

Berlin, im November 2010  
Stellungnahme Nr. 69/2010

abrufbar unter  
[www.anwaltverein.de](http://www.anwaltverein.de)

## **Stellungnahme des Deutschen Anwaltvereins**

**durch den Ausschuss Gefahrenabwehrrecht**

**zum**

**Gesetzesentwurf der Landesregierung**

**zur Änderung des Polizei- und Ordnungsbehördengesetzes**

**Rheinland-Pfalz (LT-Drs. 15/4879)**

Mitglieder des Ausschusses Gefahrenabwehrrecht:

Rechtsanwältin Dr. Heide Sandkuhl, Potsdam (Vorsitzende u. Berichterstatterin)  
Rechtsanwalt Wilhelm Achelpöehler, Münster (Berichterstatter)  
Rechtsanwalt Prof. Dr. Matthias Dombert, Potsdam  
Rechtsanwalt Prof. Dr. Rainer Hamm, Frankfurt am Main  
Rechtsanwalt Sönke Hilbrans, Berlin  
Rechtsanwalt Dr. Stefan König, Berlin  
Rechtsanwältin Dr. Regina Michalke, Frankfurt am Main (Berichterstatterin)  
Rechtsanwältin Kerstin Oetjen, Freiburg

Zuständiger DAV-Geschäftsführer:

Rechtsanwalt Franz Peter Altemeier

Verteiler:

- Bundeskanzleramt
- Bundesministerium des Innern
- Bundesministerium der Justiz
  
- Bundesrat
- Deutscher Bundestag - Rechtsausschuss
- Deutscher Bundestag - Innenausschuss
  
- Arbeitsgruppen Inneres der im Deutschen Bundestag vertretenen Parteien
- Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien
  
- Justizministerien der Länder
- Landesministerien und Senatsverwaltungen des Innern
- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
- Landesdatenschutzbeauftragte
- Innenausschüsse der Landtage
- Rechtsausschüsse der Landtage
  
- Bundesrechtsanwaltskammer
- Deutscher Richterbund
- Bundesverband der Freien Berufe
- Gewerkschaft der Polizei (Bundesvorstand)
- Deutsche Polizeigewerkschaft im DBB
- Verd.di, Recht und Politik
  
- Vorstand und Landesverbände des DAV
- Vorsitzende der Gesetzgebungs- und Geschäftsführenden Ausschüsse des DAV
- Vorsitzende des FORUM Junge Anwaltschaft des DAV
  
- Frankfurter Allgemeine Zeitung
- Süddeutsche Zeitung
- Berliner Zeitung

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit ca. 68.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

---

#### **A. Übersicht und Zusammenfassung:**

Die Landesregierung Rheinland-Pfalz hat einen Gesetzesentwurf zur Änderung des Polizei- und Ordnungsbehördengesetzes mit dem Ziel vorgelegt, „ein modernes und effizientes Polizei- und Ordnungsbehördengesetz zu schaffen“<sup>1</sup>. Der Gesetzesentwurf nimmt für sich in Anspruch, Folgerungen aus aktuellen Entscheidungen des Bundesverfassungsgerichtes zum Gefahrenabwehrrecht umzusetzen und unter Berücksichtigung der rechtsstaatlichen Grundsätze vor allem die erforderlichen polizeilichen Befugnisse zu schaffen oder bestehende Ermächtigungen anzupassen<sup>2</sup>. Nach dem Entwurf soll die Polizei unter anderem zum verdeckten Zugriff auf informationstechnische Systeme (sogenannte Online-Durchsuchung) ermächtigt werden. Das Land Rheinland-Pfalz wäre damit das erste Bundesland, das nach Inkrafttreten des BKA-Gesetzes zum 1. Januar 2009 die Online-Durchsuchung einführt.

Aus der Begründung des Gesetzesentwurfes geht hervor, dass die Landesregierung in der Tat bemüht war, zahlreiche Entscheidungen des Bundesverfassungsgerichts, insbesondere zum niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung (NdsSOG)<sup>3</sup>, zur Rasterfahndung<sup>4</sup>, zum automatisierten Kfz-Kennzeichenabgleich<sup>5</sup>, zur Online-Durchsuchung<sup>6</sup> und zur Vorratsdatenspeicherung<sup>7</sup> zu berücksichtigen und die vom Bundesverfassungsgericht postulierten verfassungsrechtlichen Vorgaben umzusetzen. Dass dies jedoch nicht immer gelungen ist, wird – beispielhaft genannt – an den Befugnissen der Polizei zum verdeckten Zugriff auf informationstechnische Systeme (§ 31 c E-POG) und zur Rasterfahndung (§ 38 E-POG) ebenso deutlich wie an der Regelung des § 39 a E-POG, der den Schutz des Kernbereichs privater Lebensgestaltung für verdeckte Maßnahmen der Datenerhebung regelt.

---

<sup>1</sup> LT-Drs. 15/4879, S. 1.

<sup>2</sup> Ebenda.

<sup>3</sup> U. v. 27. Juli 2005 (1 BvR 668/04).

<sup>4</sup> B. v. 4. April 2006 (1 BvR 518/02).

<sup>5</sup> U. v. 11. März 2008 (1 BvR 2074/05, 1 BvR 1254/07).

<sup>6</sup> U. v. 27. Februar 2008 (1 BvR 370/07, 1 BvR 595/07).

<sup>7</sup> U. v. 2. März 2010 (1 BvR 256/08).

Zu begrüßen ist aber, dass der Entwurf den Schutz zeugnisverweigerungsberechtigter Berufsheimnisträger gemäß § 51 Abs. 1 und § 53 a Abs. 1 StPO ausnahmslos gewährleistet, den automatisierten Kfz-Kennzeichnungsabgleich abschafft, die Online-Durchsuchung der parlamentarischen Kontrolle unterstellt und eine Verpflichtung zur Evaluation der Wohnraumüberwachung (§ 29 E-POG), Telekommunikationsüberwachung (§ 31 E-POG), Auskunft über Nutzungsdaten (§ 31 b E-POG), Online-Überwachung (§ 31 c E-POG), Funkzellenabfrage (§ 31 e E-POG) und der Rasterfahndung (§ 38 E-POG) bestimmt sowie die Landesregierung verpflichtet, ihren Bericht unter Mitwirkung einer Stelle, die eine wissenschaftlich fundierte Überprüfung der Maßnahmen gewährleistet, anzufertigen (§ 100 Abs. 2 E-POG).

## **B. Einzelne Regelungen:**

### **I. Schutz zeugnisverweigerungsberechtigter Personen, § 39 b E-POG**

Anders als § 20 u BKA-G regelt § 39 b Abs. 1 S. 1 E-POG, dass verdeckte Datenerhebungen in einem durch ein Berufsgeheimnis geschützten Vertrauensverhältnis im Sinne des § 53 Abs. 1 und des § 53 a Abs. 1 StPO unzulässig sind. S. 3 dieser Vorschrift regelt ein gesetzliches Verwertungsverbot, S. 2 bestimmt, dass dennoch erlangte Daten unverzüglich zu löschen sind.

Soweit es um offene Ermittlungen, mithin um die Befragung und Auskunftspflicht geht, regelt § 9 a Abs. 3 S. 3 E-POG korrespondierend, dass eine in § 53 Abs. 1 oder § 53 a Abs. 1 StPO genannte Person auch in den Fällen des § 9 a Abs. 3 S. 2 E-POG zur Verweigerung der Auskunft berechtigt ist. Für andere Personen als Berufsheimnisträger gilt dies nicht. Diese sind auch nicht unter den in den §§ 52, 55 StPO genannten Voraussetzungen zur Weigerung der Auskunft berechtigt, soweit die Auskunft zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person unerlässlich ist.

1. Der ausnahmslose Schutz der Berufsheimnisträger (§§ 53 Abs. 1, 53 a Abs. 1 StPO) ist zu begrüßen. Hiermit wird eine Forderung erfüllt, die der DAV bereits in seiner Stellungnahme zum Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung anderer verdeckter Ermittlungsmaßnahmen und zur Umsetzung der Richtlinie 2006/24/EG<sup>8</sup> sowie in der Stellungnahme zum Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das

---

<sup>8</sup> DAV-Stellungnahme Nr. 41/2007.

Bundeskriminalamt vom 13. August 2008<sup>9</sup> und nicht zuletzt mit (ergänzender) Stellungnahme zum Referentenentwurf eines Gesetzes zur Stärkung des Schutzes von Vertrauensverhältnissen zu Rechtsanwälten im Straf- und Prozessrecht<sup>10</sup> erhoben hatte.

2. Problematisch und im Ergebnis unter dem Aspekt des Art. 4 GG nicht hinzunehmen ist jedoch die Diskriminierung der Geistlichen, die keinen öffentlich-rechtlichen Religionsgemeinschaften angehören. Nach der Begründung des Gesetzesentwurfes sollen von dem Zeugnisverweigerungsrecht nur Geistliche der öffentlich-rechtlichen Religionsgemeinschaften erfasst werden, und dies auch nur insoweit, als sie im konkreten Fall seelsorgerisch tätig werden<sup>11</sup>. Eine solche Differenzierung aber ist im Grundgesetz nicht angelegt. Grund des besonderen Schutzes seelsorgerischer Tätigkeit ist vielmehr das besondere Vertrauensverhältnis zwischen Geistlichem und Gläubigem, ohne das eine seelsorgerische Beratung oder eine Beichte nicht denkbar ist<sup>12</sup>. Dass der Staat sich einer besonderen Verfassungstreue des Seelsorgers sicher sein kann, ist nicht Grund des besonderen Schutzes seelsorgerischer Tätigkeit. Grund ist ausschließlich das Vertrauensverhältnis zwischen Geistlichem und Gläubigem. Dies hat der Bundesgerichtshof nicht zuletzt mit Entscheidung vom 15. April 2010<sup>13</sup> ausdrücklich klargestellt.

## **II. Befragung und Auskunftspflicht, § 9 a E-POG**

Gemäß § 9 a Abs. 1 S. 1 und § 9 a POG können die allgemeinen Ordnungsbehörden und die Polizei jede Person befragen, wenn anzunehmen ist, dass sie sachdienliche Angaben machen kann, die für die Erfüllung einer bestimmten ordnungsbehördlichen oder polizeilichen Aufgabe erforderlich sind.

Während nach § 9 a Abs. 3 S. 1 POG die betroffene Person zur Weigerung der Auskunft unter den in den §§ 52 bis 55 StPO genannten Voraussetzungen berechtigt ist, soll dies nach § 9 a Abs. 3 S. 2 E-POG nicht gelten, soweit die Auskunft zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person unerlässlich ist. Ausweislich der Gesetzesbegründung mache es eine Güteabwägung in diesen Fällen erforderlich, dem Schutz hochrangiger Rechtsgüter im Interesse einer effektiven Gefahrenabwehr grundsätzlich Vorrang vor dem Interesse des Einzelnen auf Auskunftsverweigerung einzuräumen.

---

<sup>9</sup> DAV-Stellungnahme Nr. 49/2008.

<sup>10</sup> DAV-Stellungnahme Nr. 16/2010.

<sup>11</sup> LT-Drs 15/4879, S. 23.

<sup>12</sup> *Baum/Schantz* ZRP 2008, 137, 139 m. w. N..

<sup>13</sup> U. v. 15. April 2010, 4 StR 650/09.

Die „Rückausnahme“ für die nach §§ 52, 55 StPO Zeugnis- und Auskunftsverweigerungsberechtigten führt dazu, dass der Auskunftspflichtige auch solche Auskünfte erteilen muss, die ihn selbst oder nahe Angehörige in strafrechtlicher Hinsicht belasten. Damit die Selbstbezeichnung das Persönlichkeitsrecht des Auskunftspflichtigen nicht unverhältnismäßig beeinträchtigt<sup>14</sup>, muss sichergestellt sein, dass wegen des offenbaren Sachverhalts kein Strafverfahren gegen den Auskunftspflichtigen oder nahe Angehörige eingeleitet wird. Fehlt eine solche Schutzvorkehrung, wäre die Auskunftsverpflichtung zur Zweckerreichung ungeeignet, also wiederum unverhältnismäßig. Denn nur ein Verfolgungsverbot gewährleistet, dass der zur Auskunft Verpflichtete auch wahrheitsgemäße Mitteilungen machen und auf diese Weise zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person beitragen wird. Das in § 9 Abs. 3 S. 5 E-POG geregelte Verwendungsverbot – hiernach dürfen Auskünfte, die gemäß S. 2 erlangt werden, nur für den dort bezeichneten Zweck verwendet werden – wird vorstehenden Maßgaben nur gerecht, wenn es als **Strafverfolgungshindernis** respektive eine den Ermittlungen entgegenstehende landesgesetzliche Verwendungsregelung im Sinne des § 160 Abs. 4 StPO verstanden wird. Dies muss klargestellt werden.

### III. Aufgaben der allgemeinen Ordnungsbehörden und der Polizei, § 1 Abs. 7 E-POG

Nach § 1 Abs. 7 E-POG ist die Polizei zuständig für die „Sicherstellung von Sachen, sofern deren Beschlagnahme zum Zweck des Verfalls oder der Einziehung in einem Strafverfahren aufgehoben worden ist“.

Diese Regelung ist nicht nachvollziehbar. Ausweislich der Gesetzgebung soll hiermit sichergestellt werden, dass die ausschließliche Zuständigkeit der Polizei in den Fällen gegeben sei, in denen die Beschlagnahme zum Zweck der Vermögensabschöpfung in einem Strafverfahren aufgehoben worden sei, die Sache jedoch unter den Voraussetzungen des § 22 POG sichergestellt werden könne<sup>15</sup>.

Nach § 22 POG können die Polizei und die allgemeinen Ordnungsbehörden eine Sache sicherstellen, um eine gegenwärtige Gefahr abzuwehren (§ 22 Nr. 1 POG), um den Eigentümer oder den rechtmäßigen Inhaber der tatsächlichen Gewalt vor Verlust oder Beschädigung einer Sache zu schützen (§ 22 Nr. 2 POG) oder wenn sie von einer Person mitgeführt wird, die nach diesem Gesetz oder anderen Rechtsvorschriften

---

<sup>14</sup> Vgl. hierzu *BVerfGE* 56, 37, 50 f..

<sup>15</sup> LT-Drs. 15/4879, S. 22, 23.

festgehalten wird, und die Sache verwendet werden kann, um sich zu töten oder zu verletzen, Leben oder Gesundheit anderer zu schädigen, fremde Sachen zu beschädigen oder die Flucht zu ermöglichen oder zu erleichtern (§ 22 Nr. 3 POG).

Soweit in der Gesetzesbegründung ausgeführt wird, die Sicherstellung der Sache zum Zweck der Gefahrenabwehr komme in Betracht, wenn die Beschlagnahme zum Zwecke der Vermögensabschöpfung in einem Strafverfahren aufgehoben worden sei, weil die Instrumente der Vermögensabschöpfung an enge gesetzliche Anforderungen gebunden seien und im Verfahren nicht immer nachgewiesen werden könnten, ist dies rechtsstaatlich nicht hinnehmbar. Einziger Zweck etwa der Verfallsvorschriften ist die Gewinnabschöpfung als Ausgleich unrechtmäßiger Vermögensverschiebungen. Die Vorschriften erlauben Eingriffe in das Vermögen bereits bei **schuldlos**-rechtswidrigen Taten. Zudem knüpfen die Normen an das Bruttonprinzip an, tragen also bereits das Risiko besonders ungerechter Ergebnisse im Einzelfall in sich. Liegen nicht einmal die weitgefassten Voraussetzungen des §§ 73 ff. StGB vor, erschließt sich nicht, aus welchen Gründen die Sache anschließend zur „Gefahrenabwehr“ beschlagnahmt werden soll. Ungeachtet der Tatsache, dass die Gesetzesbegründung keinen Fall nennt, in dem die polizeirechtlichen Voraussetzungen erfüllt sein sollen, steht fest, dass Art. 14 GG verletzt wird, wenn die Beschlagnahme im Strafverfahren aufgehoben und anschließend die Sicherstellung „zum Zweck der Gefahrenabwehr“ vorgenommen wird.

#### **IV. Rasterfahndung, § 38 E-POG**

§ 38 E-POG ermächtigt die Polizei, Zugriff auf personenbezogene Daten bei allen öffentlichen und nicht-öffentlichen Stellen zu nehmen.

Die Übermittlungsbefugnis umfasst somit sämtliche personenbezogene Daten, die bei irgendeiner öffentlichen oder nicht-öffentlichen Stelle vorhanden sind. Es handelt sich damit um einen „Eingriff von hoher Intensität“<sup>16</sup>.

Ob seitens des Landes Rheinland-Pfalz hier eine Evaluierung der im Jahre 2001/2002 durchgeführten Rasterfahndung erfolgt ist, lässt sich der Gesetzesbegründung nicht entnehmen. Seit dem Jahre 2004 wurde von diesem Instrument kein Gebrauch mehr gemacht (LT-Drs. 15/4615, S. 8).

---

<sup>16</sup> BVerfG, Beschluss vom 04.04.2006, 1 BvR 518/02.

Angesichts des mit der Rasterfahndung verbundenen schwerwiegenden Eingriffs in das informationelle Selbstbestimmungsrecht einerseits und der nicht unerheblichen Belastung des Polizeiapparats bei der Durchführung der Maßnahme andererseits, stellt sich deshalb im Hinblick auf den Grundrechtsschutz der betroffenen Bürger und der Effektivität polizeilichen Handelns die Frage, ob das Instrument der Rasterfahndung sich insoweit als taugliches Mittel zur Gefahrenabwehr erweist.

Das Max-Planck-Institut für ausländische und internationales Strafrecht hat das strafprozessuale Instrument der Rasterfahndung nach den §§ 98a ff. StPO evaluiert und kam zu ernüchternden Ergebnissen<sup>17</sup>. So stellte sich z.B. heraus, dass die richterliche Kontrolle mangelhaft ist, die vorgesehene Benachrichtigung des Datenschutzbeauftragten oder betroffener Personen im Regelfall unterbleibt und Ermittlungserfolge, die sich in einer Identifizierung von Straftätern oder der Aufklärung von Straftaten niederschlagen, die Ausnahme bilden.

Die präventive Rasterfahndung nach dem 11. September 2001 ist in mehreren Bundesländern evaluiert worden, ohne dass sich insoweit belastbare Anhaltspunkte für eine Geeignetheit der Maßnahme ergeben haben.

Dies vorangeschickt, entspricht der Gesetzentwurf weitgehend den verfassungsrechtlichen Anforderungen des Bundesverfassungsgerichtes in seinem Beschluss vom 04.04.2006<sup>18</sup>, entwickelt hat.

Der Gefahrenbegriff ist der Rechtsprechung des Bundesverfassungsgerichtes angepasst worden. Darüber hinaus ist der verfassungsrechtlich nicht erforderliche Richtervorbehalt eingeführt worden.

Das ist zu begrüßen, wenn auch die bisherigen Befunde im Hinblick auf die richterliche Anordnung der (strafprozessualen) Rasterfahndung nach den Feststellungen des Max-Planck-Instituts eher ernüchternd sind. Insoweit heißt es etwa: *„Die richterliche Anordnung ist lediglich ein formaler Akt.“*

Dies spricht indessen nicht dagegen, die Durchführung der Rasterfahndung von einer richterlichen Anordnung abhängig zu machen, vielmehr ergeben sich daraus besondere Anforderungen an die Umsetzung der richterlichen Kontrolle.

---

<sup>17</sup><http://www.iuscrim.mpg.de/ww/de/pub/forschung/forschungsarbeit/kriminologie/rasterfahndung.htm>

<sup>18</sup> 1 BvR 518/02.

Zu kritisieren ist, dass die Novelle nicht zum Anlass genommen worden ist, die „Heimlichkeit“ des Eingriffs auf das notwendige Maß zu beschränken.

Das Bundesverfassungsgericht hat darauf hingewiesen, dass die Intensität des Grundrechtseingriffs der mit der Rasterfahndung verbunden ist, davon beeinflusst wird, dass die gesetzliche Regelung heimlich durchgeführt wird. Dies führt „zur Erhöhung ihrer Intensität“<sup>19</sup>.

Die Gesetzesnovelle sieht indessen keinerlei Regelung vor, nach der die Betroffenen nach Durchführung der Maßnahme über die erfolgte Rasterfahndung zu informieren sind, um ihnen die Möglichkeit der nachträglichen richterlichen Überprüfung der Maßnahme zu geben.

Eine solche Vorschrift, wie sie das Polizeirecht anderer Bundesländer (etwa § 31 Abs. 5 PolG NRW) kennt, wäre deshalb im Sinne einer Garantie effektiven Rechtsschutzes für die Betroffenen erforderlich.

Denn ohne Kenntnis ist den Betroffenen die Überprüfung der Maßnahmen nicht möglich. Eine richterliche Kontrolle kann mithin nachträglich nicht mehr erfolgen. Dieses geringe Maß an richterlicher Kontrolle könnte de facto dazu führen, dass die Anhebung der Gefahrenschwelle nicht die vom Gesetzgeber gewünschte Wirkung erlangt.

## **V. Online-Durchsuchung, § 31 c E-POG**

Nach § 31 c E-POG soll die Polizei unter bestimmten Voraussetzungen die Befugnis zum verdeckten Zugriff auf informationstechnische Systeme erhalten, um personenbezogene Daten zu erheben. § 31 c E-POG wird ergänzt durch § 39a E-POG („*Schutz des Kernbereichs privater Lebensgestaltung*“).

Die Vorschrift des § 31e E-POG lehnt sich in zum großen Teil wortgetreu an die zwischenzeitlich in Kraft getretene Bestimmung des § 20k BKAG („Verdeckter Eingriff in informationstechnische Systeme“) an. Selbst die Begründung des hier vorliegenden Entwurfs entspricht z. T. wortgetreu der gesetzgeberischen Begründung zu § 20k BKAG. Der DAV hatte bereits zu dem damaligen Entwurf des BKAG zur Onlinedurchsuchung und -überwachung ausführlich Stellung genommen<sup>20</sup>. Es kann demzufolge weitgehend

---

<sup>19</sup> Ebenso BVerfGE 107, 299 (321), BVerfG NJW 2006, S. 976.

<sup>20</sup> DAV-Stellungnahme Nr. 89/2008.

auf die damalige Stellungnahme verwiesen werden, wobei diese in ihren wichtigsten Passagen, die unmittelbar für den Entwurf des Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz einschlägig sind, nachfolgend noch einmal zusammengefasst dargestellt werden.

Einleitend soll darauf hingewiesen werden, dass § 31c E-POG im Vergleich zu § 20k BKAG eine Regelung enthält, die über den Befugnisrahmen des BKA-Gesetzes hinausgeht. Während § 20k BKAG in seinem Absatz 1 die Befugnis zum Eingriff in informationstechnische Systeme in einem jeden Fall davon abhängig macht, dass bestimmte Tatsachen die Annahme rechtfertigen, dass eine Gefahr vorliegt für Leib, Leben oder Freiheit einer Person oder Güter der Allgemeinheit, deren Bedeutung die Grundlage oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, sieht § 31c E-POG vor, dass ein solcher Eingriff auch schon dann befugt sein soll, wenn er allein mit der *„Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person oder die entsprechenden Güter der Allgemeinheit“* begründet wird. Damit sind aber Grundlage des Eingriffs nicht „bestimmte Tatsachen“, sondern lediglich eine (subjektive) Einschätzung dahingehend, dass eine Gefahr besteht – oder besser gesagt: bestehen soll. Dies bedeutet nichts anderes, als dass ein solcher Eingriff frei von Tatsachengrundlagen auch auf einer bloßen Einschätzung der Polizeibehörden erfolgen kann.

Adressaten einer solchen Maßnahme sind nach § 31c Abs. 1 Ziff. 1 E-POG Personen, die eine Gefahr verursachen (§ 4 POG), die Verantwortlichen für Tiere oder Sachen, von denen eine Gefahr ausgeht (§ 5 POG) oder auch, und dies erscheint ganz besonders bedenklich, „nicht verantwortliche Personen“ (§ 7 POG).

Da durch den Eingriff in informationstechnische Systeme zwangsläufig immer auch Daten aus dem hochpersönlichen Lebensbereich mit erhoben werden, liegt in dieser Regelung ein eklatanter Grundrechtsverstoß.

Des Weiteren leidet der Entwurf daran, dass generell nicht dargelegt ist, wie sich die Polizeibehörden den Zugriff in die informationstechnischen Systeme verschaffen. Sollte dies nur dadurch ermöglicht werden, dass die Anbieter von informationstechnischen Kommunikationssystemen generell dafür besondere Vorkehrungen in den technischen Geräten (*„informationstechnischen Systemen“*) bereithalten, die ein technisches Eindringen überhaupt erst ermöglichen, kann dies nicht „klammheimlich“ geschehen. Es bedarf hierzu gesetzlicher Vorgaben, die erst noch geschaffen werden müssen, wenn sie überhaupt zulässig sein sollten; denn es liegt auf der Hand, dass das Bereitstellen von Zugangsvorkehrungen nicht nur von den Polizei- und Ermittlungsbehörden, sondern auch

von Dritten („Hackern“), auch für deren höchst privaten Zwecke (aus)genutzt werden könnten.

Diese Fragen werden im Entwurf offen gelassen.

Unter Bezugnahme auf die oben bereits erwähnte Stellungnahme des Gefahrenabwehrausschusses und des Strafrechtausschusses des DAV ist der Entwurf aber auch aus folgenden Gründen bedenklich:

Die in § 31c E-POG normierte Befugnis zur Onlinedurchsuchung und Onlineüberwachung ist erkennbar geprägt von einer grundlegenden Fehlinterpretation der Entscheidung des Bundesverfassungsgerichts vom 27.02.2008 (Az.: 1 BvR 370/07).

Das BVerfG hat unter Betonung und Abgrenzung der Reichweite von Art. 10 GG, Art 13 GG und dem bereits seit dem Volkszählungsurteil bekannten Grundrecht auf informationelle Selbstbestimmung für die zwischen diesen drei Schutzbereichen klaffenden Lücken ein neues Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme definiert, um dem Gesetzgeber die Mindestbedingungen aufzugeben, bei deren Vorliegen ein staatlicher Eingriff erlaubt werden darf.

Zu diesen Mindestvoraussetzungen gehört nicht nur die vom BVerfG selbst noch allgemein formulierte, vom einfachen Gesetzgeber an den Rechtsanwender „weiterzugebende“ Tatbestandsvoraussetzung (*„tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut wie Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt“*), sondern insbesondere auch die Erfüllung der Konkretisierungsaufgabe des einfachen Gesetzgebers selbst.

Der vorliegende Entwurf leistet aber weder das eine noch das andere. Der Umfang der Vorschriften erklärt sich nämlich gerade nicht aus einem Versuch der Verfasser, über die vom BVerfG bezeichneten Mindestanforderungen hinaus den Polizeibehörden des Landes Rheinland-Pfalz und den mit der Frage der Legalität der Maßnahme befassten Gerichten klare Grenzen und konkrete Voraussetzungen an die Hand zu geben. Der Wortreichtum der entworfenen Vorschriften findet eher im Gegenteil seine Erklärung in dem Bemühen der Verfasser des Entwurfs, die vom BVerfG formulierten Mindestbedingungen für den schweren Grundrechtseingriff unter teilweise wörtlicher Übernahme von Begründungselementen so in das Gesetz zu transportieren, dass auch noch jeder sprachlich denkbare Interpretationsspielraum in Richtung auf eine Zulässigkeit

der Maßnahme ausgeschöpft werden könnte. Bereits diese Tendenz zu einer „In-dubio-pro-Eingriff-Regel“ widerspricht diametral dem Geist und den Grundaussagen der Entscheidung des BVerfG.

Nach den eindeutigen Aussagen des Bundesverfassungsgerichts handelt es sich bei dem *„Grundrecht auf Gewährung der Vertraulichkeit und Integrität informationstechnischer Systeme“* keineswegs nur um einen gegen die anderen Schutzgüter abzuwägenden Wertbegriff, der schon dann zurückzutreten hat, wenn irgendwelche Gefahren für Leib, Leben oder die Grundlagen des Staates oder der Existenz der Menschen als Gefahrenabwehrgegenstände in Rede stehen.

Es handelt sich vielmehr um ein vollwertiges Grundrecht, in das nur eingegriffen werden kann, wenn es dem dies legitimierenden Gesetzgeber gelingt, hinreichend bestimmt und vorbehaltlos Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung von vorne herein zu verhindern und die Auswertung von informationstechnischen Systemen im Übrigen auf den allein verfassungsrechtlich zulässigen Zweck zu beschränken.

Die Verfasser des Entwurfs haben offenbar erkannt, dass diese verfassungsrechtlichen Vorgaben durch den einfachen Gesetzgeber schwer (oder auch gar nicht) zu erfüllen sind. Statt daraus dann jeweils die verfassungsrechtlich zwingende Konsequenz zu ziehen, den Eingriffs zu verbieten, haben die Entwurfsverfasser eine Reihe von nur scheinbar bestimmten oder auch offen unbestimmte Öffnungsklauseln eingebaut, die bei Inkrafttreten des Entwurfs als Gesetz letztlich auf eine mit den Grundaussagen des Bundesverfassungsgerichts unvereinbare Durchlöcherung des Grundrechtsschutzes hinauslaufen würden.

Die an mehreren Stellen eingestreuten Vorbehalte wie „soweit technisch möglich“ (§ 31c Abs. 2 Ziff. 2, § 39a Abs. 3 E-POG), oder auch *„nach dem Stand der Technik“* (§ 31 c Abs. 2 Ziff 2 E-POG) schließen jeweils das Zugeständnis ein, dass letztlich auch grundrechtsunverträgliche Angriffe unvermeidbar bleiben.

Dies gilt auch für die scheinbar auf ein Höchstmaß an Grundrechtsschonung hindeutende Formulierung in § 31c Abs. 2 Ziff.2 E-POG:

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

Der Standard „Stand der Wissenschaft und Technik“ (im Entwurf hat man sich freilich auf den Begriff „Stand der Technik“ beschränkt) wird in anderen Rechtsgebieten verwendet, um noch über die „allgemein anerkannten Regeln der Wissenschaft und Technik“ hinaus die Genehmigungsfähigkeit potentiell hochgefährlicher Anlagen von der Einhaltung einer in den betreffenden Fachkreisen klar definierten Risikominimierung abhängig zu machen.

Der Entwurf suggeriert mit der Übernahme jener Formel, es sollten auch die Grundrechtseingriffe bei der Onlinedurchsuchung einem ähnlich hohen Sicherheitsstandard unterworfen werden. Dabei wird aber verschwiegen, dass sich bei der Entwicklungsgeschwindigkeit von Informationstechnik der „Stand von Technik“ nahezu täglich ändert. Davon zeugen z.B. die laufend notwendigen Updates der Schutzprogramme gegen Viren, Trojaner und sonstige „Mal-ware“, ohne die der von den Internetnutzern sinnvoller- und notwendigerweise betriebene Selbstschutz gegen kriminelle Angreifer auf ihre mit dem WEB verbundenen Computer stets schon nach wenigen Tagen veraltet wären. Die darin zum Ausdruck kommende Flüchtigkeit des jeweils optimalen Sicherheitsstandards bedeutet auch, dass die Einhaltung des Standes der Technik – zumal im Nachhinein – praktisch nicht zu kontrollieren wäre. Die Folge wäre, dass auch die richterliche Kontrolle der Einhaltung dieser „fließenden“ Standards praktisch leer liefe.

Ähnliches gilt für den Umgang des Entwurfs mit dem verfassungsgerichtlichen Auftrag an den Gesetzgeber, neben der Vertraulichkeit auch die **Integrität** der Nutzung informationstechnischer Systeme zu sichern.

Indem § 31c E-POG vorschreibt, dass „*an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind*“ (Hervorh. nur hier), gestehen die Entwurfsverfasser zu, dass diese Maßnahme überhaupt nur möglich ist, indem auch Veränderungen auf den Datenspeichern (Festplatte) des Computers vorgenommen werden. Deshalb sollen solche Veränderungen nach § 31c Abs. 2 Ziff. 2 E-POG nur „*bei Beendigung der Maßnahme, soweit technisch möglich, automatisch rückgängig gemacht werden*“. Auch darin steht das (zutreffende) Eingeständnis, dass eine restlose Beseitigung der Manipulationen bzw. automatisch bewirkten „Sachbeschädigungen“ an der Hardware und Programmänderungen an der Software nicht möglich ist.

In der Begründung (LT-Drs. 15/4879, S. 37) heißt es dazu:

„*Satz 1 Nr. 1 (Erg.: des § 31 E-POG) bestimmt, dass bei Einsatz des technischen Mittels sicherzustellen ist, dass an dem informationstechnischen System nur solche*

*Veränderungen vorgenommen werden, die für die Datenerhebung unbedingt erforderlich sind. Zu schützen sind dabei nicht nur die von der Nutzerin oder dem Nutzer des informationstechnischen Systems angelegten Anwenderdateien, sondern auch die für die Funktion des informationstechnischen Systems erforderlichen Systemdateien. Auch Beeinträchtigungen der Systemleistung sind auf das technisch Unvermeidbare zu begrenzen. ... Nach Satz 1 Nr. 2 sind bei Beendigung der Maßnahme alle an den infiltrierten System vorgenommenen Veränderungen rückgängig zu machen, soweit dies technisch möglich ist. Insbesondere ist die auf dem informationstechnischen System installierte Überwachungssoftware vollständig zu löschen und es sind Veränderungen an den bei der Installation der Überwachungssoftware vorgefundenen Systemdateien rückgängig zu machen. Die Rückgängigmachung der vorgenommenen Veränderungen hat im Interesse einer möglichst zuverlässigen und einfachen Abwicklung grundsätzlich automatisiert zu geschehen. Soweit eine automatisierte Rückgängigmachung technisch unmöglich ist, sind die vorgenommenen Veränderungen, sofern die Möglichkeit besteht, manuell rückgängig zu machen.“ (Hervorh. nur hier)*

Abgesehen davon, dass es z.B. in den Betriebssystemen von Microsoft seit Windows NT eine sogenannte Registrierungsdatenbank („Registry“) gibt, in deren tiefsten Hierarchieschichten Veränderungen an den Programmen auch dann noch Spuren hinterlassen, wenn die Programme wieder deinstalliert wurden, und dass dies auch Auswirkungen auf die Funktionalität des ganzen Systems haben kann, wäre hier zu prüfen, ob die vorgeschlagene Regelung mehr der Vermeidung eines Entdeckungsrisikos für die Maßnahme selbst als dem Grundrechtsschutz dienen soll.

Es fällt auch auf, dass der Begründungssatz, wonach die *„Beeinträchtigungen der Systemleistung auf das technisch unvermeidbare zu begrenzen“* seien, keine Entsprechung im vorgeschlagenen Gesetzestext findet. Auch dies erweckt den Eindruck, als gehe es letztlich darum, dass der Betroffene nicht – etwa wegen der plötzlich beobachteten Verlangsamung seines Computers – Verdacht schöpft, sodass die Heimlichkeit oder gar der Erfolg der Maßnahme gefährdet werde.

Auch die in § 31 Abs. 2 Ziff. 2 E-POG vorgesehene Vorschrift, wonach die eingesetzten technischen Mittel („nach dem Stand der Technik“ s.o.) *„gegen unbefugte Nutzung zu schützen“* seien, dürften mehr die Interessen der die Maßnahme durchführenden Dienststelle als die der jeweiligen Grundrechtsträger im Blick haben. Aber immerhin kann man darin auch das Eingeständnis erkennen, dass eine einmal zum Zwecke der Durchführung der Maßnahme geöffnete Backdoor eines Computers auch von anderen – weniger im Allgemeinwohl tätigen – an Infiltration Interessierten als die staatlichen Gefahrenabwehrbehörden genutzt werden kann.

Unter ähnlichen technischen Aspekten ist auch äußerste Skepsis angezeigt gegen den Versuch, in § 39a des Entwurfs den **Kernbereich privater Lebensgestaltung** gegen jeglichen Eingriff zu sichern. Dass (wiederum nur „soweit möglich“, § 39a Abs. 3 E-POG) hier eine technische Vorsorge gegen die Datenerhebung vorgeschrieben werden soll, wäre ebenso wie die dann folgenden Verwertungsverbote für alle anderen Fälle prinzipiell zu begrüßen, wenn nicht die technische Untrennbarkeit der sonstigen von den Kernbereichsdaten ein genereller Einwand gegen die Zulassung der Maßnahme für polizeirechtliche Zwecke wäre. Dass auf diesem hochsensiblen Gebiet des Eingriffs in die Vertraulichkeit der informationstechnischen Intimsphäre der Grundsatz vorherrschen sollte: „in dubio pro libertate“, erschließt sich unmittelbar aus der Entscheidung des Bundesverfassungsgerichts vom 27.02.2008 und die vorausgegangene Entscheidung zum „großen Lauschangriff“<sup>21</sup>. Beide Urteile zwingen dazu, jedenfalls solche gesetzliche Ermächtigung für Grundrechtseingriffe gänzlich zu unterlassen, die geradezu denotwendig zu einem Eindringen des Staates in den privaten Kernbereich des Persönlichkeitsrechts führen müssen.

Genau dies soll aber mit dem hier vorgeschlagenen Gesetzesvorhaben legalisiert werden.

§ 39a E-POG („Schutz des Kernbereichs privater Lebensgestaltung“) räumt das verdeckt ein, indem er formuliert:

*„Die Datenerhebung nach §§ 31, 31b oder 31c darf nur angeordnet werden, falls nicht tatsächliche Anhaltspunkte für die Annahme vorliegen, dass allein Erkenntnisse aus dem Bereich privater Lebensgestaltung erlangt werden.“* (Hervorh. nur hier)

Das bedeutet im Umkehrschluss, dass die Maßnahme (beim Vorliegen der sonstigen Voraussetzungen) stets schon dann zulässig ist, wenn sich auf dem betreffenden Datenträger bzw. in der mit kernbereichsrelevanten Informationen beschriebenen Festplatten-Partition auch die eine oder andere unverfängliche Eintragung (z.B. ein abgespeicherter Pressebericht oder eine Podcast-Version der Tagesschau) befindet. Mit anderen Worten: Da es wohl kaum jemanden gibt, der für sein intimes Tagebuch, seine privaten Briefe und für seine Internettelefonate mit Familienangehörigen oder heimlichen Liebschaften einen „Extra-Computer“ betreibt, mithin das gleichzeitige Vorhandensein von kernbereichsrelevanten und sonstigen personenbezogenen bis öffentlich bekannten Informationen die nahezu ausnahmslose Regel sein dürfte, liefe bei der vorgeschlagenen Regelung der eigentlich „absolute“ und sogar abwägungsfeste Schutz des Kernbereichs privater Persönlichkeit ins Leere.

---

<sup>21</sup> BVerfGE 109, 279.

## VI. Gerichtliche Zuständigkeit

Nach dem Gesetzesentwurf soll für Entscheidungen über die Anordnung **verdeckter Ermittlungsmaßnahmen** nach den §§ 29, 31, 31 b, 31 c, 31 d und 31 e E-POG das Oberverwaltungsgericht Rheinland-Pfalz zuständig sein. Für diese Fälle soll – so die Gesetzesbegründung – „durch die Verlagerung der bisherigen Zuständigkeit der Amtsgerichte auf das Oberverwaltungsgericht Rheinland-Pfalz die Wirksamkeit des Richtervorbehalts akzentuiert werden, da für die richterliche Beurteilung derart intensiver Grundrechtseingriffe profunde Kenntnisse des Verfassungs- und Verwaltungsrecht sowie entsprechende Erfahrungen förderlich sind“<sup>22</sup>. Gesetzlich verankert werden soll dies in § 29 Abs. 6 S. 1 E-POG, auf den die anderen Vorschriften über verdeckte Ermittlungsmaßnahmen verweisen. S. 2 dieser Vorschrift regelt zudem, dass das Oberverwaltungsgericht nach Maßgabe der Verwaltungsgerichtsordnung entscheidet.

Grundsätzlich ist diese Zuständigkeitsverlagerung zu begrüßen. Bereits mit Stellungnahme zum Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG<sup>23</sup> hatte der DAV umfassend dargetan, dass die Anordnungs-kompetenz das Nadelöhr darstellt, durch das die Behörden von ihnen beabsichtigte Eingriffe in Freiheitsrechte der Bürgerinnen und Bürger fädeln müssen und daher an die berufliche Qualifikation des Richters, der die Maßnahme anordnet, besondere Anforderungen zu stellen sind, diese Richterpersönlichkeit die Voraussetzungen des § 10 DRiG erfüllen muss und über die unter Richtervorbehalt gestellten Eingriffe in Freiheitsrechte der Bürgerinnen und Bürger nur von Gerichten entschieden werden darf, die über genügend Berufserfahrung verfügen, die ihnen ein souveränes Abwägen ermöglicht. Daher ist es grundsätzlich richtig, dass die Anordnung einem Senat eines Oberverwaltungsgerichtes übertragen wird, der mit drei Berufsrichtern besetzt ist<sup>24</sup>. Zudem ist es konsequent, die Entscheidung der Verwaltungsgerichtsbarkeit vorzubehalten, da diese ohnehin mit Fragen des Polizei- und Sicherheitsrechtes befasst ist.

Bedenken ergeben sich jedoch in zweierlei Sicht:

---

<sup>22</sup> LT-Drs. 15/4879, S. 30.

<sup>23</sup> DAV-Stellungnahme Nr. 41/2007.

<sup>24</sup> Vgl. § 9 Abs. 3 S. 1 VwGO.

1. Gemäß § 152 Abs. 1 VwGO können Entscheidungen des Oberverwaltungsgerichts vorbehaltlich des § 99 Abs. 2 VwGO und des § 133 Abs. 1 VwGO sowie des § 17 a Abs. 4 S. 4 GVG nicht mit der Beschwerde an das Bundesverwaltungsgericht angefochten werden. Regelt also § 29 Abs. 6 S. 2 E-POG, dass das Oberverwaltungsgericht nach Maßgabe der Verwaltungsgerichtsordnung entscheidet, bedeutet dies, dass das Oberverwaltungsgericht im (nachträglichen) Rechtsschutzverfahren letztinstanzlich entscheidet. Hierauf weist die Gesetzesbegründung ebenso hin<sup>25</sup>. Damit effektiver Rechtsschutz gewährleistet ist, muss die fehlende Beschwerdemöglichkeit zum Bundesverwaltungsgericht aufgefangen werden – dadurch, dass im Geschäftsverteilungsplan des Oberverwaltungsgerichtes Zuständigkeitsregelungen geschaffen werden, die sicherstellen, dass der Senat, der heimliche Datenerhebungen angeordnet hat, insoweit im nachträglichen Rechtsschutzverfahren unzuständig ist und ein anderer Senat nachträglich über die Rechtmäßigkeit der angeordneten Maßnahmen zu entscheiden hat.
2. Nach dem Gesetzesentwurf sollen die Amtsgerichte weiterhin zuständig sein für die richterliche Entscheidung über Zulässigkeit und Fortdauer der Freiheitsentziehung einer festgehaltenen Person (§ 15 Abs. 1 POG) und für die Anordnung der Durchsuchung von Wohnungen (§ 21 Abs. 1 S. 1 POG). Insoweit soll lediglich geändert werden, dass sich das Verfahren nach dem Gesetz über das Verfahren in Familiensachen und in Angelegenheiten der freiwilligen Gerichtsbarkeit vom 17. Dezember 2008 richtet<sup>26</sup>. Das aber ist nicht konsequent. Mit der Durchsuchung von Wohnungen und dem Festhalten einer Person sind ebenso „intensive Grundrechtseingriffe“ verbunden (Art. 13, 2 GG). Ist eine solche Eingriffsschwere Anlass dafür, die Zuständigkeit der Amtsgerichte auf das Oberverwaltungsgericht Rheinland-Pfalz zu verlagern, muss dies daher auch für Wohnungsdurchsuchung und Freiheitsentziehung gelten.

## VII. Evaluierung

Ausdrücklich zu begrüßen sind § 100 Abs. 1 S. 1, Abs. 2 E-POG. Hiernach sollen die Ermächtigungen zur Wohnraumüberwachung (§ 29 E-POG), zur Telekommunikationsüberwachung (§ 31 E-POG), zur Auskunft über Nutzungsdaten (§ 31 b E-POG), zur Online-Durchsuchung (§ 31 c E-POG), zur Funkzellenabfrage (§ 31 e E-POG) und zur Rasterfahndung (§ 38 E-POG) evaluiert werden – dadurch, dass die Landesregierung dem Landtag über die Wirksamkeit der Maßnahmen berichtet<sup>27</sup> und gemäß § 100 Abs. 2

---

<sup>25</sup> LT-Drs. 15/4879, S. 30.

<sup>26</sup> Vgl. § 15 Abs. 2 S. 2 E-POG und § 21 Abs. 1 S. 3 E-POG.

<sup>27</sup> Der Berichtszeitraum erstreckt sich auf fünf Jahre, siehe LT-Drs. 15/4879, S. 48.

E-POG die Anfertigung des Berichts der Landesregierung unter Mitwirkung einer Stelle zu erfolgen hat, die eine wissenschaftlich fundierte Überprüfung der Maßnahme gewährleistet. Ausweislich der Gesetzesbegründung könnte eine solche Stelle etwa die Deutsche Hochschule für Verwaltungswissenschaften in Speyer sein<sup>28</sup>.

Ferner wird in der Gesetzesbegründung klargestellt, dass der Bericht insbesondere die im künftigen § 100 Abs. 3 S. 1 E-POG genannten Kriterien zur Wirksamkeit der Maßnahmen darlegen und bewerten muss, um dem Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen zur Verfügung zu stellen<sup>29</sup>. Hiermit wird eine parlamentarische Kontrolle ermöglicht, die aufgrund der Schwere der Grundrechtseingriffe, die mit einem Vollzug der Regelungen verbunden sind, ermöglicht.

Eine parlamentarische Kontrolle wird ferner dadurch gewährleistet, dass gemäß § 29 Abs. 12 POG bzw. gemäß § 29 Abs. 8 E-POG die Landesregierung den Landtag jährlich über den erfolgten Einsatz technischer Mittel in oder aus Wohnungen zu unterrichten hat und die parlamentarische Kontrollkommission auf der Grundlage dieses Berichts die parlamentarische Kontrolle ausübt. Für die Online-Durchsuchung (§ 31 c E-POG) gilt dies ebenso, da § 31 c Abs. 6 E-POG auf § 29 Abs. 5 und 8 E-POG verweist.

### **VIII. Zuständigkeit des Landeskriminalamtes**

Gemäß § 79 Abs. 3 E-POG wird die Zuständigkeit des Landeskriminalamtes um Aufgaben zur Abwehr von Gefahren erweitert. Damit ist die Befugnis des Landeskriminalamtes nicht mehr auf Fälle der Verfolgung von Straftaten begrenzt, sondern es wird erstmals befugt, zur Abwehr von Gefahren in Fällen von überregionaler oder besonderer Bedeutung die Zuständigkeit einer anderen als der örtlich zuständigen Polizeibehörde zu übertragen oder selbst zu übernehmen. Insoweit aber hat es der Gesetzesentwurf versäumt, das Landeskriminalamt zu verpflichten, die Generalstaatsanwaltschaft des Landes Rheinland-Pfalz über solche Sachverhalte zu informieren, die deren strafverfolgende („repressive“) Zuständigkeit begründen<sup>30</sup>. Dieses Regelungsdefizit wird sich bei den Delikten auswirken, bei denen – wie etwa bei § 129 a StGB – schon durch den gesetzlichen Straftatbestand die Strafbarkeit in das Vorfeld konkreter Rechtsgutgefährdungen verlagert ist. Wann Personen, die miteinander Gedanken über Anschläge austauschen, welche bereits eine Gefahr für die Allgemeinheit

---

<sup>28</sup> LT-Drs. 15/4879, S. 48.

<sup>29</sup> LT-Drs. 15/4879, S. 48.

<sup>30</sup> Vgl. insoweit zum BKAG *Roggan* NJW 2009, S. 257, 258.

bedeuten, die Schwelle zur Unterstützung einer terroristischen Vereinigung überschreiten, kann im Einzelfall fraglich sein. Mit ihrer Beantwortung ist es für das Landeskriminalamt aber weitgehend steuerbar, ob es auf eigene Faust agiert oder sich der Herrschaft der Generalstaatsanwaltschaft und strafprozessualen Beschränkungen unterwirft.

Dass das Landeskriminalamt durchaus ein Interesse haben könnte, die Generalstaatsanwaltschaft des Landes außen vor zu lassen, zeigt nicht zuletzt die in § 31 c E-POG geregelte Befugnis, in informationstechnische Systeme heimlich einzugreifen (Online-Durchsuchung). Da die Strafprozessordnung eine solche Ermächtigung nicht vorsieht – hierauf wird in der Gesetzesbegründung zutreffend hingewiesen<sup>31</sup> –, dürfte eine Online-Durchsuchung nicht erfolgen oder müsste unverzüglich beendet werden, wenn das Landeskriminalamt die Generalstaatsanwaltschaft unterrichtet hält. Damit die Verfahrensherrschaft der Generalstaatsanwaltschaft, mithin Strafverfolgung unter der justiziellen Herrschaft nach Strafprozessrecht, gewährleistet wird, muss das Landeskriminalamt gesetzlich verpflichtet werden, die Generalstaatsanwaltschaft umgehend über solche Sachverhalte zu informieren, die deren strafverfolgende („repressive“) Zuständigkeit begründet.

---

<sup>31</sup> LT-Drs. 15/4879, S. 39.