Frist zur Abgabe der Stellungnahme: 15.08.2008 Stand: 14.08.2008

Teil 2

Ausschussvorlage INA/17/3

eingegangene Stellungnahmen zu der

Anhörung des Innenausschusses

zu dem

Gesetzentwurf
der Fraktion der FDP für ein Zehntes Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG)
– Drucks. 17/133 –

Polizeipräsidium München
Prof. Dr. jur. Wilhelm Schmidbauer
Polizeipräsident

Ettstraße 2
80333 München

Vermittlung: (089) 29 10-0
Telefon: (089) 29 10-24 00
Fax: (089) 29 10-48 63

Hessischer Landtag
– Innenausschuss –
Schlossplatz 1-3

65022 Wiesbaden

München, den 11.08.2008

Schriftliche Anhörung zum Gesetzentwurf der Fraktion der FDP für ein Zehntes Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) – (Drucksache 17/133) –

Sehr geehrte Damen und Herren,

hiermit wird unter Bezugnahme auf Ihr Schreiben vom 12.06.2008 hinsichtlich des Gesetzentwurfes der Fraktion der FDP für ein Zehntes Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) – (Drucksache 17/133) schriftlich Stellung genommen. Soweit allerdings die Ausführungen vom 20.09.2004 zu den Gesetzentwürfen für ein Achtes Gesetz zur Änderung des Hessischen Gesetzes über die Öffentliche Sicherheit und Ordnung (Drucksache 16/731 bzw. 2352) durch die Änderungsvorschläge nicht tangiert werden, wird auf diese weiterverwiesen.

Allgemein kann konstatiert werden, dass die im Polizei- und Sicherheitsrecht zwischenzeitlich, insbesondere im Frühjahr dieses Jahres, ergangene Rspr. des BVerfG (Urteil vom 03.03.2004, Az.: 1 BvR 2378/98 bzw. 1 BvR 1084/9 – akustische

Wohnraumüberwachung; Urteil vom 27.07.2005; Az. 1 BvR 668/04 – präventive Telekommunikationsüberwachung; Beschluss vom 04.04.2006, Az. 1 BvR 518/02, – präventive polizeiliche Rasterfahndung; Urteil vom 27.02.2008, Az. 1 BvR 370/07 u. 1 BvR 595/07 – Online-Durchsuchung; Beschluss vom 11.03.2008, Az. 1 BvR 256/08 – Vorratsdatenspeicherung; Beschluss vom 11.03.2008, Az. 1 BvR 2074/05 u. 1 BvR 1254/07 – automatische Kfz-Kennzeichenerfassung) gesetzlich nachvollzogen werden sollte. Dies gilt insbesondere für die letztgenannte Entscheidung, mit der die hessische Regelung zur automatisierten Erfassung von Kfz-Kennzeichen in § 14 Abs. 5 HSOG für verfassungswidrig und damit nichtig erklärt wurde. Insgesamt gewährleistet eine solche Berücksichtigung der Rspr. die Rechtsbeständigkeit des Gesetzes und eine stärkere Rechtssicherheit für dessen Anwender. Allerdings sollten die gesetzlichen Möglichkeiten, die die Verfassungsrechtsprechung weiterhin offenhält, auch ausgenutzt werden. Dies ist notwendig, um den immer höheren Herausforderungen, welche die Erscheinungsformen der Kriminalität, namentlich des globalisierten Terrorismus und der organisierten Kriminalität, im Computer- und Kommunikationszeitalter an die Polizeibehörden stellen, wirksam begegnen zu können.

Zu den einzelnen vorgesehenen Änderungen wird insofern wie folgt Stellung genommen:

1. § 14 Abs. 5 HSOG (Automatisierte Erhebung von Kraftfahrzeugkennzeichen)

Im Freistaat Bayern wurden in den vergangenen Jahren sehr positive Erfahrungen mit der automatischen Kennzeichenlese- und -auswertetechnik gesammelt. Daher ist es natürlich zu begrüßen, dass das Mittel der automatisierten Kennzeichenerfassung „auch künftig den Polizeibehörden in Hessen zu Zwecken der Gefahrenabwehr zur Verfügung stehen soll“ (vgl. die Begründung des Gesetzentwurfes). Allerdings sollten die Anforderungen an den Einsatz dieses wichtigen polizeilichen Mittels der Gefahrenabwehr nicht so hoch angesetzt werden, dass eine zweckmäßige Anwendung de facto nicht mehr möglich ist. Insofern führt eine Orientierung an der aktuellen brandenburgischen Rechtslage zwar dazu, dass die Neuregelung in jedem

Falle verfassungskonform sein wird – dies wurde vom Bundesverfassungsgericht festgestellt (vgl. BVerfG, Beschluss vom 11.03.2008, Az. 1 BvR 2074/05 – automatische Kfz-Kennzeichenerfassung, Absatz-Nr. 183). Für eine effektive Gefahrenabwehr müssen aber auch hier – wie in der am 01.08.2008 in Kraft getretenen Neuregelung des BayPAG – die darüber hinaus noch belassenen verfassungsrechtlichen Spielräume ausgenutzt werden.

Das Bundesverfassungsgericht hat zunächst darauf hingewiesen, dass in einer dem Bestimmtheitsgebot genügenden Regelung ausdrücklich festgelegt werden muss, welche Daten erhoben werden dürfen (BVerfG, a. a. O., Absatz-Nr. 157 ff.). Insofern ist die Bezugnahme nur auf „Kennzeichen von Fahrzeugen“ in § 14 Abs. 5 S. 1 HSOG nicht nur aus polizeilicher Sicht ungenügend. Schließlich sollte die erhebbare Information auch Ort, Datum und Uhrzeit der Erfassung sowie Fahrtrichtung des Kraftfahrzeugs umfassen. Dies sollte auch normiert werden, da unter dem Begriff „Kennzeichen“ lediglich die Ziffern- und Zeichenfolge des Kennzeichens verstanden wird.

Auch muss eine Ermächtigung zur automatisierten Kennzeichenerkennung den rechtsstaatlichen Anforderungen der Bestimmtheit und Klarheit genügen. Insbesondere bedarf es einer hinreichenden bereichsspezifischen und normenklaren Bestimmung des Anlasses und des Verwendungszwecks der automatisierten Erhebung (BVerfG, a. a. O., Absatz-Nr. 98 f.). Ausreichender Erhebungsanlass für eine automatisierte Kennzeichenerkennung soll nach der Neuregelung in § 14 Abs. 5 S. 1 HSOG nur mehr in drei Fällen bestehen, nämlich wenn dies entweder zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person oder zur Abwehr einer gegenwärtigen Gefahr erforderlich ist und die Voraussetzungen für eine Identitätsfeststellung nach § 18 Abs. 2 Nr. 1, 3 oder 5 HSOG vorliegen oder eine Person oder ein Fahrzeug nach § 17 HSOG ausgeschrieben wurde und Tatsachen die Annahme rechtfertigen, dass die für die Ausschreibung relevante Begehung von Straftaten unmittelbar bevorsteht. Somit muss die Gefahr zum einen bereits „gegenwärtig“ und gegen bestimmte Schutzgüter gerichtet sein, vgl. § 14 Abs. 5 S. 1 Nr. 1 bzw. 2 HSOG. Demgegenüber genügt nach bayerischer Rechtslage (vgl. Art. 33 Abs. 2 Satz 2 i. V. m. Art. 13 Abs. 1 Nr. 1 BayPAG) richtigerweise die Abwehr einer (konkreten) Gefahr. Zum anderen ist größtes Manko aber das Fehlen einer

Erhebungsbefugnis im Hinblick auf die sog. Schleierfahndung, § 18 Abs. 2 Nr. 6 HSOG. In diesem Bereich ist demgegenüber bei Lageerkenntnissen zur grenzüberschreitenden Kriminalität gem. Art. 33 Abs. 2 Satz 2 i. V. m. Art. 13 Abs. 1 Nr. 5 BayPAG eine Datenerhebung möglich.

Weiterhin ist etwas verwunderlich, dass Erhebungsdaten nur mit den aus diesen Anlässen gespeicherten Daten abgeglichen werden dürfen, vgl. § 14 Abs. 5 S. 2 HSOG. Dies ist weder erforderlich noch zielführend. Vielmehr wird für den abzugleichenden polizeilichen Datenbestand nur vorausgesetzt, dass deren Umfang sich nicht laufend oder in unvorhersehbarer Weise verändern darf (vgl. Urteil vom 11.03.2008, Az. 1 BvR 2074/05 u. 1 BvR 1254/07, Abs.-Nr. 131). Auch aus polizeifachlicher Sicht wäre es zweckmäßig, einen über § 14 Abs. 5 S. 2 HSOG hinausgehenden Abgleich mit anderen polizeilichen Dateien zuzulassen. Dementsprechend sieht die Neuregelung in Art. 33 Abs. 2 Satz 3 und 4 BayPAG auch mehrere polizeiliche Fahndungsbestände vor, mit denen ein Abgleich der erfassten Kennzeichen erfolgen darf. Ein auch für Hessen interessanter Anwendungsfall wäre z. B. der Abgleich mit polizeilichen Dateien über bekannte Störer (etwa der Datei „Gewalttäter Sport“) bei Vorfeldkontrollen zu Großveranstaltungen (z. B. Fußballspielen). Denn ein Abgleich sollte auch mit polizeilichen Dateien erfolgen können, die zur Abwehr von Gefahren im Einzelfall oder im Hinblick auf bestimmte Ereignisse allgemein bestehender Gefahren errichtet wurden. Der Abgleich ist in diesem Fall daran gebunden, dass dies zur Abwehr einer solchen Gefahr erforderlich ist. Schließlich muss diese Gefahr Anlass für den Einsatz des automatisierten Kennzeichenerkennungssystems sein (vgl. BVerfG, a. a. O., Absatz-Nr. 175).

Die geringe Intensität des vorgesehenen Eingriffs ergibt sich daraus, dass die Regelung grundsätzlich vorsieht, dass von Autofahrern gerade keine „Bewegungsprofile“ erstellt werden, vgl. § 14 Abs. 5 S. 4 HSOG. Das Bundesverfassungsgericht hat zudem festgestellt, dass die automatisierte Kennzeichenerkennung in das Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG dann nicht eingreift, wenn das Kennzeichen nach dem Abgleich und ohne weitere Auswertung sofort wieder gelöscht wird (BVerfG, a. a. O., Absatz-Nr. 68 f.). Diesem Erfordernis wird durch § 14

Abs. 5 S. 7 HSOG Rechnung getragen. Um den Umfang der Kennzeichenerfassung einzugrenzen (vgl. BVerfG, a. a. O., Absatz-Nr. 171 f.) musste richtigerweise auch mit § 14 Abs. 5 S. 7 HSOG das Verbot der flächendeckenden automatisierten Kraftfahrzeugkennzeichenerkennung eingefügt werden.

2. § 15 Abs. 4 HSOG (akustische Wohnraumüberwachung)

Entgegen der in der Gesetzesbegründung dargelegten Auffassung ist es nach polizeilicher Sicht nicht zu begrüßen, dass über die Rspr. des Bundesverfassungsgerichts (Urteil vom 27.02.2008, Az. 1 BvR 370/07 u. 1 BvR 595/07 – Online-Durchsuchung) hinaus, die den Kernbereichsschutz von der Erhebungs- in die Auswertungsphase verlagert hat, in § 15 Abs. 4 S. 2 und 3 HSOG vorgesehen wird, dass Daten mit Kernbereichsbezug unverzüglich gelöscht und ihre Auswertung ausgeschlossen wird. Auch das Bundesverfassungsgericht stellt in obiger Entscheidung fest, dass es bei einem heimlichen Zugriff auf ein informationstechnisches System praktisch unvermeidbar sei, Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann (BVerfG, a. a. O., Absatz-Nr. 277). Hier sollte die Abwehr hochwertiger Gefahren Vorrang vor der Gewährleistung eines überhöhten Schutzniveaus haben, derzufolge im Falle einer erkennbaren Kernbereichsberührung ein sofortiger Abbruch der Überwachungsmaßnahme vorzunehmen ist. Insbesondere unterschlägt die Neuregelung, dass das Bundesverfassungsgericht anerkannt hat, dass von dem grundsätzlichen Erhebungsverbot kernbereichsrelevanter Daten eine Ausnahme zu machen ist, wenn konkrete Anhaltspunkte dafür bestehen, dass kernbereichsbezogene Kommunikationsinhalte mit Inhalten verknüpft werden, die dem Ermittlungsziel unterfallen, um eine Überwachung zu verhindern (BVerfG, a. a. O., Absatz-Nr. 281).

3. § 15a Abs. 4 HSOG (Telekommunikationsüberwachung)

Da § 15a Abs. 4 HSOG inhaltlich den Schutzvorkehrungen zur Wohnraumüberwachung entspricht, wird insoweit auf die Ausführungen zu **2.** verwiesen.

4. § 26 Abs. 1 Satz 1 HSOG (Rasterfahndung)

Zunächst ist festzuhalten, dass das Bundesverfassungsgericht in seinem Beschluss zur präventiven Rasterfahndung nach dem Polizeigesetz des Landes Nordrhein-Westfalen (Beschluss vom 04.04.2006, Az. 1 BvR 518/02) anerkannt hat, dass die präventive Rasterfahndung mit dem Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG vereinbar ist. Es hat allerdings bestimmte Anforderungen an die Voraussetzungen und die Durchführung der Maßnahme gestellt. Insoweit ist eine Klarstellung, dass eine Rasterfahndung nur bei Vorliegen einer konkreten Gefahr für hochrangige Rechtsgüter zulässig ist, notwendig.

Die in § 26 Abs. 1 Satz 1 HSOG aufgezählten Rechtsgüter sind aber diesbezüglich nicht ausreichend. Insbesondere fehlt der Schutz von Sachen, für die eine gemeine Gefahr besteht, d. h. eine Gefahr, die im Einzelfall einer unbestimmten Vielzahl von Sachen, die einen erheblichen Wert haben, droht, vgl. z. B. Art. 44 Abs. 1 Satz 1 Nr. 1 a. E. BayPAG. Insofern ist anzumerken, dass sich das Bundesverfassungsgericht in der Entscheidung vom 04.04.2006 ausdrücklich nur mit der Zulässigkeit der Rasterfahndung zum Zweck der Abwehr von Gefahren für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person befasst hat, da das Polizeigesetz des Landes Nordrhein-Westfalen die Rasterfahndung nur zu diesem Zweck vorsieht. Aus den Ausführungen des Gerichts ergibt sich aber nicht, dass die genannten Rechtsgüter, zu deren Schutz eine Rasterfahndung zulässig sein kann, abschließend aufgezählt wurden. So können

ausreichend gewichtige Sachgefahren selbst erhebliche Grundrechtseingriffe rechtfertigen (vgl. BVerfG, Urteil vom 03.03.2004, Az.: 1 BvR 2378/98 bzw. 1 BvR 1084/9 – akustische Wohnraumüberwachung, Rn. 345).

Darüber hinaus ist zur Verhinderung von Schutzlücken eine Rasterfahndung zuzulassen, wenn konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass eine schwerwiegende Straftat begangen werden wird. Insbesondere dann, wenn, wie im Waffen- oder im Betäubungsmittelrecht, die geschützten Güter nicht ohne Weiteres benannt werden können, muss der Gesetzgeber zum Zweck des präventiven Rechtsgüterschutzes auf die Verhinderung von Straftaten abstellen. Um dem Grundsatz der Verhältnismäßigkeit zu genügen, ist insoweit allerdings erforderlich, dass die geschützten Rechtsgüter ein ausreichendes Gewicht aufweisen, vgl. insoweit Art. 44 Abs. 1 Satz 1 Nr. 2. E. BayPAG. Konkret kann es sich dabei um Straftaten wie die Verbreitung von Kinderpornographie, die Vorbereitung eines Explosionsverbrechens, ferner um Straftaten, die im Zusammenhang mit den Erscheinungsformen des internationalen Terrorismus und der Organisierten Kriminalität stehen, so z. B. bei der Bildung krimineller Vereinigungen und dem Menschenhandel, handeln.

5.

Abschließend sei noch darauf hingewiesen, dass der Entwurf leider – anders als die Gesetzeslage des Freistaats Bayern – keine Einführung der Online-Durchsuchung vorsieht und eine solche anscheinend auch zukünftig nicht gewollt ist (vgl. MMR aktuell, XXVI/2008).

Mit freundlichen Grüßen

Prof. Dr. Schmidbauer

DVD Deutsche Vereinigung für Datenschutz e. V.

Deutsche Vereinigung für Datenschutz e.V., Bonner Talweg 33–35, 53113 Bonn

Hessischer Landtag
– Innenausschuss –
Postfach 32 40
65022 Wiesbaden

Bonner Talweg 33–35
53113 Bonn

Telefon: 0228 222498
Telefax: 0228 2438470

dvd@datenschutzverein.de
www.datenschutzverein.de

Stellungnahme zum Entwurf eines Zehnten Gesetzes zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG), Drucksache 17/133

A. Grundsätzliches

Der Gesetzentwurf befasst sich mit der näheren Ausgestaltung der automatisierten Kfz-Kennzeichenerfassung, der Datenerhebung in Wohnungen (Wohnraumüberwachung) und der Rasterfahndung. Die Deutsche Vereinigung für Datenschutz lehnt diese Überwachungsmaßnahmen grundsätzlich ab. Kennzeichenerfassung und Rasterfahndung richten sich nicht nur gegen Personen, von denen Gefahren ausgehen, sondern überwiegend gegen völlig Unbeteiligte. Derartige breit gefächerte Grundrechtseingriffe sollten in einem Rechtsstaat keine polizeilichen Standardmaßnahmen sein. Die akustische und visuelle Wohnraumüberwachung gehört zu den Maßnahmen, die tief in die Sozial- und Privatsphäre der Zielperson und ggf. unbeteiligter Dritter eindringt. Verletzungen des Kernbereichs privater Lebensgestaltung sind in der Praxis kaum zu vermeiden.

Die Deutsche Vereinigung für Datenschutz fordert den Hessischen Landtag und den Innenausschuss deshalb auf, diese Maßnahmen nicht (erneut) gesetzlich zu legitimieren, sondern aus dem HSOG zu streichen.

B. Zu den einzelnen Regelungen des Gesetzentwurfs

1. Zu Ziffer 1: Neufassung des § 14 Abs. 5 HSOG (Kfz-Kennzeichenerfassung)

Die ursprüngliche Vorschrift ist durch das Bundesverfassungsgericht am 11.03.2008 für mit dem Grundgesetz unvereinbar und nichtig erklärt worden. Damit ist allen entsprechenden Maßnahmen die rechtliche Grundlage entzogen worden: Eine Kfz-Kennzeichenerfassung durch die hessische Polizei ist derzeit mangels Rechtsgrundlage nicht zulässig.

Mit dem Gesetzentwurf soll die Kennzeichenerfassung wieder eingeführt werden. Vorbild der Regelung ist § 36a des Brandenburgischen Polizeigesetzes (BbgPolG). Ob das Land Hessen mit der Übernahme dieser Vorschrift verfassungsrechtlich auf der sicheren Seite steht, ist fraglich. § 36a BbgPolG ist nämlich nicht – wie in der Gesetzesbegründung behauptet – vom Bundesverfassungsgericht als verfassungskonform bewertet worden. Das Verfassungsgericht hat festgestellt, dass ein weit gefasster Verwendungszweck nur dann verfassungsrechtlich unbedenklich ist, wenn er mit engen Eingriffsvoraussetzungen verbunden ist, wie es die derzeitige Brandenburgische Regelung vorsieht. Es hat § 36a BbgPolG jedoch keine „Karlsruher Unbedenklichkeitsbescheinigung“ ausgestellt.

§ 14 Abs. 5 S. 7 HSOG-E schließt den flächendeckenden stationären Einsatz von Kennzeichen-Erfassungsgeräten aus. Eine flächendeckende Überwachung mit mobilen Geräten wäre demnach erlaubt. Hier stellt sich die Frage, wie der stationäre vom nicht-stationären Einsatz abzugrenzen ist. Ein Kennzeichenscanner in einem Polizeiwagen wird grundsätzlich mobil eingesetzt, jedoch ist es vorstellbar, dass Polizei-Kfz und Erfassungsgerät längere Zeit an einem Ort verbleiben, beispielsweise auf dem Standstreifen einer Autobahn. Nach einem gewissen Zeitablauf könnte müsste man wohl von einem stationären Einsatz ausgehen.

Nicht definiert ist zudem, wann ein Einsatz „flächendeckend“ und damit unzulässig gemäß § 14 Abs. 5 S. 7 HSOG-E wäre. Eine automatische Beobachtung des gesamten hessischen Verkehrsraums kann nicht gemeint sein, da eine solche Maßnahme weder technisch noch personell auch nur ansatzweise umzusetzen ist. Der Begriff müsste also genauer definiert werden. Sinnvoll und praktikabel wäre es, die Zahl der maximal zur gleichen Zeit einzusetzenden Erfassungsgeräte im Gesetz festzuschreiben.

§ 14 Abs. 5 S. 7 HSOG-E unterscheidet nicht zwischen dem öffentlichen Verkehrsraum und privaten Grundstücken. Demzufolge wäre eine Kfz-Kennzeichenscanning auch auf Privatgrundstücken, z. B. Supermarktparkplätzen, zulässig. Wenn dies so gemeint und gewollt ist, sollte es im Gesetzestext klar formuliert werden. Andernfalls müsste § 14 Abs. 5 S. 7 HSOG-E durch den Einschub *„auf öffentlichen Straßen und Plätzen“* präzisiert werden.

Der neuen Eingriffsnorm zum Kfz-Kennzeichenscanning fehlt darüber hinaus die notwendige Zweckbindungsklausel. Sie erlaubt bei Datenübereinstimmung eine polizeiliche Verarbeitung der Daten ohne zugleich festzuschreiben, dass die Verarbeitung nur zu dem Zweck erfolgen darf, zu dem die Daten erhoben wurden (siehe § 14 Abs. 5 HSOG-E). Der Verzicht auf eine Zweckbindung dürfte verfassungswidrig sein.

Ungeachtet dieser rechtlichen Bedenken sollte das Land Hessen angesichts des geringen Nutzens der automatischen Kfz-Kennzeichenerfassung grundsätzlich auf dieses Instrument verzichten. Schleswig-Holstein und Bremen sind diesbezüglich mit gutem Beispiel voran gegangen. Hessen sollte folgen.

2. Zu Ziffer 2: Neufassung des § 15 Abs. 4 HSOG (Datenerhebung in Wohnungen)

Die Vorschrift erlaubt in ihrer jetzigen Fassung die akustische und visuelle Überwachung von Wohnungen, umgangssprachlich als „großer Lausch- und Spähangriff“ bekannt. Eingriffe in den Kernbereich privater Lebensgestaltung sind durch diese Art der Datenerhebung vorgezeichnet. Deshalb soll § 15 Abs. 4 HSOG-E zusätzlich zum bereits bestehenden Verwertungsverbot die Polizeibehörden verpflichten, die Maßnahme abzubrechen, wenn der Kernbereich erkennbar berührt wird. Diese Regelung dürfte in der Praxis schwierig umzusetzen sein. Es wird – das kann prognostiziert werden – zwangsläufig zu Kernbereichsverletzungen kommen. Deshalb lehnt die Deutsche Vereinigung für Datenschutz diese Regelung im HSOG ab.

Eine grundrechtsschonende Wohnraumüberwachung müsste sich an den entsprechenden Regelungen in der Strafprozessordnung (StPO) orientieren. Das bedeutet:

- Die Maßnahme darf nur durchgeführt werden, wenn auf Grund tatsächlicher Anhaltspunkte, insbesondere zu der Art der zu überwachenden Räumlichkeiten und dem Verhältnis der zu überwachenden Personen zueinander, anzunehmen ist, dass durch die Überwachung keine Daten erhoben werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind (vgl. § 100c Abs. 4 S. 1 StPO).

- Eventuelle Kernbereichsverletzungen sind zu dokumentieren.

- Informationen, die durch Kernbereichsverletzungen gewonnen wurden, sind zu löschen.

- Die Löschung ist zu dokumentieren.

Die Ergänzung des § 15 Abs. 4 HSOG ist damit zwar ein Schritt in die richtige Richtung. Er genügt jedoch nicht, um Kernbereichsverletzungen auszuschließen.

Will man § 15 HSOG „verfassungsfest“ ausgestalten, müsste darüber hinaus auch der„Einsatz technischer Mittel“ (§ 15 Abs. 1 Nr. 2 HSOG) neu definiert werden. Die derzeitige Definition ist derart weit gefasst, dass § 15 HSOG sogar als (verfassungswidrige) Rechtsgrundlage für Online-Durchsuchungen greifen würde.

3. Zu Ziffer 3: Ergänzung des § 15a HSOG (Einschränkung der Datenerhebung durch Telekommunikationsüberwachung)

Die vorgesehene Ergänzung des § 15a HSOG wird begrüßt. Hinsichtlich des Kernbereichschutzes wird auf die obigen Ausführungen zu Ziffer 2 verwiesen.

4. Zu Ziffer 4: Änderung des § 26 Abs. 1 S. 1 HSOG (Rasterfahndung)

Die Deutsche Vereinigung für Datenschutz lehnt die Rasterfahndung grundsätzlich ab. Die vorgesehene Neufassung des § 26 Abs. 1 S. 1 HSOG ist nicht geeignet, die mit jeder Rasterfahndung einhergehenden Nachteile für unbeteiligte Menschen auf ein akzeptables Maß zu reduzieren.

Das Bundesverfassungsgericht hat in seinem Beschluss vom 04.04.2006 (1 BvR 518/02) dargelegt, dass von Maßnahmen wie der Rasterfahndung Einschüchterungseffekte ausgehen könnten, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen. Dies müsse nicht nur zum Schutze der subjektiven Rechte der betroffenen Einzelnen vermieden werden, sondern auch zum Schutz des Gemeinwohls. Dieses werde ebenfalls beeinträchtigt, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens sei. Es gefährde die Unbefangenheit des Verhaltens, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass ein Gefühl des Überwachtwerdens entsteht.

Mögliche Einschüchterungseffekte oder das Gefühl des Überwachtwerdens können durch die vorgeschlagene Änderung des § 26 Abs. 1 S. 1 HSOG nicht vermieden werden. Die Deutsche Vereinigung für Datenschutz hält daher die Streichung des gesamten § 26 HSOG für erforderlich.

Sollten Innenausschuss und Landtag an der Rasterfahndung festhalten, so sollte zumindest die Einführung eines Richtervorbehalts erwogen werden. Die Deutsche Vereinigung für Datenschutz schlägt für diesen Fall vor, § 26 Abs. 4 HSOG wie folgt neu zu fassen:

> *„Die Maßnahme nach Abs. 1 darf nur auf schriftlichen Antrag der Behördenleitung durch den Richter angeordnet werden. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Von der Maßnahme ist die oder der Hessische Datenschutzbeauftragte durch die Polizeibehörde unverzüglich zu unterrichten.“*

Dieser Regelungsvorschlag lehnt sich an § 31 Abs. 4 des Polizeigesetzes des Landes Nordrhein-Westfalen an.

Dr. ROLF GÖSSNER

RECHTSANWALT / PUBLIZIST
VIZEPRÄSIDENT DER >INTERNATIONALEN LIGA FÜR MENSCHENRECHTE< (Berlin)

Rechtsanwalt Dr. Rolf Gössner [redacted] Bremen

Hessischer Landtag
Vorsitzender des Innenausschusses,
Herrn Horst Klee, MdL
Postfach 3240

65022 Wiesbaden

Bremen, den 14. August 2008

Schriftliche Anhörung des Innenausschusses im Hessischen Landtag

Betr.: Gesetzentwurf der Fraktion der FDP für eine Zehntes Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG)
– LT-Drs. 17/133 –

Rechtspolitische Stellungnahme

Vorbemerkung

Das Hessische Gesetz über die öffentliche Sicherheit und Ordnung (HSOG), zuletzt geändert 2005, dürfte mit einigen seiner Regelungen gegen das Grundgesetz verstoßen. Spätestens die Grundsatzentscheidungen des Bundesverfassungsgerichts (BVerfG) der vergangenen Jahre zu diversen polizeilichen und geheimdienstlichen Befugnissen auf Bundes- und Länderebene legen diese Vermutung nahe. Ob zwischenzeitliche Novellierungen im HSOG ausreichend konsequent waren und damit diesen höchstrichterlichen Vorgaben genügen, ist zweifelhaft und soll im Folgenden ebenfalls untersucht werden.

Die FDP-Fraktion im Hessischen Landtag geht offenbar ebenfalls von einem solchen Befund aus und unternimmt mit dem vorliegenden Gesetzentwurf, der hier zur Begutachtung ansteht, den Versuch, das HSOG entsprechend der neueren Rechtsprechung des Bundesverfassungsgerichts in Sachen Sicherheitsgesetzen zu novellieren und in diesem Zusammenhang die einschlägigen Befugnisse im HSOG zu konkretisieren und einzuschränken.

Dabei wird Bezug genommen auf die BVerfG-Urteile zur

- akustischen Wohnraumüberwachung (Gr. Lauschangriff), BVerfGE v. 3.03.2004, Az. 1 BvR 2378/98 und 1 BvR 1084/99)
- präventiven Telefonüberwachung (BVerfGE v. 27.07.2005, Az. BvR 668/04; BVerfGE vom 3.03.2004, Az. 1 BvR 3/92)

- präventiven Rasterfahndung (BVerfGE v. 4.04.2006, AZ. 1 BvR 518/02),
- Online-Durchsuchung von Computern (BVerfGE v. 27.02.2008, Az. BvR 370/07 und 1 BvR 595/07) und
- automatischen Erfassung von Kfz-Kennzeichen (BVerfGE v. 11.03.2008, Az. 1 BvR 2074/05; 1 BvR 1254/07).

Von dem Gesetzentwurf der FDP-Fraktion sind folgende Regelungsmaterien des HSOG betroffen:

1. Automatische Kfz-Kennzeichen-Erkennung/–Abgleich zur Gefahrenabwehr (§ 14)
2. Elektronische Wohnraumüberwachung zur Gefahrenabwehr (§ 15)
3. Präventive Telekommunikationsüberwachung (§ 15a)
4. Präventive Rasterfahndung (§ 26)

Ziel des Gesetzentwurfs ist es, aus den genannten BVerfG-Entscheidungen die notwendigen gesetzgeberischen Konsequenzen zu ziehen.[1] Dieses Vorhaben ist überfällig, nachdem die zugrundeliegenden Gerichtsentscheidungen bereits aus den Jahren 2004, 2005, 2006 und zwei der Urteile aus Februar und März 2008 stammen.

I. AUTOMATISCHES KENNZEICHEN-SCREENING
Automatische Kfz-Kennzeichen-Erkennung und –Abgleich zur Gefahrenabwehr
(§ 14 Abs. 5 HSOG)

Die automatisierte Kennzeichenerkennung ist ein technisches Mittel zur massenhaften Kontrolle des öffentlichen Verkehrsraums. *„Durch die Möglichkeit, sowohl die Kennzeichenerfassung als auch den Abgleich automatisiert vorzunehmen, wird eine systematische, räumlich weitreichende Sammlung von Informationen über das Bewegungsverhalten von Fahrzeugen und damit auch von Personen technisch und mit relativ geringem Aufwand möglich"*, so das Bundesverfassungsgericht in seiner Entscheidung vom 11.03.2008.[2] Die Automatische Kfz-Kennzeichen-Erkennung dürfte am ehesten mit einer Kombination aus Rasterfahndung, Schleierfahndung und Videoüberwachung zu vergleichen sein. Ebenso wie bei diesen Maßnahmen ist daher prinzipiell von einer hohen Eingriffsintensität auszugehen.[3] Insofern handelt es sich keinesfalls um einen „Grundrechtseingriff an der Bagatellgrenze", wie Hessens Innenminister vor dem Urteil des Bundesverfassungsgerichts noch behauptet hatte.[4]

Regelung in HSOG: verfassungswidrig und nichtig

Die gesetzliche Ermächtigung zur automatisierten, heimlichen und verdachtslosen Kfz-Kennzeichenerkennung im öffentlichen Verkehrsraum und zum Abgleich mit polizeilichen Fahndungsdateien gemäß § 14 Abs. 5 HSOG ist vom Bundesverfassungsgericht am 11.

---

[1] Nach § 31 Abs. 1 BVerfGG sind die Entscheidungen des BVerfG auch und gerade für den Gesetzgeber verbindlich.
[2] BVerfGE vom 11. März 2008, AZ: 1 BvR 2074/05 und 1 BvR 1254/07, Rndr. 142 f.
[3] So auch der baden-württembergische Datenschutzbeauftragte, Peter Zimmermann, in einem Gutachten vom 18.04.2008, dokumentiert in: Polizei in guter Verfassung? Dokumentation der Anhörung der Grünen im Landtag (9. Mai 2008), hrg. v. Bündnis 90/Die Grünen im baden-württembergischen Landtag, S. 34 ff.
[4] SZ 21.11.07; taz 30.01.08, S. 6.

März 2008 für verfassungswidrig und damit nichtig erklärt worden.[5] Begründung: Diese Polizeibefugnis verletze das allgemeine Persönlichkeitsrecht in seiner Ausprägung als „Grundrecht auf informationelle Selbstbestimmung" (Art. 2 Abs. 1 in Verbindung mit Art. 1 GG), das auch im öffentlichen Raum zu schützen ist. Dieses Grundrecht umfasst auch öffentlich zugängliche Daten wie etwa Nummernschilder. Der Schutzbereich dieses Grundrechts ist jedenfalls dann tangiert bzw. verletzt, wenn der Datenabgleich nicht unverzüglich erfolgt und das Kennzeichen nicht ohne weitere Auswertung sofort und spurenlos gelöscht wird.

Die massenhafte, heimliche automatische Erfassung der Kfz-Daten, ihre Speicherung und Verwertung, so wie sie im HSOG geregelt waren, sind nicht verfassungskonform. Nach dem BVerfG-Urteil ist es unzulässig, ohne konkreten Verdacht oder Anlass private Kfz-Kennzeichnen einzuscannen und mit nicht eingrenzbaren polizeilichen Dateien des Fahndungsbestands abzugleichen – nicht zuletzt auch deswegen, weil es das Verhalten der Menschen beeinflussen kann, die sich solchen Überwachungsmaßnahmen ausgesetzt sehen, zumal, wenn sie den Eindruck ständiger Kontrolle gewinnen. Das Bundesverfassungsgericht dazu wörtlich:

„Das sich einstellende Gefühl des Überwachtwerdens kann (...) zu Einschüchterungseffekten und in der Folge zu Beeinträchtigungen bei der Ausübung von Grundrechten führen. Hierdurch sind nicht nur die individuellen Entfaltungschancen des Einzelnen betroffen, sondern auch das Gemeinwohl, weil die Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlich demokratischen Gemeinwesens ist."

Die im HSOG als Standardmaßnahme ausgestaltete Polizeibefugnis zum Massenabgleich genügte nicht dem Gebot der Normenbestimmtheit und Normenklarheit, da Anlass, Eingriffsschwellen sowie Ermittlungs- und Verwendungszweck nicht benannt und nicht eindeutig definiert wurden. Der massenhafte Abgleich von Nummernschildern darf nicht ohne besonderen Anlass – also ohne konkrete Gefährdungslage oder gesteigertes Risiko - routinemäßig und flächendeckend durchgeführt werden. Oder anders ausgedrückt: Die systematische Massenkontrolle des mobilen Verhaltens aller motorisierten Bürger ohne konkreten Anlass ist verfassungswidrig. Mit der unbestimmten Weite dieser Norm, so das Gericht, werde zudem gegen das verfassungsrechtliche Gebot der Verhältnismäßigkeit verstoßen.

Gesetzgeberische Konsequenzen

Es gibt für den Gesetzgeber zwei Möglichkeiten, Konsequenzen aus dieser Entscheidung zu ziehen:

- Die für nichtig erklärte Regelung des § 14 Abs. 5 HSOG wird verfassungskonform ausgestaltet.
- Oder die Regelung wird aus dem Gesetz ersatzlos gestrichen.

1. Verfassungskonforme Ausgestaltung

Die FDP-Fraktion versucht mit ihrem Gesetzentwurf, die automatisierte Kfz-Kennzeichenerkennung und –erfassung verfassungskonform auszugestalten. Damit soll diese Präventionsmaßnahme den Polizeibehörden in Hessen auch künftig zur Verfügung stehen. Dabei orientieren sich die Urheber des Gesetzentwurfs an der aktuellen brandenburgischen Rege-

[5] BVerfG, 1 BvR 2074/05; 1 BvR 1254/07.

lung, die das Bundesverfassungsgericht als verfassungskonform bewertet hat.[6] Mit der vorgeschlagenen Regelung und ihren relativ eng begrenzten Eingriffsvoraussetzungen soll die heimliche Erstellung von Bewegungsprofilen von Autos und Personen weitgehend ausgeschlossen und die Einrichtung von Dauer-Kontrollstellen untersagt werden.[7]

Die Regelung der FDP-Fraktion im ihrem Gesetzentwurf sieht in einem neuen § 14 Abs. 5 folgendes vor:

1.1 Grundsatz der automatischen Kfz-Kennzeichen-Erfassung (Satz 1):

„Die Polizeibehörden können die Kennzeichen von Fahrzeugen ohne Wissen der Person durch den offenen Einsatz technischer Mittel automatisiert erheben..."

Wichtig sind hier zwei Bedingungen:

- *„ohne Wissen der Person"* – es ist davon auszugehen, dass damit der/die Kfz-Führer/in gemeint ist, der/die von dem gesamten Vorgang nichts mitbekommt;
- *„durch den offenen Einsatz technischer Mittel"* – also nicht durch heimlichen bzw. verdeckten Einsatz, so dass die potentiellen „Opfer" ihre Erfassung bemerken können.

Wenn der Einsatz nur offen zulässig sein soll, dann müssten die Erfassungsgeräte zumindest für aufmerksame und informierte Kfz-Fahrer erkennbar sein; die Geräte dürften also nicht etwa in Mautbrücken oder sonst versteckt zur Anwendung kommen.

1.2 Eingeschränkte Daten-Erfassungszwecke

„... wenn

1. *dies zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person erforderlich ist,*
2. *dies zur Abwehr einer gegenwärtigen Gefahr erforderlich ist und die Voraussetzungen für eine Identitätsfeststellung .... vorliegen oder*
3. *eine Person oder ein Fahrzeug ... ausgeschrieben wurde und Tatsachen die Annahme rechtfertigen, dass die für die Ausschreibung relevante Begehung von Straftaten unmittelbar bevorsteht."*

Voraussetzung nach Nr. 1 soll also sein, dass eine „gegenwärtige Gefahr für Leib oder Leben einer Person" besteht/bevorsteht oder – gemäß Nr. 3 - die für eine Personen-/Kfz-Ausschreibung relevante Begehung von Straftaten unmittelbar bevorsteht. Damit sollen anlasslose „Fahndungen ins Blaue hinein" ausgeschlossen werden.

Eine *gegenwärtige Gefahr* ist gegeben, wenn das schädigende Ereignis bereits begonnen hat oder sein Eintritt mit an Sicherheit grenzender Wahrscheinlichkeit umgehend bzw. unmittelbar bevorsteht. Die Gefahr kann sich also jederzeit verwirklichen und der drohende Schaden kann jederzeit eintreten.[8] Bei einer Gefahr für Leib und Leben drohen schwerste Gesundheitsgefahren, bei denen ein tödlicher Ausgang möglich ist.

Ungenau bzw. zu weit ist aber die Nr. 2 formuliert: Hier dient die Maßnahme *zur Abwehr einer gegenwärtigen Gefahr,* wobei nicht gesagt wird, für welche Rechtsgüter diese Gefahr

---

[6] BvR 2074/05, Nr. 181 ff, 183. Auch das einschlägige Gutachten von Alexander Roßnagel kommt zu diesem Ergebnis: Roßnagel, Kennzeichenscanning – verfassungsrechtliche Bewertung. Eine Studie im Auftrag des ADAC zur Mobilität (Januar 2008).

[7] Vgl. S. 4 zu Art. 1, Nr. 1 des vorliegenden Gesetzentwurfs.

[8] Aus einer konkreten Gefahr wird eine gegenwärtige Gefahr, wenn eine Sachlage entsteht, bei der die Einwirkung des schädigenden Ereignisses bereits begonnen hat oder bei der diese Einwirkung unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorsteht (vgl. die Legaldefinitionen in § 2 BremPolG und § 2 Nds. Nieders.SOG).

drohen muss. Jedenfalls geht es hier nicht nur um eine *gegenwärtige Gefahr für Leib oder Leben einer Person,* sondern um jede gegenwärtige Gefahr – eingeschränkt lediglich dadurch, dass zusätzlich *die Voraussetzungen für eine Identitätsfeststellung nach § 18 Abs. 2 Nr. 1, 3 oder 5 HSOG vorliegen* müssen:

> ***§ 18 Abs. 2 Nr. 1, 3 oder 5 HSOG***
>
> *(2) Die Polizeibehörden können die Identität einer Person feststellen, wenn*
>
> *1. die Person sich an einem Ort aufhält,*
>
> *a) von dem aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass dort*
>
> *aa) Personen Straftaten verabreden, vorbereiten oder verüben,*
>
> *bb) sich Personen ohne erforderlichen Aufenthaltstitel treffen oder*
>
> *cc) sich Straftäterinnen oder Straftäter verbergen, oder*
>
> *b) an dem Personen der Prostitution nachgehen...*
>
> *3. die Person sich in einer Verkehrs- oder Versorgungsanlage oder -einrichtung, einem öffentlichen Verkehrsmittel, Amtsgebäude oder einem anderen besonders gefährdeten Objekt oder in dessen unmittelbarer Nähe aufhält und tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass in oder an diesen Objekten Straftaten begangen werden sollen, durch die in oder an diesen Objekten befindliche Personen oder diese Objekte selbst unmittelbar gefährdet sind, und dies aufgrund der Gefährdungslage oder auf die Person bezogener Anhaltspunkte erforderlich ist,...*
>
> *5. die Person an einer Kontrollstelle angetroffen wird, die von der Polizeibehörde auf öffentlichen Straßen oder Plätzen oder an anderen öffentlich zugänglichen Orten eingerichtet worden ist, um eine der in § 100a der Strafprozessordnung bezeichneten Straftaten oder eine Straftat nach § 27 des Versammlungsgesetzes zu verhüten. Die Einrichtung von Kontrollstellen ist nur mit Zustimmung des für die Polizei zuständigen Ministeriums oder von ihm benannter Stellen zulässig, es sei denn, dass Gefahr im Verzug vorliegt,...*

Zwischenergebnis: Mit der § 14 Abs. 5 Nr. 2 des Gesetzentwurfs würde der Anwendungsbereich für Kfz-Kennzeichen-Scannings angesichts dieser Voraussetzungen für eine Identitätsfeststellung möglicherweise wieder unverhältnismäßig ausgedehnt – etwa auf die Suche nach Straftätern oder nach Menschen ohne Aufenthaltstitel (Fahndungstatbestände mit bundesrechtlicher Regelungskompetenz). Mit den in Nr. 1 und 3 verankerten Voraussetzungen dürfte der Kfz-Kennzeichenerhebung dagegen wirkungsvoll begrenzt werden.

1.3 Der automatische Abgleich der erhobenen Daten mit polizeilichen Gefahrenabwehr-Daten wird mit § 14 Abs. 5 Satz 2 des Gesetzentwurfs für zulässig erklärt, d.h. der Abgleich mit Fahndungsdateien nach Straftätern ist danach mangels Regelungskompetenz des Landes zurecht unzulässig. Im Fall einer Datenübereinstimmung sieht der Gesetzentwurf folgende Schritte vor:

- es sind *„unverzüglich Maßnahmen zur Klärung des Sachverhalts zu ergreifen"*;
- die übereinstimmenden Daten können *„polizeilich verarbeitet"* werden;
- die Daten sind „andernfalls" nach dem Abgleich *„unverzüglich zu löschen"*

Ausnahmen im Falle von Polizeilichen Ausschreibungen:

- Die Daten dürfen zusammen mit den gewonnenen Erkenntnissen (also weitergehenden Informationen) an die ausschreibende Stelle übermittelt werden, wenn *„eine Person oder ein Fahrzeug ... ausgeschrieben wurde und Tatsachen die Annahme rechtfertigen, dass die für die Ausschreibung relevante Begehung von Straftaten unmittelbar bevorsteht" (Abs. 5, S. 1 Nr. 3).* Nur in diesem Fall dürfen also außer dem Kennzeichen, Zeit und Ort auch noch weitere Informationen erfasst und übermittelt werden, wie etwa über etwaige Begleitpersonen, das Kfz und die Kfz-Führerin oder den -Führer sowie über mitgeführte Sachen, Verhalten, Vorhaben

und sonstige Umstände des Antreffens. Der Eingriff erhält in diesem Fall also eine veränderte Qualität mit gesteigerter Intensität.

- Unter denselben Voraussetzungen dürfen auch *Bewegungsprofile* erstellt werden, aber nur im Fall einer Ausschreibung zur polizeilichen Beobachtung nach § 17 HSOG.

„Der flächendeckende stationäre Einsatz der technischen Mittel ist unzulässig"; damit soll die Einrichtung von Dauer-Kontrollstellen untersagt werden.

Fazit und weitergehende Anforderungen/Vorschläge

Mit diesen gesetzlichen Voraussetzungen ist das Instrument des Kfz-Kennzeichen-Scannings gegenüber der für nichtig erklärten Fassung erheblich eingeschränkt worden – mit einer Ausnahme in § 14 Abs. 5 S. 1 Nr. 2. Sowohl die Datenerhebung als auch die Datenverarbeitung sollen ausschließlich Zwecke der Gefahrenabwehr und der Straftatenverhütung verfolgen.

Sinnvoll wäre es, auch noch den Absatz (3) des § 36a Brandenburgisches Polizeigesetz, das der FDP-Fraktion als Vorbild dient, einzufügen: *„Das für Inneres zuständige Mitglied der Landesregierung erstattet dem Ausschuss für Inneres des Landtages jährlich einen Bericht über jede Maßnahme, der Angaben enthält über deren Anlass, Ort und Dauer."*

Die Bürgerrechtsvereinigung *Humanistische Union* (HU) weist zusammen mit dem *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung* (FifF) darauf hin, dass bei der Umsetzung der verfassungsgerichtlichen Vorgaben in der Praxis ein *„alternatives Verfahren bei der rechtlichen und technischen Gestaltung dieser Polizeibefugnis"* Anwendung finden müsste, um die Gefahr polizeilicher Bewegungsprofile *„zumindest für die übergroße Zahl der nicht gespeicherten, in jeder Hinsicht unverdächtigen VerkehrsteilnehmerInnen (das sind 99,7 %) technisch weitgehend auszuschließen"* und datenschutzrechtliche Mindestanforderungen zu gewährleisten. Dazu gehört etwa die sofortige automatische Löschung im Nicht-Trefferfall. Dieses Verfahren wird in der HU-Pressemitteilung vom 6.05.2008 näher beschrieben.[9] Dort heißt es:

> „Wenn kein Treffer erzielt wird, dann wird sowohl das Videobild als auch das erkannte alphanumerische Kennzeichen durch das nächste erfasste Bild bzw. Kennzeichen im Arbeitsspeicher oder falls es dort auch hingelangt ist, auf der Festplatte, überschrieben. Alle Nicht-Treffer werden somit unmittelbar nach erfolgtem Abgleich im lokalen Gerät sicher gelöscht und unbrauchbar gemacht. Eine Übertragung auf andere Medien, andere Geräte oder Systeme wird verlässlich unterbunden."

Um personelle Verantwortlichkeiten festzulegen und um Transparenz und Kontrolle der Maßnahmen zu verbessern, sollten zusätzliche – über den Gesetzentwurf hinausgehende – Anforderungen gesetzlich normiert werden:

- Schriftliche Anordnung der automatisierten Kennzeichenüberwachung nur durch den Behördenleiter; darin müssen der Anlass, die jeweiligen Orte, die Zeitdauer der Maßnahme und der Grund für die Maßnahme genau bezeichnet werden.
- Qualifizierte Dokumentation der Anzahl der kontrollierten Fahrzeuge und der Zahl der Treffer sowie der getroffenen polizeilichen Maßnahmen und deren Erfolg.
- Bericht der Polizei an den Landtag über den Einsatz der Maßnahme und deren Erfolg, mit allen notwendigen Angaben, die für eine parlamentarische Überprüfung/Kontrolle/Evaluation benötigt werden. Der Bericht ist öffentlich zugänglich zu machen.

---

[9] Presseerklärung der Humanistischen Union, Landesverband Baden-Württemberg, vom 06.05.2008: Vorschlag zu einer datenschutzrechtlichen Eindämmung der Befugnis der automatischen Kennzeichenerfassung".

- Befristung der gesetzlichen Regelung (zwei Jahre) mit der Möglichkeit einer Verlängerung durch Parlamentsbeschluss nach vorheriger unabhängiger wissenschaftlicher Evaluation hinsichtlich Verhältnismäßigkeit, Bürgerrechtsverträglichkeit (Auswirkungen auf effektiven Grundrechtsschutz) und Effizienz.

2. Ersatzlose Streichung des Kfz-Kennzeichenscannings

Angesichts der zahlreichen Freiheitsbeschränkungen der letzten Jahre, die im Namen der Sicherheit und Terrorabwehr in Bund und Ländern gesetzlich verankert wurden und die sich zu einem erschreckend hohen Anteil als ganz oder teilweise verfassungswidrig herausgestellt haben, wäre zur Wiederherstellung und Stärkung der Freiheitsrechte der Bürger und Bürgerinnen daran zu denken, diesen *„weiteren Mosaikstein in einer Überwachungsinfrastruktur, die alle möglichen Lebensbereiche betrifft"* (so der Bundesdatenschutzbeauftragte Peter Schaar) zu entfernen und das Kfz-Kennzeichenscanning nicht zu legalisieren – auch nicht in eingeschränkter Form. Damit könnte Hessen etwa dem Weg der Bremer Bürgerschaft folgen, die ihre – ebenfalls grundrechtswidrige – Regelung in § 29 Abs. 6 Bremisches Polizeigesetz ersatzlos gestrichen hat. Begründung im Gesetzentwurf der Regierungsfraktionen SPD und Bündnisgrüne: Es gebe keinen Bedarf an einer Ermächtigung zur automatisierten Kennzeichenerkennung zu Zwecken der Gefahrenabwehr, weshalb eine Nachbesserung der Voraussetzungen verzichtbar und eine Aufhebung der Regelung geboten sei.[10]

Diese einfachere und klarere Lösung ist einer komplizierten und möglicherweise unpraktikablen Regelung vorzuziehen, auch wenn letztere den verfassungsgerichtlichen Vorgaben entsprechen sollte – zumal nicht alles, was verfassungsrechtlich noch zulässig ist, in der Rechtspraxis auch umgesetzt werden muss bzw. sollte. Im Übrigen ist dieses Instrument recht fehleranfällig, wodurch Menschen in falschen Verdacht geraten können – mit zum Teil gravierenden Folgen. Mit einem Verzicht könnte dem Trend eines immer umfangreicheren vorsorglichen maschinellen Abgleichs der Bevölkerung mit polizeilichen Datenbanken entgegengewirkt werden.

Der Einwand, damit sei ein gravierender Sicherheitsverlust verbunden, ist nicht nachvollziehbar, zumal die bisherigen „Erfolge" nicht gerade überzeugend sind. Die Erfahrungen – etwa aus Bayern oder Hessen, wo dieses Instrument ziemlich exzessiv angewandt worden ist –[11] zeigen: Dem Grundrechtseingriff steht mit einer Trefferquote von nur 0,3 Promille ein verschwindend geringer Erfolg gegenüber, wobei es zumeist um fehlende Haftpflichtversicherung oder zu spät entrichtete Versicherungsbeiträge geht und keineswegs etwa um schwerwiegende Gefahren oder Straftaten aus den Bereichen der Organisierten Kriminalität oder des Terrorismus, die es abzuwehren gilt.[12] Nicht zuletzt dieses eklatante Missverhältnis zwischen Aufwand und Ertrag macht die umstrittene Kfz-Überwachung zu einem überflüssigen und damit unverhältnismäßigen Eingriff.

---

[10] Vgl. Bremische Bürgerschaft, Drs. 17/358 v. 17.04.08 – Antrag der Regierungsfraktionen SPD und Bündnis 90/Die Grünen.

[11] Allein in Hessen wurden 2007 über eine Million Kfz-Kennzeichen automatisch gescannt und mit Fahndungsdateien abgeglichen. In Bayern sollen es sogar über 5 Millionen pro Monat gewesen sein. Die „Ausbeute" (Trefferquote") in Hessen lag bei nur 0,3 Promille. Ins Netz gingen der Polizei meist Autobesitzer, die ihre Versicherungsbeiträge nicht oder nicht rechtzeitig bezahlt hatten oder wegen anderer „Bagatellen" (heise-online v. 11.03.2008; Der Spiegel 47/2007, S. 55). In Schleswig-Holstein sind seit August 2007 über 130.000 Autos durch die Überwachung gerollt, 26 Wagen wurden ohne korrekte Versicherung erwischt (taz nord v. 12.3.2008).

[12] So auch die Fraktion Bündnis 90/Die Grünen im Bayerischen Landtag: Gesetzentwurf zur Streichung des Kfz-Kennzeichen-Scannings, LT-Drs. 15/10477; vgl. auch die Tageszeitung v. 12.3.08, S. 2.

II. ELEKTRONISCHE WOHNRAUMÜBERWACHUNG zur Gefahrenabwehr (§ 15 HSOG)

Großer Lausch- und Spähangriff in und aus Wohnungen

Bei der Elektronischen Wohnraumüberwachung – umgangssprachlich: Großer Lauschangriff, evtl. kombiniert mit Großem Spähangriff - handelt es sich um die heimliche elektronisch-akustisch (-visuelle) Ausforschung des nicht öffentlich gesprochenen Wortes und von intimen Lebensvorgängen und –äußerungen aller Art in oder aus einer Wohnung, einem Büro oder Hotelzimmer zum Zwecke der Aufklärung von schwerwiegenden Straftaten (strafprozessual) oder zum Zwecke der Gefahrenabwehr (polizeirechtlich). Damit wird das Recht auf Unverletzlichkeit der Wohnung nach Art. 13 Abs. 1 GG in erheblichem Maße eingeschränkt, wenn nicht gar zeitweise suspendiert.

Die elektronische Wohnraumüberwachung *„schränkt die für die Verwirklichung des Persönlichkeitsrechts und eines menschenwürdigen Lebens unverzichtbare Möglichkeit ein, sich in eine Wohnung zurückzuziehen, sich darin frei zu entfalten und von jedermann unbeobachtet zu kommunizieren. Anders als beim staatlichen Zugriff auf die Telekommunikation, auf den Briefverkehr oder auf Gespräche, die in der Kneipe oder auf der Straße geführt werden, gibt es vor der Überwachung von Gesprächen in Wohnungen schlechterdings keine weitere Rückzugsmöglichkeit für den Betroffenen".*[13]

In jedem Fall handelt es sich um ein offensives Eindringen staatlicher Sicherheitsorgane mit technischen Mitteln – größtenteils verbunden mit einem körperlichen Eindringen oder heimlichen Einbrechen – in die Privat- und Intimsphäre der Bewohner einer betroffenen Wohnung, in der sich mutmaßlich Verdächtige und deren Kontaktpersonen, also auch Unbeteiligte und Unverdächtige aufhalten (könnten).

Art. 10 Abs. 4 Grundgesetz (GG) ermächtigt die Bundes- und Landesgesetzgeber zur Regelung des Großen Lausch- und Spähangriffs in und aus Wohnungen zur Gefahrenabwehr:

„Zur Abwehr dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, dürfen technische Mittel zur Überwachung von Wohnungen nur auf Grund richterlicher Anordnung eingesetzt werden..."

Danach ist der Einsatz also nur zur Abwehr dringender Gefahren, insbesondere einer gemeinen Gefahr oder Lebensgefahr zulässig. Nach der Begründung des Bundestags soll damit, wie auch durch die ausdrücklich genannten Beispiele der Lebensgefahr und der Gemeinen Gefahr unterstrichen wird, zum Ausdruck gebracht werden, dass die präventive Wohnraumüberwachung nur zum Schutz hochrangiger Rechtsgüter eingesetzt werden darf.[14]

Soweit § 15 Abs. 4 HSOG eine Wohnraumüberwachung zur Abwehr einer *gegenwärtigen* Gefahr von Leib, Leben oder Freiheit einer Person zulässt, wird diese Anforderung erfüllt.[15]

Die Ausforschung der Wohnung zur Abwehr solcher dringender oder gegenwärtiger Gefahren kann – so der GG-Wortlaut *„technische Mittel zur Überwachung von Wohnungen"* – prinzi-

---

[13] Stellungnahme aus 2004 des Berliner Beauftragten für Datenschutz und Informationsfreiheit, des Landesbeauftragten für den Datenschutz Bremen, des Hamburgischen Datenschutzbeauftragten, des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern, des Landesbeauftragten für den Datenschutz Niedersachsen, der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen sowie des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein.

[14] So BVerfGE 17, 232, 251; BVerwGE 47, 31

[15] BVerfG, NJW 2004, 999, 1019.

piell akustisch oder/und optisch erfolgen; diese Entscheidung haben die jeweiligen Gesetzgeber in Bund und Ländern zu treffen.[16]

§ 15 Abs. 4 HSOG ermöglicht bislang – so der Wortlaut *„in oder aus Wohnungen ... ohne Kenntnis der betroffenen Person Daten ... erheben"* – sowohl den Großen Lauschangriff mittels elektronischen Wanzen oder Richtmikrophonen als auch den Spähangriff mittels Infrarotkameras oder Mini-Videokameras. Zumeist wird diese Ermächtigung jedoch, entgegen ihres Wortlauts, lediglich als akustische Wohnraumüberwachung interpretiert.

Die Vorschrift enthält in Satz 2 den Zusatz, dass *„Erkenntnisse aus dem Kernbereich privater Lebensgestaltung ... einem Verwertungsverbot"* unterliegen.

Der „unantastbare Kernbereich privater Lebensgestaltung"...

Mit seinem Urteil vom 3. März 2004 hat das Bundesverfassungsgericht die bundesrechtliche Lausch-Regelung zum Zwecke der Strafverfolgung zwar nicht komplett, aber doch in wesentlichen Teilen für verfassungswidrig erklärt.[17] Dabei erinnern die Richter Gesetzgeber und Regierung eindringlich an tragende Säulen der Verfassung, die in diesem Zusammenhang sträflich vernachlässigt worden sind. Die Richter bestätigen, dass es – trotz aller Sicherheitsbedenken – einen *„unantastbaren Kernbereich privater Lebensgestaltung"* gibt, den der Staat zu achten hat und der auch nicht mit Verweis auf eine effektive Strafverfolgung relativiert werden darf. Das Gericht erinnert an die Grundwerte der Menschenwürde und des Persönlichkeitsrechts, wobei es die Privatwohnung zum *„letzten Refugium"* der Wahrung der Menschenwürde erklärt. Dies verlange einen absoluten Schutz des Verhaltens in diesen Räumen, soweit es sich als individuelle Entfaltung im Kernbereich privater Lebensgestaltung darstelle. Das Gericht erinnert an den Schutz der Privat- und Intimsphäre sowie an den Grundsatz der Verhältnismäßigkeit.

L e i t s ä t z e zum Bundesverfassungsgerichtsurteil des Ersten Senats vom 3. März 2004

- 1 BvR 2378/98 – und – 1 BvR 1084/99 (Auszüge)

- Zur Unantastbarkeit der Menschenwürde gemäß Art. 1 Abs. 1 GG gehört die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung. In diesen Bereich darf die akustische Überwachung von Wohnraum zu Zwecken der Strafverfolgung (Art. 13 Abs. 3 GG) nicht eingreifen. Eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes zwischen der Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und dem Strafverfolgungsinteresse findet insoweit nicht statt.
- Die auf die Überwachung von Wohnraum gerichtete gesetzliche Ermächtigung muss Sicherungen der Unantastbarkeit der Menschenwürde enthalten sowie den tatbestandlichen Anforderungen des Art. 13 Abs. 3 GG und den übrigen Vorgaben der Verfassung entsprechen.
- Führt die auf eine solche Ermächtigung gestützte akustische Wohnraumüberwachung gleichwohl zur Erhebung von Informationen aus dem absolut geschützten Kernbereich privater Lebensgestaltung, muss sie abgebrochen werden und Aufzeichnungen müssen gelöscht werden; jede Verwertung solcher Informationen ist ausgeschlossen.

[16] Anders als bei der elektronischen Wohnraumüberwachung zur Strafverfolgung gemäß Art. 13 Abs. 3 GG: Hier ist bislang nur die akustische Überwachung (Gr. Lauschangriff) zulässig.

[17] BVerfG, Urteil vom 3.03.2004 – 1 BvR 2378/98 und BvR 1084/99; vgl. Sonnen, in: Neue Kriminalpolitik 2/2004, S. 76 f.

All diese gerichtlich aufgestellten Hürden dürften die ohnehin schon aufwändigen und kostenträchtigen Lauschangriffe in und aus Wohnungen noch aufwändiger und teurer machen,[18] denn jedes Mal, wenn der besagte Kernbereich bei privat-vertraulichen Gesprächen betroffen ist, müssen die Geräte sofort abgeschaltet und, falls bereits aufgezeichnet wurde, die Aufzeichnungen unverzüglich gelöscht werden. Mit diesen Restriktionen besteht die Chance, dass dieser Grundrechtseingriff von höchster Intensität zu einer wirklichen „Ultima-ratio"-Maßnahme wird, die elektronische Wanze zum wirklich allerletzten Mittel der Strafverfolgung.

In diesem Zusammenhang ist die Feststellung des Bundesverfassungsgerichts von Belang, dass der mit einer Wohnraumüberwachung verbundene Eingriff in die Grundrechte der Betroffenen tiefer geht als bei den sonstigen polizeilichen Ermittlungsmaßnahmen und eine größere Nähe zum Kernbereich privater Lebensgestaltung aufweist.[19]

... gilt auch im Gefahrenabwehrbereich

Der mit den gefahrenabwehrrechtlichen Regelungen verfolgte gesetzgeberische Zweck ist grundsätzlich ein anderer als der der strafprozessualen Vorschriften, deren Verfassungsmäßigkeit vom Bundesverfassungsgericht mit o.g. Urteil geprüft worden ist. Bei der Gefahrenabwehr geht es nicht um die staatliche Sanktionierung einer bereits erfolgten, aber nicht mehr zu verhindernden Rechtsgutsverletzung, sondern darum, das bedrohte hochrangige Rechtsgut vor einer drohenden Verletzung zu schützen.[20] Trotz dieser unterschiedlichen Zwecke sind bestimmte Verfassungsgrundsätze in beiden Bereichen gültig und zu beachten.

1. Absoluter Schutz des Kernbereichs privater Lebensgestaltung

1.1 Nach Auffassung des Bundesverfassungsgerichts folgt aus Artikel 13 Abs. 1 i.V.m. Artikel 1 Abs. 1 und Artikel 2 Abs. 1 GG ein **absoluter Schutz** des Kernbereichs privater Lebensgestaltung; dieser darf nicht durch Verhältnismäßigkeitserwägungen relativiert werden, so dass in diesen Kernbereich selbst zur Aufklärung besonders gravierender Formen von Kriminalität nicht eingegriffen werden darf.[21] Zur Umsetzung dieses Schutzes müssen die gesetzlichen Regelungen, die die Wohnraumüberwachung ermöglichen,

"*unter Beachtung des Grundsatzes der Normenklarheit sicherstellen, dass die Art und Weise der akustischen Wohnraumüberwachung nicht zu einer Verletzung der Menschenwürde führt. Die Überwachung muss in Situationen von vornherein unterbleiben, in denen Anhaltspunkte bestehen, dass die Menschenwürde durch die Maßnahme verletzt wird. Führt die akustische Wohnraumüberwachung im Übrigen unerwartet zur Erhebung von absolut geschützten Informationen, muss sie abgebrochen werden, und die Aufzeichnungen müssen gelöscht werden; jede Verwendung solcher im Rahmen der Strafverfolgung erhobener absolut geschützter Daten ist ausgeschlossen.*"[22]

1.2 Wenn der Schutz des Kernbereichs privater Lebensgestaltung aber nach Auffassung des Bundesverfassungsgerichts *absolut und daher in keiner Weise relativierbar* ist, dann sind staatliche bzw. polizeiliche Eingriffe in diesen Schutzbereich auch aus anderen als Strafverfolgungszwecken unzulässig. Das bedeutet, dass die vom Bundesverfassungsgericht formu-

[18] Allein 2005 beliefen sich die Kosten für große Lauchangriffe auf etwa 70.000 Euro (bei nur 7 Maßnahmen).
[19] BVerfG, NJW 2004, 999, 1010.
[20] Vgl. BVerfGE 100, 313, 394.
[21] BVerfG, NJW 2004, 999, 1002.
[22] Ebda., S. 1003.

lierten Anforderungen konsequenterweise auch für gesetzliche Regelungen gelten müssen, die die Wohnraumüberwachung zu Zwecken der Gefahrenabwehr zulassen.

2. Erhebungsverbot und Verwertungsverbot

2.1 Um den Kernbereich privater Lebensgestaltung zu schützen, müssen die gesetzlichen Regelungen

"*das Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes in Wohnungen untersagen, wenn Anhaltspunkte dafür bestehen, dass absolut geschützte Gespräche erfasst werden.*"[23]

Diese Anhaltspunkte sind

"*typischerweise beim Abhören von Gesprächen mit engsten Familienangehörigen, sonstigen engsten Vertrauten und einzelnen Berufsgeheimnisträgern gegeben. Bei diesem Personenkreis dürfen Überwachungsmaßnahmen nur ergriffen werden, wenn konkrete Anhaltspunkte dafür bestehen, dass die Gesprächsinhalte zwischen dem Beschuldigten und diesen Personen keinen absoluten Schutz erfordern, insbesondere bei einer Tatbeteiligung der das Gespräch führenden Personen. Ein konkreter Verdacht auf solche Gesprächsinhalte muss schon zum Zeitpunkt der Anordnung bestehen. Er kann nicht erst durch eine akustische Wohnraumüberwachung begründet werden.*"[24]

Daraus folgt, dass eine zeitliche und räumliche Rundumüberwachung grundsätzlich unzulässig ist – sowohl im Strafverfolgungs- als auch im Gefahrenabwehrbereich.[25] Der Gesetzgeber hat diesen Grenzen der Datenerhebung aus Wohnräumen durch ein gesetzlich ausdrücklich konkretisiertes Verbot der Ausforschung/Aufzeichnung von Gesprächen und Lebensumständen, die aus besonderen Vertrauensverhältnissen stammen, klar und deutlich Rechung zu tragen. Die gesetzliche Regelung hat sicherzustellen, so das Gericht,

"*dass eine Überwachung jedenfalls dann ausgeschlossen bleibt, wenn sich der Beschuldigte allein mit seinen engsten Familienangehörigen oder anderen engsten Vertrauten in der Wohnung aufhält und keine Anhaltspunkte für deren Tatbeteiligung bestehen.*"[26]

Darüber hinaus ist auch die Überwachung von Gesprächen mit Berufsgeheimnisträgern unzulässig – und zwar soweit dies zum Schutz der Menschenwürde erforderlich ist, wie etwa bei Gesprächen mit Geistlichen, Strafverteidigern oder Ärzten.[27]

Die gesetzliche Regelung hat hinreichende Vorkehrungen dafür zu treffen, dass die Überwachung unverzüglich abgebrochen wird, wenn unerwartet eine Situation eintritt, die dem unantastbaren Kernbereich privater Lebensgestaltung zuzurechnen ist. In solchen Fällen ist die Fortsetzung der Überwachung rechtswidrig.[28]

2.2 § 15 Abs. 4 HSOG spricht bislang für aufgezeichnete Erkenntnisse aus dem Bereich privater Lebensgestaltung lediglich ein Verwertungsverbot aus, aber kein Überwachungsverbot. Es fehlt bislang die gesetzliche Verpflichtung, eine Überwachungsmaßnahme unverzüglich abzubrechen, wenn sich die Situation entgegen der Prognose so verändert, das der Kernbereich privater Lebensgestaltung betroffen ist – es sich etwa um Gespräche mit engsten Famili-

---

[23] Ebda., S. 1006.
[24] BVerfG, NJW 2004, 999, 1006.
[25] Ebda., S.1004.
[26] Ebda., S. 1006.
[27] Ebda., S. 1004.
[28] Ebda., S. 1004, 1006.

enangehörigen und sonstigen engen Vertrauten handelt. Insoweit entspricht die Regelung im HSOG nicht den verfassungsrechtlichen Anforderungen.

Auch der Schutz von Kontakten und Gesprächen mit Berufsgeheimnisträgern ist bislang noch nicht bereichsspezifisch geregelt.

2.3 Das Bundesverfassungsgericht hat ein ausdrückliches gesetzliches Verwertungsverbot für jene Erkenntnisse gefordert, die unter Verletzung des Kernbereichs privater Lebensgestaltung erlangt worden sind. Dieses Verwertungsverbot ist einfachgesetzlich zu konkretisieren und bedarf einer gesetzlich verankerten verfahrensrechtlichen Sicherung.[29]

Das Verwertungsverbot muss zum einen jene Fälle erfassen, in denen ein von Anfang an bestehendes Erhebungsverbot von der Polizei rechtswidrig missachtet wurde. Zum anderen dürfen jene Gespräche dann nicht verwertet werden, wenn sich erst im Nachhinein ergeben sollte, dass das abgehörte Gespräch höchstpersönlichen Inhalt hatte.[30]

2.4 Das HSOG enthält bislang keine verfahrensrechtlich abgesicherten Verwertungsverbote für die unter Verletzung des Kernbereichs gewonnenen Erkenntnisse. Insoweit genügen die gefahrenabwehrrechtlichen Vorschriften den vom Bundesverfassungsgericht erhobenen verfassungsrechtlichen Anforderungen nicht.

3. Befristung

3.1 Nach § 100d Abs. 4 Satz 1 StPO ist die Anordnung zur akustischen Wohnraumüberwachung (zum Zwecke der Strafverfolgung) *auf höchstens vier Wochen zu befristen.* Diese Frist gewährleistet nach Auffassung des Bundesverfassungsgerichts

> *"eine der Tiefe des Grundrechtseingriffs angemessene regelmäßige gerichtliche Überprüfung der Überwachung".*[31]

Die Effektivität der richterlichen Anordnungs- und Prüfungsbefugnisse erfordere im Hinblick auf den einschneidenden Eingriff der akustischen Wohnraumüberwachung eine vorausschauende Beurteilung, die *verantwortungsvoll nur für einen überschaubaren Zeitraum* wahrgenommen werden könne.[32] Diese Anforderung muss in gleicher Weise auch für die präventive Wohnraumüberwachung gelten.[33]

4.2 Nach § 15 Abs. 5 ist jedoch eine wesentlich längere Frist zulässig: Danach ist die Anordnung auf höchstens drei Monate zu befristen; außerdem ist eine dreimalige Verlängerung um jeweils höchstens drei weitere Monate zulässig, soweit die Voraussetzungen fortbestehen. Dies dürfte jedoch den vom Bundesverfassungsgericht geforderten *"überschaubaren Zeitraum"* deutlich überschreiten.[34] Dabei ist zu beachten, dass mit der elektronischen Wohnraumüberwachung ein wesentlich tieferer Grundrechtseingriff verbunden ist als mit der Telekommunikationsüberwachung; außerdem kann die präventive Wohnraumüberwachung, wie im HSOG geregelt, nicht nur den Großen Lausch-, sondern auch den Spähangriff umfassen.

Eine längere Frist dürfte auch deswegen unverhältnismäßig sein und den Anforderungen an einen ausreichenden Grundrechtsschutz nicht genügen, weil die Wohnraumüberwachung nach § 15 Abs. 4 HSOG – entsprechend der verfassungsrechtlichen Vorgaben – nur zur Abwehr einer gegenwärtigen Gefahr zulässig ist. Es ist nur schwer vorstellbar, dass eine Gefahr tatsäch-

---

[29] Vgl. BVerfG, NJW 2004, 999, 1008.
[30] Vgl. BVerfG, NJW 2004, 999, 1007.
[31] BVerfG, NJW 2004, 999, 1015.
[32] BVerfG, NJW 2004, 999, 1015.
[33] Vgl. auch Kühne in Sachs, GG, 3. Aufl., Artikel 13 Rn. 46; Hermes in Dreier, GG, 2. Aufl., Artikel 13 Rn. 83.
[34] Vgl. BVerfG, NJW 2004, 999, 1010.

lich über drei Monate oder gar im Höchstfall über 12 Monate „gegenwärtig" sein soll: Denn eine gegenwärtige Gefahr liegt nur dann vor, wenn eine Sachlage entsteht, *„bei der die Einwirkung des schädigenden Ereignisses bereits begonnen hat oder bei der diese Einwirkung unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorsteht"*.[35]

Unmittelbar oder in allernächster Zeit ist mit drei Monaten oder gar 12 Monaten Wohnraumüberwachung jedenfalls nicht mehr vereinbar.

Fazit

1. Bewertung des Gesetzentwurfs

Nach der Rechtsprechung des BVerfG sind Regelungen erforderlich, die die Datenerhebung aus diesem Kernbereich von vornherein verbieten bzw. einen Abbruch der Abhörmaßnahme verlangen, wenn überraschend der Kernbereich berührt wird. Für gleichwohl erhobene Daten bedarf es eines absoluten, gesetzlich verankerten Verwertungsverbots, dessen Einhaltung durch eine unabhängige Stelle überprüft wird. Zudem muss die uneingeschränkte Verpflichtung geregelt werden, die durch eine rechtswidrige Wohnraumüberwachung erhobenen Daten sofort zu löschen, verbunden mit der Dokumentation der rechtswidrig erfolgten Datenerhebung. Diese verfassungsgerichtlichen Vorgaben setzt der Gesetzentwurf der FDP-Fraktion in weiten Teilen um, allerdings noch nicht konsequent genug.

1.1 Es ist zwar konsequent, wenn der Gesetzentwurf der FDP-Fraktion in § 15 Abs. 4 (neu) die Räume der in § 53 Strafprozessordnung genannten Berufsgeheimnisträger von der Überwachungsbefugnis von vornherein ausnimmt. Aber diese Einschränkung reicht insofern nicht, als auch Gespräche mit Berufsgeheimnisträgern außerhalb von deren Geschäftsräumen einem absoluten Schutz unterliegen müssen.

1.2 Die gesetzliche Verankerung eines Erhebungs- bzw. Überwachungsverbots im Falle von Gesprächen aus dem Kernbereich privater Lebensgestaltung, wie es der Gesetzentwurf vorsieht, entspricht den verfassungsgerichtlichen Vorgaben. Ob es allerdings ausreicht, zu regeln, dass die Überwachungsmaßnahme sofort abzubrechen ist, wenn durch die Maßnahme Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist fraglich. Es sollte zumindest gesetzlich klargestellt werden, dass ein Überwachungs- bzw. Erhebungsverbot von vornherein besteht, wenn erkennbar ist, dass die Maßnahme den Kernbereich privater Lebensgestaltung betrifft.

2. Weitergehender Änderungsbedarf/Vorschläge

2.1 ***Verankerung weiterer Begrenzungen in § 15 Abs. 4 HSOG:*** Da es sich bei der elektronischen Wohnraumüberwachung um einen Grundrechtseingriff von höchster Intensität handelt, sollte die Maßnahme noch weiter begrenzt werden, um dem Verfassungsgrundsatz der Verhältnismäßigkeit zu genügen:
a) Zum einen sollte der *Große Spähangriff* ausgeschlossen werden, weil dadurch – vor allem in Kombination mit dem Großen Lauschangriff – praktisch alle Lebens(ent)äußerungen und Aktionen in der Privat- und Intimsphäre ausgeforscht werden.
b) Zum zweiten sollte die verbleibende akustische Wohnraumüberwachung nur zulässig sein *zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person, wenn Tatsachen die Annahme rechtfertigen, dass sich die Person, der die Gefahr droht oder von der die Gefahr ausgeht, in der Wohnung aufhält, und die Gefahr auf andere*

[35] Vgl. die Legaldefinitionen in § 2 BremPolG und § 2 NdsSOG)

Weise nicht abgewendet werden kann. Damit wäre die Überwachung von anderen Wohnungen weitgehend ausgeschlossen. Es dürfen aus Wohnräumen nur Gespräche abgehört werden, die der potentielle Straftäter führt, da sich nur aus solchen Gesprächen Informationen gewinnen lassen, die die Gefahr der Begehung der Tat abwenden können.
c) Zum dritten sind alle Vorkehrungen zu treffen, um den jederzeitigen Abbruch der Überwachungsmaßnahme zu ermöglichen. Bei in einer fremden Sprache geführten Gesprächen ist dies durch die Anwesenheit eines Dolmetschers zu gewährleisten.

2.2 ***Berufsgeheimnisträger und ihre Hilfspersonen:*** Erforderlich ist darüber hinaus eine Erweiterung des Erhebungsverbots auf die in § 53a StPO genannten Hilfspersonen, soweit mit ihnen Gespräche geführt werden, die dem Kernbereich zuzuordnen sind. Zudem ist, wie oben bereits erwähnt, die Beschränkung des Schutzes auf die Wohnungen bzw. Geschäftsräume der Berufsgeheimnisträger problematisch; die Gespräche müssen in gleicher Weise geschützt werden, wenn sie in anderen Wohnungen, etwa in der Wohnung der Zielperson selbst, stattfinden; d.h. eine Überwachung von Gesprächen mit Berufsgeheimnisträgern ist prinzipiell für unzulässig zu erklären.

2.3 ***Die Höchstdauer*** einer richterlich angeordneten Überwachungsmaßnahme in § 15 Abs. 5 HSOG sollte unbedingt von drei Monaten auf einen Monat bzw. vier Wochen verkürzt werden; eine Verlängerung sollte lediglich einmal um höchstens weitere vier Wochen möglich sein. Denn mit zunehmender Dauer steigt die Eingriffstiefe des Lauschangriffs oder einer sonstigen geheimen Überwachungsmaßnahme in die Rechte sämtlicher Betroffenen, da sich immer mehr ein ganzheitliches Bild über ihre Lebensgewohnheiten und -äußerungen ergibt. Im Übrigen geht es um die Abwehr einer gegenwärtigen Gefahr, so dass eine längere Frist damit nicht vereinbar wäre.

2.4 ***Die richterlichen Prüfungs- und Begründungsanforderungen*** sollten erhöht werden, besonders im Falle einer Verlängerung der Überwachungsmaßnahme. Der Richtervorbehalt für die Wohnraumüberwachung zu Zwecken der Gefahrenabwehr dient (wie der zum Zweck der Strafverfolgung) der vorbeugenden Rechtskontrolle; er kann der Aufgabe einer verstärkten Sicherung des Grundrechts aus Artikel 13 Abs. 1 GG nur gerecht werden, wenn die richterliche Entscheidung Angaben zu Art, Umfang (auch räumliche Begrenzung) und Dauer der Maßnahme enthält und in nachvollziehbarer Weise unter Angabe der maßgeblichen Erwägungen begründet wird.[36] Darüber hinaus sollte auch eine **richterliche Verlaufs- und Erfolgskontrolle** gesetzlich verankert werden. Der/die Richter/in (oder die Kammer) sollte konsequenterweise auch die Befugnis zum jederzeitigen Abbruch der Überwachungsmaßnahme sowie zur Löschung der dem Verwertungsverbot unterliegenden Informationen erhalten, inklusive Dokumentation der Rechtswidrigkeit der Datenerhebung. Das Bundesverfassungsgericht hat dem anordnenden Gericht auch die Verpflichtung auferlegt, den Abbruch der Maßnahme anzuordnen, wenn sie fortgesetzt wird, obwohl die gesetzlichen oder in der Anordnung festgelegten Voraussetzungen fehlen.[37] Dies ist nur möglich, wenn den die Maßnahme durchführen-

---

[36] Vgl. BVerfGE 103, 142, 152. "*Es ist die Aufgabe und Pflicht des anordnenden Gerichts, sich eigenverantwortlich ein Urteil darüber zu bilden, ob die beantragte akustische Wohnraumüberwachung zulässig und geboten ist. Dazu gehören eine sorgfältige Prüfung der Eingriffsvoraussetzungen und eine umfassende Abwägung der zur Feststellung der Angemessenheit des Eingriffs im konkreten Fall führenden Gesichtspunkte. Der Anordnungsbeschluss muss den Tatvorwurf so beschreiben, dass der äußere Rahmen abgesteckt wird, innerhalb dessen die heimliche Maßnahme durchzuführen ist (vgl. BVerfGE 107, 299 <325>). Die maßgeblichen Erwägungen des Gerichts sind in der Begründung der Anordnung hinreichend zu dokumentieren. Das Gericht hat durch geeignete Formulierungen des Anordnungsbeschlusses im Rahmen des Möglichen und Zumutbaren sicherzustellen, dass der Eingriff in die Grundrechte messbar und kontrollierbar bleibt (vgl. BVerfGE 103, 142 <151 f.>).*"

[37] Vgl. BVerfG 2004, NJW 2004, 999, 1015.

den Stellen eine in bestimmten Abständen durchzuführende Unterrichtung des Gerichts aufgegeben wird.[38]

2.5 ***Verwertungsverbot und Löschgebot bei Gefahr-im-Verzug-Anordnung:*** Falls die Anordnung gemäß § 15 Abs. 5 S. 8 nicht binnen drei Tagen richterlich bestätigt wird und außer Kraft tritt, sind die bis dahin gewonnenen Erkenntnisse sofort zu löschen; sie unterliegen einem Verwertungsverbot.

2.6 ***Benachrichtigung der Betroffenen:*** Nach § 29 Abs. 6 HSOG sind Betroffene von verdeckten Polizeimaßnahmen nach Abschluss der Maßnahmen auch ohne deren Antrag zu unterrichten. Betroffen sind die Personen, gegen die sich die Maßnahme gerichtet hat, deren Gesprächspartner sowie der Inhaber einer Wohnung in den Fällen des § 15 Abs. 4. Allerdings gibt es weitreichende Ausnahmen: *„Die Unterrichtung unterbleibt, soweit dies im überwiegenden Interesse der Person liegt, gegen die sich die Maßnahme gerichtet hat, oder wenn die Ermittlung der betroffenen Person oder deren Anschrift einen unverhältnismäßigen Verwaltungsaufwand erfordern würde. Eine Unterrichtung unterbleibt ferner, solange sie den Zweck der Maßnahme, ein sich an den auslösenden Sachverhalt anschließendes strafrechtliches Ermittlungsverfahren oder Leib, Leben oder Freiheit einer Person gefährden würde."*

Diese Ausnahmen dürften im Fall der präventiven Wohnraumüberwachung zu weit gehen. Das Bundesverfassungsgericht hat in seinem Urteil aus 2004 zum Großen Lauschangriff festgestellt,[39] dass den von der heimlichen Wohnraumüberwachung betroffenen Grundrechtsträgern grundsätzlich ein Anspruch auf nachträgliche Unterrichtung über Anordnung und Durchführung der Maßnahme zustehe; dies ergebe sich aus Artikel 13 Abs. 1 GG in Verbindung mit dem Erfordernis eines effektiven gerichtlichen Rechtsschutzes nach Artikel 19 Abs. 4 GG. Die Begrenzung der Mitteilungspflicht stelle ihrerseits einen Eingriff in die Grundrechte aus Artikel 13 Abs. 1 und Artikel 19 Abs. 4 GG dar, bedürfe einer Rechtfertigung und müsse den Anforderungen der Verhältnismäßigkeit genügen. Eine Zurückstellung sei auf das unbedingt Erforderliche zu beschränken.

Grundsätzliche Überlegung zur präventiven elektronischen Wohnraumüberwachung

Die elektronische Wohnraumüberwachung in ihrer Ausprägung als Lausch- und Spähangriff lässt von dem unantastbaren Kernbereich des Art. 13 GG kaum noch etwas übrig. Sie berührt die Privatheit in allerhöchstem Maße und belässt die einzelnen Betroffenen – zu einem überwiegenden Teil unbeteiligte, unverdächtige, unschuldige Personen – nicht mehr ihre verfassungsrechtlich garantierte Möglichkeit zum privaten Rückzug.

„Der große Lauschangriff berührt ein sich dramatisch verknappendes persönliches und gesellschaftliches Gut, die Privatheit, in ihren letzten Refugien und damit höchste verfassungsrechtliche Maßstäbe", stellten bereits 2004 sieben Landesdatenschutzbeauftragte fest und sie fragen: *„Was kann vom Wesensgehalt des Art. 13 GG noch übrig bleiben, wenn sämtliche Lebensäußerungen in der ‚unverletzlichen' Wohnung staatlich belauscht werden können, weil sich ‚vermutlich' ein Beschuldigter in ihr aufhält?"*

Der Lausch- (und Späh-) Angriff dringt noch tiefer als die anderen polizeilichen Instrumente in die Privatsphäre ein; er muss daher, will man ihn überhaupt zulassen, gegenüber jenen wirksam als Ultima-Ratio-Maßnahme ausgestaltet werden – was in besonderem Maße für Eingriffe in Wohnungen Unbeteiligter gilt. Denn betroffen werden durch diesen Eingriff als

---

[38] Die Argumentation des BVerfG ist insoweit etwas widersprüchlich, weil das Gericht nur eine Berechtigung, nicht aber eine Verpflichtung zu einer solchen Anordnung hat, vgl. NJW 2004, 999, 1014.

[39] Vgl. BVerfG, NJW 2004, 999, 1015 f.

"unvermeidbar betroffene Dritte" vor allem eine Vielzahl Unbeteiligter - alle unverdächtigen Gesprächspartner des Verdächtigen oder in den Räumen anwesende andere Personen -, die mit einer Überwachung ihrer Gespräche und Handlungen gar nicht rechnen. Potentielle „Terroristen" oder „Organisierte Kriminelle" werden sich der Überwachung auf unterschiedlichste Weise und unter Nutzung aller, auch kostspieliger Möglichkeiten entziehen können.

Angesichts dieser tiefgreifenden staatlichen Eingriffsmöglichkeiten sind an den Verfassungsgrundsatz der Verhältnismäßigkeit besondere Anforderungen zu stellen. Doch die Erforderlichkeit der elektronischen Wohnraumüberwachung zur Gefahrenabwehr ist bisher in keinem Bundesland und im Besonderen in Hessen nicht überzeugend belegt worden. Es gibt m.E. keine unabhängige und kritische Evaluation bzw. Tatsachenanalyse der bisherigen Erfahrungen – gerade auch nicht zu der Frage, ob das eingesetzte Mittel mit seiner gravierenden Eingriffstiefe überhaupt in einem angemessenen Verhältnis zu dem jeweils erreichten Zweck der Gefahrenabwehr steht. Wenn das in der Rechtspraxis jedoch nicht der Fall sein sollte, dann wäre der Große Lausch- und Spähangriff zum Zwecke der Gefahrenabwehr insgesamt nicht verhältnismäßig und deshalb verfassungswidrig. Als reines Vorratsgesetz für alle Fälle ließe sich diese Norm nicht aufrecht erhalten.

III. PRÄVENTIVE TELEKOMMUNIKATIONSÜBERWACHUNG
(§ 15a HSOG)

Aktuelle Regelung im HSOG

Der hessischen Polizei ist auch präventiv ein Eingriff in das Telekommunikationsgeheimnis des Art. 10 GG möglich – also das vorsorgliche Abhören von Telefonen und Handys sowie das vorsorgliche Mitlesen von Faxen, SMS und E-Mails, ohne dass eine Straftat oder ein konkreter Anfangsverdacht vorliegen muss. Beim Reinhören könnte sich ja der Verdacht auf eine schwerwiegende Straftat ergeben, so die Logik des Gesetzgebers, der auch andere Bundesländer gefolgt sind.

Im Gegensatz zu einigen anderen Bundesländern erfolgt jedoch in § 15a Abs. 1 HSOG eine Beschränkung dieses Instruments auf Fälle der Gefahrenabwehr – konkret: zur *„Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person"*. Insoweit entspricht die Eingriffsschwelle der der elektronischen Wohnraumüberwachung in § 15 Abs. 4 HSOG.

Neben dem Auskunftsanspruch gegenüber den Telekommunikationsanbietern/Providern auf Inhalt und Umstände der Telekommunikation kann die Polizei außerdem mit Hilfe des sog. IMSI-Catchers den Standort von Handys ermitteln lassen.

Die präventive Telekommunikationsüberwachung (TKÜ) steht unter einem Richtervorbehalt.

Die geltende Regelung im HSOG ist von der Rechtsprechung des Bundesverfassungsgerichts zur präventiven TKÜ betroffen und muss daher entsprechend angepasst werden.

BVerfG: TKÜ-Regelungen in NSOG und AWG unverhältnismäßig und nichtig

Ein Oldenburger Richter hatte gegen die vorbeugende TKÜ im Niedersächsischen Polizeigesetz Verfassungsbeschwerde eingelegt. Als Besucher einer Kneipe, in der eine Leninbüste

aufgestellt sei und auch „Linksradikale" verkehrten, könne er rasch als Kontaktperson potentieller Straftäter in die präventiven Abhörmaßnahmen geraten. Er bekam in Karlsruhe Recht. Der Erste Senat des Bundesverfassungsgerichts erklärte in seinem Urteil vom 27.07.2005 die Bestimmung im Niedersächsischen Polizeigesetz wegen Verstoßes gegen das Fernmeldegeheimnis (Art. 10 Abs. 1 GG) für nichtig.[40] Abgesehen davon, dass der Gesetzgeber teilweise seine Gesetzgebungskompetenz überschritten habe (formelle Verfassungswidrigkeit), sei die Regelung nicht hinreichend bestimmt und genüge nicht den Anforderungen des Verhältnismäßigkeitsgrundsatzes. Das Gesetz, das solche Überwachungsmaßnahmen schon im Vorfeld möglicher Straftaten zulässt, schütze unbescholtene Personen nicht ausreichend davor, abgehört zu werden. Auf vage Prognosen mit hohem „Fehlprognose-Risiko", so die Richter, dürfe sich ein so massiver Eingriff in die Grundrechte nicht stützen. Im übrigen fehlten im Gesetz hinreichende Vorkehrungen zur Vermeidung von Eingriffen in den absolut geschützten Kernbereich privater Lebensgestaltung (materielle Verfassungswidrigkeit).

Auch die präventive Postkontroll- und TKÜ-Befugnis des Zollkriminalamtes nach dem Außenwirtschaftsgesetz (AWG) erklärte das Bundesverfassungsgericht 2004 für verfassungswidrig.[41] In diesem Zusammenhang hat das Gericht für die Telekommunikationsüberwachung festgestellt, dass der Gesetzgeber die sichernden Grundsätze der Gerichtsentscheidung zur akustischen Wohnraumüberwachung auch in diesem Bereich entsprechend zu beachten habe. Danach sind insbesondere gesetzliche und technische Sicherungen erforderlich, dass Kommunikationsinhalte des höchstpersönlichen Lebensbereichs nicht erhoben werden, und wenn sie ausnahmsweise dennoch erhoben wurden, unverzüglich gelöscht werden müssen und keinesfalls verwertet werden dürfen.

Novellierungsbedarf im HSOG

***1) Kernbereich privater Lebensgestaltung*:** Die stets garantierte Unantastbarkeit der Menschenwürde fordere also auch im Gewährleistungsbereich des Art. 10 GG, so das Bundesverfassungsgericht, klare Vorkehrungen zum Schutz individueller Entfaltung im Kernbereich privater Lebensgestaltung. Wie beim Großen Lauchangriff bedarf es auch bei der präventiven TKÜ kernbereichsschützender Regelungen.[42] Solche Sicherungen sind bislang im HSOG nicht verankert.

Der hessische Datenschutzbeauftragte (LfD) hatte schon seit Längerem das Fehlen entsprechender Regelungen bemängelt, die den Kernbereich privater Lebensführung schützen[43] – Regelungen, die nun mit dem Gesetzentwurf der FDP-Fraktion in § 15a Abs. 1 HSOG Eingang finden sollen.

2) Schutz von Kommunikationspartnern: Geschützt werden müssen bei der präventiven TKÜ, so der LfD, auch *„Gespräche, die keinen Bezug zu der abzuwehrenden Gefahr haben... Zu beachten ist dabei, dass auch Nichtstörer Inhaber der überwachten Anschlüsse sein können und von den Überwachungsmaßnahmen insbesondere auch die Gesprächspartner betroffen sind."*

Denn mit der präventiven TKÜ geraten außer den „vorverdächtigen" Personen zwangsläufig auch deren unverdächtige, teils zufällige Kommunikationspartner ins Visier der Polizei, also

---

[40] BVerfG Urteil vom 27.7.2005 - Az. 1 BvR 668/04 = NJW 2005, 2603; Rath, Intimsache Telefon, in: taz 28.7.05, S. 3.

[41] BVerfG-Beschluss vom 3.03.2004, Az. 1 BvF 3/92.

[42] Vg. Dazu ausführlich: Bergemann, in: Roggan (Hg.), Lisken-GS, Berlin 2004, S. 69 ff.

[43] Im 33. Tätigkeitsbericht vom 31. Dezember 2004 unter 5.1.1.2.3

Verwandte, Bekannte, Nachbarn oder Arbeitskollegen. Darunter fallen auch bloße Kontakt- und Begleitpersonen von Vorverdächtigten. Auch die Kommunikation mit unverdächtigen Vertrauenspersonen wie Rechtsanwälten, Abgeordneten, Ärzten, Journalisten, Psychotherapeuten oder Seelsorgern ist davon nicht explizit ausgenommen – und zwar ungeachtet der besonderen Schweigepflichten, denen solche Personen unterliegen. Der Schutz von Informanten, das Redaktions- oder Mandatsgeheimnis sind also mit der aktuellen Regelung in § 15a HSOG nicht mehr zu gewährleisten.[44]

Bewertung des Gesetzentwurfs und weitergehende Anforderungen/Vorschläge

1. Nach dem neu einzufügenden Absatz 4 des vorliegenden Gesetzentwurfs

- sind die Überwachungsmaßnahmen sofort abzubrechen, wenn erkennbar wird, dass durch die Maßnahmen Erkenntnisse aus dem absolut geschützten Kernbereich privater Lebensgestaltung erlangt werden.
- Außerdem sollen die in § 53 Strafprozessordnung genannten Berufsgeheimnisträger vor der präventiven TKÜ geschützt werden. Dazu gehören u.a. Geistliche, Strafverteidiger, Rechtsanwälte, Patentanwälte, Notare, Wirtschaftsprüfer, Steuerberater, Ärzte, Psychotherapeuten, Apotheker, Drogenberater, Mitglieder der Parlamente, Redakteure und Journalisten.

2. Diese Regelungen sind zwar absolut notwendig, greifen aber noch zu kurz. Um der jüngeren Rechtsprechung des Bundesverfassungsgerichts zur Konkretisierung des Menschenwürdeschutzes durch die Unantastbarkeit der Kernbereiche des Wohnungs- und des Telekommunikations-Grundrechts zu genügen, müsste die Regelung zumindest wie folgt ergänzt werden:[45]

- Es sind alle Vorkehrungen zu treffen, um den jederzeitigen Abbruch der Überwachungsmaßnahme zu ermöglichen. Bei in ausländischer Sprache geführten Telefonaten ist dies durch die Anwesenheit eines Dolmetschers zu gewährleisten.
- Für Telekommunikationsverbindungen und Gespräche mit Vertrauenspersonen gilt eine Vermutung, dass diese Kontakte und die Gesprächsinhalte zum Kernbereich privater Lebensgestaltung gehören. Etwas anderes gilt, wenn der Straftatverdacht auch gegen die Vertrauensperson des Verdächtigen besteht, soweit der Gesprächsinhalt nicht den Kernbereich betrifft.
- Auch bei erkennbaren Telekommunikationskontakten dritter Personen untereinander hat die Überwachung von vornherein zu unterbleiben.
- Ergibt sich erst im Gesprächsverlauf, dass ein Bezug zum Beschuldigten nicht besteht oder dass der Kernbereich privater Lebensgestaltung betroffen ist, ist die weitere Überwachung sofort einzustellen. Die bis dahin erfolgten Aufzeichnungen und erlangten Informationen sind unverzüglich zu löschen und unterliegen einem absoluten Verwertungsverbot; die Rechtswidrigkeit der Datenerhebung ist zu dokumentieren.

---

[44] Vgl. dazu Gössner, in: Frankfurter Rundschau vom 25.10.03.
[45] Vgl. dazu LG Ulm, Beschl. Vom 19.04.2004 – 1 Qs 1036/04 und Anmerkung von Roggan.

IV. PRÄVENTIVE RASTERFAHNDUNG
(§ 26 HSOG)

Die Rasterfahndung ist eine besondere polizeiliche „Fahndungsmethode" unter Nutzung der elektronischen Datenverarbeitung. Unter Rasterfahndung versteht man den automatisierten, also maschinellen Abgleich personenbezogener Daten aus dem polizeilichen Fahndungsbestand mit personenbezogenen Daten aus fremden Dateien anderer öffentlicher und privater Stellen, die ursprünglich für ganz andere Zwecke erhoben worden sind (also entgegen dem Zweckbindungsprinzip des Datenschutzrechts).

Die Rasterfahndung ist ein Massengrundrechtseingriff in die informationelle Selbstbestimmung von erheblichem Gewicht, der für die Betroffenen zumeist unbemerkt stattfindet. Bei der präventiven Rasterfahndung richtet sich der polizeiliche Eingriff nicht gegen einzelne Tatverdächtige, Polizeipflichtige/Störer oder potentielle Täter, sondern Objekte der polizeilichen Aktivität werden alle Personen, die Träger gleicher persönlicher Merkmale entsprechend einem zuvor festgelegten Suchraster sind, nach denen „gefahndet" wird.

Zur Vorgeschichte

1. Suche nach sich unverdächtig verhaltenden potentiellen Tätern („Schläfer-Profil")

Als Reaktion auf die Terroranschlägen in den USA am 11. September 2001 führten die Sicherheitsbehörden bundesweit in einer konzertierten Aktion umfangreiche Rasterfahndungen durch –[46] die umfangreichsten seit Einführung dieser elektronischen Datenabgleichsmaßnahme in den 70er Jahren. Ziel war es, mutmaßliche „islamistische Schläfer" zu enttarnen. Dazu wurde als Suchraster ein sogenanntes Schläfer-Pofil entwickelt mit folgenden Kriterien: jüngere, reiselustige Männer mit legalem Aufenthaltsstatus und islamischem Hintergrund (bzw. aus bestimmten arabischen Staaten), Technikstudium, ohne Finanzprobleme und bisher keine Konflikte mit dem Gesetz.[47]

Die Rasterfahndung hat zum Ziel, mit Hilfe solcher elektronischer Merkmalsraster aus einer beliebig großen Personenzahl eine möglichst kleine Gruppe von Personen herauszufiltern, auf die die „tätertypischen" Suchkriterien zutreffen, denen gegenüber sich also ein „Verdacht" verdichtet. Je gröber das Raster, desto mehr potentiell „Verdächtige" bleiben hängen. Diese herausgefilterten Merkmalsträger werden dann, obwohl in der Regel unbeteiligt bzw. unschuldig, mit herkömmlichen Polizeimethoden überprüft (polizeiliche Ermittlungen, Befragung/Verhöre, ggfls. Observationen, Hausdurchsuchungen, Beschlagnahmen, Abhörmaßnahmen etc.). Ermittelt wird also zu einem hohen Prozentsatz gegen Unbeteiligte und Unverdächtige, die Träger gleicher persönlicher Merkmale sind, Kriterien, die in der Regel für sich genommen und auch kumulativ vollkommen unverdächtig sind – wie die Merkmale des „Schläfer"-Pofils nach dem 11.9.2001 deutlich zeigen. Hier wurde gerade die Unauffälligkeit und Angepasstheit des Verhaltens zu einem maßgeblichen Kriterium der Suche erhoben.

Kennzeichnend für die Rasterfahndung ist, dass der „konkrete" Verdacht gegen eine oder mehrere Personen, sie könnte(n) künftig möglicherweise bestimmte Straftaten begehen, am Ende und nicht am Anfang der Maßnahme steht. Damit hebt diese Methode die Schutzwirkung traditioneller Polizeieingriffe in Grundrechte auf, die einen konkreten Verdacht gegen eine bestimmte Person voraussetzt. Mit der Rasterfahndung geraten jedenfalls viele Men-

---

[46] Auf Grundlage eines Beschlusses der Innenministerkonferenz vom 18.9.2001. Die Untergruppe „Raster" der Koordinierungsgruppe Internationaler Terrorismus (KG IntTE) entwickelte die Kriterien und legte sie fest.

[47] Ausführlicher dazu: Gössner, Schuldvermutung per Computerausdruck, in: ders., Menschenrechte in Zeiten des Terrors, Hamburg 2007, S. 143 ff.

schen, die mit Verbrechen nichts zu tun haben, ins Visier der Fahnder, was die Rasterfahndung zu einem schwerwiegenden Grundrechtseingriff gegen Unverdächtige macht. Selbst sensible Persönlichkeitsprofile können mit der Verknüpfung unterschiedlicher Daten erstellt werden.

2. Nachrüstende Sicherheitspolitik

Die gesetzlichen Voraussetzungen, unter denen Rasterfahndungen durchgeführt werden können, erlebten seit dem 11.9.2001 eine erstaunliche Metamorphose. Ursprünglich setzten die meisten Regelungen in den Polizeigesetzen der Bundesländer eine gegenwärtige oder konkrete Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes sowie für Leib, Leben oder Freiheit einer Person voraus sowie einen Richtervorbehalt.[48]

Nachdem einige Verwaltungsgerichte die damaligen Rasterfahndungen beanstandeten, weil die gesetzlichen Eingriffsvoraussetzungen nicht vorgelegen hatten, sollte die vorbeugende Rasterfahndung in den Polizeigesetzen auch schon zur Verhütung möglicher „Straftaten von erheblicher Bedeutung" erlaubt werden, wenn „tatsächliche Anhaltspunkte die Annahme rechtfertigen", dass dies hierfür erforderlich sei. Hessen folgte mit seiner Gesetzesnovellierung den Vorbildern Baden-Württemberg und Bayern, die damals die niedrigste Eingriffsschwelle aufzuweisen hatten und keine richterliche Vorabkontrolle kannten.

Nach Inkrafttreten der neuen Regelung hat Hessen auf Anordnung des Landeskriminalamts die gerichtlich gestoppten Rasterfahndungen Anfang 2003 wieder aufgenommen. Die überwiegende Zahl der Landesgesetzgeber hat das Vorliegen einer Gefahr als Voraussetzung insgesamt fallengelassen, die Ermächtigung zur Rasterfahndung also vollkommen entgrenzt.[49]

BVerfG erklärt entgrenzte Regelungen für unverhältnismäßig und verfassungswidrig

Das Bundesverfassungsgericht hat im April 2006 mit einem „fulminanten Urteil" (so Heribert Prantl in der „Süddeutschen Zeitung")[50] die präventive Rasterfahndung nach etlichen dieser Polizeigesetze rückwirkend für unverhältnismäßig und verfassungswidrig erklärt und dem Grundrechtsschutz auch in Zeiten des Terrors wieder Geltung verschafft.[51] Nur wenn eine hinreichend konkrete Gefahr für hochrangige Rechtsgüter wie Leib und Leben bestehe, dürften Personendaten nach bestimmten Suchkriterien gerastert werden, um potentielle Terroristen schon vor einer möglichen Tat zu enttarnen. Eine „allgemeine Bedrohungslage", wie sie nach dem 11.09.2001 bestand, genüge ebenso wenig wie etwa außenpolitische Spannungslagen und vage Vermutungen. Voraussetzung für solche schwerwiegenden Eingriffe in das informationelle Selbstbestimmungsrecht können also nur fundierte Tatsachen und klare Hinweise sein auf die Vorbereitung terroristischer Anschläge oder darauf, dass sich in Deutschland Personen für solche Anschläge bereithalten und präparieren.

Obwohl das Urteil unmittelbar nur für Nordrhein-Westfalen gilt, müssen doch etliche Bundesländer ihre Polizeigesetze ändern und die Hürde wieder höher legen, nachdem einige von ihnen sie in den vergangenen Jahren erst abgesenkt hatten. So auch Hessen. Nur Berlin, Brandenburg und Mecklenburg-Vorpommern erfüllten zum Zeitpunkt des Urteils die Anforderun-

---

[48] Vgl. Koch, Datenerhebung und -verarbeitung in den Polizeigesetzen der Länder, 1999, S. 187 ff.

[49] Eine solche Ermächtigung zu Vorfeldmaßnahmen kennen beispielsweise Baden-Württemberg (§ 40 PolG), Bayern (Art. 44 BayPAG), Hamburg (§ 23 PolDVG HA), Hessen (§ 26 HSOG), Rheinland Pfalz (§ 38 POG), Sachsen-Anhalt (§ 31 LSA), Thüringen (§ 44 PAG).

[50] Prantl, Die Raster der Hysterie, in: SZ 24.5.06.

[51] BVerfGE, 1 BvR 518/02 vom 4.4.2006, bezieht sich auf eine Entscheidung des OLG Düsseldorf.

gen, indem sie eine „gegenwärtige Gefahr" als Voraussetzung für eine Rasterfahndung verlangen.

Die Verfassungsrichter geben in ihrer Entscheidung auch zu bedenken, dass Rasterfahndungen durchaus Vorurteile produzieren und die konkret betroffenen Bevölkerungsgruppen in der öffentlichen Wahrnehmung stigmatisieren könnten. Wer nicht mit hinreichender Sicherheit überschauen könne, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermöge, *„kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden"*.[52]

Leitsätze des Ersten Senats des Bundesverfassungsgerichts vom 4. April 2006

(Bundesverfassungsgericht - 1 BvR 518/02)

1. „Eine präventive polizeiliche Rasterfahndung der in § 31 PolG NW 1990 geregelten Art ist mit dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) nur vereinbar, wenn eine konkrete Gefahr für hochrangige Rechtsgüter wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben ist. Im Vorfeld der Gefahrenabwehr scheidet eine solche Rasterfahndung aus.
2. Eine allgemeine Bedrohungslage, wie sie im Hinblick auf terroristische Anschläge seit dem 11. September 2001 durchgehend bestanden hat, oder außenpolitische Spannungslagen reichen für die Anordnung der Rasterfahndung nicht aus. Vorausgesetzt ist vielmehr das Vorliegen weiterer Tatsachen, aus denen sich eine konkrete Gefahr, etwa für die Vorbereitung oder Durchführung terroristischer Anschläge, ergibt."

Grundrechtseingriffe, die sowohl durch Verdachtslosigkeit als auch durch eine große Streubreite gekennzeichnet sind, so das Bundesverfassungsgericht, bei denen also zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr eigenes Verhalten auch nicht veranlasst haben – *„weisen grundsätzlich eine hohe Eingriffsintensität auf"*. Denn der Einzelne sei in seiner grundrechtlichen Freiheit umso intensiver betroffen, je weniger er selbst für einen staatlichen Eingriff Anlass gegeben hat. Von solchen Eingriffen könnten Einschüchterungseffekte ausgehen, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen könnten. *„Es gefährdet die Unbefangenheit des Verhaltens, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen."*[53]

Gesetzliche Konsequenzen aus dem BVerfG-Urteil

Der vorliegende Gesetzentwurf der FDP-Fraktion versucht, mit einer Neufassung des § 26 Abs. 1 S. 1 geeignete Konsequenzen aus dem Urteil zu ziehen. Danach sollen künftig Polizeibehörden des Landes von öffentlichen Stellen oder Stellen außerhalb des öffentlichen Bereichs die Übermittlung von personenbezogenen Daten bestimmter Personengruppen zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen dürfen – aber nur

- *„zur Abwehr einer konkreten Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind..." und*

[52] Ebda., mit Bezug auf: BVerfGE 65, 1, 42 f.

[53] So die BVerfGE, 1 BvR 518/02 vom 4.4.2006 mit Verweisen auf BVerfGE 65, 1 <42>; 113, 29 <46>, BVerfGE 100, 313 <376, 392>; 107, 299 <320 f.>; 109, 279 <353>; 113, 29 <53>; 113, 348 <383>, BVerfGE 107, 299 <328>

- *„wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Abwehr der Gefahr erforderlich und dies auf andere Weise nicht möglich ist".*

Als *konkrete Gefahr* wird eine Sachlage bezeichnet, welche bei ungehindertem Geschehensablauf und in überschaubarer Zukunft mit hinreichender Wahrscheinlichkeit zu einem Schaden führen wird.[54] Entsprechendes gilt für ein von Personen ausgehendes Verhalten. Die konkrete Gefahr muss im Übrigen für hochrangige Rechtsgüter drohen – etwa im Fall der mutmaßlichen Vorbereitung oder Durchführung terroristischer Anschläge. Für diese geforderten Kriterien muss es *hinreichende tatsächliche Anhaltspunkte* – besser wäre: *bestimmte Tatsachen* – geben.[55]

Fazit: Bewertung und weitergehende Vorschläge

Mit dieser Tatbestandsvoraussetzung ist klargestellt, dass die präventive Rasterfahndung keine bloße Vorfeldmaßnahme ist, nicht zur allgemeinen Gefahrenvorsorge und auch nicht zur Verhütung möglicher „Straftaten von erheblicher Bedeutung" zulässig ist. Es wird klargestellt, dass eine allgemeine Bedrohungslage als Tatbestandsvoraussetzung nicht reicht. Dadurch wird die präventiv-polizeiliche Rasterfahndung wieder so weit eingegrenzt, dass sie den Vorgaben des Bundesverfassungsgerichts entspricht.

Dennoch sollte im Gesetz noch ein ***Richtervorbehalt*** verankert werden, das heißt, die Anordnung der Maßnahme sollte durch den zuständigen Richter erfolgen, um eine unabhängige Vorkontrolle und möglichst auch eine Verlaufs- und Erfolgskontrolle zu gewährleisten. Etliche Polizeigesetze der Länder sahen ursprünglich eine solche gerichtliche Vorabkontrolle durch den Amtsrichter deshalb vor, weil es im Zuge von Rasterfahndungen zu schwerwiegenden Eingriffen in Grundrechtspositionen einer Vielzahl von Personen kommt, die unverdächtig sind.

Angesichts der Tatsache, dass im Herbst 2001, soweit ersichtlich, kein einziger Richter eine Anordnung verweigert hatte, fragt sich allerdings, ob diese gerichtliche Vorkontrolle in akuten Krisenfällen und zugespitzten Lagen überhaupt hält, was sie verspricht, oder ob sie in diesem Zusammenhang – wie im übrigen auch bei Telefonüberwachungsmaßnahmen – nicht letztlich versagt. Gerade in aufgeheizten Ausnahmesituationen wäre Realitätssinn und Augenmaß von unabhängiger Seite gefragt – als hinreichend verlässliche Hürde gegen den Aktionismus der herrschenden Sicherheitspolitik und unter öffentlichem Handlungsdruck stehender Sicherheitsbehörden. Das OLG Frankfurt hat in seinem Urteil zur Rasterfahndung vom 8. Januar 2002 den Sinn und Zweck des Richtervorbehalts auf den Punkt gebracht und damit zugleich die damit befassten Richter ermahnt:[56] *„Mit der Übertragung der Entscheidungskompetenz und Verantwortung auf die Gerichte ist zugleich die Erwartung verbunden, dass sich die zur Entscheidung berufenen Richterinnen und Richter – auch in Krisenzeiten – nicht von eigenen Emotionen oder Emotionen anderer, sondern ausschließlich vom Gesetz leiten lassen."*

Ein solches Verständnis zugrunde gelegt, wäre die richterliche Anordnung als Korrektiv sinnvoll. Sie sollte verbunden sein mit einer richterlichen Verlaufs- und Erfolgskontrolle.

---

[54] Vgl. § 1 PolG NRW, § 1 PolG BaWü, § 1 Nds. SOG

[55] Der Begriff der "tatsächlichen Anhaltspunkte" stellt eine noch niedrigere Eingriffsschwelle dar als die im Polizeirecht und auch in der StPO häufig verwendete Voraussetzung der "bestimmten Tatsachen".

[56] OLG Frankfurt/M. (Az. 209/01)

Verzicht auf präventive Rasterfahndung mangels Zwecktauglichkeit

Es stellt sich unter dem Aspekt der Verhältnismäßigkeit aber die Frage, ob die präventive Rasterfahndung zur Abwehr konkreter Gefahren überhaupt tauglich und damit als geeignetes Mittel anzusehen ist. So stellt das BVerfG in seiner Rasterfahndungsentscheidung fest: Die gegenwärtige Gefahr als Tatbestandsvoraussetzung führe angesichts des mit der Maßnahme verbundenen zeitlichen und technischen Aufwands bereits dazu, dass diese in den meisten Fällen zu spät kommen wird, um noch wirksam sein zu können.[57] Wie sich dies angesichts einer konkreten Gefahr als Tatbestandsvoraussetzung darstellt, wäre zu überprüfen. Als *konkrete Gefahr* wird, wie bereits erwähnt, eine Sachlage bezeichnet, welche bei ungehindertem Geschehensablauf und in überschaubarer Zukunft mit hinreichender Wahrscheinlichkeit zu einem Schaden an einem polizeilich zu schützenden Rechtsgut führen wird.[58] Damit kann es in vielen Fällen dazu kommen, dass die Zwecktauglichkeit zum Zeitpunkt der Anordnung einer Rasterfahndung nicht hinreichend prognostiziert werden kann. In etlichen Fällen dürfte von vornherein klar sein, dass der zu treibende Aufwand zu viel Zeit erfordern wird, um rechtzeitig ein Ergebnis zu erzielen und das schädigende Ereignis noch aufhalten zu können. Und nur in wenigen Fällen – etwa bei einer wochenlangen Geiselnahme - dürfte genügend Zeit bleiben, um die Rasterfahndung durchzuführen und das Ergebnis abzuwarten. Alles in allem schrumpft damit das Feld der Anwendbarkeit dieser präventiv-polizeilichen Methode enorm zusammen.[59]

Auch der hessische Innenminister Bouffier (CDU) äußerte Zweifel, ob eine Rasterfahndung überhaupt noch durchführbar sei, wenn sie nur zur Abwehr konkreter Gefahren zulässig ist.[60] Und die NRW-Datenschutzbeauftragte Bettina Sokol hatte bereits 1999 die Auffassung vertreten, dass kaum Fälle denkbar seien, in denen eine Rasterfahndung für Zwecke der Gefahrenabwehr in Betracht kommen könnten. Wenn eine derartige (konkrete) Gefahr gegeben sei, dann käme die relativ langwierige und schwerfällige Rasterfahndung zur Gefahrenabwehr regelmäßig zu spät. Die im Polizeigesetz verankerte Rasterfahndung wäre demnach ein stumpfes Schwert.[61]

Angesichts der schwerwiegenden Beeinträchtigung der informationellen Selbstbestimmung einer Vielzahl von Unverdächtigen dürfte die präventiv-polizeiliche Rasterfahndung in der überwiegenden Zahl der Fälle auch außer Verhältnis zur Bedeutung der Sache bzw. der abzuwehrenden Gefahr stehen und damit dem Übermaßverbot widersprechen. Darauf deutet auch die flächendeckende Erfolglosigkeit der bundesweiten Rasterfahndungen nach „islamistischen Schläfern" hin. Trotz des gewaltigen Aufwands, der mit den Rasterfahndungen 2002 und 2003 betrieben worden war, verfing sich kein einziger terroristischer „Schläfer" im elektronischen Netz, lediglich einige vage Verdächtige, mutmaßliche Sozialhilfebetrüger, Schleuser und Schwarzarbeiter blieben hängen. Der einzige konkrete Verdacht auf islamistisch motivierte Terroranschläge, der sich ergeben hatte, stellte sich nach einer polizeilichen Durchsuchung von sechs Wohnungen und einer Buchhandlung in Hamburg weitgehend als Flop heraus. Sieben Männer aus Marokko, Afghanistan und Ägypten wurden von der Bundesanwaltschaft verdächtigt, eine terroristische Vereinigung gebildet zu haben. Nur gegen

---

[57] BVerfG, NJW 2006, 1939 (1947).

[58] Vgl. § 1 PolG NRW, § 1 PolG BaWü, § 1 Nds. SOG

[59] Roggan, Der Verhältnismäßigkeitsgrundsatz als Raster des Rechtsstaats – Zur Verfassungsmäßigkeit der Rasterfahndungen im Landesverwaltungsgesetz, in: Brenneisen u.a. (Hg.), Polizeirechtsreform in Schleswig-Holstein, München u.a., S. 295, mit Verweis auf Volkmann, der zu Recht darauf hinweist, dass Rasterfahndungen umso überflüssiger werden, je konkreter die Gefahr ist, je mehr die Behörden also schon wissen (JZ 2006, 918 (920).

[60] Stellungnahme von 23.05.2006.

[61] Sokol, in: Bäumler, Polizei und Datenschutz, 1999, S. S. 192 f.

einen von ihnen ist ein Ermittlungsverfahren wegen des Verdachts der Unterstützung der Terrorgruppe um Atta eingeleitet, später aber wieder eingestellt worden.[62]

Alle in der Zeit nach diesen Rasterfahndungen bekannt gewordenen Verdachtsfälle und Festnahmen gingen auf konventionelle Fahndungsmethoden zurück. Da stellt sich tatsächlich die Frage, ob der gewaltige Aufwand mitsamt den damit verbundenen Grundrechtseingriffen noch in einem vernünftigen Verhältnis zur Effizienz dieser Maßnahmen steht. Ein Verlust an Sicherheit wäre also kaum zu befürchten, wenn dieses Instrument im Polizeigesetz nicht mehr zu Verfügung stünde.[63]

Hinter vorgehaltener Hand wird von Sicherheitsbehörden durchaus eingestanden, dass mit dem Aufwirbeln der Datenbestände tatsächlich weniger auf die Enttarnung potentieller Täter abgezielt worden sei – was der Bevölkerung aber weis gemacht worden ist -, als vielmehr auf die Erhöhung des Fahndungsdrucks, um potentielle „islamistische Extremisten" zu verunsichern.[64] Das Bundeskriminalamt behauptet, dass es den Polizeibehörden der Länder und des Bundes gelungen sei, aus einer Vielzahl von Daten Personen herauszufiltern, die „der islamistischen Szene zuzuordnen" seien – dafür hätten allerdings die Rasterfahndungen von vornherein nicht durchgeführt werden dürfen. Dass die Maßnahme zur Enttarnung potentieller islamistischer Terroristen geführt hat, ist dieser Stellungnahme an das Bundesverfassungsgericht nicht zu entnehmen.[65]

V. Weitergehender gesetzgeberischer Handlungsbedarf

Über die im Gesetzentwurf der FDP-Fraktion aufgenommenen Punkte hinaus bedarf das hessische Polizeigesetz noch weiterer Änderungen. Beispiel:

So sind etwa die ***Zeugnisverweigerungsrechte*** nicht nur durch das präventive Abhören der Telekommunikation oder durch die elektronische Wohnraumüberwachung gefährdet, sondern auch *durch andere heimliche Ermittlungsmethoden der Polizei*, die in den vergangenen Jahren eingeführt worden sind. So könnte beispielsweise durch einen in eine Wohnung, eine Anwaltskanzlei, Arztpraxis oder Redaktion eingeschleusten *V-Mann* das Zeugnisverweigerungsrecht der dort tätigen Personen umgangen werden.

Nach § 16 Abs. 4 HSOG dürfen *Verdeckte Ermittler der Polizei „unter ihrer Legende mit Einwilligung der berechtigten Person deren Wohnung betreten"*. Auch hier kann es schnell dazu kommen, dass der Kernbereich der privaten Lebensgestaltung oder Berufsgeheimnisse tangiert sind und verletzt werden – ohne dass es bislang ausreichende Vorkehrungen gibt, dies zu vermeiden.

Eine wirksame Gewährleistung des Schutzes der Zeugnisverweigerungsberechtigten und des Kernbereichs privater Lebensgestaltung ist bei allen verdeckten Eingriffen verfassungsrechtlich geboten und entsprechend gesetzlich zu verankern.

Bremen, den 14. August 2008 *gez. RA Dr. Rolf Gössner*

---

[62] Vgl. taz 4.07.02, 29.09.02.

[63] So auch Roggan, Der Verhältnismäßigkeitsgrundsatz als Raster des Rechtsstaats, a.a.O., S. 298.

[64] So u.a. das Bayerische Staatsministerium des Innern in seiner Antwort vom 11.4.2002, S. 5 (LT-Drs. 14/9221 v. 6.05.02).

[65] BVerfGE, 1 BvR 518/02 vom 4.4.2006, A. I. Nr. 64

Dr. jur. Rolf Gössner, Rechtsanwalt, Publizist und Vizepräsident der *„Internationalen Liga für Menschenrechte"* (Berlin), seit 2007 stellv. Richter am *Staatsgerichtshof der Freien Hansestadt Bremen* sowie Mitglied und stellv. Sprecher der *Deputation für Inneres* in der Bremer Bürgerschaft. Sachverständiger in Gesetzgebungsverfahren von Bundestag und Landtagen. Mitherausgeber des jährlich erscheinenden *„Grundrechte-Reports" (Fischer-Verlag).* Autor zahlreicher Sachbücher zu „Innerer Sicherheit" und Bürgerrechten, zuletzt: *>Geheime Informanten. V-Leute des Verfassungsschutzes: Kriminelle im Dienst des Staates<* (Knaur 2003); *>Menschenrechte in Zeiten des Terrors. Kollateralschäden an der „Heimatfront"<*, Hamburg 2007.

Literaturhinweise

Erd, Bundesverfassungsgericht versus Politik. Eine kommentierende Dokumentation der jüngsten Entscheidungen zu drei Sicherheitsgesetzen, in: Kritische Justiz 2/2008, S. 118 ff.

Landesdatenschutzbeauftragter Hessen, 33. Tätigkeitsbericht, 5.1 Polizei und Strafverfolgung

Zu Kfz- Kennzeichenscanning

Roßnagel, Kennzeichenscanning – verfassungsrechtliche Bewertung. Eine Studie im Auftrag des ADAC zur Mobilität. Januar 2008

Arzt, Automatisierte Kfz-Kennzeichenerkennung – Anlass und verdachtsunabhängige Kontrolle von Jedermann, in Roggan/Kutscha, Handbuch zum Recht der Inneren Sicherheit, 2. Aufl. 2006, 229 ff.

Roggan, Das novellierte Brandenburgische Polizeigesetz, Neue Justiz 2007,1999.

Presseerklärung der Humanistischen Union, LV Baden-Württemberg, 06.05.2008: Vorschlag zu einer datenschutzrechtlichen Eindämmung der Befugnis der automatischen Kennzeichenerfassung"

Zu Wohnraumüberwachung

Denninger, Lauschangriff – zurechtgestutzt? In: Grundrechte-Report 2005, S. 145

Müller-Heidelberg, Denn sie wissen was sie tun. Verfassungsfeinde in Bundesregierung und Bundestag, in: Grundrechte-Report 2006, Frankfurt/M.

Roggan (Hg.), Lauschen im Rechtsstaat. Zu den Konsequenzen des Urteils des Bundesverfassungsgerichtes zum großen Lauschangriff, Berlin 2004

Gesetzgebungs- und Beratungsdienst des Niedersächsischen Landtags, Vermerk: Auswirkungen der Entscheidung des Bundesverfassungsgerichts zum "großen Lauschangriff" auf das niedersächsische Recht, 84/0300-84, Az.: 5552, Hannover, 04.05.2004

Telekommunikationsüberwachung

Gössner, In der Präventionslogik mutiert der Mensch zum Sicherheitsrisiko, in: Frankfurter Rundschau vom 25.10.03.

Roggan, in: Strafverteidiger 1/2006, S. 8 ff.

Rasterfahnung

Achelpöhler, Verfassungsgrenzen für die Rasterfahndung, in: Grundrechte-Report 2007, Ffm 2007.

BKA-Kommission Staatsschutz, Evaluation der Rasterfahndungen der Länder und der Informationsverdichtung im Bundeskriminalamt anlässlich des 11.09.2001, Wiesbaden 2004.

Gössner, Schuldvermutung per Computerausdruck, in: ders., Menschenrechte in Zeiten des Terrors, Hamburg 2007, S. 143 ff. m.w.N.

Kant, Außer Spesen nicht gewesen? Eine Bilanz der Rasterfahndungen nach dem 11. September 2001, in: Bürgerrechte & Polizei 1/05, S. 13 ff. (darin: Auswertung des BKA-Evaluationsberichts).

Roggan, Der Verhältnismäßigkeitsgrundsatz als Raster des Rechtsstaats – Zur Verfassungsmäßigkeit der Rasterfahndungen im Landesverwaltungsgesetz, in: Brenneisen u.a. (Hg.), Polizeirechtsreform in Schleswig-Holstein, München u.a.

Roggan/Kutscha (Hg.), Handbuch zum Recht der Inneren Sicherheit, Berlin 2006

Dr. ROLF GÖSSNER

RECHTSANWALT / PUBLIZIST
VIZEPRÄSIDENT DER >INTERNATIONALEN LIGA FÜR MENSCHENRECHTE< (Berlin)

Rechtsanwalt Dr. Rolf Gössner [redacted] Bremen

Hessischer Landtag
Vorsitzender des Innenausschusses,
Herrn Horst Klee, MdL
Postfach 3240

65022 Wiesbaden

Bremen, den 14. August 2008

Schriftliche Anhörung im Innenausschuss des Hessischen Landtages

Betr.: Gesetzentwurf der Fraktion der FDP für eine Zehntes Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) – LT-Drs. 17/133

Auszüge, Zusammenfassung und Fazit der Rechtspolitischen Stellungnahme

von RA Dr. Rolf Gössner vom 14. August 2008

Vorbemerkung

Das Hessische Gesetz über die öffentliche Sicherheit und Ordnung (HSOG), zuletzt geändert 2005, dürfte mit einigen seiner Regelungen gegen das Grundgesetz verstoßen. Spätestens die Grundsatzentscheidungen des Bundesverfassungsgerichts (BVerfG) der vergangenen Jahre zu diversen polizeilichen und geheimdienstlichen Befugnissen auf Bundes- und Länderebene legen diese Vermutung nahe. Ob zwischenzeitliche Novellierungen im HSOG ausreichend konsequent waren und damit diesen höchstrichterlichen Vorgaben genügen, ist zweifelhaft und soll im Folgenden ebenfalls untersucht werden.

Die FDP-Fraktion im Hessischen Landtag geht offenbar ebenfalls von einem solchen Befund aus und unternimmt mit dem vorliegenden Gesetzentwurf, der hier zur Begutachtung ansteht, den Versuch, das HSOG entsprechend der neueren Rechtsprechung des Bundesverfassungsgerichts in Sachen Sicherheitsgesetzen zu novellieren und in diesem Zusammenhang die einschlägigen Befugnisse im HSOG zu konkretisieren und einzuschränken.

Ziel des Gesetzentwurfs ist es, aus den genannten BVerfG-Entscheidungen die notwendigen gesetzgeberischen Konsequenzen zu ziehen. Dieses Vorhaben ist überfällig, nachdem die zugrundeliegenden Gerichtsentscheidungen bereits aus den Jahren 2004, 2005, 2006 und zwei der Urteile aus Februar und März 2008 stammen.

I. AUTOMATISCHES KENNZEICHEN-SCREENING (§ 14 Abs. 5 HSOG)
Automatische Kfz-Kennzeichen-Erkennung und –Abgleich zur Gefahrenabwehr

Die automatisierte Kennzeichenerkennung ist ein technisches Mittel zur massenhaften Kontrolle des öffentlichen Verkehrsraums. *„Durch die Möglichkeit, sowohl die Kennzei-*

chenerfassung als auch den Abgleich automatisiert vorzunehmen, wird eine systematische, räumlich weitreichende Sammlung von Informationen über das Bewegungsverhalten von Fahrzeugen und damit auch von Personen technisch und mit relativ geringem Aufwand möglich", so das Bundesverfassungsgericht in seiner Entscheidung vom 11.03.2008.[1] Die Automatische Kfz-Kennzeichen-Erkennung dürfte am ehesten mit einer Kombination aus Rasterfahndung, Schleierfahndung und Videoüberwachung zu vergleichen sein. Ebenso wie bei diesen Maßnahmen ist daher prinzipiell von einer hohen Eingriffsintensität auszugehen. Insofern handelt es sich keinesfalls um einen „Grundrechtseingriff an der Bagatellgrenze", wie Hessens Innenminister vor dem Urteil des Bundesverfassungsgerichts noch behauptet hatte.[2]

Die im HSOG als Standardmaßnahme ausgestaltete Polizeibefugnis zum Massenabgleich genügte laut Urteil des Bundesverfassungsgerichts nicht dem Gebot der Normenbestimmtheit und Normenklarheit, da Anlass, Eingriffsschwellen sowie Ermittlungs- und Verwendungszweck nicht benannt und nicht eindeutig definiert wurden. Der massenhafte Abgleich von Nummernschildern darf nicht ohne besonderen Anlass – also ohne konkrete Gefährdungslage oder gesteigertes Risiko – routinemäßig und flächendeckend durchgeführt werden. Oder anders ausgedrückt: Die systematische Massenkontrolle des mobilen Verhaltens aller motorisierten Bürger ohne konkreten Anlass ist verfassungswidrig. Mit der unbestimmten Weite dieser Norm, so das Gericht, werde zudem gegen das verfassungsrechtliche Gebot der Verhältnismäßigkeit verstoßen.

Gesetzgeberische Konsequenzen

Es gibt für den Gesetzgeber zwei Möglichkeiten, Konsequenzen aus dieser BVerfG-Entscheidung zu ziehen:

- Die für nichtig erklärte Regelung des § 14 Abs. 5 HSOG wird verfassungskonform ausgestaltet.
- Oder die Regelung wird aus dem Gesetz ersatzlos gestrichen.

1. Verfassungskonforme Ausgestaltung

Die FDP-Fraktion versucht mit ihrem Gesetzentwurf, die automatisierte Kfz-Kennzeichenerkennung und –erfassung verfassungskonform auszugestalten. Damit soll diese Präventionsmaßnahme den Polizeibehörden in Hessen auch künftig zur Verfügung stehen. Dabei orientieren sich die Urheber des Gesetzentwurfs an der aktuellen brandenburgischen Regelung, die das Bundesverfassungsgericht als verfassungskonform bewertet hat.[3] Mit der vorgeschlagenen Regelung und ihren relativ eng begrenzten Eingriffsvoraussetzungen soll die heimliche Erstellung von Bewegungsprofilen von Autos und Personen weitgehend ausgeschlossen und die Einrichtung von Dauer-Kontrollstellen untersagt werden.[4]

Fazit und weitergehende Anforderungen/Vorschläge

Mit diesen im vorliegenden Gesetzentwurf verankerten Voraussetzungen wird das Instrument des Kfz-Kennzeichen-Scannings gegenüber der für nichtig erklärten Fassung erheblich eingeschränkt – mit einer Ausnahme in § 14 Abs. 5 S. 1 Nr. 2: Hier dient die Maßnahme *zur Abwehr einer gegenwärtigen Gefahr,* wobei nicht gesagt wird, für welche Rechtsgüter diese Gefahr drohen muss. Jedenfalls geht es hier nicht nur um eine *gegenwär-*

---

[1] BVerfGE vom 11. März 2008, AZ: 1 BvR 2074/05 und 1 BvR 1254/07, Rndr. 142 f.
[2] SZ 21.11.07; taz 30.01.08, S. 6.
[3] BvR 2074/05, Nr. 181 ff, 183. Auch das Gutachten von Roßnagel, Kennzeichenscanning – verfassungsrechtliche Bewertung. Eine Studie im Auftrag des ADAC zur Mobilität (Januar 2008), kommt zu diesem Ergebnis
[4] Vgl. S. 4 zu Art. 1, Nr. 1 des vorliegenden Gesetzentwurfs.

tige Gefahr für hochrangige Rechtsgüter, wie Leib oder Leben einer Person, sondern um jede gegenwärtige Gefahr – eingeschränkt lediglich dadurch, dass zusätzlich *die Voraussetzungen für eine Identitätsfeststellung nach § 18 Abs. 2 Nr. 1, 3 oder 5 HSOG vorliegen* müssen. Damit würde der Anwendungsbereich für Kfz-Kennzeichen-Scannings angesichts der Voraussetzungen für eine Identitätsfeststellung wieder unverhältnismäßig ausgedehnt – etwa auf die Suche nach Straftätern oder nach Menschen ohne Aufenthaltstitel (Fahndungstatbestände mit bundesrechtlicher Regelungskompetenz). Mit den in Nr. 1 und 3 verankerten Voraussetzungen dürfte der Kfz-Kennzeichenerhebung dagegen wirkungsvoll begrenzt werden.

Sowohl die Datenerhebung als auch die Datenverarbeitung sollen nach dem Gesetzentwurf ausschließlich Zwecke der Gefahrenabwehr und der Straftatenverhütung verfolgen.

Sinnvoll wäre es, auch noch den Absatz (3) des § 36a Brandenburgisches Polizeigesetz, das der FDP-Fraktion als Vorbild dient, einzufügen: *„Das für Inneres zuständige Mitglied der Landesregierung erstattet dem Ausschuss für Inneres des Landtages jährlich einen Bericht über jede Maßnahme, der Angaben enthält über deren Anlass, Ort und Dauer."*

Die Bürgerrechtsvereinigung *Humanistische Union* (HU) weist zusammen mit dem *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung* (FifF) darauf hin, dass bei der Umsetzung der verfassungsgerichtlichen Vorgaben in der Praxis ein *„alternatives Verfahren bei der rechtlichen und technischen Gestaltung dieser Polizeibefugnis"* Anwendung finden müsste, um die Gefahr polizeilicher Bewegungsprofile *„zumindest für die übergroße Zahl der nicht gespeicherten, in jeder Hinsicht unverdächtigen VerkehrsteilnehmerInnen (das sind 99,7 %) technisch weitgehend auszuschließen"* und datenschutzrechtliche Mindestanforderungen zu gewährleisten. Dazu gehört etwa die sofortige automatische Löschung im Nicht-Trefferfall. Dieses Verfahren wird in der HU-Pressemitteilung vom 6.05.2008 näher beschrieben.[5] Dort heißt es:

> „Wenn kein Treffer erzielt wird, dann wird sowohl das Videobild als auch das erkannte alphanumerische Kennzeichen durch das nächste erfasste Bild bzw. Kennzeichen im Arbeitsspeicher oder falls es dort auch hingelangt ist, auf der Festplatte, überschrieben. Alle Nicht-Treffer werden somit unmittelbar nach erfolgtem Abgleich im lokalen Gerät sicher gelöscht und unbrauchbar gemacht. Eine Übertragung auf andere Medien, andere Geräte oder Systeme wird verlässlich unterbunden."

Um personelle Verantwortlichkeiten festzulegen und um Transparenz und Kontrolle der Maßnahmen zu verbessern, sollten zusätzliche – über den Gesetzentwurf hinausgehende – Anforderungen gesetzlich normiert werden:

- Schriftliche Anordnung der automatisierten Kennzeichenüberwachung nur durch den Behördenleiter; darin müssen der Anlass, die jeweiligen Orte, die Zeitdauer der Maßnahme und der Grund für die Maßnahme genau bezeichnet werden.
- Qualifizierte Dokumentation der Anzahl der kontrollierten Fahrzeuge und der Zahl der Treffer sowie der getroffenen polizeilichen Maßnahmen und deren Erfolg.
- Bericht der Polizei an den Landtag über den Einsatz der Maßnahme und deren Erfolg, mit allen notwendigen Angaben, die für eine parlamentarische Überprüfung/Kontrolle/Evaluation benötigt werden. Der Bericht ist öffentlich zugänglich zu machen.
- Befristung der gesetzlichen Regelung (zwei Jahre) mit der Möglichkeit einer Verlängerung durch Parlamentsbeschluss nach vorheriger unabhängiger wissenschaftlicher Evaluation hinsichtlich Verhältnismäßigkeit, Bürgerrechtsverträglichkeit (Auswirkungen auf effektiven Grundrechtsschutz) und Effizienz.

---

[5] Presseerklärung der Humanistischen Union, Landesverband Baden-Württemberg, vom 06.05.2008: Vorschlag zu einer datenschutzrechtlichen Eindämmung der Befugnis der automatischen Kennzeichenerfassung".

2. Ersatzlose Streichung des Kfz-Kennzeichenscannings

Angesichts der zahlreichen Freiheitsbeschränkungen der letzten Jahre, die im Namen der Sicherheit und Terrorabwehr in Bund und Ländern gesetzlich verankert wurden und die sich zu einem erschreckend hohen Anteil als ganz oder teilweise verfassungswidrig herausgestellt haben, wäre zur Wiederherstellung und Stärkung der Freiheitsrechte der Bürger und Bürgerinnen daran zu denken, diesen *„weiteren Mosaikstein in einer Überwachungsinfrastruktur, die alle möglichen Lebensbereiche betrifft"* (so der Bundesdatenschutzbeauftragte Peter Schaar) zu entfernen und das Kfz-Kennzeichenscanning nicht zu legalisieren – auch nicht in eingeschränkter Form. Damit könnte Hessen etwa dem Weg der Bremer Bürgerschaft folgen, die ihre – ebenfalls grundrechtswidrige – Regelung in § 29 Abs. 6 Bremisches Polizeigesetz ersatzlos gestrichen hat. Begründung im Gesetzentwurf der Regierungsfraktionen SPD und Bündnisgrüne: Es gebe keinen Bedarf an einer Ermächtigung zur automatisierten Kennzeichenerkennung zu Zwecken der Gefahrenabwehr, weshalb eine Nachbesserung der Voraussetzungen verzichtbar und eine Aufhebung der Regelung geboten sei.[6]

Diese einfachere und klarere Lösung ist einer komplizierten und möglicherweise unpraktikablen Regelung vorzuziehen, auch wenn letztere den verfassungsgerichtlichen Vorgaben entsprechen sollte – zumal nicht alles, was verfassungsrechtlich noch zulässig ist, in der Rechtspraxis auch umgesetzt werden muss bzw. sollte. Im Übrigen ist dieses Instrument recht fehleranfällig, wodurch Menschen in falschen Verdacht geraten können – mit zum Teil gravierenden Folgen. Mit einem Verzicht könnte dem Trend eines immer umfangreicheren vorsorglichen maschinellen Abgleichs der Bevölkerung mit polizeilichen Datenbanken entgegengewirkt werden.

Der Einwand, damit sei ein gravierender Sicherheitsverlust verbunden, ist nicht nachvollziehbar, zumal die bisherigen „Erfolge" nicht gerade überzeugend sind. Die Erfahrungen – etwa aus Bayern oder Hessen, wo dieses Instrument ziemlich exzessiv angewandt worden ist –[7] zeigen: Dem Grundrechtseingriff steht mit einer Trefferquote von nur 0,3 Promille ein verschwindend geringer Erfolg gegenüber, wobei es zumeist um fehlende Haftpflichtversicherung oder zu spät entrichtete Versicherungsbeiträge geht und keineswegs etwa um schwerwiegende Gefahren oder Straftaten aus den Bereichen der Organisierten Kriminalität oder des Terrorismus, die es abzuwehren gilt.[8] Nicht zuletzt dieses eklatante Missverhältnis zwischen Aufwand und Ertrag macht die umstrittene Kfz-Überwachung zu einem überflüssigen und damit unverhältnismäßigen Eingriff.

II. PRÄVENTIVE ELEKTRONISCHE WOHNRAUMÜBERWACHUNG (§ 15 HSOG)

Bei der Elektronischen Wohnraumüberwachung – umgangssprachlich: Großer Lauschangriff, evtl. kombiniert mit Großem Spähangriff - handelt es sich um die heimliche elektronisch-

---

[6] Vgl. Bremische Bürgerschaft, Drs. 17/358 v. 17.04.08 – Antrag der Regierungsfraktionen SPD und Bündnis 90/Die Grünen.

[7] Allein in Hessen wurden 2007 über eine Million Kfz-Kennzeichen automatisch gescannt und mit Fahndungsdateien abgeglichen. In Bayern sollen es sogar über 5 Millionen pro Monat gewesen sein. Die „Ausbeute" (Trefferquote") in Hessen lag bei nur 0,3 Promille. Ins Netz gingen der Polizei meist Autobesitzer, die ihre Versicherungsbeiträge nicht oder nicht rechtzeitig bezahlt hatten oder wegen anderer „Bagatellen" (heise-online v. 11.03.2008; Der Spiegel 47/2007, S. 55). In Schleswig-Holstein sind seit August 2007 über 130.000 Autos durch die Überwachung gerollt, 26 Wagen wurden ohne korrekte Versicherung erwischt (taz nord v. 12.3.2008).

[8] So auch die Fraktion Bündnis 90/Die Grünen im Bayerischen Landtag: Gesetzentwurf zur Streichung des Kfz-Kennzeichen-Scannings, LT-Drs. 15/10477; vgl. auch die Tageszeitung v. 12.3.08, S. 2.

akustisch (-visuelle) Ausforschung des nicht öffentlich gesprochenen Wortes und von intimen Lebensvorgängen und –äußerungen aller Art in oder aus einer Wohnung, einem Büro oder Hotelzimmer zum Zwecke der Aufklärung von schwerwiegenden Straftaten (strafprozessual) oder zum Zwecke der Gefahrenabwehr (polizeirechtlich). Damit wird das Recht auf Unverletzlichkeit der Wohnung nach Art. 13 Abs. 1 GG in erheblichem Maße eingeschränkt, wenn nicht gar zeitweise suspendiert.

Bewertung des Gesetzentwurfs und weitergehende Forderungen

1. Bewertung des Gesetzentwurfs

Nach der Rechtsprechung des BVerfG sind in diesem Zusammenhang Regelungen erforderlich, die die Datenerhebung aus dem Kernbereich privater Lebensgestaltung von vornherein verbieten bzw. einen Abbruch der Abhörmaßnahme verlangen, wenn überraschend der Kernbereich berührt wird. Für gleichwohl erhobene Daten bedarf es eines absoluten, gesetzlich verankerten Verwertungsverbots, dessen Einhaltung durch eine unabhängige Stelle überprüft wird. Zudem muss die uneingeschränkte Verpflichtung geregelt werden, die durch eine rechtswidrige Wohnraumüberwachung erhobenen Daten sofort zu löschen, verbunden mit der Dokumentation der rechtswidrig erfolgten Datenerhebung. Diese verfassungsgerichtlichen Vorgaben setzt der Gesetzentwurf der FDP-Fraktion in weiten Teilen um, allerdings noch nicht konsequent genug.

1.1 Es ist zwar konsequent, wenn der Gesetzentwurf der FDP-Fraktion in § 15 Abs. 4 (neu) die Räume der in § 53 Strafprozessordnung genannten Berufsgeheimnisträger von der Überwachungsbefugnis von vornherein ausnimmt. Aber diese Einschränkung reicht insofern nicht, als auch Gespräche mit Berufsgeheimnisträgern außerhalb von deren Geschäftsräumen einem absoluten Schutz unterliegen müssen.

1.2 Die gesetzliche Verankerung eines Erhebungs- bzw. Überwachungsverbots im Falle von Gesprächen aus dem Kernbereich privater Lebensgestaltung, wie es der Gesetzentwurf vorsieht, entspricht den verfassungsgerichtlichen Vorgaben. Ob es allerdings ausreicht, zu regeln, dass die Überwachungsmaßnahme sofort abzubrechen ist, wenn durch die Maßnahme Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist fraglich. Es sollte zumindest gesetzlich klargestellt werden, dass ein Überwachungs- bzw. Erhebungsverbot von vornherein besteht, wenn erkennbar ist, dass die Maßnahme den Kernbereich privater Lebensgestaltung betrifft.

2. Weitergehender Änderungsbedarf/Vorschläge

2.1 ***Verankerung weiterer Begrenzungen in § 15 Abs. 4 HSOG:*** Da es sich bei der elektronischen Wohnraumüberwachung um einen Grundrechtseingriff von höchster Intensität handelt, sollte die Maßnahme noch weiter begrenzt werden, um dem Verfassungsgrundsatz der Verhältnismäßigkeit zu genügen:

a) Zum einen sollte der *Große Spähangriff* ausgeschlossen werden, weil dadurch – vor allem in Kombination mit dem Großen Lauschangriff – praktisch alle Lebens(ent-) äußerungen und Aktionen in der Privat- und Intimsphäre ausgeforscht werden.

b) Zum zweiten sollte die verbleibende akustische Wohnraumüberwachung nur zulässig sein *zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person, wenn Tatsachen die Annahme rechtfertigen, dass sich die Person, der die Gefahr droht oder von der die Gefahr ausgeht, in der Wohnung aufhält, und die Gefahr auf andere Weise nicht abgewendet werden kann.* Damit wäre die Überwachung von anderen Wohnungen weitgehend ausgeschlossen. Es dürfen aus Wohnräumen nur Gespräche abgehört

werden, die der potentielle Straftäter führt, da sich nur aus solchen Gesprächen Informationen gewinnen lassen, die die Gefahr der Begehung der Tat abwenden können.

c) Zum dritten sind alle Vorkehrungen zu treffen, um den jederzeitigen Abbruch der Überwachungsmaßnahme zu ermöglichen. Bei in einer fremden Sprache geführten Gesprächen ist dies durch die Anwesenheit eines Dolmetschers zu gewährleisten.

2.2 ***Berufsgeheimnisträger und ihre Hilfspersonen:*** Erforderlich ist darüber hinaus eine Erweiterung des Erhebungsverbots auf die in § 53a StPO genannten Hilfspersonen, soweit mit ihnen Gespräche geführt werden, die dem Kernbereich zuzuordnen sind. Zudem ist, wie oben bereits erwähnt, die Beschränkung des Schutzes auf die Wohnungen bzw. Geschäftsräume der Berufsgeheimnisträger problematisch; die Gespräche müssen in gleicher Weise geschützt werden, wenn sie in anderen Wohnungen, etwa in der Wohnung der Zielperson selbst, stattfinden; d.h. eine Überwachung von Gesprächen mit Berufsgeheimnisträgern ist prinzipiell für unzulässig zu erklären.

2.3 ***Die Höchstdauer*** einer richterlich angeordneten Überwachungsmaßnahme in § 15 Abs. 5 HSOG sollte unbedingt von drei Monaten auf einen Monat bzw. vier Wochen verkürzt werden; eine Verlängerung sollte lediglich einmal um höchstens weitere vier Wochen möglich sein. Denn mit zunehmender Dauer steigt die Eingriffstiefe des Lauschangriffs oder einer sonstigen geheimen Überwachungsmaßnahme in die Rechte sämtlicher Betroffenen, da sich immer mehr ein ganzheitliches Bild über ihre Lebensgewohnheiten und -äußerungen ergibt. Im Übrigen geht es um die Abwehr einer gegenwärtigen Gefahr, so dass eine längere Frist damit nicht vereinbar wäre.

2.4 ***Die richterlichen Prüfungs- und Begründungsanforderungen*** sollten erhöht werden, besonders im Falle einer Verlängerung der Überwachungsmaßnahme. Der Richtervorbehalt für die Wohnraumüberwachung zu Zwecken der Gefahrenabwehr dient (wie der zum Zweck der Strafverfolgung) der vorbeugenden Rechtskontrolle; er kann der Aufgabe einer verstärkten Sicherung des Grundrechts aus Artikel 13 Abs. 1 GG nur gerecht werden, wenn die richterliche Entscheidung Angaben zu Art, Umfang (auch räumliche Begrenzung) und Dauer der Maßnahme enthält und in nachvollziehbarer Weise unter Angabe der maßgeblichen Erwägungen begründet wird. Darüber hinaus sollte auch eine **richterliche Verlaufs- und Erfolgskontrolle** gesetzlich verankert werden. Der/die Richter/in (oder die Kammer) sollte konsequenterweise auch die Befugnis zum jederzeitigen Abbruch der Überwachungsmaßnahme sowie zur Löschung der dem Verwertungsverbot unterliegenden Informationen erhalten, inklusive Dokumentation der Rechtswidrigkeit der Datenerhebung. Das Bundesverfassungsgericht hat dem anordnenden Gericht auch die Verpflichtung auferlegt, den Abbruch der Maßnahme anzuordnen, wenn sie fortgesetzt wird, obwohl die gesetzlichen oder in der Anordnung festgelegten Voraussetzungen fehlen.[9] Dies ist nur möglich, wenn den die Maßnahme durchführenden Stellen eine in bestimmten Abständen durchzuführende Unterrichtung des Gerichts aufgegeben wird.

2.5 ***Verwertungsverbot und Löschgebot bei Gefahr-im-Verzug-Anordnung:*** Falls die Anordnung gemäß § 15 Abs. 5 S. 8 nicht binnen drei Tagen richterlich bestätigt wird und außer Kraft tritt, sind die bis dahin gewonnenen Erkenntnisse sofort zu löschen; sie unterliegen einem Verwertungsverbot.

2.6 ***Benachrichtigung der Betroffenen:*** Nach § 29 Abs. 6 HSOG sind Betroffene von verdeckten Polizeimaßnahmen nach Abschluss der Maßnahmen auch ohne deren Antrag zu unterrichten. Betroffen sind die Personen, gegen die sich die Maßnahme gerichtet hat, deren Gesprächspartner sowie der Inhaber einer Wohnung in den Fällen des § 15 Abs. 4.

---

[9] Vgl. BVerfG 2004, NJW 2004, 999, 1015.

Allerdings gibt es weitreichende Ausnahmen: *„Die Unterrichtung unterbleibt, soweit dies im überwiegenden Interesse der Person liegt, gegen die sich die Maßnahme gerichtet hat, oder wenn die Ermittlung der betroffenen Person oder deren Anschrift einen unverhältnismäßigen Verwaltungsaufwand erfordern würde. Eine Unterrichtung unterbleibt ferner, solange sie den Zweck der Maßnahme, ein sich an den auslösenden Sachverhalt anschließendes strafrechtliches Ermittlungsverfahren oder Leib, Leben oder Freiheit einer Person gefährden würde."*

Diese Ausnahmen dürften im Fall der präventiven Wohnraumüberwachung zu weit gehen. Das Bundesverfassungsgericht hat in seinem Urteil aus 2004 zum Großen Lauschangriff festgestellt,[10] dass den von der heimlichen Wohnraumüberwachung betroffenen Grundrechtsträgern grundsätzlich ein Anspruch auf nachträgliche Unterrichtung über Anordnung und Durchführung der Maßnahme zustehe; dies ergebe sich aus Artikel 13 Abs. 1 GG in Verbindung mit dem Erfordernis eines effektiven gerichtlichen Rechtsschutzes nach Artikel 19 Abs. 4 GG. Die Begrenzung der Mitteilungspflicht stelle ihrerseits einen Eingriff in die Grundrechte aus Artikel 13 Abs. 1 und Artikel 19 Abs. 4 GG dar, bedürfe einer Rechtfertigung und müsse den Anforderungen der Verhältnismäßigkeit genügen. Eine Zurückstellung sei auf das unbedingt Erforderliche zu beschränken.

Grundsätzliche Überlegung zur präventiven elektronischen Wohnraumüberwachung

Die elektronische Wohnraumüberwachung in ihrer Ausprägung als Lausch- und Spähangriff lässt von dem unantastbaren Kernbereich des Art. 13 GG kaum noch etwas übrig. Sie berührt die Privatheit in allerhöchstem Maße und belässt die einzelnen Betroffenen – zu einem überwiegenden Teil unbeteiligte, unverdächtige, unschuldige Personen – nicht mehr ihre verfassungsrechtlich garantierte Möglichkeit zum privaten Rückzug.

„Der große Lauschangriff berührt ein sich dramatisch verknappendes persönliches und gesellschaftliches Gut, die Privatheit, in ihren letzten Refugien und damit höchste verfassungsrechtliche Maßstäbe", stellten bereits 2004 sieben Landesdatenschutzbeauftragte fest und sie fragen: *„Was kann vom Wesensgehalt des Art. 13 GG noch übrig bleiben, wenn sämtliche Lebensäußerungen in der ‚unverletzlichen' Wohnung staatlich belauscht werden können, weil sich ‚vermutlich' ein Beschuldigter in ihr aufhält?"*

Der Lausch- (und Späh-) Angriff dringt noch tiefer als die anderen polizeilichen Instrumente in die Privatsphäre ein; er muss daher, will man ihn überhaupt zulassen, gegenüber jenen wirksam als Ultima-Ratio-Maßnahme ausgestaltet werden – was in besonderem Maße für Eingriffe in Wohnungen Unbeteiligter gilt. Denn betroffen werden durch diesen Eingriff als "unvermeidbar betroffene Dritte" vor allem eine Vielzahl Unbeteiligter - alle unverdächtigen Gesprächspartner des Verdächtigen oder in den Räumen anwesende andere Personen -, die mit einer Überwachung ihrer Gespräche und Handlungen gar nicht rechnen. Potentielle „Terroristen" oder „Organisierte Kriminelle" werden sich der Überwachung auf unterschiedlichste Weise und unter Nutzung aller, auch kostspieliger Möglichkeiten entziehen können.

Angesichts dieser tiefgreifenden staatlichen Eingriffsmöglichkeiten sind an den Verfassungsgrundsatz der Verhältnismäßigkeit besondere Anforderungen zu stellen. Doch die Erforderlichkeit der elektronischen Wohnraumüberwachung zur Gefahrenabwehr ist bisher in keinem Bundesland und im Besonderen in Hessen nicht überzeugend belegt worden. Es gibt m.E. keine unabhängige und kritische Evaluation bzw. Tatsachenanalyse der bisherigen Erfahrungen – gerade auch nicht zu der Frage, ob das eingesetzte Mittel mit seiner gravierenden Eingriffstiefe überhaupt in einem angemessenen Verhältnis zu dem jeweils erreichten Zweck der Gefahrenabwehr steht. Wenn das in der Rechtspraxis jedoch nicht der Fall sein sollte, dann

[10] Vgl. BVerfG, NJW 2004, 999, 1015 f.

wäre der Große Lausch- und Spähangriff zum Zwecke der Gefahrenabwehr insgesamt nicht verhältnismäßig und deshalb verfassungswidrig. Als reines Vorratsgesetz für alle Fälle ließe sich diese Norm nicht aufrecht erhalten.

III. PRÄVENTIVE TELEKOMMUNIKATIONSÜBERWACHUNG (§ 15a HSOG)

Bewertung des Gesetzentwurfs und weitergehende Anforderungen/Vorschläge

1. Nach dem in § 15a neu einzufügenden Absatz 4 des vorliegenden Gesetzentwurfs

- sind die Überwachungsmaßnahmen sofort abzubrechen, wenn erkennbar wird, dass durch die Maßnahmen Erkenntnisse aus dem absolut geschützten Kernbereich privater Lebensgestaltung erlangt werden.
- Außerdem sollen die in § 53 Strafprozessordnung genannten Berufsgeheimnisträger vor der präventiven TKÜ geschützt werden. Dazu gehören u.a. Geistliche, Strafverteidiger, Rechtsanwälte, Patentanwälte, Notare, Wirtschaftsprüfer, Steuerberater, Ärzte, Psychotherapeuten, Apotheker, Drogenberater, Mitglieder der Parlamente, Redakteure und Journalisten.

2. Diese Regelungen sind zwar absolut notwendig, greifen aber noch zu kurz. Um der jüngeren Rechtsprechung des Bundesverfassungsgerichts zur Konkretisierung des Menschenwürdeschutzes durch die Unantastbarkeit der Kernbereiche des Wohnungs- und des Telekommunikations-Grundrechts zu genügen, müsste die Regelung zumindest wie folgt ergänzt werden:[11]

- Es sind alle Vorkehrungen zu treffen, um den jederzeitigen Abbruch der Überwachungsmaßnahme zu ermöglichen. Bei in ausländischer Sprache geführten Telefonaten ist dies durch die Anwesenheit eines Dolmetschers zu gewährleisten.
- Für Telekommunikationsverbindungen und Gespräche mit Vertrauenspersonen gilt eine Vermutung, dass diese Kontakte und die Gesprächsinhalte zum Kernbereich privater Lebensgestaltung gehören. Etwas anderes gilt, wenn der Straftatverdacht auch gegen die Vertrauensperson des Verdächtigen besteht, soweit der Gesprächsinhalt nicht den Kernbereich betrifft.
- Auch bei erkennbaren Telekommunikationskontakten dritter Personen untereinander hat die Überwachung von vornherein zu unterbleiben.
- Ergibt sich erst im Gesprächsverlauf, dass ein Bezug zum Beschuldigten nicht besteht oder dass der Kernbereich privater Lebensgestaltung betroffen ist, ist die weitere Überwachung sofort einzustellen. Die bis dahin erfolgten Aufzeichnungen und erlangten Informationen sind unverzüglich zu löschen und unterliegen einem absoluten Verwertungsverbot; die Rechtswidrigkeit der Datenerhebung ist zu dokumentieren.

IV. PRÄVENTIVE RASTERFAHNDUNG (§ 26 HSOG)

Die Rasterfahndung ist eine besondere polizeiliche „Fahndungsmethode" unter Nutzung der elektronischen Datenverarbeitung. Unter Rasterfahndung versteht man den automatisierten, also maschinellen Abgleich personenbezogener Daten aus dem polizeilichen Fahndungsbestand mit personenbezogenen Daten aus fremden Dateien anderer öffentlicher und privater Stellen, die ursprünglich für ganz andere Zwecke erhoben worden sind (also entgegen dem Zweckbindungsprinzip des Datenschutzrechts).

---

[11] Vgl. dazu LG Ulm, Beschl. Vom 19.04.2004 – 1 Qs 1036/04 und Anmerkung von Roggan.

Die Rasterfahndung ist ein Massengrundrechtseingriff in die informationelle Selbstbestimmung von erheblichem Gewicht, der für die Betroffenen zumeist unbemerkt stattfindet. Bei der präventiven Rasterfahndung richtet sich der polizeiliche Eingriff nicht gegen einzelne Tatverdächtige, Polizeipflichtige/Störer oder potentielle Täter, sondern Objekte der polizeilichen Aktivität werden alle Personen, die Träger gleicher persönlicher Merkmale entsprechend einem zuvor festgelegten Suchraster sind, nach denen „gefahndet" wird.

Konsequenzen des Gesetzgebers aus dem BVerfG-Urteil

Der vorliegende Gesetzentwurf der FDP-Fraktion versucht, mit einer Neufassung des § 26 Abs. 1 S. 1 geeignete Konsequenzen aus dem Urteil des Bundesverfassungsgerichts in Sachen Rasterfahndung zu ziehen. Danach sollen künftig Polizeibehörden des Landes von öffentlichen Stellen oder Stellen außerhalb des öffentlichen Bereichs die Übermittlung von personenbezogenen Daten bestimmter Personengruppen zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen dürfen – aber nur

- *„zur Abwehr einer konkreten Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind..." und*
- *„wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Abwehr der Gefahr erforderlich und dies auf andere Weise nicht möglich ist".*

Fazit: Bewertung und weitergehende Vorschläge

Mit diesen Tatbestandsvoraussetzungen wird klargestellt, dass die präventive Rasterfahndung keine bloße Vorfeldmaßnahme ist, nicht zur allgemeinen Gefahrenvorsorge und auch nicht zur Verhütung möglicher „Straftaten von erheblicher Bedeutung" zulässig ist. Es wird klargestellt, dass eine allgemeine Bedrohungslage als Tatbestandsvoraussetzung nicht reicht. Dadurch wird die präventiv-polizeiliche Rasterfahndung wieder so weit eingegrenzt, dass sie den eingrenzenden Vorgaben des Bundesverfassungsgerichts entspricht.

Dennoch sollte im Gesetz noch ein ***Richtervorbehalt*** verankert werden, das heißt, die Anordnung der Maßnahme sollte durch den zuständigen Richter erfolgen, um eine unabhängige Vorkontrolle und möglichst auch eine Verlaufs- und Erfolgskontrolle zu gewährleisten. Etliche Polizeigesetze der Länder sahen ursprünglich eine solche gerichtliche Vorabkontrolle durch den Amtsrichter deshalb vor, weil es im Zuge von Rasterfahndungen zu schwerwiegenden Eingriffen in Grundrechtspositionen einer Vielzahl von Personen kommt, die unverdächtig sind. Die richterliche Anordnung sollte als Korrektiv dienen und verbunden sein mit einer richterlichen Verlaufs- und Erfolgskontrolle.

Verzicht auf präventive Rasterfahndung mangels Zwecktauglichkeit

Es stellt sich unter dem Aspekt der Verhältnismäßigkeit aber die Frage, ob die präventive Rasterfahndung zur Abwehr konkreter Gefahren überhaupt tauglich und damit als geeignetes Mittel anzusehen ist. So stellt das BVerfG in seiner Rasterfahndungsentscheidung fest: Die gegenwärtige Gefahr als Tatbestandsvoraussetzung führe angesichts des mit der Maßnahme verbundenen zeitlichen und technischen Aufwands bereits dazu, dass diese in den meisten Fällen zu spät kommen wird, um noch wirksam sein zu können.[12] Wie sich dies angesichts einer konkreten Gefahr als Tatbestandsvoraussetzung darstellt, wäre zu überprüfen. Als *konkrete Gefahr* wird, wie bereits erwähnt, eine Sachlage bezeichnet, welche bei ungehindertem Geschehensablauf und in überschaubarer Zukunft mit hinreichender Wahrscheinlichkeit zu ei-

[12] BVerfG, NJW 2006, 1939 (1947).

nem Schaden an einem polizeilich zu schützenden Rechtsgut führen wird.[13] Damit kann es in vielen Fällen dazu kommen, dass die Zwecktauglichkeit zum Zeitpunkt der Anordnung einer Rasterfahndung nicht hinreichend prognostiziert werden kann. In etlichen Fällen dürfte von vornherein klar sein, dass der zu treibende Aufwand zu viel Zeit erfordern wird, um rechtzeitig ein Ergebnis zu erzielen und das schädigende Ereignis noch aufhalten zu können. Und nur in wenigen Fällen – etwa bei einer wochenlangen Geiselnahme - dürfte genügend Zeit bleiben, um die Rasterfahndung durchzuführen und das Ergebnis abzuwarten. Alles in allem schrumpft damit das Feld der Anwendbarkeit dieser präventiv-polizeilichen Methode enorm zusammen.[14]

Auch der hessische Innenminister Bouffier (CDU) äußerte Zweifel, ob eine Rasterfahndung überhaupt noch durchführbar sei, wenn sie nur zur Abwehr konkreter Gefahren zulässig ist.[15] Und die NRW-Datenschutzbeauftragte Bettina Sokol hatte bereits 1999 die Auffassung vertreten, dass kaum Fälle denkbar seien, in denen eine Rasterfahndung für Zwecke der Gefahrenabwehr in Betracht kommen könnten. Wenn eine derartige (konkrete) Gefahr gegeben sei, dann käme die relativ langwierige und schwerfällige Rasterfahndung zur Gefahrenabwehr regelmäßig zu spät. Die im Polizeigesetz verankerte Rasterfahndung wäre demnach ein stumpfes Schwert.[16]

Angesichts der schwerwiegenden Beeinträchtigung der informationellen Selbstbestimmung einer Vielzahl von Unverdächtigen dürfte die präventiv-polizeiliche Rasterfahndung in der überwiegenden Zahl der Fälle auch außer Verhältnis zur Bedeutung der Sache bzw. der abzuwehrenden Gefahr stehen und damit dem Übermaßverbot widersprechen. Darauf deutet auch die flächendeckende Erfolglosigkeit der bundesweiten Rasterfahndungen nach „islamistischen Schläfern" hin. Trotz des gewaltigen Aufwands, der mit den Rasterfahndungen 2002 und 2003 betrieben worden war, verfing sich kein einziger terroristischer „Schläfer" im elektronischen Netz, lediglich einige vage Verdächtige, mutmaßliche Sozialhilfebetrüger, Schleuser und Schwarzarbeiter blieben hängen. Der einzige konkrete Verdacht auf islamistisch motivierte Terroranschläge, der sich ergeben hatte, stellte sich nach einer polizeilichen Durchsuchung von sechs Wohnungen und einer Buchhandlung in Hamburg weitgehend als Flop heraus. Sieben Männer aus Marokko, Afghanistan und Ägypten wurden von der Bundesanwaltschaft verdächtigt, eine terroristische Vereinigung gebildet zu haben. Nur gegen einen von ihnen ist ein Ermittlungsverfahren wegen des Verdachts der Unterstützung der Terrorgruppe um Atta eingeleitet, später aber wieder eingestellt worden.[17]

Alle in der Zeit nach diesen Rasterfahndungen bekannt gewordenen Verdachtsfälle und Festnahmen gingen auf konventionelle Fahndungsmethoden zurück. Da stellt sich tatsächlich die Frage, ob der gewaltige Aufwand mitsamt den damit verbundenen Grundrechtseingriffen noch in einem vernünftigen Verhältnis zur Effizienz dieser Maßnahmen steht. Ein Verlust an Sicherheit wäre also kaum zu befürchten, wenn dieses Instrument im Polizeigesetz nicht mehr zu Verfügung stünde.[18]

Hinter vorgehaltener Hand wird von Sicherheitsbehörden durchaus eingestanden, dass mit dem Aufwirbeln der Datenbestände tatsächlich weniger auf die Enttarnung potentieller Täter

---

[13] Vgl. § 1 PolG NRW, § 1 PolG BaWü, § 1 Nds. SOG

[14] Roggan, Der Verhältnismäßigkeitsgrundsatz als Raster des Rechtsstaats -- Zur Verfassungsmäßigkeit der Rasterfahndungen im Landesverwaltungsgesetz, in: Brenneisen u.a. (Hg.), Polizeirechtsreform in Schleswig-Holstein, München u.a., S. 295.

[15] Stellungnahme von 23.05.2006.

[16] Sokol, in: Bäumler, Polizei und Datenschutz, 1999, S. S. 192 f.

[17] Vgl. taz 4.07.02, 29.09.02.

[18] So auch Roggan, Der Verhältnismäßigkeitsgrundsatz als Raster des Rechtsstaats, a.a.O., S. 298.

abgezielt worden sei – was der Bevölkerung aber weis gemacht worden ist -, als vielmehr auf die Erhöhung des Fahndungsdrucks, um potentielle „islamistische Extremisten" zu verunsichern.[19] Das Bundeskriminalamt behauptet, dass es den Polizeibehörden der Länder und des Bundes gelungen sei, aus einer Vielzahl von Daten Personen herauszufiltern, die „der islamistischen Szene zuzuordnen" seien – dafür hätten allerdings die Rasterfahndungen von vornherein nicht durchgeführt werden dürfen. Dass die Maßnahme zur Enttarnung potentieller islamistischer Terroristen geführt hat, ist dieser Stellungnahme an das Bundesverfassungsgericht nicht zu entnehmen.[20]

V. Weitergehender gesetzgeberischer Handlungsbedarf

Über die im Gesetzentwurf der FDP-Fraktion aufgenommenen Punkte hinaus bedarf das hessische Polizeigesetz noch weiterer Änderungen. Beispiel:

So sind etwa die ***Zeugnisverweigerungsrechte*** nicht nur durch das präventive Abhören der Telekommunikation oder durch die elektronische Wohnraumüberwachung gefährdet, sondern auch *durch andere heimliche Ermittlungsmethoden der Polizei*, die in den vergangenen Jahren eingeführt worden sind. So könnte beispielsweise durch einen in eine Wohnung, eine Anwaltskanzlei, Arztpraxis oder Redaktion eingeschleusten *V-Mann* das Zeugnisverweigerungsrecht der dort tätigen Personen umgangen werden.

Nach § 16 Abs. 4 HSOG dürfen *Verdeckte Ermittler der Polizei „unter ihrer Legende mit Einwilligung der berechtigten Person deren Wohnung betreten"*. Auch hier kann es schnell dazu kommen, dass der Kernbereich der privaten Lebensgestaltung oder Berufsgeheimnisse tangiert sind und verletzt werden – ohne dass es bislang ausreichende Vorkehrungen gibt, dies zu vermeiden.

Eine wirksame Gewährleistung des Schutzes der Zeugnisverweigerungsberechtigten und des Kernbereichs privater Lebensgestaltung ist bei allen verdeckten Eingriffen verfassungsrechtlich geboten und entsprechend gesetzlich zu verankern.

Bremen, den 14. August 2008 *gez. RA Dr. Rolf Gössner*

Dr. jur. Rolf Gössner, Rechtsanwalt, Publizist und Vizepräsident der *„Internationalen Liga für Menschenrechte"* (Berlin), seit 2007 stellv. Richter am *Staatsgerichtshof der Freien Hansestadt Bremen* sowie Mitglied und stellv. Sprecher der *Deputation für Inneres* in der Bremer Bürgerschaft. Sachverständiger in Gesetzgebungsverfahren von Bundestag und Landtagen. Mitherausgeber des jährlich erscheinenden *„Grundrechte-Reports" (Fischer-Verlag)*. Autor zahlreicher Sachbücher zu „Innerer Sicherheit" und Bürgerrechten, zuletzt: >*Menschenrechte in Zeiten des Terrors. Kollateralschäden an der „Heimatfront"*<, Hamburg 2007.

[19] So u.a. das Bayer. Staatsministerium des Innern in seiner Antwort v. 11.4.02, S. 5 (LT-Drs. 14/9221).
[20] BVerfGE, 1 BvR 518/02 vom 4.4.2006, A. I. Nr. 64