Landesbeauftragter
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

LDI NRW, Postfach 20 04 44, 40102 Düsseldorf
An die Präsidentin
des Landtags Nordrhein-Westfalen
Frau Carina Gödecke MdL
Platz des Landtags 1
40221 Düsseldorf

LANDTAG
NORDRHEIN-WESTFALEN
16 WAHLPERIODE

STELLUNGNAHME
16/682

Alle Abg

26. April 2013

Aktenzeichen
bei Antwort bitte angeben
23.1.1

Telefon 0211 38424-
Fax 0211 38424-10

vorab per Mail an:
anhoerung@landtag.nrw.de
Stichwort: "Novellierung VSG NRW – Anhörung HPA IA – 2.5.13"

Anhörung des Hauptausschusses am 02.05.2013 zu

- Reform der Ausrichtung des Verfassungsschutzes NRW und des Verfassungsschutzgesetzes NRW konsequent umsetzen, Antrag der Fraktion der FDP, Drucksache 16/2119

- Gesetz zur Neuausrichtung des Verfassungsschutzes in Nordrhein-Westfalen Gesetzentwurf der Landesregierung, Drucksache 16/2148

- Gesetz zur Änderung des Gesetzes über die Ausführung des Gesetzes zu Artikel 10 Grundgesetz (AG G10 NRW) Gesetzentwurf der Fraktion der PIRATEN, Drucksache 16/2135

Dienstgebäude und Lieferanschrift:
Kavalleriestraße 2 - 4
40213 Düsseldorf
Telefon 0211 38424-0
Telefax 0211 38424-10
poststelle@ldi.nrw.de
www.ldi.nrw.de

Öffentliche Verkehrsmittel:
Rheinbahnlinien 704, 709, 719
Haltestelle Poststraße

Sehr geehrte Frau Präsidentin,

für die Einladung zur Anhörung und die Gelegenheit zur Stellungnahme bedanke ich mich. Im Interesse einer übersichtlichen, die Zusammenhänge wahrenden Darstellung nehme ich zu nachstehenden Themenkomplexen Stellung:

1. Regelungssystematik des Gesetzes (u. a. Fragen 4, 10, 41, 43, 45)

2. Maßnahmen / Befugnisse (§ 5 Abs. 2 Nr. 10, 11 und 15, Fragenkomplex III)
3. Kernbereichsschutz (u. a. Fragen 24, 25, 43, 62-64)
4. Verfahrensvorschriften (Unabhängige Kontrolle, Benachrichtigungspflichten, Mitwirkung des LDI NRW im PKG, u. a. Fragen 15, 16, 61 und 88)
5. Recherchierbarkeit personenbezogener Daten (Fragenkomplex V)
6. Datenübermittlung an das Bundesamt für Verfassungsschutz

1. Regelungssystematik des Gesetzes (u. a. Fragen 4, 10, 41, 43, 45)

Das Verfassungsschutzgesetz Nordrhein-Westfalen enthält bereits in der geltenden Fassung an zentralen Stellen unübersichtliche Verweise, die zu Schwierigkeiten bei der Anwendung führen können. Diese werden durch die aktuellen Änderungsvorschläge nicht gelöst, sondern zum Teil sogar verstärkt.

Dies betrifft vor allem die neu geschaffenen §§ 5 bis 7c VSG NRW. Die zentrale Vorschrift des § 5 VSG NRW-E regelt in neun Absätzen die Befugnisse der Verfassungsschutzbehörde. § 5 Abs. 2 VSG NRW-E enthält einen Hinweis auf den Schutz des Kernbereichs privater Lebensgestaltung (geregelt in § 5a VSG NRW-E) und beinhaltet einen Maßnahmenkatalog mit 15 Ziffern. Die Ziffern 1, 6, 7 und 10 bis 15 enthalten weitere Verweise auf die neugeschaffenen §§ 7 bis 7c VSG NRW-E. Diese Vorschriften verweisen wiederum auf andere Normen.

Auch die Regelungen zur Verarbeitung personenbezogener Daten nach §§ 8 bis 11 VSG NRW-E werfen nach wie vor Abgrenzungsprobleme auf. So unterscheidet § 8 Abs. 1 VSG NRW-E lediglich zwischen schriftlichen oder elektronischen Akten und zur Person geführten Dateien. Die Begriffe "schriftlich" und "elektronisch" beziehen sich auf die "äußere" Beschaffenheit. Die Bezeichnung "zur Person geführt" ist inhaltsbezogen; eine Legaldefinition fehlt. Dieser Mangel setzt sich in den darauffolgenden Vorschriften fort.

Im Interesse der Rechtsklarheit sollte auch insoweit eine grundlegende Überarbeitung der Regelungsstruktur erfolgen. Es sollte zwischen schriftlichen oder elektronischen Akten und automatisierten oder nicht automatisierten Dateien unterschieden und definiert werden, in welchen Fällen Akten und Dateien "zur Sache" oder "zur Person" geführt werden.

Dies könnte entweder in § 8 VSG NRW-E oder in einer gesonderten Norm erfolgen. Die Regelung in einer gesonderten Norm hätte den Vorteil, Legaldefinitionen (z.B. solche aus § 3 Abs. 6 und 7 VSG NRW-E) an zentraler Stelle zusammen zu fassen. Eine solche zentrale Vorschrift fehlt bislang.

2. Maßnahmen / Befugnisse (§ 5 Abs. 2 Nr. 10, 11 und 15 des Entwurfs, Fragenkomplex III)

Das Anliegen, die Vorgaben der Entscheidung des Bundesverfassungsgerichts vom 27. Februar 2008 (Az.: 1 BvR 370/07) bei der Novelle des Verfassungsschutzgesetzes zu erfüllen, ist zu begrüßen. Hierbei handelt es sich ohne Zweifel um ein Vorhaben von besonderer Komplexität, insbesondere weil es darum geht, das Spannungsverhältnis zwischen dem Recht auf informationelle Selbstbestimmung einerseits und dem Schutz der verfassungsmäßigen Ordnung andererseits aufzulösen.

Gleichwohl bestehen erhebliche datenschutzrechtliche Bedenken insbesondere im Hinblick auf die vorgesehenen Befugnisse in § 5 Abs. 2 Nr. 10, 11 und 15 VSG NRW-E.

Im Einzelnen:

2.1 Maßnahmen nach § 5 Abs. 2 Nr. 10 VSG NRW-E

Abhören und Aufzeichnen der Telekommunikation und der Nutzung von Telemediendiensten sowie Öffnen und Einsehen der dem Brief- und Postgeheimnis unterliegenden Sendungen unter den Voraussetzungen des § 7a

Die Vorschrift genügt dem grundgesetzlich geforderten Bestimmheitserfordernis nicht:
Hier wird aus dem Wortlaut nicht eindeutig klar, was mit dieser Befugnis erreicht werden soll. Die Gesetzesbegründung

„Darüber hinaus wird auch ausdrücklich die Ausleitung der Daten über die Nutzung von Telemediendiensten erfasst. Darunter fallen Auskünfte über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und die von der Nutzerin, dem Nutzer in Anspruch genommenen Telemedien." (Seite 55 LT-Drs. 16/2148)

führt nicht wirklich weiter. Falls Nutzungsdaten im Sinne von § 15 Absatz 1 TMG gemeint sein sollten, unterfallen diese über § 15 Absatz 5 Satz 4 TMG bereits dem Auskunftsausspruch nach § 14 Absatz 2 TMG.

Die Einholung von Auskünften nach § 14 Absatz 2 TMG regelt der Gesetzentwurf aber eigenständig unter § 5 Absatz 2 Nr. 15.

Sofern über die Regelung in Nummer 10 Inhaltsdaten erfasst werden sollen – was die Begründung zum Gesetzentwurf gerade nicht erwähnt – erscheint die doppelte Möglichkeit zur Inanspruchnahme von Nutzungsdaten nicht durchdacht. Zum einen wird für den gleichen Vorgang an unterschiedliche Voraussetzungen angeknüpft, da für Nr. 10 die Anforderungen nach § 7a verlangt werden, für Nr. 15 die - erleichterten! - Voraussetzungen nach § 7c Absatz 3. Zum anderen bedingt dies eine unterschiedliche Unterrichtungsverpflichtung. In Nr. 15 wird die Unterrichtung untersagt, in Nr. 10 aber gerade nicht.

Überdies nimmt § 7 c Abs. 3 des Entwurfs nur auf das Telekommunikationsgesetz und nicht auf das Telemediengesetz Bezug.

Sinn macht eine solche Doppelregelung nur, wenn Nr. 10 des Entwurfes auf den Inhalt der Nutzung von Telemediendiensten – beispielsweise Mitteilungen in Chats, Foren etc. - abstellt.

In der Norm werden zugleich Eingriffsbefugnisse in das Telekommunikations- , Post- und Briefgeheimnis geregelt. Demnach muss angenommen werden, dass die Norm in der Tat insgesamt, also auch im Hinblick auf Telemediendienste, Eingriffe in grundrechtlich geschützte Bereiche erlauben soll und nicht lediglich das Beobachten offener Inhalte des Internets ermöglichen soll.

Vor diesem Hintergrund erschließt sich nicht eindeutig, inwiefern diese Befugnis sich von der in § 5 Abs. 2 des Entwurfs vorgesehenen Befugnis unterscheidet.

2.2. Maßnahmen nach § 5 Abs. 2 Nr. 11 i.V.m. § 7a VSG NRW–E

Zugriff auf zugangsgesicherte Bereiche von Telekommunikation und Telemediennutzung

§ 5 Abs. 2 Nr.11 VSG NRW-E regelt die Befugnis der Verfassungsschutzbehörde, in zugangsgesicherte Bereiche von Telekommunikation und Telemediennutzung im Internet einzudringen. Soweit einer Behörde, deren Betätigungsfeld vor allem im Vorfeld von Gefahrenlagen im polizeirechtlichen Sinne liegt, eine derart gravierende Befugnis erteilt werden soll, müssen hohe Anforderungen an die Bestimmtheit der Eingriffsermächtigung erfüllt und strenge materielle und formelle Voraussetzungen festgeschrieben werden.

Die Regelung im vorliegenden Entwurf genügt diesen Anforderungen nicht.

2.2.1. Bestimmtheit
Zunächst ist nicht klar genug beschrieben, welche Maßnahmen erlaubt werden sollen. § 5 Abs. 2 Nr. 11 regelt die Befugnis zur Beobachtung zugangsgesicherter Bereiche des "Internets", ohne diese zu definieren. Insbesondere wird aus der Formulierung der Vorschrift nicht deutlich, was mit dem Zugriff "auf dem technisch hierfür vorgesehen Weg" gemeint sein soll. Es genügt für die verfassungsrechtlichen Bestimmtheitsanforderungen nicht, wenn sich lediglich aus der Gesetzesbegründung Hinweise darauf ergeben, was mit der gesetzgeberischen Formulierung gemeint sein soll.

Zur rechtsklaren Beschreibung der beabsichtigten Maßnahmen gehört auch, dass die Funktion deutlich wird, die der in § 5 Abs. 2 Nr.15 geregelten Erhebung von Bestandsdaten einschließlich Zugangssicherungsdaten im Rahmen der Eingriffsbefugnis nach § 5 Abs. 2 Nr.11 zukommen soll. Offenbar kann die Maßnahme erst durchgeführt werden, wenn Zugangsdaten nach § 5 Abs. 2 Nr. 15 des Entwurfs erlangt worden sind. Für die Erhebung dieser Daten gelten wiederum andere Voraussetzungen. (s. dazu auch unten zu § 5 Abs. 2 Nr.15).

2.2.2. Eingriffsschwelle
Der Entwurf legt für diese Befugnis die gleiche Eingriffsschwelle fest, wie für bestimmte andere, besonders grundrechtsintensive Maßnahmen (Abhören außerhalb von Wohnungen, Beobachten des Funkverkehrs, Telekommunikationsüberwachung).

Die Befugnis weist eine erhöhte Eingriffsintensität auf, weil sie, nachdem ein Zugangscode oder ein Passwort einmal verschafft worden ist, der Behörde einen Zugriff nunmehr unabhängig von der Mitwirkung anderer

Stellen eröffnet, der im Übrigen inhaltlich, zeitlich und räumlich unbegrenzt ist.

Aufgrund der Überwindung spezifischer Zugriffsschutzeinrichtungen, unter Umständen auch der damit verbundenen Möglichkeit der Behörde, sich wie der Nutzer zu gerieren, weist das Gefahrenpotenzial dieser Maßnahme insoweit Elemente der Gefahrenlage auf, wie sie bei einer "Online-Durchsuchung" vorliegt. Daher sind die Anforderungen, die das Bundesverfassungsgericht in seiner Entscheidung zu sogenannten "Online-Durchsuchung" (BVerfGE 120, 274) aufgestellt hat, auch hier in den Blick zu nehmen.

Das Bundesverfassungsgericht hat in der genannten Entscheidung (Rn. 224) folgendes festgestellt:

"Der Grundrechtseingriff, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, entspricht im Rahmen einer präventiven Zielsetzung angesichts seiner Intensität nur dann dem Gebot der Angemessenheit, wenn bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen, selbst wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt."

Derart überragend wichtige Rechtsgüter können nach dem Bundesverfassungsgericht (a.a.O. Rn. 247) "solche Güter der Allgemeinheit" sein, "deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt." Als mögliches Beispiel nennt das Bundesverfassungsgericht "die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen".

Diese Gefahrensituation wird in § 7a Abs. 3 VSG NRW-E nicht näher bestimmt. Im Gegenteil formuliert der Entwurf nur vage, es müssten *"bestimmte Tatsachen die Annahme rechtfertigen, dass eine drohende Gefahr für die freiheitlich-demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes (...) vorliegt".* Diese allgemeine Formulierung stellt keine den Anforderungen des Bundesverfassungsgerichts a.a.O. entsprechende Hürde auf.

Als zusätzliche Elemente der Gefahrensituation fordert § 7a des Entwurfs in Absatz 4 zwar tatsächliche Anhaltspunkte für das Begehen oder die Planung einer Katalogstraftat. Dies kann die zu allgemeine Definition

der gefährdeten Güter jedoch nicht kompensieren. Zudem ist der Straftatenkatalog im Wesentlichen ein auf die Ziele des Verfassungsschutzes bezogener Ausschnitt aus dem Straftatenkatalog der strafprozessualen Ermächtigungsgrundlage für eine Telekommunikationsüberwachung (§ 100a StPO), er ist jedoch nicht auf schwere Straftaten beschränkt und enthält z.B. zusätzliche Tatbestände aus dem Vereinsgesetz, die vom Strafrahmen her teilweise nicht einmal dem Bereich der mittleren Kriminalität zuzurechnen sind.

2.3. Maßnahmen nach § 5 Abs. 2 Nr. 15 i. V. m. § 7c Abs. 3

Erhebung von Daten nach dem Telekommunikationsgesetz und dem Telemediengesetz

Die Eingriffsschwelle in § 5 Abs. 2 Nr. 15 VSG NRW-E i. V .m. § 7 c Abs. 3 VSG NRW-E liegt insgesamt zu niedrig, da in § 7c Abs. 3 VSG NRW-E keine spezifischen Eingriffsvoraussetzungen für Bestandsdatenerhebungen geregelt werden und die damit anwendbare Erlaubnisnorm in § 5 Abs. 1 VSG NRW zu allgemein und weit gefasst ist und insoweit wiederum dem Bestimmtheitserfordernis nicht entspricht. Wegen der unterschiedlich tiefen Grundrechtsbetroffenheit wäre zudem eine Differenzierung der Eingriffsvoraussetzungen nach einfachen Bestandsdatenauskünften, Erhebung unter Verwendung dynamischer IP-Adressen, von PIN und PUK-Nummern oder sogar Passwörtern erforderlich.

2.3.1. Bestandsdaten allgemein

Nach dem Gesetzentwurf sollen "einfache" Bestandsdatenauskünfte (z. B. Auskunft über die zu einer Person gehörende Anschlussnummer vor der Überwachung dieser Person) allein auf Grundlage der § 5 Abs. 1 VSG NRW-E i. V. m. § 3 Abs. 1 VSG NRW-E und damit auch im Zuge bloßer Vorfeldermittlungen zulässig sein. Dies wird den verfassungsrechtlichen Anforderungen an einen derartigen Grundrechtseingriff nicht gerecht. Auch für einfache Bestandsdatenauskünfte vom Telekommunikationsanbieter muss zumindest eine Beschränkung der Datenerhebung auf Einzelfälle geregelt werden (vgl. BVerfGE v. 24.01.2012, Az.: 1 BvR 1299/05, Rn. 177). Dies bedeutet für die Erhebung durch Nachrichtendienste, dass die Auskunft zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung geboten sein muss (BVerfGE v. 24.01.2012, Az.: 1 BvR 1299/05, Rn. 177).

2.3.2 Dynamische IP-Adressen

Bei dynamischen IP-Adressen zeigt sich ein enger Zusammenhang zwischen Bestandsdaten einerseits und Verbindungs- und Inhaltsdaten andererseits. Insbesondere die Beauskunftung unter Verwendung dynamischer IP-Adressen bedeutet nicht nur praktisch die Auskunft über einen Verbindungsteilnehmer, sondern oft zugleich auch über die Inhalte der von ihm aufgerufenen Website oder sonstigen Zieladresse, da diese im Internet in der Regel auch nachträglich noch abrufbar sind (BVerfGE v. 02.03.2010, Az.: 1 BvR 256/08, Rn. 259; ebenso BVerfGE v. 24.01.2012, Az.: 1 BvR 1299/05, Rn. 174). Die Beauskunftung unter Verwendung dynamischer IP-Adressen stellt daher einen Eingriff in Art. 10 GG dar (BVerfGE v. 24.01.2012, Az.: 1 BvR 1299/05, Rn 116 f., 120 und 173).

Zwar regelt § 5 Abs. 2 Nr. 15 ausdrücklich die Abfrage von Bestandsdatenauskünften "auch anhand einer zu bestimmten Zeitpunkten zugewiesenen Internetprotokolladresse (§ 113 Absatz 1 Satz 3 TKG)" und knüpft insoweit an die vom Bundesverfassungsgericht getroffene Feststellung zu § 113 TKG an, dass eine normenklare Befugnis zur Identifizierung von dynamischen IP-Adressen im Rahmen der Bestandsdatenauskunft nicht bestehe (Entscheidung vom 24.01.2012, 1 BvR 1288/05, Rn. 174). Die Vorschrift des VSG NRW-E legt aber keine hinreichend hohe Eingriffsschwelle für diesen Eingriff in das Fernmeldegeheimnis nach Art. 10 GG fest.

Aus dem Eingriff in das Fernmeldegeheimnis folgt, dass der Eingriff nicht unter den gleichen materiellen Voraussetzungen zulässig sein kann, wie einfache Bestandsdatenauskünfte, die nur in das informationelle Selbstbestimmungsrecht eingreifen. § 5 Abs. 2 Nr. 15 i. V .m. § 7c Abs. 3 VSG NRW-E trifft hierzu keine Regelung. Die allgemeine Datenerhebungserlaubnis nach § 5 Abs. 1 VSG NRW-E i. V. m. § 3 Abs. 1 VSG NRW-E, die schon für einfache Bestandsdatenauskünfte nicht hinreicht, genügt erst recht nicht als Grundlage für einen derartig gesteigerten Grundrechtseingriff. Voraussetzung für die Beauskunftung dynamischer IP-Adressen ist auch für Nachrichtendienste zumindest eine auf tatsächliche Anhaltspunkte gestützte konkrete Gefahr; die rechtlichen und tatsächlichen Grundlagen entsprechender Auskunftsbegehren sind aktenkundig zu machen (BVerfGE v. 02.03.2010, Az.: 1 BvR 256/08, Rn. 261).

Auch für diesen Eingriff halte ich eine Vorabprüfung durch einen Richter oder eine in gleicher Weise unabhängige Instanz (G 10-Kommission) für erforderlich.

2.3.3. Zugangssicherungsdaten (PIN/PUK, Passwörter)

§ 5 Abs. 2 Nr.15 i. V. m. § 7c Abs. 3 VSG NRW-E befasst sich mit der Erhebung von Zugangssicherungsdaten bei TK-Anbietern. Hierbei wird es sich in der Regel um die Erhebung von PIN und PUK, eventuell auch Passwörtern handeln, was sich im Übrigen ohne Fachkenntnis der Materie allein aus dem Wortlaut des § 7c Abs. 3 des Entwurfs kaum erschließt. Ich halte es außerdem mit Blick auf die Rechtsklarheit nicht für akzeptabel, dass durch Verweisungstechnik Eingriffsbefugnisse von besonderer Intensität erst im Weiteren erkennbar werden.

Diese Zugangssicherungsdaten weisen gegenüber anderen Bestandsdaten einen erhöhten Schutzbedarf auf, da sie den Zugang zu den Endgeräten und Speichereinrichtungen verschaffen. Bezüglich der Erhebung von Passwörtern ist zu beachten, dass ein Grundrechtseingriff erheblich intensiviert wird, wenn durch eine Überwachungsmaßnahme Maßnahmen des informationellen Selbstschutzes der betroffenen Person vereitelt werden (vgl. BVerfGE v. 27.02.2008, Az.: 1 BvR 370/1, Rn. 218). Deshalb sind sowohl an die Klarheit der Eingriffsgrundlage als auch an die Rechtfertigung des Eingriffs hohe Anforderungen zu stellen. Diesen genügen die Vorschriften des Entwurfs nicht.

Im Vergleich der Regelungsgegenstände von § 5 Abs. 2 Nr. 15 und § 7c Abs. 3 des Entwurfs zeigt sich folgende Unklarheit: Sind mit der Erhebungsbefugnis nach § 5 Abs. 2 Nr. 15 auch Passwörter für die Nutzung von Telemediendiensten gemeint, was nach dem weiten Wortlaut der Fall sein dürfte, so eröffnet sich hier eine gravierende Gesetzeslücke, weil in § 7 c Abs. 3 die besonderen Eingriffsvoraussetzungen für die Erhebung von Zugangssicherungsdaten nur für den Bereich des § 113 TKG geregelt sind.

Außerdem ist die Eingriffsschwelle weder für die Erhebung von PIN- und PUK-Nummern noch für die Ermittlung von Passwörtern hinreichend klar normiert. Welche Eingriffsvoraussetzungen § 7c Abs. 3 VSG NRW-E über die Grundsatznorm des § 5 Abs. 1 VSG NRW-E hinaus festlegen will, bleibt nach dem Gesetzeswortlaut

- *"ein Verlangen, über die dort genannten Zugangssicherungsdaten Auskunft zu erhalten "ist nur zulässig, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen"* -

und der systematischen Auslegung des Gesetzes unklar, da besondere Vorschriften mit gesetzlichen Voraussetzungen für die Nutzung von Zugangsschutzdaten im Gesetzentwurf fehlen und die allgemeine Datenverarbeitungsvorschrift des § 5 Abs. 1 VSG NRW-E hier keine beschränkende Wirkung besitzt.

Hier wird lediglich ein Zitat des Bundesverfassungsgerichts ins Gesetz aufgenommen, das ohne den argumentativen Zusammenhang der Entscheidung nicht verständlich ist. Es ist dringend eine gesetzgeberische Klarstellung erforderlich.

Im Entwurf der Gesetzesbegründung (S. 10) heißt es, mit den "gesetzlichen Voraussetzungen für die Nutzung der Daten" in § 7c Abs. 3 seien die "gesetzlichen Voraussetzungen für die Nutzung der damit zu erlangenden Daten" gemeint. Es fehlen jedoch im Gesetzentwurf entsprechende Daten**nutzungs**vorschriften. Geregelt sind vielmehr Voraussetzungen für bestimmte Daten**erhebungs**maßnahmen (§ 5 Abs. 2 i. V m. §§ 7, 7a-c). Diese sollen offenbar auch unter Verwendung der mit einer Maßnahme nach § 5 Abs. 2 Nr. 15 i. V. m. § 7c erlangten Zugangsschutzdaten durchgeführt werden können.

Auch die entsprechende Passage aus der Entscheidung des Bundesverfassungsgerichts vom Januar 2012, die hier offenbar umgesetzt werden soll (vgl. BVerfGE v. 24.01.2012, Az.: 1 BvR 1299/05, Rn. 185), liest sich so, dass es bei den Voraussetzungen für die Nutzung um die Nutzung der Zugangssicherungsdaten im Rahmen einer weiteren Maßnahme gehen soll (ebenso BVerfG 1 BvR 256/08 vom 02.03.2012 Rn. 258 ff.). So verstanden wären die zu prüfenden zusätzlichen gesetzlichen Voraussetzungen für die Nutzung der Daten je nach Maßnahme, in deren Rahmen sie verwendet werden sollen, dem § 5 Abs. 2 VSG NRW-E, den darin in Bezug genommenen Vorschriften, und den §§ 5 Abs. 3, 4, 8, 9, 5a, 5b, 5c VSG NRW-E zu entnehmen. Diesen gesetzlichen Voraussetzungen käme zwar eine eingriffsbeschränkende Wirkung zu. Dass dies mit "Voraussetzungen der Nutzung" gemeint ist, kommt aber im Gesetz nicht hinreichend zum Ausdruck.

Ferner erfüllt die bloße Wiedergabe der abstrakten Anforderung des Bundesverfassungsgerichts im Gesetzestext nicht die Pflicht des Gesetzgebers, die Zulässigkeitsvoraussetzungen für die Datenerhebung im Gesetz konkret festzulegen. Die Zulässigkeitsvoraussetzungen der Erhebung von Zugangssicherungsdaten müssen in Abhängigkeit von der unter Verwendung dieser Daten geplanten Maßnahme vom Gesetzgeber klar bezeichnet werden.

Dabei ist insbesondere festzulegen, dass im Zeitpunkt der Erhebung der Zugangsschutzdaten bereits feststehen muss, für welche Maßnahme diese verwendet werden sollen, das heißt, welche Überwachungsmaßnahme auf welcher Rechtsgrundlage mit Hilfe der Zugangsberechtigungsdaten durchgeführt werden soll (vgl. den "in der Abfragesituation damit konkret erstrebten Nutzungszweck", BVerfGE v. 24.01.2012, Az.: 1 BvR 1299/05, Rn. 185 a. E.), denn es ist erforderlich, die Zulässigkeit der Erhebung der Passwörter bereits im Zeitpunkt des Auskunftsverlangens beurteilen zu können. Ferner muss sichergestellt sein, dass die so erlangten Daten nur für diese Maßnahme und nicht etwa für höherschwellige Maßnahmen eingesetzt werden dürfen.

2.3.4 Richtervorbehalt/ G 10-Kommission

Entsprechend der jeweiligen Eingriffsintensität sind die von § 5 Abs. 2 Nr. 15 VSG NRW-E umfassten Maßnahmen in die Verweisungen der §§ 5b und 5c VSG NRW-E aufzunehmen.

Zugriffe auf Zugangsberechtigungsdaten ohne Wissen des Betroffenen dürfen nur nach einer Vorabkontrolle durch ein Gericht oder ein gleichwertiges Gremium (G 10-Kommission) durchgeführt werden. Entsprechend beabsichtigt auch der Bundesgesetzgeber (Beschluss des Bundestags vom 21. März 2013, BR-Drs. 251/13) inzwischen, für die Abfrage solcher Daten durch Ermittlungsbehörden im geplanten § 100j StPO einen Richtervorbehalt einzufügen und im Bereich des Verfassungsschutzes die Verfahrensregeln des § 8b BVerfSchG für anwendbar zu erklären.

3. Kernbereichsschutz (u. a. Fragen 24, 25, 43, 62-64)

Zwar wird mit der Aufnahme eines neuen § 5a VSG NRW-E erstmals eine Regelung zum Schutz des Kernbereichs privater Lebensgestaltung

im Verfassungsschutzgesetz NRW getroffen. Allerdings werden die vom Bundesverfassungsgericht bisher dazu aufgestellten Maßgaben nicht vollständig umgesetzt. Zur Gewährleistung der verfassungsrechtlichen Vorgaben wäre es erforderlich, weitere konkrete Regelungen zu den jeweiligen Ermächtigungsnormen zu schaffen. Diese sollten flankierende Verfahrensregelungen für die jeweiligen Fallgruppen enthalten.

Zu den Regelungen im Einzelnen:

3.1 § 5a Abs. 1 VSG NRW-E (Unzulässigkeit der Datenerhebung)

Die Regelung zur Unzulässigkeit von Datenerhebungen, die den Kernbereich privater Lebensgestaltung berühren, wird ausdrücklich begrüßt. Sie entspricht dem sogenannten Stufenmodell des Bundesverfassungsgerichts (BVerfG, Urt. v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 280 ff.). Begrüßt wird auch die Klarstellung zur Geltung für Berufsgeheimnisträger sowie insbesondere die Konkretisierung der Anforderungen im Bereich der Brief- und Postsendungen und automatisiert erhobenen Daten.

3.2 § 5a Abs. 2 VSG NRW-E (Unterbrechung der Datenerhebung)

Die in § 5a Abs. 2 VSG NRW-E enthaltene Pflicht zur Unterbrechung der Datenerhebung bei Bekanntwerden von Anhaltspunkten für eine Betroffenheit des Kernbereichs privater Lebensgestaltung steht unter dem Vorbehalt, dass die Unterbrechung "informationstechnisch und ermittlungstechnisch möglich" ist. Die Begriffe werden nicht legaldefiniert. Dies kann zu Unsicherheiten bei der Rechtsanwendung führen. Zudem genießt der Kernbereich privater Lebensgestaltung absoluten Schutz. Demnach müssten jedenfalls bei tatsächlich festgestellten Beeinträchtigungen des Kernbereichs Maßnahmen nach § 5 Abs. 2 VSG NRW-E kategorisch abgebrochen werden (vgl. ausführlich Sachs/Krings, NWVBl 2010, 165, 167 f. mit zahlreichen Verweisen auf die einschlägige Rspr. des BVerfG). Die Unterbrechung einer Datenerhebung darf somit nicht von informations- oder ermittlungstechnischen Umständen abhängen.

Weiter ist dem Wortlaut nach zwar die "Erhebung" von Daten zu unterbrechen. Ausweislich der Gesetzesbegründung soll jedoch lediglich die "Aufzeichnung" unterbrochen werden. Ein "Live-Mithören" bleibt zur Wahrnehmung tatsächlicher Anhaltspunkte, dass keine kernbereichsrelevanten Daten mehr erhoben werden, zulässig. Ein solches Grundverständnis begegnet vor dem Hintergrund der vorbenannten Vorgaben des Bundesverfassungsgerichts erheblichen Bedenken. Zudem unter-

scheidet beispielsweise § 100c Abs. 5 StPO für die Wohnraumüberwachung zwischen "Abhören" und "Aufzeichnen" und fordert im Bedarfsfall einen Abbruch beider Maßnahmen.

Im Übrigen ist die Erhebung gemäß § 5a Abs. 2 VSG NRW-E "solange wie erforderlich" zu unterbrechen. Diese Regelung ist unvollständig und bleibt hinter den in anderen Vorschriften enthaltenen Verfahrensvorgaben zurück.

Zur Datenerhebung durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen enthält z. B. § 18 Abs. 4 PolG NRW folgende Präzisierungen:

"Die Datenerhebung ist unverzüglich zu unterbrechen, sofern sich während der Überwachung tatsächliche Anhaltspunkte dafür ergeben, dass Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Bestehen insoweit Zweifel, darf statt der unmittelbaren Wahrnehmung nur noch eine automatisierte Aufzeichnung erfolgen. Nach einer Unterbrechung oder einer Aufzeichnung gemäß Satz 2 darf die Erhebung fortgesetzt werden, wenn zu erwarten ist, dass die Gründe, die zur Unterbrechung oder zur Aufzeichnung geführt haben, nicht mehr vorliegen. Die automatisierte Aufzeichnung ist unverzüglich dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen. Für die nicht verwertbaren Teile ordnet das Gericht die unverzügliche Löschung an. Das Gericht unterrichtet die Polizeibehörde unverzüglich über den Inhalt der verwertbaren Teile der Aufzeichnung. Die Tatsachen der Datenerfassung und der Löschung sind zu dokumentieren. Die Maßnahme ist abzubrechen, wenn die Voraussetzungen des Absatzes 1 nicht mehr vorliegen."

Vor dem Hintergrund, dass die Verfassungsschutzbehörde NRW anders als die Polizei im Vorfeld von Straftaten, Strafermittlungen oder tatsächlich bestehenden konkreten Gefahren im polizeirechtlichen Sinne agiert, erscheint die in § 5a Abs. 2 VSG NRW-E aufgenommene Beschränkung der Datenerhebung ("solange wie erforderlich") demnach nicht ausreichend. Insbesondere fehlen gesonderte verfahrensrechtliche Vorgaben für den Fall der Fortsetzung der Datenerhebung nach einer Unterbrechung.

4. Verfahrensvorschriften
Unabhängige Kontrolle, Benachrichtigungspflichten, Mitwirkung des LDI NRW im PKG

4.1. Rolle der G 10-Kommission (§ 5b VSG NRW-E)

Nach der Intention des Gesetzentwurfs soll an Stelle des Richtervorbehalts eine Kontrollkompetenz der G 10-Kommission bestehen. Die Gleichwertigkeit dieses Instruments mit dem Richtervorbehalt, wie er im Strafprozessrecht normiert ist, würde mit dem Gesetzentwurf aber nicht hergestellt.

Zum Vergleich: Im Strafverfahren können die unter Richtervorbehalt stehenden Ermittlungsmaßnahmen im Normalfall nur vom Richter angeordnet werden. Im Eilfall muss für die dann mögliche staatsanwaltschaftliche Anordnung eine richterliche Bestätigung innerhalb von 3 Tagen eingeholt werden.

Eine vergleichbare grundrechtsschützende Bedeutung kann die Kontrolle durch die G 10-Kommission nur besitzen, wenn die Einschaltung der G 10-Kommission die gleiche Funktion der Vorabkontrolle erhält wie der Richtervorbehalt im strafrechtlichen Ermittlungsverfahren. Hierzu genügt es nicht, dass die G 10-Kommission durch Unterrichtung Gelegenheit zur Prüfung der Maßnahme hat. Es ist vielmehr erforderlich, dass die Zustimmung der G 10-Kommission eine Zulässigkeitsvoraussetzung für die Anordnung oder zumindest für den Vollzug der Maßnahme darstellt. Dies ist nach der bisherigen Fassung des Entwurfs nicht gewährleistet:

Nach § 5b Abs. 1 des Entwurfs wird die Maßnahme von der Leitung der Verfassungsschutzabteilung beantragt und vom Innenminister/ von der Innenministerin angeordnet. Die G 10-Kommission muss vor Vollzug der Maßnahme nur "unterrichtet" werden. Lediglich dann, wenn aus Eilgründen vor Anordnung keine "Unterrichtung" der G 10-Kommission erfolgen konnte, wird von einer "Entscheidung" der G 10-Kommission gesprochen, die unverzüglich nachzuholen sei.

Der Wortlaut des Gesetzes ist hier unklar.

Es muss gesetzlich festgelegt sein, dass im "Normalfall" die Entscheidung der G 10-Kommission vor Durchführung der Maßnahme eingeholt wird und sie ohne Zustimmung der G 10-Kommission unzulässig ist.

4.2 Benachrichtigungspflichten, Rolle der G 10-Kommission (§ 5 Abs. 5 VSG NRW-E, u. a. Fragen 15, 61)

Grundsätzlich hat die Benachrichtigung Betroffener mit Beendigung der Maßnahme zu erfolgen.

Bestimmtheit:
Problematisch sind hier die Verfahrensregelungen zu den Ausnahmefällen, in denen die Benachrichtigungen zunächst unterbleiben müssen, jedoch Prüffristen laufen. Die diesbezüglichen Vorschriften sind nicht bestimmt genug gefasst. Es ist dem Wortlaut nach ins Ermessen der zuständigen Stelle gestellt, ob die Benachrichtigung unterbleiben soll. Ferner ist im Falle des Unterbleibens nur bei besonders schwerwiegenden Eingriffen nach 12 Monaten eine Entscheidung der G 10-Kommission vorgesehen, deren Verfahren jedoch nicht gesetzlich normiert wird.

Eingriffsschwelle:
Diese Regelungen entsprechen vor dem Hintergrund, dass Betroffene ohne Kenntnis von den über sie gespeicherten Speichertatbeständen vom Rechtsschutz gemäß Artikel 19 Abs. 4 Grundgesetz gänzlich abgeschnitten werden, nicht den verfassungsrechtlich vorgesehenen Maßgaben.

4.3 Mitwirkung des LDI NRW im Parlamentarischen Kontrollgremium (Frage 88)

Bei der Entscheidung über die Zusammensetzung des Parlamentarischen Kontrollgremiums dürfte zu berücksichtigen sein:

- Die Kontrolle des Verfassungsschutzes wird in Nordrhein-Westfalen durch das Parlament wahrgenommen. Die Kontrolle umfasst auch auf der Grundlage des Gesetzes zu Artikel 10 Grundgesetz angeordnete Beschränkungsmaßnahmen, § 23 Abs. 1 VSG NRW

- Das Parlamentarische Kontrollgremium sowie die G 10-Kommission können aber bereits nach der gegenwärtigen und weiter vorgesehenen Rechtslage dem Landesbeauftragten für den Datenschutz und Informationsfreiheit Gelegenheit zur Stel-

lungnahme in Fragen des Datenschutzes geben, § 25 Abs. 5 VSG NRW-E sowie § 3 Abs. 5 AG G 10 NRW bzw. § 30 Abs. 5 Satz 4 VSG NRW-E

- Die Mitwirkung eines Landesbeauftragten in einem Gremium zur Kontrolle des Verfassungsschutzes stellt dessen Unabhängigkeit in Frage, weil sie zu einer operativen Mitverantwortung des Landesbeauftragten führt oder mindestens zu führen vermag.

Insbesondere mit Blick auf meine Unabhängigkeit befürworte ich, an der gegenwärtigen bzw. weiter vorgesehenen Regelung festzuhalten, nach der Gelegenheit zur Stellungnahme in Fragen des Datenschutzes besteht.

5. Recherchierbarkeit personenbezogener Daten (Fragenkomplex V)

§ 8 Abs. 4 VSG NRW-E enthält besondere Regelungen zu elektronischen Sachakten mit zu weitgehenden Befugnissen für Recherchen nach Personen oder nach Informationen zu Personen. Auch diese Befugnisnormen sind an den hohen Schwellen der Rechtsprechung zum Recht auf informationelle Selbstbestimmung zu messen.

Gemäß § 8 Abs. 4 **Satz 3 Alternative 2** VSG NRW-E ist eine Abfrage personenbezogener Daten zulässig, wenn für sie die Voraussetzungen der Speicherung nach § 8 Abs. 1 VSG NRW-E vorliegen. Diese Regelung begegnet durchgreifenden datenschutzrechtlichen Bedenken.

Nach der bisher geltenden Fassung der Vorschrift dürfen personenbezogene Daten ab dem Zeitpunkt der Löschung der zur Person geführten Dateien nicht mehr elektronisch recherchierbar sein. Durch diese Beschränkung wird sichergestellt, dass die besonderen Regelungen für die Speicherung in personenbezogenen Dateien nicht durch die Möglichkeiten des automatisierten Zugriffs auf elektronische Sachakten umgangen werden können, oder dass personenbezogene Daten nur dann recherchiert werden dürfen, sobald und solange gleichzeitig eine zur Person geführte Datei existiert.

Diese Sicherung wird durch den Verweis auf § 8 Abs. 1 VSG NRW-E aufgegeben. Ein sachlicher Grund ist hierfür nicht erkennbar.

Im Übrigen widersprechen sich die Regelungen. Einerseits bleibt in Absatz 4 der Satz 3 der geltenden Fassung bestehen. Danach wird, wie zuvor ausgeführt, die Recherchierbarkeit von personenbezogenen Daten für Zwecke des Verfassungsschutzes beschränkt. Andererseits sieht die Neuregelung gerade eine – wie beschrieben, unzureichende – Beschränkung vor.

Eingriffsschwelle:
Ausweislich der Begründung soll der Schutz solcher personenbezogener Daten verstärkt werden, die im Rahmen einer automatisierten Volltexterfassung im Kontext anderer Personen oder Organisationen zwangsläufig mitgespeichert wurden, ohne selbst die in Absatz 1 genannten Speichervoraussetzungen zu erfüllen (u. a. Mitbetroffene oder Randpersonen). Dieses Ziel wird jedoch nicht erreicht. Die Recherchierbarkeit von in Sachakten gespeicherten personenbezogenen Daten darf nicht schon bei bloßem Vorliegen der Voraussetzungen für eine Speicherung in der Amtsdatei nach Absatz 1 möglich sein. Erst die tatsächlich erfolgte Speicherung in der Amtsdatei soll die elektronische Recherchierbarkeit in einer Sachkate ermöglichen.

Dies ist auch von der verwaltungsgerichtlichen Rechtsprechung für den Zeitraum, in dem eine zur Person geführte Datei noch nicht existiert, so entschieden worden. Die Möglichkeit der elektronischen Recherchierbarkeit personenbezogener Daten in Sachakten müsse ganz allgemein an die gleichzeitige Speicherung einer zu der jeweiligen Person geführten Datei gekoppelt sein. Dadurch sei bereits zum erstmaligen Speicherungszeitpunkt der personenbezogenen Daten eines Betroffenen in der elektronischen Sachakte sichergestellt, dass die Möglichkeit einer gezielten elektronischen Recherche nach diesen Daten wirksam ausgeschlossen sei.

Im Ergebnis dürfen in elektronischen Sachakten personenbezogene Daten nur dann recherchiert werden, sobald und solange gleichzeitig eine zur Person geführte Datei existiert. Dies ist im Text des § 8 Abs. 4 S. 3 Alt. 2 VSG NRW-E zu verankern. Die einfache Bezugnahme auf Absatz 1 der Vorschrift geht fehl.

6. Datenübermittlung an das Bundesamt für Verfassungsschutz

Zu § 18 Abs. 1 VSG NRW-E (Datenübermittlung an das BfV)

Zukünftig wird der Verfassungsschutzbehörde NRW die Pflicht auferlegt, "alle sachdienlichen Informationen" an das Bundesamt für Verfassungsschutz zu übermitteln, "sofern sie für dessen Aufgabenerfüllung erforderlich sind". Zwar werden die Aufgaben des BfV aufgrund seiner Koordinierungsfunktion allein bundesgesetzlich festgelegt. Die Bindung der Datenübermittlung an diese Voraussetzungen auf der Empfängerseite entspricht jedoch dem auch im Datenschutzgesetz NRW verankerten Erforderlichkeitsprinzip. Voraussetzung hierfür muss aber sein, dass die Sicherheitsarchitektur des Verfassungsschutzes in Bund und Ländern unverändert von den tragenden verfassungsrechtlichen Prinzipien ausgeht.

(Lepper)