@av-bw.de

08. August 2017

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

Az. 3-1101.2/268

Entwurf eines Gesetzes zur Änderung des Polizeigesetzes BW und eines Gesetzes über die Ladenöffnung in Baden-Württemberg
- Stellungnahme des Anwaltsverbandes Baden-Württemberg im DAV e. V. -

Sehr geehrter Herr Doktor Strohs,
sehr geehrter Herr Frank,

vielen Dank für die Übermittlung der Anhörungsunterlagen zum Entwurf eines Gesetzes zur Änderung des Polizeigesetzes und des Gesetzes über die Ladenöffnung in Baden-Württemberg nebst Anlagen mit Schreiben vom 27. Juni 2017. Der Anwaltsverband nimmt 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 Olympiastadion 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 Gesetzesentwurfs 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 verliedernden 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).

Wenig Verständnis hat der Anwaltsverband für den geplanten Einsatz von „Staatstrojanern“ zur Ausspähung auch verschlüsselter Internet-Kommunikation (§ 23b Abs. 2 PolG BW – 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. Es kann nicht sein, dass hier einzelne Betroffene – an einer Kommunikation beteiligte unbescholtene Bürger - 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.

Genauso wenig Verständnis hat der Anwaltsverband für die Schaffung einer neuen Kategorie sog. „Gefährder“ im Polizeirecht (§ 27b und c PolG BW – neu -). Solchen Personen dürfen aus dem Grundsatz der Verhältnismäßigkeit keine Aufenthaltsgebote auferlegt und elektronische Fußfesseln angelegt werden. Aus dem Strafrecht ist bereits jetzt schon hinlänglich bekannt, dass derartige Maßnahmen kaum Gewalttaten zu verhüten vermögen.

Äußerst kritisch sieht der Anwaltsverband den beabsichtigten Einsatz von Explosivmitteln durch Polizeibehörden (§ 54 PolG BW - neu -). Die Gesetzesbegründung benennt nicht einen einzigen Fall aus der Vergangenheit, in dem eine solche Befugnis als hilfreich für die Gefahrenabwehr erwiesen hätte.

Die vorgeschlagenen Maßnahmen scheinen recht kostenintensiv, aber im Einzelfall wenig erfolgversprechend zu sein. Der Anwaltsverband regt an, die finanziellen Mittel besser für die effektivere Handhabung der bisher zur Verfügung stehenden Maßnahmen bei gleichzeitiger Verbesserung der personellen und sächlichen Ausstattung einzusetzen.

2. Im Einzelnen

a) § 9a Abs. 1 S. 1 PolG BW – neu –

Durch die Streichung von „§§ 23, 25 bis“ wird der Schutz zeugnisverweigerungsberechtigter Berufsheimnisträger im Sinne des § 9a PolG auch auf polizeiliche Maßnahmen nach § 23a und § 23b erstreckt. Diese Regelung, die den Schutz der Berufsheimnisträger erweitert, wird vom Anwaltsverband ausdrücklich begrüßt. Dass auch § 24 PolG mit erfasst wird, dürfte im Zusammenhang mit Berufsheimnisträgern ohne praktische Auswirkung und deshalb unschädlich sein.

b) § 10a PolG BW – neu –

Ermächtigung für Kommunen, an Brennpunkten Alkoholkonsum zeitlich zu untersagen (nur Alkohol?, welche Mengen?, mögliche Sanktionen) – Unterschied zu flächendeckendem Alkoholverkaufsverbot (von 22.00 – 5.00 Uhr, in § 3a Ladenöffnungsgesetz BW, seit 2010)

Der Anwaltsverband hält den mit dem Gesetzentwurf eingeschlagenen Weg, durch Schaffung einer Ermächtigungsgrundlage an einschlägigen öffentlichen Orten den Alkoholkonsum zeitlich befristet durch eine – verhältnismäßige - Polizeiverordnung der Kommunen untersagen zu können, für sinnvoll. Die Vorgaben für die Prognose einer abstrakten Gefahr gemäß der Entscheidung

vgl. VGH Bad.-Württ., Urteil vom 28.07.2009 – 1 S 2200/08 –, VBIBW 2010, 29

dürften erfüllt sein, wengleich sich die Bedeutung der Formulierung, der zufolge

„sich die Belastung dort durch die Häufigkeit alkoholbedingter Straftaten oder Ordnungswidrigkeiten oder deren Bedeutung von der des übrigen Gemeindegebiets deutlich“

abheben soll, nicht bereits beim ersten Lesen erschließt. Es wird nicht deutlich, was mit „Belastung“ gemeint ist. Einfacher zu handhaben wäre wohl eine Ermächtigungsgrundlage, die darauf abstellt, dass

„sich die Häufigkeit oder Bedeutung der dort festgestellten alkoholbedingten Straftaten oder Ordnungswidrigkeiten von der des übrigen Gemeindegebiets deutlich“

unterscheiden.

Bedenken an der Wirksamkeit der gefundenen Regelung hat der Anwaltsverband aber bei der Frage, ob die Ermächtigungsgrundlage sich nur auf ein mögliches Verbot von Alkoholkonsum oder das Mitführen von Alkohol beziehen sollte. Es stellt sich die Frage, ob die Regelung nicht auch auf den Konsum anderer bisher ebenfalls legaler psychoaktiver Substanzen oder beispielsweise das öffentliche Wasserpfeifen-Rauchen (Shisha) ausgedehnt werden müsste. In manchen kommunalen Parks sammeln sich viele Jugendgruppen, deren Rauchkonsum für Passanten, insbesondere Kinder und (Freizeit-)Sportler, ebenfalls eine erhebliche Belästigung darstellt. Bereits das Vorbeigehen an solchen Gruppen bedeutet für die Passanten u. U. eine enorme psychische Belastung, etwa aufgrund verbaler Aussprüche und Drohgebärden, wengleich solche Gruppen – außer lautem Musikhören und Rufen - überwiegend friedlich sind und in der Regel keine Straftaten verüben. Damit mögen sie sich vom Gefährdungspotential alkoholisierter Ansammlungen zu unterscheiden. Dennoch können der gemeinsame (Drogen-)Genuss derartiger Ansammlungen in der Öffentlichkeit und die von ihnen ausgehende Gruppendynamik zu einer Störung zumindest der öffentlichen Ordnung werden.

c) § 21 Abs. 4 PolG BW – neu –

Das Grundgesetz versagt dem Staat ein in Grundrechte eingreifendes Handeln, außer ein Gesetz sieht dies ausdrücklich vor. Dies erfordert sowohl das rechtsstaatliche Bestimmtheitsgebot als auch der - im Demokratieprinzip und den Grundrechten wurzelnde - Vorbehalt des Gesetzes

BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83 –, BVerfGE 65, 1 (Volkszählungsurteil, Grundrecht auf informationelle Selbstbestimmung).

Derzeit existiert in § 21 PolG BW eine Eingriffsgrundlage, die der Polizei herkömmliche Videoüberwachungsmaßnahmen zur Abwehr von Gefahren sowie zur Strafverfolgungsvorsorge gestattet. Diese Regelung wurde vom Verwaltungsgerichtshof in der Entscheidung

VGH Bad.-Württ., Urteil vom 21.07.2003 – 1 S 377/02 –, VBIBW 2004, 20.

als grundsätzlich rechtmäßig gebilligt; sie wird in der Gesetzesbegründung angeführt.

Allerdings stellen der Vorbehalt des Gesetzes und das Bestimmtheitsgebot keine geringen Anforderungen an diese Befugnisnorm. Sie soll klar und präzise erkennen lassen, welche Maßnahmen von ihr gedeckt sind, damit die staatlichen Stellen die Reichweite und die Grenze ihrer Handlungskompetenz kennen. Auf der anderen Seite sollen sich die Bürger auf die Eingriffe sowie deren Voraussetzungen und Gewicht einstellen können

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

Schließlich soll die Einführung neuer Eingriffsinstrumente dem parlamentarischen Gesetzgeber vorbehalten bleiben.

Daran wird deutlich, dass die bestehenden Rechtsgrundlagen den Einsatz intelligenter Videoüberwachung nicht ohne vorhergehende und positiv geklärte Prüfung verfassungsgemäß vorsehen können. Die Grundrechtsrelevanz einer Überwachungsmaßnahme entscheidet darüber, ob sie noch von einem Gesetz gedeckt ist.

Durch den technischen Fortschritt verändert sich die Auswertung der Bilder von der visuellen Wahrnehmung einer menschlichen Person hin zur automatisierten Analyse durch Software anhand zuvor festgelegter Algorithmen. Dieser Modus der **Automatisierung ist als eingriffsintensivierend zu bewerten**

ähnlich BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220, zu dem Einsatz moderner, insbesondere dem Betroffenen verborgener Ermittlungsmethoden und dem Gefährdungspotenzial, das einem „additiven“ Grundrechtseingriff innewohnt.

Das wird auch in der hiesigen Gesetzesbegründung eingeräumt. Die Automatisierung kann beispielsweise eine größere Datenmenge wesentlich schneller verknüpfen. Mit der leistungsstärkeren Auswertung wird es für die Polizei möglich, größere Räume und mehr Menschen zu überwachen. Die automatische Auswertung selbst einer intelligenten Videoüberwachung kann zu Fehleinschätzungen von Situationen führen, die fehlerhafte Reaktionen der Einsatzkräfte nach sich ziehen.

Der Anwaltsverband erachtet deswegen die Schaffung einer eigenen Rechtsgrundlage für die automatisierte Auswertung von Bildaufzeichnungen für unabdingbar; auf deren Formulierung ist besondere Sorgfalt zu verwenden.

Der Gesetzentwurf schränkt in § 21 Abs. 4 S. 2 PolG BW – neu - den Gebrauch der automatischen Auswertung auf das Erkennen solcher Verhaltensmuster ein, die auf die Begehung einer Straftat hindeuten. Hierdurch wird versucht, die Grundrechtsbelastung so gering wie möglich zu halten. Dies wird vom Anwaltsverband begrüßt. Gleichwohl muss gewährleistet sein, dass die Entscheidung über präventiv-polizeiliche Einsätze nicht ebenfalls automatisch von Algorithmen getroffen wird, sondern von verantwortlichen Beamten. Die automatische Auswertung darf nur Hilfsmittel für den Polizeivollzugsdienst sein, keinesfalls aber automatisch Einsätze veranlassen.

d) § 23b PolG BW – neu –

aa) Allgemein

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)**, **Telekommunikations-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 aus-

dehnt, ihre Durchführbarkeit erleichtert und Verknüpfungen erlaubt, die bis hin zur Erstellung von Persönlichkeitsprofilen reichen. Solche Eingriffsbefugnisse erhalten daher ein besonderes Eingriffsgewicht.

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 informationstechnischer 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 für die Polizeibehörden zur Erkennung und damit Abwehr terroristischer Gefahren legitime Ziele verfolgt.

bb) Zu § 23b Abs. 1 Nr. 1, 2, 3 PolG BW – neu –

Damit die polizeilichen Befugnisse dem Verhältnismäßigkeitsgrundsatz genügen, müssen derart **gravierende Grundrechtseingriffe**, wie sie im jetzigen Gesetzentwurf vorgesehen sind, durch den **Schutz hinreichend gewichtiger Rechtsgüter** und **hinreichend konkret absehbare Gefahren** gerechtfertigt werden.

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 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.

Allerdings 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)

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.

Die in § 23b Abs. 1 PolG BW – neu - gefundenen Regelungen erfüllen die verfassungsrechtlichen Vorgaben hinsichtlich des Adressatenkreises und der zu schützenden Rechtsgüter. Insbesondere Satz 2 enthält mit den Tatbestandsmerkmalen „sonst ... aussichtslos oder wesentlich erschwert“ eine begrüßenswerte Konkretisierung des Verhältnismäßigkeitsgebotes.

Gerade deshalb fällt die mangelnde Bestimmtheit folgender Begriffe auf:

- „übersehbarer Zeitraum“ und
- „zumindest ihrer Art nach konkretisierte Weise“ der Begehung einer Straftat, und

- Einschüchterung der Bevölkerung „auf erhebliche Weise“.

Nähere Umschreibungen oder gar Legaldefinitionen fehlen. Welcher Zeitraum soll noch als „übersehbar“ gelten können? Wie konkret soll die Art der Straftat zu bestimmen sein? Gewalt wird regelmäßig bei Straftaten gegen das Leben, gegen die körperliche Unversehrtheit oder Raub und Erpressung eingesetzt; soll dieses Element genügen, um eine Straftat ihrer Art nach zu konkretisieren? Soll die Einschüchterung der Bevölkerung auf erhebliche Weise an Personenzahl der betroffenen Bevölkerungskreise festgemacht werden oder an der Brutalität der geplanten Straftat? Wann ist von einer Einschüchterung der Bevölkerung auszugehen, wenn etwa die Politik nach jedem Terrorakt dazu aufruft, das Leben in seinen gewohnten Bahnen fortzuführen, weil anderenfalls die Terroristen ihr Ziel erreicht hätten?

Diese wenigen Beispiele zeigen, dass der Katalog von Merkmalen trotz des anzuerkennenden Bemühens um Konkretisierung in unüberbrückbarem Widerspruch zu der Vorgabe des Bundesverfassungsgerichts, Prognoseanforderungen hinreichend gehaltvoll auszugestalten. Eine solche Ausgestaltung kann nicht dadurch ersetzt werden, dass nur abstrakte Formulierungen aus höchstrichterlichen Entscheidungen im Wortlaut übernommen, aber nicht auf ein praxistaugliches Maß „heruntergebrochen“ werden. Dass das Bundesverfassungsgericht dem Gesetzgeber einen Rahmen vorgegeben hat, entbindet ihn nicht von seiner Aufgabe, diese durch klare und verständliche Regelungen auszufüllen.

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.

Es ist deshalb unabdingbar, die Ermächtigungsgrundlage hinsichtlich der genaueren Definition, ab welcher konkreten Gefahrenlagen die TKÜ eingesetzt werden darf, nachzubessern. Das Bundesverfassungsgericht hat verlangt, dass die Regelungen ausreichend bestimmt und normenklar sind. Dies soll eine Vorhersehbarkeit von Eingriffen für die Bürge-

rinnen und Bürger herstellen, die Befugnisse der Polizeibehörden wirksam begrenzen sowie eine effektive Kontrolle durch die Gerichte ermöglichen. Dem wird der bislang vorliegende Entwurf nicht gerecht.

cc) Zu § 23b Abs. 1 Nr. 4, 5 PolG BW – neu –

Das Bundesverfassungsgericht hat in seinen Entscheidungen

BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07 –, BVerfGE 120, 274, und
BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220,

die verfassungsrechtlichen Anforderungen aufgelistet, die bei sog. Online-Durchsuchungen durch Sicherheitsbehörden zu beachten sind.

Danach umfasst das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, sei verfassungsrechtlich nur zulässig, wenn **tatsächliche Anhaltspunkte einer konkreten Gefahr** für ein **überragend wichtiges Rechtsgut** bestehen. Überragend wichtig seien Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme könne schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lasse, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte **Tatsachen** auf eine **im Einzelfall durch bestimmte Personen** drohende Gefahr für das überragend wichtige Rechtsgut hinweisen würden.

Die heimliche Infiltration eines informationstechnischen Systems sei grundsätzlich unter den **Vorbehalt richterlicher Anordnung** zu stellen. Das Gesetz, das zu einem solchen Eingriff ermächtige, müsse Vorkehrungen enthalten, um den **Kernbereich privater Lebensgestaltung** zu schützen.

Soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränke, durch welche die Inhalte und Umstände der **laufenden** Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet würden, sei der Eingriff an **Art. 10 Abs. 1 GG** zu messen. Verschaffe sich der Staat Kenntnis von Inhalten der Internetkommunikation auf dem dafür technisch vorgesehenen Weg, so liege darin nur dann ein Eingriff in Art. 10

Abs. 1 GG, wenn die staatliche Stelle nicht durch Kommunikationsbeteiligte zur Kenntnisnahme autorisiert sei.

§ 23b Abs. 1 PolG BW – neu – wird den verfassungsgerichtlichen Vorgaben insofern gerecht, als dass er die Verursacher bzw. Verantwortlichen und damit die Adressaten der Überwachungsmaßnahme explizit benennt. Sinnvoll kann eine Kommunikationsüberwachungsmaßnahme nur sein, wenn durch sie die Geräte erfasst werden, von denen aus die Kommunikation erfolgt. Insoweit erscheint die Ausweitung des Anwendungsbereichs auf Nachrichtensmittler oder Gerätebereitsteller in § 23b Abs. 1 Nr. 4 und 5 PolG BW – neu – sinnvoll. Der Anwaltsverband würde es mit Blick auf die betroffenen Grundrechte und die Verhältnismäßigkeit des Eingriffs jedoch begrüßen, wenn höhere Anforderungen gestellt und „hinreichend bestimmte Tatsachen“ zur Eingriffsvoraussetzung gemacht würden.

Nur unter eingeschränkten Voraussetzungen dürfen solche polizeilichen Maßnahmen auch unbeteiligte Dritte 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 eingriff-intensive Überwachungsmaßnahmen eingesetzt werden.

Wenngleich die Verwendung unbestimmter Rechtsbegriff gesetzestechnisch insbesondere im Gefahrenabwehr recht, grundsätzlich nicht zu beanstanden ist, hält es der Anwaltsverband mit Blick auf die betroffenen Grundrechte und die Verhältnismäßigkeit des Eingriffs für geboten, höhere Anforderungen zu stellen und „hinreichend bestimmte Tatsachen“ zur Eingriffsvoraussetzung zu machen. Auf diese Weise könnten Bedenken gegen die Regelungen in § 23b Abs. 1 Nr. 4 und 5 PolG BW – neu – ausgeräumt werden.

dd) § 23b Abs. 2 PolG BW – neu -

Die Wohnraumüberwachung und der mit dem Gesetzentwurf in § 23b PolG BW – neu - beabsichtigte Zugriff auf informationstechnische Systeme (TKÜ und „Staatstrojaner“) dringen besonders tief in die Privatsphäre ein.

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.

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 exportierenden 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.

Die in § 23b Abs. 1 PolG BW – neu – vorgenommene Erweiterung der genannten Rechtsgüter um „Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt“, steht in Widerspruch zu der vom Bundesverfassungsgericht angenommenen Wertigkeit der Rechtsgüter und stellt somit einen Systembruch dar. Die gewählte Begrifflichkeit gilt etwa für zahlreichen Einrichtungen der Daseinsvorsorge, deren Beeinträchtigung aber weder die Grundlagen oder gar den Bestand des Staates oder die Grundlagen menschlicher Existenz bedroht. Überspitzt formuliert, wäre die Voraussetzung bereits erfüllt, wenn eine bedeutende Kunstsammlung von einem Diebstahl bedroht wäre; dass eine solche Tat präventiv-polizeiliche Überwachungsmaßnahmen der in Rede stehenden Art nicht gemäß den verfassungsrechtlichen Anforderungen rechtfertigen könnte, liegt auf der Hand. Das – bewusst überzeichnete – Beispiel verdeutlicht die mangelnde Bestimmtheit der Erweiterung, die deshalb abzulehnen ist.

Zur mangelnden Bestimmtheit einer „Einschüchterung der Bevölkerung auf erhebliche Weise“ hatten wir uns bereits zuvor geäußert; dieselben Bedenken gelten auch im vorliegenden Zusammenhang.

Die in § 23b Abs. 2 PolG BW – neu – genannten Schutzgüter sind daher teilweise nicht schwerwiegend genug, um den Einsatz der Quellen-TKÜ nach den verfassungsgerichtlichen Maßstäben zu rechtfertigen. Der Anwaltsverband schlägt vor, hier – auch aus Gründen der besseren Handhabbarkeit – einen eigenen Schutzgüterkatalog anstelle der jetzigen Verweisungstechnik zu definieren.

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

Von Experten wird u. a. die technische Umsetzbarkeit einer Quellen-TKÜ bezweifelt: Antivirenprogramme würden alle Schadprogramme gleich behandeln. Tjark Auerbach, Geschäftsführer 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 bleibt auch 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 nach § 55 PolG BW 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 Überwachungsmaßnahmen. Es wird bezweifelt, dass der Staat sicherstellen kann, dass nicht genau die Sicherheitslücke, die er durch das Einschleusen eines Trojaners 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 Gefahrenabwehr 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 Bedenken gegen die Ermöglichung der heimlichen Manipulation vorhandener informationstechnischer Systeme und lehnt diese Regelung ab.

ee) Zu § 23b Abs. 4 und 5 PolG BW – neu –

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. Die Ausgestaltung des Antragsverfahrens in § 23b Abs. 4 PolG BW – neu – entspricht weitgehend den Vorgaben der zitierten Entscheidung.

ff) Zu § 23b Abs. 6 PolG BW – neu –

An die – unabhängig und eigenverantwortlich zu treffende – **gerichtliche Anordnung** werden strenge Anforderungen hinsichtlich deren Inhalt und Begründung gestellt.

Die Ausgestaltung des Anordnungsverfahrens in § 23b Abs. 6 PolG BW – neu – entspricht den weitgehend Vorgaben des Bundesverfassungsgerichts. Durch den Verweis auf § 23 Abs. 3 Sätze 2 bis 7 PolG BW eine Höchstdauer von drei Monaten vorgesehen. Das Verfahren soll sich – durch den Verweis auf § 31 Abs. 5 S. 2 bis 4 PolG BW – nach den Vorschriften des FGG richten.

gg) Zu § 23b Abs. 7 PolG BW – neu –

Für die hier beabsichtigte Regelung (Ausnahme vom Richtervorbehalt für die Überwachungsanordnung) vermag der Anwaltsverband keine Rechtfertigung zu finden.

Insbesondere hat das Bundesverfassungsgericht eine solche Möglichkeit in seiner Entscheidung

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

nicht vorgesehen. Es hat bei Gefahr im Verzug lediglich die vorherige Sichtung erhobener Daten zum Herausfiltern von Informationen aus dem privaten Kernbereich als möglich erachtet.

In praktischer Hinsicht fragt sich, wie lange es dauert, bis eine Polizeibehörde die Notwendigkeit des Mithörens von Telefonaten oder Mitlesens von E-Mails und Chats erkannt hat, weil mildere Mittel nicht erfolgversprechend erscheinen, und dann die technische Einrichtung der Überwachung funktionsfähig bereit gestellt hat. Hierfür muss der Polizeivollzugsdienst etwa wissen, über welchen Telekommunikationsanbieter mit welcher Telefonnummer die Person kommuniziert. Weshalb es dann nicht möglich sein soll, eine richterliche Anordnung desjenigen Amtsrichters der Bereitschaftsdienst hat, zu beschaffen, ist nicht ersichtlich.

Erfahrungsgemäß führen große Telekommunikationsunternehmen das Einrichten einer TKÜ mittels eigenen Fachpersonals durch. Bevor sie damit beginnen, prüfen sie aber selbst auch noch einmal die Rechtmäßigkeit der ihnen abverlangten Maßnahmen, etwa durch das Lesen des entsprechenden gerichtlichen Beschlusses und Abarbeiten einer internen Checkliste. In der Technik müssen Vorkehrungen für die angeordnete Laufzeit, Reichweite sowie deren Kontrolle getroffen werden.

Kleinere Telekommunikationsanbieter halten solche Spezialisten oft nicht selbst vor, sondern können sich entsprechender Dienstleister bedienen. Mit denen müssen sie aber u. U. erst noch Verträge abschließen. Denkbar ist auch, dass vom Betroffenen und seinem Umfeld ein Telekommunikationsanbieter aus dem Ausland verwendet wird. Hier könnte allein schon eine etwaige Sprachübersetzung - der wohl in Deutsch verfassten - gerichtlichen Anordnung Zeit kosten. Das technische Einrichten der TKÜ kann so auch einige Stunden dauern.

Das Eindringen ins informationstechnische System eines Verdächtigen dürfte ebenfalls einige Zeit in Anspruch nehmen. Solche Maßnahmen werden bisher wohl vom BKA oder LKA mit eigenen Spezialisten vorgenommen.

Hier können also nur Fälle gemeint sein, in denen es erforderlich erscheint, mit der TKÜ und Quellen-TKÜ schon sofort beginnen zu müssen und nicht abwarten zu können, bis die richterliche Anordnung eingeht. Solche Fälle dürften, da zuvor gegebenenfalls sehr aufwändig viel mehr ermittelt werden muss, z. B. wo eine Person sich aufhält und welchen Anschluss sie benutzt, sehr selten sein. Wenn beide Vorgänge (technische Einrichtung der TKÜ und Antrag auf richterliche Anordnung) zeitgleich begonnen werden, müsste es möglich sein, über den erforderlichen richterlichen Beschluss zu verfügen, bis die TKÜ tatsächlich beginnt.

Der Anwaltsverband vermag die Notwendigkeit der vorgesehenen Regelung nicht zu erkennen. Unabhängig davon schlägt er eine **Ergänzung analog zum Strafprozessrecht** vor. Dort kann bei Gefahr im Verzug notfalls auch die Staatsanwaltschaft eine TKÜ anordnen und muss sich unverzüglich um einen gerichtlichen Beschluss bemühen; dies entspricht in etwa § 23b Abs. 7 PolG BW – neu -. Zwingend zu erweitern ist diese Befugnis jedoch für den Fall, dass trotz der hiesigen Bedenken an ihr festgehalten werden sollte, dahin, dass – wenn die richterliche Anordnung nicht innerhalb von drei (Werk-)Tagen erfolgt -, die Maßnahme als nicht genehmigt gilt und unverzüglich einzustellen ist (vgl. § 100b StPO).

hh) § 23b Abs. 9 PolG BW – neu –

Das Bundesverfassungsgericht fordert in seiner Entscheidung

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

dass der Kernbereich privater Lebensführung (Wahrung der Menschenwürde) sowie der Schutz von Berufsgeheimnisträgern zu gewährleisten ist.

Bereits bei der Datenerhebung sind Vorkehrungen zu treffen, dass eine unzulässige Mit-erfassung von Kernbereichsinformationen unterbleibt, etwa durch einen **unverzüglichen Abbruch** der Überwachungsmaßnahme. Bei der nachgelagerten Auswertung sind die Folgen unzulässiger Datenmit-erhebung zu minimieren,

vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 126).

Dies kann durch eine **vorherige Sichtung** der erfassten Daten durch eine unabhängige Stelle geschehen, die unzulässige Informationen herausfiltert, bevor die übrigen zulässigen Daten von den Sicherheitsbehörden verwendet werden.

Für Fälle, bei denen **Gefahr im Verzug** ist, dürfen hier Ausnahmen gemacht werden

vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 129).

Der Gesetzgeber muss aber bei unzulässigen Datenerhebungen die **sofortige Löschung** vorsehen. Eine solche Löschung ist so zu **protokollieren**, dass eine **spätere Kontrolle möglich** ist.

Diesen Anforderungen wird § 23b Abs. 9 PolG BW – neu - zwar gerecht. Praktisch dürfte die Sichtung erlangter Daten durch eine unabhängige Stelle auf deren Kernbereichsrelevanz jedoch aufgrund der regelmäßig anfallenden Datenmenge **kaum umsetzbar** sein. So verfügen moderne informationstechnische Systeme über enorme Speicherkapazitäten von zum Teil mehreren Terabyte. Die Überprüfung aller nach § 23 b Abs. 2 PolG BW - neu - erhobenen Daten dürfte daher die Grenzen der Belastbarkeit der möglichen „Stelle“ und erst recht mit Blick auf die erforderliche Kontrolle durch die zuständigen Gerichte regelmäßig sprengen.

ii) **Zu § 23b Abs. 10 PolG BW – neu -**

Zu den Anforderungen an die verhältnismäßige Ausgestaltung der Überwachungsmaßnahmen gehört die gesetzliche Anordnung von **Benachrichtigungspflichten**. Zur Gewährleistung subjektiven Rechtsschutzes nach Art. 19 Abs. 4 GG muss der Grundsatz gelten, dass die Betroffenen **zumindest nachträglich** immer in Kenntnis zu setzen sind. Ausnahmen sind denkbar soweit sie, z. B. zur Zweckverfolgung oder dem Schutz von Leib und Leben, erforderlich sind

vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 136).

Wenn eine nachträgliche Benachrichtigung unterbleiben soll, ist dies richterlich zu bestätigen und in regelmäßigen Abständen zu prüfen

vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 136).

Die in § 23b Abs. 10 PolG BW – neu - vorgesehene Regelung erfüllt die Anforderungen des Bundesverfassungsgerichts weitgehend. Dennoch bleiben die Gründe, die das Unterlassen der grundsätzlich gebotenen Unterrichtung nach **Satz 6** erlauben sollen, recht vage formuliert. So ist bereits nicht nachvollziehbar, aufgrund welcher Anhaltspunkte die Polizei anzunehmen berechtigt sein sollte, die heimlich überwachte Person habe kein Interesse daran von der in der Vergangenheit erfolgten Überwachung zu erfahren. Unter Berücksichtigung des Umstandes, dass eine Zurückstellung der Benachrichtigung alle sechs Monate durch eine richterliche Entscheidung bestätigt werden muss, ist es inakzeptabel, wenn von einer Unterrichtung jedenfalls abgesehen werden kann, wenn seit Beendigung der Maßnahme fünf Jahre verstrichen sind. Zunächst verhindern richterliche Entscheidungen eine Unterrichtung und dann soll sie infolge Zeitablaufs entbehrlich sein. Dies verkehrt den subjektiven Rechtsschutz in sein Gegenteil.

Nach § 23b Abs. 10 Satz 1 PolG BW – neu – sieht grundsätzlich eine Unterrichtung über heimlich erfolgte Maßnahmen der Telekommunikationsüberwachung vor. Nur bei Vorliegen einer der enumerativ beschriebenen Ausnahmen, die – wie zuvor ausgeführt – erheblichen Bedenken begegnen, soll nach pflichtgemäß auszuübenden Ermessen von einer Unterrichtung abgesehen werden können.

Gemäß § 23b Abs. 10 Satz 3 PolG BW – neu – soll nur die Zurückstellung der Unterrichtung wegen andauernder Ermittlungen und Gefährdung des Ermittlungserfolges dokumentiert werden. Für das Absehen von der Unterrichtung nach Maßgabe des § 23b Abs. 10 Satz 6 Nr. 1 bis 4 PolG BW – neu - ist hingegen keine Dokumentation vorgesehen. Das Fehlen einer Dokumentation höhlt den Grundrechtsschutz des Betroffenen aus, der auf eine nachträgliche Unterrichtung angewiesen ist. So verständlich und notwendig es ist, Maßnahmen der Telekommunikationsüberwachung unbemerkt durchzuführen, so unverzichtbar ist es, dem Betroffenen zumindest nachträglich den Rechtsschutz zu gewähren, den die Wahrung seiner Grundrechte erfordert. Das Fehlen einer Dokumentation, die selbstverständlich auch die Gründe zu umfassen hat, aus denen die Polizeibehörde glaubt, von einer nachträglichen Unterrichtung absehen zu können, führt zur Verfassungswidrigkeit der gesamten Regelung.

Zwar sieht das Bundesverfassungsgericht eine Möglichkeit, den individuellen Rechtsschutz Betroffener mit Blick auf den Erfolg solcher Maßnahmen der Gefahrenabwehr einzuschränken, verlangt aber im Gegenzug ein ausreichendes Maß an Transparenz, aufsichtsrechtlicher Kontrolle einschließlich einer gerichtlichen Überprüfung und Löschungspflichten,

vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 137).

§ 45 PolG BW i. V. mit § 21 LDatSchG erweist sich insoweit als unzureichend, weil danach gerade keine Pflicht zur Angabe der Datenherkunft besteht, weshalb der Betroffene auf diese Weise nicht erfahren kann, ob er einer TKÜ-Maßnahme unterlag, und folglich auch nicht prüfen bzw. überprüfen lassen kann, ob die Voraussetzungen für deren rechtmäßige Durchführung vorlagen.

jj) Zu § 23b Abs. 11 und 12 PolG BW – neu –

Zu den übergreifenden Verhältnismäßigkeitsanforderungen gehört auch die Regelung von Löschungspflichten nach der begrenzten Verwendung. Die abschließende Löschung der Daten ist ebenfalls zu protokollieren,

vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 144).

Die im Gesetzentwurf vorgesehenen Protokollierungspflichten bei der Datenerhebung erscheinen geeignet, die vom Bundesverfassungsgericht geforderte effektive Kontrollmöglichkeit durch den Betroffenen oder den Datenschutzbeauftragten zu gewährleisten. Angesichts dieser detaillierten Regelung fällt umso mehr auf, das – bezogen auf das Absehen von einer Unterrichtung – jegliche Dokumentations- bzw. Protokollierungspflicht fehlt.

kk) Zu § 23b Abs. 13 PolG BW – neu –

Da die Ermöglichung individuellen Rechtsschutzes bei heimlichen Überwachungsmaßnahmen nur sehr eingeschränkt sichergestellt werden kann, muss im Gegenzug eine effektive aufsichtliche Kontrolle gewährleistet sein. Dies ist Aufgabe des Landesbeauftragten für den Datenschutz,

vgl. zur analogen Zuständigkeit des Bundesbeauftragten für den Datenschutz BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220.

Dieser kann eine solche Kontrolle nur wirksam ausüben, wenn die Datenerhebungen vollständig protokolliert sind. Die Kontrollen müssen zur Kompensation des eingeschränkten

individuellen Rechtsschutzes regelmäßig durchgeführt werden. Der Abstand zwischen solchen Kontrollen darf nicht größer als zwei Jahre sein

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

Diesem Erfordernis wird durch die beabsichtigte Regelung in § 23b Abs. 13 PolG BW – neu - Rechnung getragen. Erfreulich ist hier die Aufnahme der Vorgabe „mindestens“, die dem Landesbeauftragten für den Datenschutz ermöglicht, derartige Kontrollen auch in kürzeren Zeitabständen durchzuführen.

Das Bundesverfassungsgericht hat aber auch die Vorgabe gemacht, dass die Aufsichtsinstanz entsprechend auszustatten ist, damit sie ihre Kontrollfunktion effektiv ausführen kann. Angesichts des zunehmenden Umfangs an zu bewältigenden Aufgaben ist der Landesbeauftragte für den Datenschutz dementsprechend mit Personal und Sachmitteln auszustatten; zumindest in die Gesetzesbegründung sollte deshalb an geeigneter Stelle dringend folgender Zusatz aufgenommen werden:

„Das Land verpflichtet sich, dem Landesbeauftragten für den Datenschutz die hierfür erforderlichen personellen und sachlichen Mittel zur Verfügung zu stellen.“

II) Zu § 23b Abs. 14 PolG BW – neu –

Die Transparenz der Datenerhebung und -verarbeitung soll dazu beitragen, dass Vertrauen und Rechtssicherheit entstehen können und der Umgang mit den Daten in einen demokratischen Diskurs eingebunden bleibt. Durch sie soll, soweit möglich, den Betroffenen subjektiver Rechtsschutz ermöglicht und zugleich einer diffusen Bedrohlichkeit geheimer staatlicher Überwachung entgegengewirkt werden. Je weniger die Gewährleistung subjektiven Rechtsschutzes möglich ist, desto größere Bedeutung erhalten die aufsichtliche Kontrolle und Transparenz des Behördenhandels gegenüber der Öffentlichkeit,

vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 135).

Die erforderliche Transparenz der heimlichen staatlichen Datenerhebung verlangt auch eine **gesetzliche** Regelung von Berichtspflichten der Polizeibehörden gegenüber dem Parlament

vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 142, 143).

Sie müssen so hinreichend gehaltvoll sein, dass sie eine öffentliche Diskussion über Art und Ausmaß staatlicher TKÜ ermöglichen. Die Unterrichtung muss regelmäßig erfolgen. Die Berichte müssen auch die Handhabung der Benachrichtigungs- und Löschungspflichten umfassen.

Insoweit bedarf § 23b Abs. 14 PolG BW - neu – der Ergänzung, als die Anforderungen an den Inhalt bzw. die Qualität des Berichts zu konkretisieren sind. Es wäre wünschenswert und als Zeichen des Respekts des Staates vor der Sensibilität im Umgang mit den betroffenen Grundrechten zu sehen, wenn die vom Bundesverfassungsgericht als Mindeststandard definierte Frist von zwei Jahren nicht vollständig ausgeschöpft würde. Durch eine Unterrichtung des Landtags in kürzeren Abständen, etwa einmal jährlich, würde die Thematik öfter in den politischen Diskurs eingebracht. Dies dürfte unschwer möglich sein, weil die Behörden ohnehin jährliche Statistiken – auch bei § 100a StPO – erstellen und nach § 23 Abs. 10 PolG BW die Landesregierung ebenfalls zu einem jährlichen Bericht über die TKÜ verpflichtet ist.

mm) Weitere verfassungsrechtliche Aspekte

Nach der Rechtsprechung des Bundesverfassungsgerichts setzt eine verhältnismäßige Ausgestaltung wirksame Sanktionen bei Rechtsverletzungen voraus. Würden auch schwere Verletzungen der Eingriffsvoraussetzungen im Ergebnis sanktionslos bleiben mit der Folge, dass der Schutz des Persönlichkeitsrechts angesichts der immateriellen Natur dieses Rechts verkümmern würde, widerspräche dies der Verpflichtung der staatlichen Gewalt, die Entfaltung der Persönlichkeit wirksam zu schützen. Dies kann insbesondere der Fall sein, wenn eine unberechtigte Erhebung oder Verwendung der Daten mangels materiellen Schadens regelmäßig ohne einen der Genugtuung der Betroffenen dienenden Ausgleich bliebe,

vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 139)

Insofern vermisst der Anwaltsverband wirksame Sanktionen; eine ausdrückliche Regelung für den Ersatz materieller und immaterieller Schäden nennt der Gesetzentwurf nicht.

3. Zu §§ 27b bis 27c bis

a) § 27b Abs. 1 PolG BW – neu -

Regelungen zu Aufenthaltsverboten an bestimmten Örtlichkeiten für Personen, von denen die Begehung einer Straftat erwartet werden kann, sind mit deutlich geringeren Eingriffsvoraussetzungen, bereits heute nach § 27a PolG BW möglich. Anwendungsfälle sind beispielsweise die Verhütung von Straftaten im Zusammenhang mit Fußballspielen

vgl. VGH Bad.-Württ., Urteil vom 18.05.2017 – 1 S 1193/16 –, juris; VGH Bad.-Württ., Urteil vom 18.05.2017 – 1 S 160/17 –, juris,

oder ein Annäherungsverbot beim Stalking. In diesen Fällen ist die abzuwehrende Gefahr, gewalttätige Auseinandersetzungen im Zusammenhang mit Fußballspielen oder versuchte Nötigung, bereits konkret absehbar.

Neu an der jetzt in § 27b PolG BW vorgesehenen Regelung ist die Ermächtigung der Polizeibehörden den Betroffenen den Aufenthalt in einem bestimmten Bereich vorzuschreiben. Derartige Regelungen sehen die Polizeigesetze der Länder bislang nicht vor, sieht man von den Regelungen zum polizeilichen Gewahrsam ab, die nur unter strengen Voraussetzungen zulässig sind. Da der „Bereich“ des vorgeschriebenen Aufenthalts räumlich nicht näher begrenzt ist, könnte dies theoretisch bis zum Hausarrest gehen. Der Eingriff in Art. 2 GG (Freiheit der Person) ist offenkundig. Jede Einschränkung dieser Freiheit ist stets der strengen Prüfung am **Grundsatz der Verhältnismäßigkeit** zu unterziehen. Für präventive Eingriffe in die Freiheit der Person gilt dies nach der Rechtsprechung des Bundesverfassungsgerichts in besonderem Maße, da diese Einschränkungen der Freiheit nicht dem Schuldausgleich dienen. Sie sind deshalb nur zulässig, wenn der **Schutz hochwertiger Rechtsgüter** dies unter strikter Beachtung des Verhältnismäßigkeitsgrundsatzes erfordert. Die Beschränkung des Aufenthalts auf einen bestimmten Bereich ist deshalb ein Grundrechtseingriff von erheblichem Gewicht, der erfordert, dass eine Gefährdung von Rechtsgütern hinreichend konkret absehbar sein muss. Die Gesetzesbegründung führt auf S. 49 „das Gebiet eines Bundeslandes, einen bestimmten Radius um den Aufenthaltsort oder ein oder mehrere Stadtbezirke“ einer Großstadt als möglichen Bereich einer Aufenthaltsbeschränkung an. Ausländerrechtlich gibt es entsprechende Befugnisse nach § 62 Abs. 3 Nr. 1a AufenthG.

Die in § 27b Abs. 1 geregelte Aufenthaltsvorgabe richtet sich an Personen, die weder Verdächtige (Anfangsverdacht i. S. des § 152 StPO) noch Verursacher einer Gefahr (Störer i. S. des § 6 PolG BW) sind. Die Norm enthält erstmals Regelungen für Eingriffe gegenüber „Gefährdern“. Eine – informelle – Definition des „Gefährders“ gab es in der Arbeitsgemeinschaft der Landeskriminalämter und des Bundeskriminalamtes „AG Kripo“. Danach sollte ein „Gefährder“ eine Person sein, bei der

bestimmte Tatsachen die Annahme rechtfertigen, dass sie politisch motivierte Straftaten von erheblicher Bedeutung, insbesondere solche i. S. des § 100 a StPO, begehen wird (Schriftliche Antwort der Bundesregierung auf die Frage des MdB Wolfgang Neskovic vom 20.11.2006, BT-Drucks. 16/3570 vom 24.11.2006).

Bei der „Verhütung von Straftaten“ geht es um einen „ungleich geringeren Wahrscheinlichkeitsgrad einer künftigen Straftatbegehung als bei einer Gefahrenprognose“. Die Eingriffsschwelle des § 27b Abs. 1 PolG BW – neu - knüpft damit an weit im Vorfeld einer Gefahr liegende Umstände an, bei denen per definitionem nur relativ diffuse Anhaltspunkte für mögliche künftige Gefahren bestehen können. Die Tatsachenlage ist dann häufig durch eine hohe Ambivalenz der Bedeutung einzelner Beobachtungen gekennzeichnet. Die Geschehnisse können in harmlosen Zusammenhängen verbleiben, sich aber auch konkretisieren und in eine Gefahr münden. In einer solchen Situation mögen Überwachungsmaßnahmen möglich sein. Eingriffe der Informationsbeschaffung sind jedoch weit weniger intensiv also solche, mit dem einer Person der Aufenthalt in einem bestimmten Bereich vorgeschrieben wird. Dieser Eingriff in die persönliche Freiheit durch eine Beschränkung des Aufenthalts geht über eine Überwachungsmaßnahme weit hinaus. Denn bei einer Überwachungsmaßnahme bleibt die Bewegungsfreiheit einer Person grundsätzlich unberührt. Für einen solchen Eingriff in die persönliche Freiheit ist eine Konkretisierung der Gefahrenlage in jedem Falle erforderlich. Ohne eine solche Konkretisierung der Gefahrenlage bleibt auch unklar, wie der Bereich umschrieben werden soll, an dem sich die Person nicht aufhalten darf, bzw. in dem sie sich aufhalten muss. Jede Beschränkung des Aufenthaltsbereichs einer Person ist rechtfertigungsbedürftig. Wie soll aber eine Beschränkung des Aufenthaltsbereichs aus Gründen der Gefahrenabwehr eingegrenzt werden, wenn die abzuwehrende Gefahr, deren Entstehung allenfalls befürchtet wird, nicht hinreichend konkret ist?

Es stellt sich auch die Frage der Geeignetheit von Aufenthaltsge- oder verboten zur Abwehr möglicher terroristischer Gewalttaten. Wird dem „Gefährder“ nämlich auferlegt, einen oder zwei bestimmte Stadtbezirke nicht zu verlassen, wird er möglicherweise davon abgehalten, in einem dritten oder vierten Bezirk Anschläge zu verüben. Er ist aber nicht gehindert, sich in dem Bereich, in dem er sich frei bewegen darf, Ziele wie Schulen, Kindergärten, Einkaufs-Zentren oder andere öffentliche Orte auszusuchen, die es in allen Stadtbezirken gibt. Bei dem Personenkreis, der als terroristischer „Gefährder“ in Betracht kommt, ist, wie die Erfahrung mit Anschlägen in den letzten Jahren zeigt, eine Vorhersehbarkeit der Angriffsziele nicht gegeben. Daher sind Aufenthaltsge- und verbote, wenn sie nicht wie ein haftähnlicher Hausarrest ausgestaltet werden (was dann andere verfassungsrechtliche Fragen aufwerfen würde), auch unter dem Gesichtspunkt fehlender Geeignetheit unverhältnismäßig.

Es soll zum Beispiel ausreichen, dass das individuelle Verhalten der betroffenen Person anhand bestimmter Tatsachen die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines überschaubaren Zeitraums eine schwere Straftat, wie eine Katalogtat aus § 129a StGB, begehen wird. Mit diesem neuen Begriff des „Gefährders“ wird der Bereich der Gefahrenabwehr noch weiter vorverlagert, als er dies ohnehin schon ist. Der damit verbundene Grundrechtseingriff ist unverhältnismäßig.

Wie aus der öffentlichen Diskussion der letzten Monate zu entnehmen ist, bestehen starke Bedenken, korrekt festlegen zu können, wen man für einen solchen „Gefährder“ hält. Der Fall Amri hat gezeigt, dass er zwar gegenüber mehreren Sicherheits- und Justizbehörden auffällig geworden ist, er aber dennoch nicht für so gefährlich gehalten wurde, als dass man ihn permanent überwacht hätte.

Umgekehrt verbietet auch die Unschuldsvermutung, jemanden vorschnell als Gefährder einzustufen. Es kann verschiedene Motive geben, warum jemand sich in einem als einschlägig für gefährlich eingestuften Umfeld aufhält. Es muss nicht zwingend die Absicht sein, selbst zum Täter zu werden.

Selbst die eindeutige Radikalisierung einer Person, etwa durch ihr optisches Erscheinungsbild, das bevorzugte Hören bestimmter Musik oder stundenlanges Surfen auf bestimmten Internetseiten, stellt noch keine konkrete Gefährdung der Inneren Sicherheit dar. Hier sei an die jahrelange Diskussion erinnert, ob der Konsum gewaltverherrlichender Computerspielen deren Nutzer zu Gewalttätigern in der Realität macht. Bisher ist man sich hier nur einig, dass ein solcher Konsum einen Beitrag leisten kann und eventuell auch ein Indiz darstellt. Der vollwertige Beweis einer solchen Wirkung auf alle Nutzer gleichermaßen ist aber noch nicht geführt. Um jemanden als „Gefährder“ einzustufen zu können, müsste man also sehr starken Einblick in die Innenwelt der Person haben. Das ist bekanntermaßen schwierig. Provokante Texte könnte jemand im Internet auch nur deshalb veröffentlichen, um auf sich aufmerksam zu machen.

Aus den vorgenannten Gründen ist die Schaffung dieser Ermächtigungsgrundlage (Aufenthaltsvorgaben für Gefährder) für den Polizeivollzugsdienst abzulehnen.

Darüber hinaus vermisst der Anwaltsverband Regelungen zum Rechtsschutz für den Betroffenen. Bei Eingriffen in die persönliche Freiheit kommt dem Rechtsschutz durch ein effektives Verfahren besondere Bedeutung zu. Stehen polizeiliche Maßnahmen unter Richtervorbehalt, dann wird die Zuweisung dieser Verfahren an die Amtsgerichte damit gerechtfertigt, dass – etwa bei der Inge-wahrsamnahme – das Amtsgericht das ortsnähere Gericht ist und eine Anhörung des Betroffenen und damit effektiver Rechtsschutz besser gewährleistet werden kann, als durch das Verwaltungsgericht. Auf diese Weise ist es insbesondere möglich Rechtsschutzgesuche, etwa im Hinblick auf

die Erlaubnis zum Verlassen des zugewiesenen Aufenthaltsbereichs, ortsnahe zu bescheiden. Denkbar ist aber auch eine Zuständigkeit des Verwaltungsgerichts. Auch ausländerrechtlichen Auflagen hinsichtlich des Aufenthalts ist die Zuständigkeit der Verwaltungsgerichte gegeben.

b) § 27b Abs. 2 PolG BW – neu -

Das in § 27b Abs. 2 PolG BW – neu - geregelte Kontaktverbot richtet wiederum an die vermeintlichen „Gefährder“ nach Abs. 1. Da solche Personen weder Verdächtige im Sinne der StPO noch Verursacher einer Gefahr (Störer) sind, ist der damit verbundene Grundrechtseingriff unverhältnismäßig.

Auch ein Kontaktverbot greift in Art. 2 GG ein.

Nicht hinreichend deutlich wird, was mit „bestimmten Personen oder Personen einer bestimmten Gruppe“ gemeint sein soll. Auch hier hat der Gesetzgeber die Aufgabe, die doch sehr unbestimmten Begriffe mit Inhalt auszufüllen.

c) § 27b Abs. 3 und 4 PolG BW – neu -

Die Ausgestaltung des Anordnungsverfahrens für die Aufenthaltsvorgabe und das Kontaktverbot zur Verhütung terroristischer Straftaten entsprechen den Grundsätzen, die vom Bundesverfassungsgericht entwickelt wurden.

Geboten erscheint aber angesichts der Eingriffstiefe der freiheitsbeschränkenden Maßnahmen, etwa in § 27b Abs. 5 PolG BW – neu - auch noch die Verpflichtung zu einer Rechtsbehelfsbelehrung (ähnlich wie in § 31 Abs. 5 Satz 3 PolG BW – Beschwerde) aufzunehmen. Gerade ein der deutschen Sprache nicht ausreichend mächtiger und mit dem hiesigen Rechtssystem wenig vertrauter ausländischer vermeintlicher „Gefährder“, dem z. B. der Besuch eines bestimmten Treffpunktes oder der Kontakt zu seinen Freunden untersagt wurde, muss sich aus Gründen effektiven Rechtsschutzes schnell orientieren können.

d) § 27b Abs. 5 und 6 PolG BW – neu -

Richtig erscheint – wenn man denn an den für bedenklich gehaltenen Regelungen zum Aufenthalt und Kontakt festhalten will – die Aufnahme einer strengen Verhältnismäßigkeitsregelung, wie hier mit „erforderlicher Umfang“ geschehen.

Die Aufnahme der Frist von „höchstens 3 Monaten“ kann nachvollzogen werden.

e) **§ 27c PolG BW – neu -**

§ 27c PolG BW-neu ermächtigt den Polizeivollzugsdienst, eine Person dazu zu verpflichten, eine „elektronische Fußfessel“ zur Überwachung des Aufenthaltsorts in betriebsbereitem Zustand am Körper bei sich zu führen und dessen Funktionsfähigkeit nicht zu beeinträchtigen. Tatbestandliche Voraussetzung dieser Verpflichtung ist es allein, dass diese Person als „Gefährder“ anzusehen ist.

Auch hier ist zu kritisieren, dass die Begriffe „bestimmte Tatsachen“, „übersehbarer Zeitraum“, „ihrer Art nach konkretisierte Weise“ und „individuelles Verhalten“ nicht bestimmt genug sind, um den verfassungsrechtlichen Vorgaben zu genügen. Der Gesetzgeber muss diese Begriffe mit Inhalt füllen.

Ebenso ist hier die Vorverlagerung von der bisherigen Gefahrenabwehr in den Verhütungsbereich zu kritisieren, da die Personen, an die hier gedacht wird, weder Verdächtige im Sinne der StPO noch Verursacher einer Gefahr (Störer) sind.

Es ist verfassungsrechtlich fraglich, ob Menschen, die noch keine Gewalttat begangen haben, auf diese Art und Weise überwacht werden dürfen. Die Fußfessel stellt als elektronische Aufenthaltsüberwachung einen schweren Eingriff in die Freiheitsrechte der Betroffenen dar. Dieser schwere Eingriff muss immer verhältnismäßig sein.

Aus guten Gründen kommt die Fußfessel bislang nur bei Verurteilungen wegen schwerer Verbrechen, wie etwa Mord oder Totschlag, in Betracht.

Schon bei der bisherigen Regelung zur Fußfessel für Straftäter durch Weisungen gemäß § 68b Abs. 1 Satz 1 Nr. 12 StGB muss das Gericht genau prüfen, worauf es die Gefahr weiterer Straftaten stützt. Dabei hat es zumindest ein rechtskräftiges Urteil gegen den Straftäter zur Hand, in dem das Geschehen bereits, soweit es geht, aufgeklärt wurde, und das allen Beteiligten bekannt ist.

Hinzu kommen in der Regel Erkenntnisse, wie sich der Straftäter während der langjährigen Haft verhalten hat, an deren Ende die Fußfessel gegebenenfalls als Maßnahme der Führungsaufsicht angeordnet wird.

Der Begründungsaufwand für Behörden, die bei Gericht eine Fußfessel für einen bisher in Freiheit lebenden Gefährder beantragen wollen, muss dagegen sehr viel höher sein. Die Behörden müssen offenlegen, warum jemand aus ihrer Sicht ein Gefährder ist, und zwar nicht nur gegenüber dem Gericht, sondern auch gegenüber dem Gefährder selbst, der sich in einem Rechtsstaat gegen die Anordnung einer Fußfessel wehren können muss.

Mit der elektronischen Aufenthaltsüberwachung (EAÜ) können in einem erheblichen Umfang Informationen über eine Person, ihre sozialen Kontakte und Beziehungen gewonnen werden. Darin liegt ein erheblicher Eingriff in das durch Art. 1, Art. 2 Abs. 1 GG geschützte Persönlichkeitsrecht.

Die elektronische Aufenthaltsüberwachung kann als Weisung im Rahmen der Führungsaufsicht auferlegt werden. Voraussetzung ist eine Verurteilung zu einer Freiheitsstrafe von mindestens drei Jahren. Sie ist also von deutlich strengeren Voraussetzungen abhängig, als nach § 27c PolG BW – neu -. In diesem Rahmen wurde die „elektronische Fußfessel“ 2015 durch Prof. Dr. Jörg Kinzig, Tübingen, evaluiert. Sie wird zurzeit bei 70 permanent überwachten ehemaligen Straftätern oder Maßregelinsassen eingesetzt, 45 dieser Fälle entfallen allein auf das Bundesland Bayern. Die Maßnahme ist für die Betroffenen mit einem erheblichen Aufwand verbunden, „da sie sich während des Ladevorgangs (mindestens zwei Stunden pro Tag, bei manchem Probanden zweimal täglich) nicht von der Steckdose entfernen können“. „Bewährungshelferinnen und Bewährungshelfer gaben zu bedenken, dass eine EAÜ die Betroffenen stigmatisiere“, etwa bei der Wohnungssuche oder bei einer Erwerbstätigkeit.

Im Hinblick auf die Eignung der elektronischen Fußfessel kommt die Studie in dem hier interessierenden Zusammenhang zu einem eindeutigen Ergebnis:

„Insgesamt sind sich alle Akteure einig, dass eine Aufenthaltsüberwachung die Begehung neuer Straftaten letztlich nicht verhindern kann“.

Bräuchle/Kinzig: Die elektronische Aufenthaltsüberwachung im Rahmen der Führungsaufsicht - Kurzbericht über die wesentlichen Befunde einer bundesweiten Studie mit rechtspolitischen Schlussfolgerungen, Tübingen 2015, S. 16.

Dies dürfte erst recht beim Einsatz gegen (vermeintliche) Straftäter aus dem Bereich des Terrorismus gelten. Die Maßnahme ist daher zwar einerseits mit erheblichen Eingriffen in das Persönlichkeitsrecht verbunden, erweist sich aber nach allen Erfahrungen als ungeeignet.

Damit wird das in der Regelung vorgesehene Tatbestandsmerkmal „um die Person ... von solchen Straftaten abzuhalten“ wohl nie erfüllt werden.

Der Anwaltsverband bezweifelt, dass die Anordnung des Tragens von elektronischen Fußfesseln einen wirksamen Schutz vor beabsichtigten Gewalttaten durch sog. „Gefährder“ darstellen würde. Eine Person, die dazu entschlossen ist, eine Gewalttat zu verüben, gegebenenfalls auch unter Inkaufnahme des eigenen Todes, wird sich durch eine solche Fußfessel oder gar die Strafbewehrung nicht davon abhalten lassen. So ist dies beispielsweise bei der Tötung des französischen 86-jährigen Priesters Jacques Hamel durch Adel Kermiche in der Kirche von Saint-Étienne-du-Rouvray im Juli 2016 geschehen. Auch aus dem oberpfälzischen Arnschwang wurde im Juni 2017 die Tötung eines 5-jährigen Kindes in einer Asylunterkunft durch einen strafrechtlich verurteilten Afghanen bekannt, der eine Fußfessel trug. Im Fall Amri hätte eine Fußfessel nur Auskunft darüber gegeben, dass er am Breitscheidplatz ist, die Tat wäre nicht verhindert worden.

Die elektronische Fußfessel hätte hier allenfalls den möglichen Vorteil, dass die Polizeibehörden früher erkennen könnten, wenn eine Person im Begriff ist, deren Wirkungsweise außer Kraft zu setzen oder den ihr zugewiesenen Aufenthaltsbereich zu verlassen. Ob die dann verbleibende Zeit zur Reaktion ausreicht, rechtzeitig am – zunächst ungewissen - Ort des Geschehens einzutreffen, ist fraglich.

Die geringe Erfolgsaussicht im Einzelfall dürfte einen so schwerwiegenden Grundrechtseingriff für eine Vielzahl von Personen kaum rechtfertigen.

f) Zu § 27c Abs. 2 PolG BW-neu –

Daten können auch innerhalb der Wohnung erhoben werden, eine Einschränkung der Datenerhebung ist (in § 27c Abs. 2 PolG BW – neu -) daran geknüpft, dass es „technisch möglich“ ist, allein den Aufenthalt der Person in der Wohnung zu registrieren.

Die Speicherung der Daten wird zwar nach § 27c PolG BW – neu - darauf begrenzt, dass sie „spätestens zwei Monate nach ihrer Erhebung zu löschen“ sind. Die Löschung der Daten steht jedoch unter dem Vorbehalt, dass sie nicht mehr für die Zwecke, zu denen sie erhoben wurden, verwendet werden. Angesichts der Weite der mit der „Verhütung von Straftaten“ bezeichnete denkbar unbestimmten Zwecke, dürfte diese Beschränkung, die nur Selbstverständliches zum Ausdruck bringt, kaum praktische Relevanz erhalten.

g) Zu § 27c Abs. 3 PolG BW - neu –

Die Vorschrift soll zu umfangreichen Datenübermittlungen zwischen Polizei- und Strafverfolgungsbehörden des Bundes und der Länder aber auch sonstigen öffentlichen Stellen ermächtigen. Da schon die Datenerhebung mittels der elektronischen Aufenthaltsüberwachung mit den in diesem Gesetzentwurf verfolgten Intentionen verfassungswidrig ist, gilt dies erst recht für die Weitergabe von auf diese Weise erhobenen Daten.

h) Zu § 27c Abs. 4 PolG BW - neu –

Wie bereits ausgeführt, hält der Anwaltsverband den Ausspruch von Bewegungs- und Kontaktverboten sowie das Anbringen eines Geräts zur elektronischen Aufenthaltsüberwachung (EAÜ) bei vermeintlichen „Gefährdern“, also Personen, die noch gar nicht verdächtig im Sinne von § 152 StPO oder wegen einer Straftat verurteilt sind, wegen der Unverhältnismäßigkeit des Eingriffs in ihre Freiheitsrechte für verfassungswidrig.

Demnach kann auch ein Verstoß gegen solche Auflagen nicht durch einen Straftatbestand kriminalisiert werden. Folgerichtig dürfte es aus rechtstaatlichen Gründen nicht zu einer entsprechenden gerichtlichen Anordnung zum Aufenthalts- oder Kontaktverbot sowie Tragen einer Fußfessel kommen. Aus diesen Gründen kann auch keine Verpflichtung von Polizeidienststellen bestehen, beispielsweise Daten des Aufenthaltsorts eines Betroffenen zum Zwecke der Strafverfolgung nach § 84b PolG BW - neu - (Verstoß gegen die Pflicht zum Fußfessel-Tragen) an Strafverfolgungsbehörden weiter zu geben

vgl. § 27c Abs. 4 Nr. 3 PolG BW – neu -.

Die Vorschrift läuft damit praktisch ins Leere, ebenso wie der eigens geschaffene Straftatbestand des § 84 b PolG BW – neu -.

i) § 27c Abs. 5, 6 und 7 PolG BW – neu –

Die elektronische Fußfessel ist nur auf Anordnung eines Gerichts zulässig. Da schon die Datenerhebung mittels der elektronischen Aufenthaltsüberwachung (EAÜ) mit den in diesem Gesetzentwurf verfolgten Intentionen verfassungswidrig ist, gilt dies erst recht für die Anordnung einer solchen Maßnahme.

Auf die Details eines möglichen Anordnungsverfahrens muss dann hier gar nicht weiter eingegangen werden. Es sollte noch einmal gesehen werden, dass elektronische Fußfesseln vielleicht bei hinreichend straffällig gewordenen Personen mit entsprechender Gefahrenprognose Sinn machen, um den Staat von einer ständigen Überwachung durch natürliche Personen zu entlasten, aber nicht bei Personen, die sich aktiv noch nicht ausreichend strafbar gemacht haben.

j) **§ 27c Abs. 8 PolG BW – neu –**

Da es nach dem Gesetzentwurf keine wirksamen Anordnungsvoraussetzungen für das Tragen einer elektronischen Fußfessel geben wird, ist auch ein Nachdenken über die Frage, wie lange so eine Anordnung höchstens sein darf bzw. unter welchen Voraussetzungen sie verlängert werden könnte, obsolet.

4. **§§ 54a , 84a, 84b und 85 PolG BW – neu -**

a) **§ 54a PolG BW – neu –**

Der Anwaltsverband versteht den Wunsch der Sicherheitsbehörden nach Waffengleichheit im wahrsten Sinne des Wortes mit Gewalttätern. Die Zulassung des Einsatzes von Explosivmitteln stellt dennoch eine gravierende Änderung des bisherigen Verständnisses des Polizeivollzugsdienstes dar, die schwerwiegenden Bedenken begegnet. Diese Ermächtigung verleiht dem Polizeizwang eine neue Qualität.

Nach § 50 Abs. 1 PolG BW ist unmittelbarer Zwang jede Einwirkung auf Personen oder Sachen durch einfache körperliche Gewalt, Hilfsmittel der körperlichen Gewalt oder Waffengebrauch. Das Innenministerium bestimmt, welche Hilfsmittel der körperlichen Gewalt und welche Waffen im Polizeidienst zu verwenden sind (§ 50 Abs. 2 PolG BW). Waffen in diesem Sinne sind: Hiebwaaffe, Reizstoffsprühgerät, Reizstoffgewehr, Mehrzweckpistole, Pistole, Revolver, Maschinenpistole und Gewehr (VwV PolG BW, Hinweis zu § 50 Abs. 2). Sprengmittel waren bislang als Hilfsmittel der körperlichen Gewalt eingestuft worden, was offensichtlich darauf zurückzuführen war, dass sie **nicht** für einen gezielten Einsatz gegen Menschen bestimmt sein sollten. Hierfür sprachen und sprechen Gründe der Verhältnismäßigkeit.

Neben die Sprengmittel als Hilfsmittel der körperlichen Gewalt stellt der Gesetzesentwurf nunmehr Explosivmittel als Waffen zum Einsatz gegen Personen. Beabsichtigt ist demnach nicht eine Einschränkung der bisherigen präventiv-polizeilichen Befugnisse im Sinne eine Konkretisierung des

Einsatzes von Sprengmitteln, sondern eine Erweiterung des verfügbaren Waffenkataloges und seiner Verwendungsmöglichkeiten.

Zweifel an der Neuregelung sind deshalb angebracht, weil damit der Rahmen herkömmlicher präventiv-polizeilicher Gefahrenabwehr verlassen wird. Explosivmittel können erfahrungsgemäß nicht mit einer solchen Präzision eingesetzt werden, dass andere Personen nicht, auch nicht mittelbar – etwa durch umherfliegende Splitter, Gebäudeteile u. Ä. – verletzt werden. Infolge des zutreffenden Verweises in § 54a Abs. 4 PolG BW – neu – auf § 53 Abs. 2 Satz 1 PolG BW erscheint bereits rechtlich der Anwendungsbereich der Neuregelung fraglich. In tatsächlicher Hinsicht fällt auf, dass die Gesetzesbegründung keinen Fall anzugeben vermag, in dem der Einsatz von Explosivmitteln zielführend gewesen wäre. Fallbeispiele hätten sich jedoch aller Voraussicht nach finden lassen, wenn berücksichtigt wird, dass der Einsatz von Explosivmitteln auf Bundesebene (§ 14 UZwG) sowie in Hessen (§ 55 HSOG) und Bayern (Art. 69 Abs. 1 BayPAG) zugelassen ist. Offenbar ist aber auch dort keine praktische Anwendung dokumentiert.

Während eine Konkretisierung des Einsatzes von Sprengmitteln gegenüber der bislang lediglich gebotenen Abwägung im Rahmen der Verhältnismäßigkeitsprüfung zu begrüßen gewesen wäre, ist der Anwaltsverband von der Notwendigkeit einer Ermächtigung zum Einsatz von Explosivmitteln gegen Personen nicht überzeugt. Die Gesetzesbegründung argumentiert mit allgemeinen Ausführungen, ohne konkret zu benennen, in welchen Situationen ein Einsatz von Explosivmitteln gegen Personen etwa im Rahmen von Antiterrorereinsätzen zielführend sein könnte, und anzugeben, wie die Verletzung Unbeteiligter zuverlässig vermieden werden kann.

b) § 84b PolG BW – neu –

Neben den oben schon mehrfach angesprochenen Bedenken gegen die Verfassungsmäßigkeit der Anordnungsmöglichkeit von Aufenthalts- und Kontaktverboten sowie einer elektronischen Aufenthaltsüberwachung gegenüber sog. Gefährdern ist auch die Sinnhaftigkeit der beabsichtigten Strafbewehrung in § 84b PolG BW - neu - zu bezweifeln. Wenn sich jemand nämlich bereits zu einer schweren Terrortat (Selbstmordanschlag oder Leben auf der ständigen Flucht vor den Strafverfolgungsbehörden) entschlossen hat, interessiert ihn eine nachgelagerte Bestrafung nicht mehr. Jedenfalls interessiert ihn die Bestrafung wegen genau der Verletzung der Aufenthaltsvorgaben oder Fußfessel-Auflagen wohl dann nicht mehr sonderlich, wenn er wegen anderer Delikte, wie Körperverletzung oder Schlimmeren angeklagt wird.

Geradezu grotesk erscheint das Ansinnen, jemandem eine zunächst offensichtlich verfassungswidrige Auflage zu machen und den Verstoß dagegen dann unter Strafe stellen zu wollen. Unter dem

Vorwand, die Person hätte sich durch den Verstoß gegen die (verfassungswidrigen) Auflagen nun strafbar gemacht, kann man eine Person kriminalisieren, indem sich nun die Indizien für einen vermeintlichen Gefährder zum Tatverdächtigen nach § 152 STPO verdichten und er nun tatsächlich in den möglichen Bereich der Polizeigesetze und Strafverfolgung gerät. Hier ist zu hoffen, dass diese Vorschriften gar nicht erst vom Landesgesetzgeber beschlossen werden, und falls doch, dass beispielsweise spätestens ein Strafrichter eine Vorlage an den Verfassungsgerichtshof oder das Bundesverfassungsgericht anstrengt.

c) **§ 85 PolG BW – neu –**

Weiter hat das Bundesverfassungsgericht in seiner Entscheidung

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

die Anforderungen an die Nutzung und Übermittlung der staatlich erhobenen Daten anhand der Grundsätze zur **Zweckbindung** und **Zweckänderung** definiert. Es hat zur Bekämpfung des internationalen Terrorismus eine Notwendigkeit anerkannt, erhobene Daten zwischen innerstaatlichen Stellen und den Sicherheitsbehörden anderer Staaten auszutauschen.

Auch die Übermittlung von Daten an öffentliche Stellen im Ausland unterliege diesen verfassungsrechtlichen Grundsätzen der Zweckänderung und Zweckbindung.

d) **Zu § 85 Abs. 3 PolG BW – neu -**

Das Bundesverfassungsgericht hat in seiner Entscheidung

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

darauf hingewiesen, dass aus dem Gesichtspunkt der **hypothetischen Datenneuerhebung** eine Zweckänderung dann zulässig sein soll, wenn „vergleichbar bedeutsame Rechtsgüter“ dies erforderten. Hinzukommen muss, dass eine Zweckänderung nur dann gerechtfertigt ist, wenn eine Neuerhebung auch mit „vergleichbar schwerwiegenden Mitteln“ zulässig wäre.

5. Art. 2 – Änderung des Gesetzes über die Ladenöffnung BW (LadÖG),

Richtig ist, das flächendeckende Alkoholverkaufsverbot aufzuheben, wenn nun als Mittel mit deutlich geringerer Eingriffsintensität in die Grundrechte der Bürgerinnen und Bürger (Art. 2 GG, Konsumenten) sowie Gewerbetreibenden (Art. 12 und 14 GG, Verkäufer) lokal begrenzte verhältnismäßige kommunale Verbote möglich sind.

Dennoch sollte dem Umstand, dass das zeitlich begrenzte flächendeckende Alkoholverkaufsverbot nach den Angaben der Evaluation tatsächlich einige positive Aspekte hinsichtlich der Straftatenbegehung gezeigt hat, mehr Beachtung geschenkt werden. So wie sich der Nichtraucherschutz in den letzten Jahren positiv entwickelt hat, z. B. mehr Schutz in Gaststätten, bei öffentlichen Verkehrsmitteln oder am Arbeitsplatz, sollte dies auch im Umgang mit Alkohol betrieben werden. Die Kosten, die für das Gemeinwesen durch Alkoholmissbrauch entstehen, sind leider nicht zu vernachlässigen.

Wir würden uns freuen, wenn unsere Hinweise und Vorschläge Berücksichtigung finden würden. 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