Der Landesbeauftragte
für den Datenschutz und die
Informationsfreiheit Rheinland-Pfalz

Der Landesbeauftragte

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit RLP
Postfach 30 40 | 55020 Mainz

Hintere Bleiche 34 | 55116 Mainz
Telefon +49 (0) 6131 208-2449
Telefax +49 (0) 6131 208-2497
lfdi@datenschutz.rlp.de
www.datenschutz.rlp.de

An den Innenausschuss
des Landtags Rheinland-Pfalz
Platz der Deutschen Republik 1
55116 Mainz

LANDTAG
Rheinland-Pfalz
16 / 3101
VORLAGE

Ihr Zeichen:	Ihre Nachricht vom:	Geschäftszeichen:	Telefondurchwahl:	Datum:
		6.05.00:0001	-2247	18.10.2013

Stellungnahme anlässlich der Anhörung des Innenausschusses am 25.10.2013 zum Gesetzentwurf der Fraktionen der SPD und Bündnis 90/Die Grünen Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes, Drs. 16/2506 v. 27.6.2013

Sehr geehrte Frau Vorsitzende,
sehr geehrte Damen und Herren Abgeordnete,

für die Gelegenheit, zu der beabsichtigten Änderung des Polizei- und Ordnungsbehördengesetzes Rheinland-Pfalz Stellung zu nehmen, danke ich Ihnen. In der mündlichen Anhörung wird mein Stellvertreter, LMR Dr. Globig, meine Stellungnahme erläutern.

Aus der Sicht des Datenschutzes möchte ich Folgendes ausführen:

1. Nummer 1 des Änderungsgesetzes betrifft eine kostenrechtliche Klarstellung, die keine datenschutzrechtliche Bedeutung hat. Deshalb sehe ich von Ausführungen zu diesem Punkt ab.

2. Unter Nummer 2 des Gesetzentwurfs wird vorgeschlagen, die körperliche Untersuchung von Personen, die der Prüfung der Gewahrsamsfähigkeit dient, nur dann von einer richterlichen Entscheidung abhängig zu machen, wenn die körperliche Untersuchung mit körperlichen Eingriffen verbunden ist.

   Die bloße Inaugenscheinnahme einer Person zur Feststellung ihrer Gewahrsamsfähigkeit fordert auch aus der Sicht des Datenschutzes nicht zwingend einen richterlichen Beschluss; es erscheint nachvollziehbar, das Erfordernis des Richtervorbehalts in Bezug auf die körperliche Untersuchung vor einer Ingewahrsam-

nahme, die mit keinem körperlichen Eingriff verbunden ist, ebenso zu behandeln wie die Ingewahrsamnahme selbst. Darauf wird in der Begründung des Gesetzentwurfs abgestellt und ich halte diese Erwägung für nachvollziehbar.

3. Nummer 3 des Entwurfs betrifft die Verwertung sichergestellter Sachen und hat keine Auswirkungen auf den Datenschutz von Personen.

4. In Nummer 4 Bst. a soll klargestellt werden, dass das Oberverwaltungsgericht Rheinland-Pfalz auch dann das zuständige Gericht ist, wenn es um die Anordnung von Überwachungsmaßnahmen zum Zweck der Eigensicherung von Vollzugsbeamten geht. Diese Klarstellung ist aus der Sicht des Datenschutzes zu begrüßen.

5. Nummer 4 Bst. c enthält eine weitere Klarstellung: Es soll ausdrücklich geregelt werden, wer innerhalb der Polizei zu entscheiden hat, wenn Daten bei einer Eigensicherungszwecken dienenden Maßnahme erhoben worden sind und im Eilfall zweckändernd verwendet werden sollen. Dann soll die Behördenleitung oder ein von ihr besonders beauftragter Beamter des höheren Dienstes zur Entscheidung befugt sein. Diese Klarstellung ist aus Datenschutzsicht zu begrüßen.

6. Die aus meiner Sicht gewichtigste Änderung im Rahmen der hier zu erörternden Novellierung betrifft die Höchstdauer einer gerichtlich angeordneten Maßnahme der Quellen-Telekommunikationsüberwachung. Diese soll von drei Monaten auf zwei Monate verkürzt werden, wobei Verlängerungen ebenfalls jeweils um zwei Monate gerichtlich angeordnet werden können.

   Zur Verdeutlichung des Problems möchte ich zunächst kurz die Ausgangslage schildern:
   Zunehmend wird über das Internet telefoniert; dabei wird regelmäßig Verschlüsselungstechnik eingesetzt, die entweder vom Anbieter vorgegeben ist (z.B. Skype) oder aktiv vom Nutzer eingesetzt wird. Diese Neuerungen bereiten den Sicherheitsbehörden Schwierigkeiten, da die Kommunikation nicht mehr auf dem – verschlüsselten – Weg vom Absender zum Empfänger mitgehört bzw. mitgelesen werden kann. Vielmehr wird es erforderlich, die Kommunikation an der Quelle selbst, also direkt am Computer abzufangen, bevor die Verschlüsselungstechnik überhaupt einsetzt. Dies geschieht – ähnlich wie bei der Online-Durchsuchung – z.B. dadurch, dass ein Trojaner in das Quellsystem (den Computer, von dem aus die Verbindung hergestellt wird) implementiert wird.

   Das Bundesverfassungsgericht hat als wesentliche Vorgabe hierfür gefordert, dass durch die eingesetzte Technik tatsächlich nur das Abhören von Gesprächsinformationen ermöglicht wird, nicht aber darüber hinausgehende Informationen (z.B. Dateikopien aus dem Speicher des betroffenen Rechners) an die Polizei übermittelt werden (BVerfG, Urteil zur Online-Durchsuchung vom 27.2.2008, Rnrn. 190, 212). Dies ist in § 31 Abs. 3 POG auch ausdrücklich so geregelt.

Derzeit steht der Polizei des Landes nach meiner Kenntnis noch keine Technik zur Verfügung, um eine Quellen-TKÜ entsprechend den verfassungsrechtlichen und gesetzlichen Anforderungen durchführen zu können. Allerdings dürften die Arbeiten bereits so weit fortgeschritten sein, dass in absehbarer Zeit mit einem einsatzfähigen Verfahren zu rechnen ist. Spätestens dann stellt sich die Frage, für welche Höchstdauer das OVG den Einsatz der Quellen-TKÜ anordnen darf.

In meiner Stellungnahme gegenüber dem Innenausschuss zu der Einfügung der Regelung zur Quellen-TKÜ in das POG vom 21.10.2010 (§ 31 Abs. 3 POG) hatte ich die Notwendigkeit technisch-organisatorischer Vorkehrungen betont, die sicherstellen, dass durch die eingesetzte Technik nicht überschießende Informationen, die über die Telekommunikation hinausgehen, vom Quellsystem abgerufen werden. Diese Anregungen und Erfordernisse sind vom Gesetzgeber in das POG übernommen worden. Vor diesem Hintergrund hatte ich erklärt, dass ich insgesamt den Einsatz dieses Aufklärungsmittels als akzeptabel ansehen würde.

Die Frage der Anordnungshöchstdauer von drei Monaten wurde seinerzeit nicht weiter problematisiert. Sie entspricht der Frist, die für die mit herkömmlichen Mitteln durchgeführte Telekommunikationsüberwachung sowohl im repressiven wie im präventiven Bereich gilt (§ 100a StPO, 31 Abs. 3 POG). Soweit andere Bundesländer die Quellen-TKÜ in ihren Polizeigesetzen geregelt haben (Hamburg, Hessen, Sachsen-Anhalt, Thüringen) gilt ebenfalls die Dreimonatsfrist. Auch das BKA-Gesetz enthält eine entsprechende Frist. Die dreimonatige Anordnungshöchstfrist für eine solche Maßnahme wurde vom Bundesverfassungsgericht nicht gerügt. Aus meiner Sicht ist die Dreimonatsfrist deshalb auch verfassungsgemäß.

Dennoch gibt es gute Argumente, die für eine Verkürzung der Dreimonatsfrist sprechen. Die für solche Maßnahmen erforderliche Technik infiltriert ein informationstechnisches System und macht es damit möglicherweise auch für Dritte angreifbar. Auch wenn die Vorgaben des technisch-organisatorischen Datenschutzes eingehalten und tatsächlich der Zugriff auf Kommunikationsdaten beschränkt wird, so wird durch eine solche Maßnahme doch ein komplexes technisches System mit seinen Sicherheitsvorkehrungen (z.B. Firewall, Virensuchprogramme etc.) kompromittiert und ein externer Zugang eröffnet. Das Bundesverfassungsgericht hat zwar erklärt, dass für den Fall eines solchen Zugriffs auf Telekommunikationsdaten das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme (das sogen. Computergrundrecht) nicht betroffen sei, sondern nur das speziellere Fernmeldegeheimnis (Art. 10 GG) gelte (BVerfG, Urteil zur Online-Durchsuchung vom 27.2.2008, Rnr. 190). Dennoch kann nicht in Abrede gestellt werden, dass eine solche Maßnahme im technischen Bereich und in der Eingriffsschwere deutliche Unterschiede zur herkömmlichen Telekommunikationsüberwachung aufweist und in die Sphäre des Betroffenen in einer besonderen Weise eingreift. Dieser Aspekt sollte auch bei der Regelung der Maßnahmen berücksichtigt werden, die als begleitende rechtsstaatliche Sicherungen

dienen. Dazu gehört die zeitliche Begrenzung solcher Eingriffe, die die Durchsetzung des Verhältnismäßigkeitsgrundsatzes zum Ziel hat.

Deshalb begrüße ich die Initiative, die Eingriffsintensität bei Quellen-TKÜ-Maßnahmen durch eine engere Zeitvorgabe zu begrenzen und zugleich ihre rechtsstaatliche Kontrolle engmaschiger zu gestalten.

Es könnte im Übrigen auch daran gedacht werden, die ins Auge gefasste Intensivierung rechtsstaatlicher Kontrollen bei der Quellen-TKÜ zusätzlich durch folgende Maßnahmen zu erreichen:

- Die Zahl der zulässigen Verlängerungsanordnungen könnte begrenzt werden (etwa auf maximal eine oder zwei). Angesichts der in § 31 Abs. 3 POG verankerten Voraussetzung der konkreten Gefahrenlage würde dies aus meiner Sicht auch naheliegen. Eine konkrete Gefahr über einen Zeitraum von mehr als vier Monaten hinweg ist wohl kaum vorstellbar.
- Es könnte auch daran gedacht werden, den maximalen Zeitraum der Verlängerungsanordnungen zu verkürzen, etwa auf jeweils einen Monat. Die Folge wäre, dass sich das Gericht im Falle von Verlängerungen jeweils nach diesem Zeitraum erneut mit dem Fall zu befassen hätte und seine Kontrolle ausüben müsste.

Entsprechende gesetzliche Konkretisierungen würden auch für die Zukunft sicherstellen, dass die bisherige verantwortungsbewusste Verfahrensweise in diesem Bereich beibehalten wird.

Abschließend möchte ich noch darauf hinweisen, dass vergleichbare Überlegungen ebenfalls in Bezug auf die Online-Durchsuchung nach § 31c POG angestellt werden sollten. Nach § 31c Abs. 5 Satz 4 POG beträgt die maximale Frist für Anordnungen solcher Online-Durchsuchungen ebenfalls drei Monate mit Verlängerungsmöglichkeiten um jeweils drei weitere Monate. Aus meiner Sicht dürften hier grundsätzlich die gleichen Überlegungen bedeutsam sein, die auch bei der Bestimmung der Anordnungshöchstfrist bei einer Quellen-Telekommunikationsüberwachung maßgeblich sind. Es sollte also erwogen werden, auch hier eine Verkürzung der Fristen vorzusehen.

7. Die Übertragung neuer Aufgaben auf die Zentralstelle für Polizeitechnik gem. § 83 POG-E enthält keine Aspekte. die aus meiner Sicht datenschutzrelevant sind.

Mit freundlichen Grüßen

Edgar Wagner