

## **BESCHLUSSEMPFEHLUNG UND BERICHT**

**des Innenausschusses (2. Ausschuss)**

**zu dem Gesetzentwurf der Landesregierung  
- Drucksache 6/1630 -**

**Entwurf eines Gesetzes zur Änderung des Landesverfassungsschutzgesetzes  
und des Sicherheits- und Ordnungsgesetzes zur Regelung der Bestandsdaten-  
auskunft**

### **A. Problem**

Nach dem Urteil des Bundesverfassungsgerichtes zum Aktenzeichen 1 BvR 1299/05 sind die Regelungen zum manuellen Auskunftsverfahren in § 113 Telekommunikationsgesetz (TKG) so auszulegen, dass sie für Auskunftsverlangen in Bereichen, deren Regelung dem Landesrecht vorbehalten ist, spezifische Rechtsgrundlagen der Länder voraussetzt, die eine Auskunftsverpflichtung der geschäftsmäßigen Anbieter von Telekommunikationsdiensten (Diensteanbieter) eigenständig begründen. Es bedarf in den jeweiligen Landesgesetzen qualifizierter Vorschriften, die den berechtigten Stellen erlauben, Telekommunikationsdaten überhaupt bei den Diensteanbietern abzufordern. Zudem gelangte das Bundesverfassungsgericht zu der Auffassung, dass § 113 Absatz 1 Satz 1 TKG nicht als Rechtsgrundlage für eine Zuordnung von dynamischen Internetprotokoll-Adressen zu ihren Anschlussinhabern herangezogen werden kann, da für diese Auskunft auf Verkehrsdaten zurückgegriffen werden muss und die Vorschrift hierzu erkennbar nicht ermächtigt. Darüber hinaus stellte das Gericht fest, dass § 113 Absatz 1 Satz 2 TKG nicht mit dem Recht auf informationelle Selbstbestimmung vereinbar ist, da die Vorschrift die Auskunft über Zugangssicherungs\_codes (wie Passwörter, PIN oder PUK) nicht an die Bedingung knüpft, dass eine Auskunft über Sicherungs\_codes nur dann verlangt werden darf, wenn auch die rechtlichen Voraussetzungen für deren Nutzung erfüllt sind.

Aufgrund des sich aus dieser Entscheidung ergebenden, gesetzgeberischen Handlungsbedarfs und angesichts der Bedeutung solcher Datenauskünfte für die Aufklärung von Gefahren und Straftaten hat das Bundesverfassungsgericht eine Übergangsregelung getroffen. Es hat die Anwendung des bestehenden § 113 TKG längstens bis zum 30. Juni 2013 zugelassen. Damit die Möglichkeit der Abfrage von Bestandsdaten nach dem neugefassten § 113 TKG der Landespolizei und der Verfassungsschutzbehörde des Landes Mecklenburg-Vorpommern auch nach Auslaufen der vom Bundesverfassungsgericht gesetzten Übergangsfrist weiter zur Verfügung steht, besteht landesgesetzgeberischer Handlungsbedarf.

## **B. Lösung**

Unter Beachtung der bundesverfassungsrechtlichen Vorgaben sind Bestimmungen im Landesrecht zu schaffen, die die Voraussetzungen für das Erlangen von Datenauskünften nach § 113 TKG von den Diensteanbietern festlegen. Diese spezifischen Befugnisse werden für die Landespolizei im Sicherheits- und Ordnungsgesetz und für die Verfassungsschutzbehörde im Landesverfassungsschutzgesetz aufgenommen. Es werden keine neuen Datenerhebungsbefugnisse geschaffen. Vielmehr werden die derzeit auf Grundlage des Bundesrechts abgeforderten Datenauskünfte nun zukünftig unter Bezugnahme auf landesrechtliche Normen, die den verfassungsrechtlichen Vorgaben entsprechen, verlangt.

## **Mehrheitsentscheidung im Ausschuss**

### **C. Alternativen**

Keine.

### **D. Kosten**

Keine.

## **Beschlussempfehlung**

Der Landtag möge beschließen,

den Gesetzentwurf der Landesregierung auf Drucksache 6/1630 mit der folgenden Maßgabe und im Übrigen unverändert anzunehmen:

Artikel 1 wird wie folgt geändert:

In Nummer 2 werden in Absatz 1 nach den Wörtern „oder daran mitwirkt,“ die Wörter „im Einzelfall“ eingefügt.

Schwerin, den 6. Juni 2013

### **Der Innenausschuss**

**Marc Reinhardt**

Vorsitzender und Berichterstatter

## **Bericht des Abgeordneten Marc Reinhardt**

### **I. Allgemeines**

Der Landtag hat den Gesetzentwurf der Landesregierung, Entwurf eines Gesetzes zur Änderung des Landesverfassungsschutzgesetzes und des Sicherheits- und Ordnungsgesetzes zur Regelung der Bestandsdatenauskunft, auf Drucksache 6/1630 in seiner 36. Sitzung am 20. März 2013 in Erster Lesung beraten und zur weiteren Beratung an den Innenausschuss überwiesen.

Der Innenausschuss hat sich in seiner 30. Sitzung am 11. April 2013 darauf verständigt, zu diesem Gesetzentwurf eine Anhörung durchzuführen. Die öffentliche Anhörung hat am 23. Mai 2013 stattgefunden. Im Rahmen des Anhörungsverfahrens hat der Innenausschuss den Landkreistag Mecklenburg-Vorpommern e. V., den Städte- und Gemeindetag Mecklenburg-Vorpommern e. V., den Landesbeauftragten für den Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, die Gewerkschaft der Polizei, Landesbezirk Mecklenburg-Vorpommern, die Deutsche Polizeigewerkschaft im dbb, Landesverband Mecklenburg-Vorpommern, Prof. Dr. Kyrill-Alexander Schwarz der Julius-Maximilians-Universität Würzburg, Institut für Staats- und Verwaltungsrecht, Rechtsphilosophie, das Bayerische Landeskriminalamt, den Deutschen Anwaltsverein, Ausschuss Gefahrenabwehrrecht, den Bund Deutscher Kriminalbeamter, Landesverband Mecklenburg-Vorpommern, Prof. Dr. Dieter Kugelmann der Deutschen Hochschule der Polizei sowie Prof. Dr. Matthias Bäcker der Universität Mannheim, Abteilung Rechtswissenschaft, gebeten, eine Stellungnahme abzugeben, wobei die drei Letztgenannten keinen Beitrag erstellt haben.

Der Innenausschuss hat den Gesetzentwurf am 6. Juni 2013 in seiner 35. Sitzung abschließend beraten und dem Gesetzentwurf mit der vom Ausschuss vorgesehenen Änderung zugestimmt.

### **II. Wesentliche Ergebnisse der Beratungen des Innenausschusses**

#### **1. Ergebnisse der schriftlichen Anhörung**

Im Folgenden werden die wesentlichen Aussagen, allgemeinen Einschätzungen und Kritikpunkte der Anzuhörenden aus den schriftlichen Stellungnahmen und mündlichen Beiträgen am Anhörungstag dargelegt.

Der Städte- und Gemeindetag Mecklenburg-Vorpommern e. V. hat mitgeteilt, dass nach inhaltlicher Prüfung eine kommunale Betroffenheit nicht gesehen werde. Der Landesverfassungsschutz und die Polizei erhielten rechtssichere Befugnisse zur Bestandsdatenauskunft, was im Sinne einer effektiven Arbeit von Polizei und Verfassungsschutz einerseits und eines verfassungsrechtlich klar formulierten Datenschutzes andererseits begrüßt werde.

Der Landkreistag Mecklenburg-Vorpommern e. V. hat schriftlich erklärt, dass der Gesetzentwurf die kommunalen Belange nicht wesentlich berühre. Insofern lägen keine Bedenken oder Änderungsvorschläge vor.

Die Gewerkschaft der Polizei Mecklenburg-Vorpommern hat die Änderung des Sicherheits- und Ordnungsgesetzes M-V (SOG M-V) und die Schaffung von § 24b Landesverfassungsschutzgesetz M-V (LVerfSchG M-V) sowie § 28a SOG M-V begrüßt. Diese Änderungen seien notwendig gewesen, nachdem das Bundesverfassungsgericht in seiner Entscheidung vom 24.01.2012, Az.: 1 BvR 1299/05, das Doppeltüren-Modell entwickelt und klargestellt habe, dass nicht nur die Übermittlung von zuvor erhobenen und gespeicherten Telekommunikationsdaten geregelt sein müsse, sondern auch die Befugnis zu deren Abfrage. Damit werde die Befugnis der zuständigen Behörden zum Datenabruf gegenüber privaten Telekommunikationsunternehmen gemäß § 113 TKG entsprechend den Vorgaben des Bundesverfassungsgerichtes endlich geregelt. Auch die mit der beabsichtigten Neuregelung getroffene bewusste Entscheidung des Gesetzgebers für eine Identifizierung dynamischer IP-Adressen werde aus polizeilicher Sicht befürwortet, wobei auch keineswegs verkannt werden solle, was für ein erhebliches Gewicht dieser Eingriff für den betroffenen Bürger habe. Es bestehe weiterer Handlungsbedarf, um eine effektivere Gefahrenabwehr und Strafverfolgung sicherzustellen. Denn sowohl im präventiven als auch im Bereich der Strafverfolgung könnten Erkenntnisse über Kontaktpersonen in der Tatplanungsphase häufig nur mit Hilfe von retrograden Verkehrsdaten (Daten über Teilnehmer, Dauer, Beginn und Ende einer Telekommunikation) gewonnen werden.

Die Deutsche Polizeigewerkschaft, Landesverband Mecklenburg-Vorpommern, hat schriftlich ausgeführt, dass dem Gesetzentwurf zugestimmt werde. Die Bestandsdatenauskunft sei ein unverzichtbares Ermittlungsinstrument für Strafverfolgungs- und Sicherheitsbehörden und unerlässlich im Alltag der Polizei, des Zolls, der Kriminalämter und der Nachrichtendienste. Sie werde zum Beispiel bei der Verfolgung von Kinderpornografie im Netz gebraucht, aber auch zur Ermittlung eines Telefonanschlusshabers, der einen Selbstmord angekündigt habe. Liege gegen eine Person ein Verdacht vor, könne die Polizei bei dem jeweiligen Telekommunikationsunternehmen eine Auskunft über Name und Anschrift des Kunden erfragen. Die jetzt vorgelegten Neuregelungen beschränkten sich auf die Umsetzung der Vorgaben des Bundesverfassungsgerichtes, ohne dabei neue Befugnisse für Strafverfolgungs- oder Sicherheitsbehörden zu schaffen. Der Gesetzentwurf sei handhabbar, positiv und umsetzbar. Er beinhalte klarstellende Regelungen und Befugnisse, ohne diese durch Formvorschriften zu überfrachten. Die in der Öffentlichkeit geführten Diskussionen zur missbräuchlichen Anwendung der Bestandsdatenauskunft würden nicht verfangen, da der Anwendungsbereich klarer gefasst werde. Eine Vorratsdatenspeicherung durch die Hintertür liege nicht vor.

Das Bayerische Landeskriminalamt hat erklärt, dass der Gesetzentwurf aus polizeipraktischer Sicht die geforderten klarstellenden Regelungen enthalte. Er entspreche dem Handlungserfordernis zur Bestandsdatenerhebung von Kunden im Zuge des sogenannten Doppeltüren-Modells aufgrund der Entscheidung des Bundesverfassungsgerichtes vom 24. Januar 2012. Maßnahmen, die eine Auskunft über Zugangssicherungs\_codes betreffen, unterlägen nicht einem grundsätzlichen, sondern in sinnvoller Weise einem selektiven Richtervorbehalt. Dieser greife nicht, wenn Daten, die sich auf einem sichergestellten Mobiltelefon befänden, ausgelesen werden sollten. Begründet werde dies damit, dass hier kein Eingriff in den Schutzbereich des Artikels 10 Absatz 1 Grundgesetz (GG) vorliege. Diese abgestufte Regelung des Richtervorbehaltes erscheine aus polizeipraktischer Sicht praktikabel. Die Regelung zur Benachrichtigung im Zuge der Beauskunftung dynamischer IP-Adressen sei unangemessen.

Diese Einschätzung beruhe zum einen auf der begrenzten Aussagekraft der erhobenen Daten. Sie gäben allein Auskunft über die Zuordnung einzelner technischer Kennungen zu ihrem Anschlussinhaber. Auch wenn sich im Rahmen konkreter Erhebungszusammenhänge daraus sensible Informationen ergeben könnten, bleibe der Informationsgehalt dieser Auskünfte als solcher doch begrenzt und hänge im Übrigen von weiteren Ermittlungen ab, deren Rechtmäßigkeit nach anderen Vorschriften zu beurteilen sei. Erst in der Gesamtschau könne die für polizeiliche Maßnahmen geforderte Konsistenz ausgebracht werden. Die Eingriffstiefe der Maßnahme sei insofern als gering anzusehen und eine Benachrichtigungspflicht - auch wenn diese abgestuft geregelt sei - eine durchaus vermeidbare Überfrachtung. Zur Auskunftserteilung durch die Diensteanbieter sei zu sagen, dass die Diensteanbieter gemäß § 28a Absatz 3 SOG M-V die zur Auskunftserteilung erforderlichen Daten unverzüglich, vollständig und richtig zu übermitteln hätten. Als grundsätzlich schwerwiegendes Defizit sowohl bei der repressiven als auch präventivpolizeilichen Beauskunftung von Bestandsdaten bleibe die fehlende gesetzliche Regelung einer Reaktionszeit der Verpflichteten außerhalb deren Regelarbeitszeit. Dieses Defizit müsse dringend über entsprechende Initiativen behoben werden. Aus Gründen der Vollständigkeit werde auf den Anpassungsbedarf in § 23 Justizvergütungs- und -entschädigungsgesetz hingewiesen. Die Vorbemerkung in Anlage 3 sehe in Absatz 2 bisher vor, dass sich die Entschädigungsbeträge nach den Nummern 100, 101, 300 bis 310, 400 und 401 um jeweils 20 Prozent reduzierten, wenn die genannten Leistungen über eine zentrale Kontaktstelle angefordert und abgerechnet würden. Mit Einführung der elektronischen Schnittstelle erscheine es auch für den Fall der zentralen Behandlung von Bestandsdatenauskünften durch die Bedarfsträger geboten, die Kostenziffern 200 und 201 der vorgenannten Anlage entsprechend anzupassen und die Möglichkeit der Ermäßigung der Entschädigung vorzusehen.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern hat festgestellt, dass die Anfang Mai verabschiedete Neuregelung der Bestandsdatenauskunft auf Bundesebene auch Auswirkungen auf den Gesetzentwurf habe und daher Änderungen vorgeschlagen würden. In § 24b LVerfSchG M-V des Gesetzentwurfes sollten die Wörter „im Einzelfall“ aufgenommen werden. Betrachte man die „weiteren Auskunftsverlangen“ im Kontext mit der Vorschrift des § 24a, so seien auch hier die Auskunftsbefugnisse nur „im Einzelfall“ gegeben. Da der Eingriff für den Betroffenen unter Umständen doch recht schwer wiege, sollte diese hier geforderte Befugnis keine Routinemaßnahme der Verfassungsschutzbehörde darstellen. Vorgeschlagen werde überdies, nach § 24b Absatz 2 den Satz: „Für Auskunftsverlangen nach § 24b Absatz 1 Satz 2 und Absatz 2 gelten die § 24a Absatz 4 Satz 2 und Satz 4 und Absatz 5 entsprechend.“ zu ergänzen. Das novellierte Telekommunikationsgesetz des Bundes habe die Beteiligung der G 10-Kommission bei Auskunftsersuchen unter Nutzung dynamischer IP-Adressen und über Zugangssicherungs-codes geregelt. Auf diese Weise sei sichergestellt, dass in den Fällen, in denen sich das Auskunftsersuchen auf Zugangssicherungs-codes beziehe oder unter Nutzung von dynamischen IP-Adressen erfolge, auch der entsprechende Behördenleitervorbehalt gelte und die G-10 Kommission des Landtages über entsprechende Anordnungen unterrichtet werde. Darüber hinaus sollte auch die Parlamentarische Kontrollkommission unterrichtet werden. Auskunftsersuchen über Zugangssicherungs-codes stellten regelmäßig eine Vorstufe zu Maßnahmen dar, die ihrerseits den Schutzbereich des Artikels 10 GG berühren könnten. Im novellierten Telekommunikationsgesetz des Bundes sei des Weiteren festgeschrieben worden, dass Auskunftsersuchen über Zugangssicherungs-codes sowie über den Inhaber einer IP-Adresse einem Richtervorbehalt unterlägen. Auch sei eine Benachrichtigung des Betroffenen bei beiden Maßnahmen vorgesehen.

Beide Vorkehrungen trügen dem Umstand Rechnung, dass es sich bei den zugrunde liegenden Maßnahmen um gewichtige Grundrechtseingriffe handele, die wesentlich schwerer wögen als die bloße Bestandsdatenabfrage. Die Zuordnung dynamischer IP-Adressen zu deren Nutzern setze eine Analyse der Verkehrsdaten voraus und greife daher in Artikel 10 GG ein, wie das Bundesverfassungsgericht in seiner Entscheidung vom 24. Januar 2012 ausdrücklich klargestellt habe. Ähnlich sei die Auskunft über Zugangssicherungs-codes wie PIN und PUK oder Passwörter zu bewerten. Diese Angaben selbst mögen zwar Bestandsdaten sein. Sie dienten der Polizei aber dazu, sich Kenntnis von weiteren Daten zu beschaffen. Diese weiteren Daten seien üblicherweise Verkehrs- und Inhaltsdaten über bereits abgeschlossene Telekommunikationsvorgänge. Als solche unterfielen sie zwar nicht unmittelbar dem Schutz des Artikels 10 GG (BVerfG vom 2.3.2006 - 2 BvR 2099/04 - Absatz-Nr.72 ff.). Sie seien jedoch vom Schutzbereich des Rechtes auf informationelle Selbstbestimmung umfasst. Die Erhebung dieser Daten stelle regelmäßig einen schwerwiegenden Eingriff in dieses Grundrecht dar. Denn hierdurch könnten zum einen der Umfang der Kommunikationsbeziehungen sowie die näheren Umstände der Kommunikation oftmals für einen weitreichenden Zeitraum erschlossen werden. Zum anderen könnten Inhalte abgeschlossener Kommunikation erfasst werden, die mit dem Kommunikationspartner in der Annahme der Vertraulichkeit der Kommunikation ausgetauscht würden und den höchstpersönlichen Bereich betreffen könnten. Sowohl die gerichtliche Befassung als auch die Benachrichtigung der Betroffenen seien aus datenschutzrechtlicher Sicht grundsätzlich geeignete Mittel, um den Schutz der Betroffenen zu erhöhen. Daher sollte auch § 28a Absatz 2 Satz 1 folgender Satz 2 SOG M-V ergänzt werden: „Auskunftsersuchen nach Absatz 1 Satz 2 und Absatz 2 Satz 1 dürfen nur auf Antrag des Leiters der Polizeibehörde oder seines Vertreters durch das Gericht angeordnet werden. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Bei Gefahr im Verzug kann die Anordnung durch den Leiter der Polizeibehörde oder seinen Vertreter getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Sätze 1 bis 3 finden keine Anwendung, wenn der Betroffene vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird. Das Vorliegen der Voraussetzungen nach Satz 4 ist aktenkundig zu machen“. Die im jetzigen Absatz 2 Satz 2 geregelte Unterrichtung des Betroffenen über die Beauskunftung greife zu kurz, da sie sich nur auf die Unterrichtung des Betroffenen beziehe, über den Auskunft als Inhaber einer dynamischen IP-Adresse erteilt worden sei. Die Unterrichtung müsse sich jedoch auch auf Fälle beziehen, in denen Auskünfte über Zugangssicherungs-codes erteilt worden seien. Daher werde vorgeschlagen, dass der jetzige Absatz 2 Satz 2 bis 6 zu Absatz 3 werde und wie folgt laute: „In den Fällen von Absatz 1 Satz 2 und Absatz 2 ist die betreffende Person über die Beauskunftung zu unterrichten.“

Prof. Dr. Kyrill-Alexander Schwarz, Julius-Maximilians-Universität Würzburg, hat erklärt, dass der Gesetzentwurf keinen verfassungsrechtlichen Bedenken begegne. Er genüge mit Blick auf die vergleichsweise geringe Eingriffsintensität den durch das Bundesverfassungsgericht aufgestellten Kriterien für die Eingriffsrechtfertigung. Weitergehende Forderungen nach Benachrichtigungspflichten oder Richtervorbehalten mögen zwar rechtspolitisch verständlich sein, verfassungsrechtlich geboten seien sie indes nicht.

Nachdem der Bund in der Zwischenzeit eine gesetzliche Regelung zur Bestandsdatenauskunft sowie zur Zuordnung dynamischer IP-Adressen verabschiedet habe und er damit für seinen Bereich die durch das Bundesverfassungsgericht vorgezeichneten Änderungen vorgenommen habe, bestehe für die Länder in Umsetzung der bundesverfassungsgerichtlichen Judikatur die Verpflichtung, in ihrem Zuständigkeitsbereich die entsprechenden Regelungen zu verabschieden. Mit dem Gesetzentwurf würden die materiellen Anforderungen des Bundesverfassungsgerichtes durch die Schaffung spezifischer Erhebungsbefugnisse in den jeweiligen Fachgesetzen umgesetzt. Mit Blick auf die Kompetenzen der Länder im Bereich des Gefahrenabwehrrechtes sei die Vorschrift in § 113 TKG so offen formuliert, dass die Länder für ihren Kompetenzbereich eine Anpassung der Landespolizeigesetze vornehmen könnten. Gerade damit die Länder auch nach dem Auslaufen der durch das Bundesverfassungsgericht gesetzten Frist ihre Landesverfassungsschutzbehörden sowie die Polizei zur Abfrage von Bestandsdaten ermächtigen könnten, bedürfe es zwingend einer Anpassung des Sicherheits- und Ordnungsgesetzes sowie des Landesverfassungsschutzgesetzes, um so das Doppeltüren-Modell des Bundesverfassungsgerichtes auch auf Landesebene zu implementieren. Soweit im Vorfeld des Gesetzgebungsverfahrens der Vorwurf erhoben worden sei, der Entwurf sei verfassungswidrig, da entgegen den Vorgaben des Bundesverfassungsgerichtes keine Beschränkung der Datenabfrage auf Fälle einer konkreten Gefahr erfolge, sei dies nicht zutreffend. Durch das Zusammenspiel einer allgemeinen bundesgesetzlichen Regelung in § 113 TKG und den jeweiligen fachspezifischen Befugnisnormen im Landesrecht sei sichergestellt, dass die Datenabfrage nicht anlassunabhängig erfolge, sondern vielmehr an das Erfordernis einer konkreten Gefahr im Einzelfall gebunden sei, wobei aber zu Recht zu betonen sei, dass diese Eingriffsschwelle keine unüberwindbaren Hürden errichte, solange im Einzelfall sicherheitsrechtlich geprägter Bezug zur Notwendigkeit der Bestandsdatenabfrage gegeben sei. Dies bedeute aber zumindest, dass regelmäßig zumindest ein Anfangsverdacht einer Ordnungswidrigkeit oder Straftat vorliegen müsse. Das Bundesverfassungsgericht habe die gesetzliche Ermächtigung (§ 113 Absatz 1 Satz 2 TKG) zur Abfrage von Zugangssicherungscodes (Passwörter, PIN und PUK), die den Zugang zu Endgeräten und Speicherungseinrichtungen sicherten und damit den Betroffenen vor einem Zugriff auf seine Daten bzw. die Kommunikationsvorgänge schützten, für verfassungswidrig erklärt, weil sie einen Zugriff auf die entsprechenden Daten und die Überwindung der damit verbundenen Barrieren unabhängig von den Voraussetzungen der jeweiligen Nutzung gestatte. Damit würden aber die nach Fachrecht bestehenden unterschiedlichen Schutzniveaus eingeebnet, weil die Frage nach der Existenz eines Richtervorbehaltes oder nach entsprechenden Benachrichtigungspflichten sich ausschließlich aus dem jeweiligen Fachrecht ableiten ließe. Allerdings gebiete der Verhältnismäßigkeitsgrundsatz auch nicht, die Erhebung der Zugangscodes ausnahmslos unter die Voraussetzungen zu stellen, die für die jeweils denkbarste eingriffsintensivste Nutzungsmöglichkeit gegeben sein müssten. Rechtsstaatlich geboten sei nur, die Auskunftserteilung über Zugangssicherung an die Voraussetzungen zu binden, die in der jeweiligen konkreten Abfragesituation für die jeweilige Maßnahme erfüllt sein müssten. Mit der jeweiligen Inbezugnahme fachspezifischer Regelungen stelle der Entwurf aber sicher, dass nur unter den jeweils fachspezifischen Anforderungen (auch in prozeduraler Hinsicht) eine Abfrage der Zugangssicherungsdaten erfolgen dürfe. Damit sei den Anforderungen des Bundesverfassungsgerichtes hinreichend Rechnung getragen.

Bei dem Ausgleich der widerstreitenden Interessen durch den Gesetzgeber, der die rechtlichen Grundlagen für Vorfeldmaßnahmen des Verfassungsschutzes einerseits und die Gefahrenabwehr andererseits zu schaffen habe, sei zu berücksichtigen, dass dem Einzelnen in seiner Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit gewisse Beeinträchtigungen zuzumuten seien, die dem Rechtsgüterschutz und Grundrechtsschutz anderer Bürger, aber auch seinem eigenen Schutz dienen. Auch im Blick darauf müsse dem Gesetzgeber ein Gestaltungsraum für den ihm obliegenden Ausgleich eingeräumt werden, um einerseits die Freiheitsrechte der Grundrechtsträger zu schützen, andererseits aber diejenigen rechtlichen Rahmenbedingungen zu schaffen, die einen effektiven Schutz der Grundrechte und Rechtsgüter der Bürger vor Verletzungen und die Aufklärung von Straftaten mit angemessenen und zumutbaren Mitteln wirksam ermöglichen. Im Ergebnis seien effektive Vorfeldmaßnahmen und wirksame Gefahrenabwehr daher nicht per se eine Bedrohung für die Freiheit der Bürger, indessen nicht ohne Maß und Grenze statthaft. Sie seien im Rahmen des Angemessenen und Zumutbaren geboten, um die Inanspruchnahme auch der Grundrechte abzusichern und die Rechtsgüter des Einzelnen zu schützen. Der Bürger müsse sich im Rechtsstaat auf effektiven Schutz durch den Staat ebenso verlassen können, wie auf den Schutz gegen den Staat. Dementsprechend habe das Bundesverfassungsgericht den Staat als verfasste Friedens- und Ordnungsmacht beschrieben und die von ihm zu gewährleistende Sicherheit seiner Bürger als Verfassungswert anerkannt, der mit anderen im gleichen Rang stehe und unverzichtbar sei, weil die Institution Staat auch davon ihre Rechtfertigung herleite. Datenschutzrelevante Grundrechtsgarantien bedürften nach der Rechtsprechung des Bundesverfassungsgerichtes organisations- und verfahrensrechtlicher Sicherungen. Der Gesetzentwurf sehe ein abgestuftes System von Benachrichtigungen der Betroffenen bei Zugriffen auf ihre Daten vor. Nach der Rechtsprechung des Bundesverfassungsgerichtes könne sich im Einzelfall aus der Rechtsschutzgarantie des Artikels 19 Absatz 4 GG ein Anspruch auf Benachrichtigung über die Erhebung personenbezogener Daten ergeben, wenn diese Form der Kenntnisgewähr Voraussetzung für die Inanspruchnahme gerichtlichen Rechtsschutzes sei, da ohne nachträgliche Kenntnis die Betroffenen weder die Unrechtmäßigkeit der Datenverwendung noch etwaige Rechte auf Löschung, Berichtigung oder ähnliches geltend machen könnten. Soweit der Entwurf in seiner Begründung auf die Rechtsprechung des Bundesverfassungsgerichtes rekurriere, um eine Benachrichtigungspflicht zu begründen, sei der Hinweis auf die Entscheidung zur Vorratsdatenspeicherung nicht zwingend, handele es sich doch gerade nicht um Verkehrsdaten, sondern um Bestandsdaten, die aber nicht Gegenstand der in Bezug genommenen Entscheidung gewesen seien. Der Gesetzgeber habe sich frei von verfassungsrechtlichen Bedenken für ein Konzept entschieden, wonach Daten jedenfalls unter bestimmten Voraussetzungen auch ohne das Wissen des Betroffenen erhoben werden dürften. Dies habe auch seinen guten Grund. Denn Ermittlungen seien regelmäßig von einer beachtlichen Dynamik gekennzeichnet und beschleunigt zu führen. Aufwände, die verfahrenssichernden und rechtsschützenden Zwecken nicht zwingend zeitnah geschuldet seien, sollten zunächst in Grenzen gehalten werden. Der Gesetzgeber habe dementsprechend eine differenzierte Regelung über die Benachrichtigung getroffen, die eine vorherige Benachrichtigung nicht vorschreibe. Zudem habe er mit der Gestattung, zunächst auch ohne Wissen des Betroffenen Verkehrsdaten zu erheben, erkennbar eine Typisierung vorgenommen, die darauf zurückgehe, dass zumeist der Untersuchungszweck, das Nichtbekanntsein des Aufenthaltsortes des Betroffenen oder die notwendige Beschleunigung der Sachaufklärung einer Vorab-Benachrichtigung entgegenstünden. Das sei ersichtlich nicht unangemessen, dem Betroffenen zumutbar und infolgedessen dem Gesetzgeber von Verfassungswegen unbenommen.

Im Übrigen sei festzustellen, dass sogar eine fehlende Benachrichtigungspflicht in Ansehung der geringen Eingriffsintensität von Verfassungswegen unproblematisch sein dürfte, weil jedenfalls eine Rechtsschutzmöglichkeit gegenüber den abschließenden behördlichen Entscheidungen bestehe. Der Rechtsordnung sei auch keine generelle Informationsverpflichtung durch Benachrichtigungen zu entnehmen, wie sie sich in Sonderheit den Bestimmungen der Strafprozessordnung entnehmen lasse. Insgesamt sei daher der Gesetzgeber nicht in jedem Fall verpflichtet, Regelungen über eine Benachrichtigungspflicht zu treffen. Dass er sie getroffen habe, sei verfassungsrechtlich nicht erforderlich, möge rechtspolitisch aber eine gewisse Befriedungsfunktion entfalten. Eine weitere Möglichkeit zur Kompensation (unterstellter) bestehender Rechtsschutzdefizite stelle der Richtervorbehalt dar. Dabei handele es sich um eine traditionelle prozedurale Vorkehrung gegenüber Datenerhebungen, die kompensieren solle, dass die überwachte Person mangels Kenntnis des Grundrechtseingriffes selbst über keinen primären, präventiven Abwehrrechtsschutz verfüge. Wenngleich ein Richtervorbehalt ausdrücklich nur für Maßnahmen bei Artikel 13 GG vorgesehen sei, so gehe das Bundesverfassungsgericht gleichwohl in ständiger Rechtsprechung von einem abgestuften Konzept grundrechtsübergreifend wirkender Richtervorbehalte aus. Gerade bei den hier in Rede stehenden Maßnahmen dürfte aber die Einforderung eines generellen Richtervorbehaltes nicht geboten sein; vielmehr seien es die maßgeblichen fachgesetzlichen Regelungen, die hinreichenden Schutz durch die dort im Einzelfall normierten prozeduralen Anforderungen garantierten. Nicht geboten erscheine dann aber in Anbetracht dieser Kautelen ein weiterer allgemein wirkender Richtervorbehalt, der gleichsam vorgelagert den (geringfügigen) Grundrechtseingriff legitimiere, der die spätere Ermittlungs- oder Überwachungsmaßnahme, die ihrerseits im Einzelfall einer richterlichen Anordnung bedürfe, erst ermögliche. Dem Verfassungsrecht - und hier in Sonderheit dem Grundsatz der Verhältnismäßigkeit - sei kein Gebot eines doppelten Richtervorbehaltes zu entnehmen, wenn die eingriffsintensivere Maßnahme selbst in prozeduraler und materieller Hinsicht gerechtfertigt sei.

Der Deutsche Anwaltsverein hat festgestellt, dass der Entwurf den Verfassungsschutzbehörden bei der Entscheidung, ob eine Datenauskunft erforderlich sei, bemerkenswert freie Hand lasse. Die Rechtmäßigkeit der Auskunft sei allein an die Voraussetzung geknüpft, dass die Datenauskunft zur Erfüllung der Aufgaben der Verfassungsschutzbehörden erforderlich sei. Das allein habe das Bundesverfassungsgericht so nicht genügen lassen wollen. Es habe im Hinblick auf die Nachrichtendienste ausdrücklich angeführt, dass es eine Erforderlichkeit im Einzelfall geben müsse. Eine Auskunft sei nur dann zulässig, wenn es zur Aufklärung einer bestimmten nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung geboten sei. Aus der Formulierung im Entwurf ergebe sich diese verfassungsrechtliche Beschränkung auf die Einzelfallbetrachtung nicht. Zu berücksichtigen sei, dass sich das Auskunftersuchen nicht etwa an eine Behörde richte, sondern an ein privates Telekommunikationsunternehmen. Angezeigt sei also eine klare und deutliche Formulierung der Voraussetzungen. Darüber hinaus sei festzustellen, dass die Nachrichtendienste grundsätzlich unabhängig von konkreten Gefahrenlagen im Vorfeld tätig werden könnten. Das sollte Anlass dafür sein, eine klare Befugnisnorm zu schaffen. Die Unterrichtung der Betroffenen bei einer Datenauskunft sei nicht der Normalfall. Das bedeute aber auch, dass sich der Betroffene im Regelfall nicht dagegen zur Wehr setzen könne, dass seine Verkehrsdaten erhoben würden. Er werde im Regelfall zum Zeitpunkt der erteilten Auskunft nichts erfahren und er werde deswegen auch die Frage nicht prüfen oder überprüfen lassen können, ob die Nutzung der Daten auch tatsächlich zulässig gewesen sei.

Werde, wie es in der Begründung des Entwurfes richtig heie, der Betroffene informiert, so stehe ihm allenfalls die Erlangung eines nachtrglichen Rechtsschutzes offen. Seien die IP-Adresse aber erst einmal bekannt und die PIN und PUK erst einmal geknackt, dann werde man dieses Wissen der Behrde wohl schwerlich zurckrufen knnen. Zu begren sei, dass in § 28a des Entwurfes zum SOG das Auskunftsverlangen ausdrcklich an die Abwehr einer im einzelnen Fall bevorstehenden Gefahr anknpfe. Damit sei dem Erfordernis des Bundesverfassungsgerichtes nach einer mglichst weitgehenden Konkretisierung ganz klar und eindeutig Rechnung getragen worden. In § 34a SOG seien im Einzelnen die gesetzlichen Voraussetzungen der Datenerhebung durch berwachung der Telekommunikation geregelt. Die Manahmen bedrften der richterlichen Anordnung, nur im Ausnahmefall sei der Behrdenleiter die genehmigungsbefugte Person. Auch hier stelle sich die Frage, wie ermglicht werden knne, dass der Betroffene, der von der Auskunftserteilung seines Telekommunikationsdienstleisters nichts wisse und erfahre, sich dagegen zur Wehr setzen knne. Und auch hier gelte, ist die Auskunft erst einmal erteilt, knne es fr den praktischen Rechtsschutz zu spt sein und es liege sogleich der unmittelbare und direkte Eingriff in das Grundrecht vor. Offen geblieben sei, ob und gegebenenfalls inwieweit die Telekommunikationsunternehmen das Vorliegen der gesetzlichen Nutzungsvoraussetzungen zu berprfen htten oder ob sie dazu gerade nicht verpflichtet seien.

## 2. Ergebnisse der Ausschussberatungen

Das Ministerium fr Inneres und Sport hat zu Artikel 1 des Gesetzentwurfes im Hinblick auf die Stellungnahmen einzelner Anzuhrender klargestellt, dass sich bereits aus den gesetzlichen Bestimmungen ergebe, dass die Verfassungsschutzbehrde die Bestandsdatenauskunfte zu dynamischen IP-Adressen und Zugangssicherungs-codes nur im Einzelfall verlangen drfe, nmlich nur dann, wenn dies zur Erfllung der Aufgaben erforderlich sei. Dies setze somit eine Prfung hinsichtlich dieser Voraussetzung in jedem Einzelfall voraus. Aus diesem Grunde sei eine entsprechende Formulierung dahingehend entbehrlich.

Auf die kritische Nachfrage der Fraktion BNDNIS 90/DIE GRNEN und den Hinweis, dass eine ausdrckliche Aufnahme der Einzelfallregelung zur Rechtsklarheit beitrage, hat das Ministerium fr Inneres und Sport eingerumt, dass inhaltlich eine Aufnahme zwar nichts ndere, diese aber auch nicht schdlich sei. Anders sehe dies bei der Einfhrung eines Behrdenleitervorbehaltes und die G 10-Beteiligung fr die PIN- und PUK-Daten und die IP-Adresse aus. Man bewege sich hier im Bereich der Gefahrenabwehr, der schnelles Handeln erfordere. Jede Verzgerung knne hier dazu fhren, dass die Manahme nicht mehr greife. Insbesondere bei der IP-Adresse handele es sich um eine dynamische Adresse, die bei jedem Eintritt in das Internet neu vergeben werde. Diese Daten wrden nur vorbergehend gespeichert. Derzeit erfolge also keine Vorratsdatenspeicherung. Dies fhre dazu, dass bei der Anwendung des Behrdenleiter- oder G 10-Verfahrens so viel Zeit verstreichen wrde, dass in vielen, wahrscheinlich sogar in den meisten Fllen eine Beauskunftung durch die verpflichteten Unternehmen gar nicht mehr mglich sei, weil die erforderlichen Daten bereits wieder gelscht seien, bevor die beantragte Beauskunftung genehmigt sei. Das Bundesverfassungsgericht habe in seiner Entscheidung sehr ausfhrlich geklrt, welche Anforderungen an die Beauskunftung der zur Diskussion stehenden Bestandsdaten zu stellen seien. Ein Behrdenleitervorbehalt und auch die Behandlung wie eine G 10-Manahme gehrten gerade nicht dazu.

Die Handlungsfähigkeit würde aufgrund des nicht vertretbaren Zeitverzuges und des damit einhergehenden Verlustes an Daten in nicht vertretbarer Weise eingeschränkt. Auch der Bund habe einen Behördenleitervorbehalt und die G 10-Beteiligung bei der IP-Adresse nicht geregelt.

Das Ministerium für Inneres und Sport hat in Auswertung der öffentlichen Anhörung zu Artikel 2 des Gesetzentwurfes erklärt, dass die Novellierung die Beauskunftung von Bestandsdaten und eben nicht die Beauskunftung von Verkehrsdaten, die dem Schutzbereich des Artikels 10 unterlägen, vorsehe und dies auch nur im konkreten Einzelfall. Die Auskunft über solche Bestandsdaten sei lediglich mit einem geringfügigen Grundrechtseingriff verbunden. Demzufolge habe auch das Bundesverfassungsgericht in seiner Entscheidung weder für die Beauskunftung von Zugangssicherungs-codes noch für die Beauskunftung von IP-Adressen ausdrücklich einen Richtervorbehalt gefordert. Soweit auf das bereits beschlossene Bundesgesetz zur Regelung der Bestandsdatenauskunft verwiesen werde, sei ausdrücklich festzuhalten, dass der darin im Zuge des Gesetzgebungsverfahrens noch nachträglich vorgenommene Einschub eines Richtervorbehaltes nicht etwa aus verfassungsrechtlichen Gründen erfolgt sei. So habe das Bundesministerium des Innern die Innenministerien der Länder in einem Schreiben ausdrücklich darauf hingewiesen, dass die im Bundesgesetzentwurf noch vorgenommenen Änderungen für die Landesgesetzgeber nicht bindend seien. Im Übrigen würde im Bundesgesetz nur die Beauskunftung von Zugangssicherungs-codes unter einen Richtervorbehalt gestellt. Er beziehe sich nicht auf die Beauskunftung der Zuordnung von IP-Adressen. Eine solche Regelung würde noch über das Bundesgesetz hinausgehen. Ungeachtet dieser Tatsache werde darauf aufmerksam gemacht, dass § 28a SOG M-V für die Erhebung von Zugangssicherungs-codes zusätzlich schon als Voraussetzung fordere, dass bereits zum Beauskunftungszeitpunkt die gesetzlichen Voraussetzungen für die Nutzung dieser Code-Daten vorliegen müssten. Das heiße, es seien also andere Vorschriften im Sicherheits- und Ordnungsgesetz im Beauskunftungsprozess zu beachten, die bereits verfahrenssichernde Regelungen enthielten. Die vorliegende Gesetzesbegründung zu § 28a SOG M-V stelle dies sehr ausführlich dar. Insofern führe die Normierung eines Richtervorbehaltes in § 28a SOG M-V zu einer Regelungsdoppelung. Die Einfügung einer grundsätzlichen Benachrichtigungspflicht nicht nur für die Beauskunftung der Zuordnung von IP-Adressen, sondern auch für die Beauskunftung von Zugangssicherungs-codes sei nicht erforderlich, denn die Beauskunftung durch die Polizei dürfe nur dann verlangt werden, wenn die gesetzlichen Voraussetzungen ihrer Nutzung gegeben seien. Insoweit bestimme sich die Frage, wann die Polizei von den Sicherungs-codes Gebrauch machen und auf die durch sie gesicherten Daten und Telekommunikationsvorgänge Zugriff nehmen dürfe nach eigenen Rechtsgrundlagen im Sicherheits- und Ordnungsgesetz, die bereits schon verfahrenssichernde Regelungen enthielten. Diese Regelungen griffen mithin immer, wenn die beauskunfteten Zugangssicherungs-codes durch die Polizei genutzt würden. Der Gesetzentwurf schaffe Eingriffsbefugnisse, die über die bisher bestehende Regelung im Telekommunikationsgesetz hinausgingen. Das Land reagiere in erster Linie darauf, dass das Bundesverfassungsgericht entschieden habe, dass Bestandsdatenauskünfte durch die Länder nach dem Doppeltüren-Modell zukünftig nur dann weiter verlangt werden könnten, wenn qualifizierte landesgesetzliche Rechtsgrundlagen bestünden, die diese Datenerhebungen zuließen.

### III. Zu den einzelnen Bestimmungen

#### Zu Artikel 1

Die Fraktion DIE LINKE hatte, gestützt auf einzelne Ausführungen bei der öffentlichen Anhörung, beantragt, in Artikel 1 Nummer 2 in § 24b Absatz 1 nach den Wörtern „oder daran mitwirkt,“ die Wörter „im Einzelfall“ einzufügen.

Die beantragende Fraktion hat dies mit dem schwerwiegenden Eingriff für den Betroffenen begründet, sodass die hier geregelte Befugnis keine Routinemaßnahme der Verfassungsschutzbehörde darstellen sollte, sondern eine Einzelfallprüfung voraussetze. Bereits das Bundesverfassungsgericht habe im Hinblick auf die Nachrichtendienste ausdrücklich angeführt, dass die Erforderlichkeit im Einzelfall gegeben sein müsse.

Der Ausschuss hat bei Abwesenheit der Fraktion der NPD diese Änderung einstimmig angenommen.

Die Fraktion DIE LINKE hatte weiterhin beantragt, in Nummer 2 in § 24b Absatz 2 folgenden Satz anzufügen: „Für Auskunftsverlangen nach § 24b Absatz 1 Satz 2 und Absatz 2 gelten die § 24a Absatz 4 Satz 2 und Satz 4 und Absatz 5 entsprechend.“

Darüber hinaus solle nach Ansicht der Fraktion DIE LINKE sichergestellt werden, dass in den Fällen, in denen sich das Auskunftersuchen auf Zugangssicherungscode beziehe oder unter Nutzung von dynamischen IP-Adressen erfolge, der entsprechende Behördenvorbehalt gelte und die G 10-Kommission des Landtages über entsprechende Anordnungen unterrichtet werde.

Der Ausschuss hat mehrheitlich mit den Stimmen der Fraktionen der SPD und der CDU gegen die Stimmen der Fraktionen DIE LINKE und BÜNDNIS 90/DIE GRÜNEN bei Abwesenheit der Fraktion der NPD diese Änderung abgelehnt.

Die Fraktion BÜNDNIS 90/DIE GRÜNEN hatte beantragt, in Artikel 1 Nummer 2 den § 24b Absatz 1 Satz 1 wie folgt zu fassen, wobei sich der Änderungsantrag hinsichtlich der bereits durch den Ausschuss einstimmig angenommenen Aufnahme einer Einzelfallregelung erledigt hatte: „Die Verfassungsschutzbehörde darf im Einzelfall von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 1 des Gesetzes vom ... (BGBl. I S. ...) geändert worden ist, erhobenen Daten verlangen (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes), soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist.“

Ferner hatte die Fraktion BÜNDNIS 90/DIE GRÜNEN beantragt, in Nummer 2 nach § 24b Absatz 2 Satz 1 folgenden Satz 2 einzufügen: „Für Auskunftsverlangen nach § 24b Absatz 1 Satz 2 und Absatz 2 gelten die § 24a Absatz 4 Satz 2, Absatz 4 Satz 4, Absatz 5 und Absatz 6 entsprechend.“

Im Hinblick auf die Nachrichtendienste ergebe sich, so die Fraktion BÜNDNIS 90/DIE GRÜNEN, nach dem Beschluss des Bundesverfassungsgerichtes vom 24. Januar 2012, „aus dem Erfordernis der Erforderlichkeit im Einzelfall, dass eine Auskunft gemäß § 113 Absatz 1 Satz 1 TKG zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung geboten sein muss.“ Dem solle die Einfügung der Wörter „im Einzelfall“ Rechnung tragen. Der neue Satz 2 stelle zudem sicher, dass in den Fällen, in denen sich das Auskunftsverlangen auf Zugangssicherungscode beziehe oder unter Nutzung dynamischer IP-Adressen erfolge, der Behördenleitervorbehalt gelte und die G 10-Kommission des Landtages sowie die Parlamentarische Kontrollkommission über entsprechende Anordnungen unterrichtet würden.

Der Ausschuss hat jeweils mehrheitlich mit den Stimmen der Fraktionen der SPD und der CDU gegen die Stimmen der Fraktionen DIE LINKE und BÜNDNIS 90/DIE GRÜNEN bei Abwesenheit der Fraktion der NPD diese Änderungen abgelehnt und dem Artikel 1 mit der beschlossenen Änderung zugestimmt.

#### **Zu Artikel 2**

Die Fraktion BÜNDNIS 90/DIE GRÜNEN hatte beantragt, in Artikel 2 Nummer 2 nach § 28a Absatz 2 Satz 1 die folgenden Sätze 2 bis 8 einzufügen: „Auskunftsverlangen nach Absatz 1 Satz 2 und Absatz 2 Satz 1 dürfen nur auf Antrag des Leiters der Polizeibehörde oder seines Vertreters durch das Gericht angeordnet werden. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Bei Gefahr im Verzug kann die Anordnung durch den Leiter der Polizeibehörde oder seinen Vertreter getroffen werden, in diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Sätze 1 bis 3 finden keine Anwendung, wenn der Betroffene vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird. Das Vorliegen der Voraussetzungen nach Satz 4 ist aktenkundig zu machen.“

Weiterhin sollten in Nummer 2 in § 28a Absatz 2 die Sätze 2 bis 6 gestrichen und nach § 28a Absatz 2 der folgende Absatz 3 eingefügt werden, wobei der bisherige Absatz 3 Absatz 4 wird: „In den Fällen des Absatzes 1 Satz 2 und des Absatzes 2 ist die betroffene Person über die Beauskunftung zu unterrichten. Die Unterrichtung erfolgt, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird. Sie unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Wird die Unterrichtung nach Satz 2 zurückgestellt oder nach Satz 3 von ihr abgesehen, sind die Gründe aktenkundig zu machen. Wurde die Unterrichtung zurückgestellt und ist sie fünf Jahre nach der Beauskunftung nicht möglich, ist der Landesbeauftragte für Datenschutz und Informationsfreiheit zu unterrichten.“

Zur Begründung ist auf die Ergebnisse der öffentlichen Anhörung verwiesen worden. Um den Schutz der Betroffenen vor unbefugten Datenerhebungen zu erhöhen, sähen die neu eingefügten Sätze 2 bis 8 einen Richtervorbehalt vor. Die Unterrichtung des Betroffenen müsse sich zudem auch auf die Fälle beziehen, in denen Auskünfte über Zugangssicherungs-codes erteilt worden seien.

Die Fraktion DIE LINKE hatte beantragt, in Artikel 2 Nummer 2 den § 28a Absatz 2 wie folgt zu fassen: „(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 Telekommunikationsgesetz). Auskunftersuchen nach Absatz 1 Satz 2 und Absatz 2 Satz 1 dürfen nur auf Antrag des Leiters der Polizeibehörde oder seines Vertreters durch das Gericht angeordnet werden. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Bei Gefahr im Verzug kann die Anordnung durch den Leiter der Polizeibehörde oder seinen Vertreter getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Sätze 2 bis 4 finden keine Anwendung, wenn der Betroffene vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird. Das Vorliegen der Voraussetzungen nach Satz 5 ist aktenkundig zu machen.“

Darüber hinaus sollte nach Ansicht der Fraktion DIE LINKE in Nummer 2 § 28a Absatz 3 wie folgt gefasst werden, wobei der bisherige Absatz 3 zu Absatz 4 wird: „(3) In den Fällen von Absatz 1 Satz 2 und Absatz 2 ist die betreffende Person über die Beauskunftung zu unterrichten. Die Unterrichtung erfolgt, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird. Sie unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Wird die Unterrichtung nach Satz 3 zurückgestellt oder nach Satz 4 von ihr abgesehen, sind die Gründe aktenkundig zu machen. Wurde die Unterrichtung zurückgestellt und ist sie fünf Jahre nach der Beauskunftung nicht möglich, ist der Landesbeauftragte für Datenschutz und Informationsfreiheit zu unterrichten.“

Die Fraktion DIE LINKE hat dazu ausgeführt, dass im novellierten (Bundes-) Telekommunikationsgesetz geregelt worden sei, dass Auskunftersuchen über Zugangssicherungs-codes sowie über den Inhaber einer IP-Adresse einem Richtervorbehalt unterlägen und der Betroffene über beide Maßnahmen zu benachrichtigen sei. Beide Vorkehrungen trügen dem Umstand Rechnung, dass es sich bei den Maßnahmen um gewichtige Grundrechtseingriffe handele. Sowohl die gerichtliche Befassung als auch die Benachrichtigung der Betroffenen seien aus datenschutzrechtlicher Sicht grundsätzlich geeignete Mittel, um den Schutz der Betroffenen zu erhöhen. Dies gelte für die Bundes- und Landesebene gleichermaßen.

Der Ausschuss hat jeweils mehrheitlich mit den Stimmen der Fraktionen der SPD und der CDU gegen die Stimmen der Fraktionen DIE LINKE und BÜNDNIS 90/DIE GRÜNEN bei Abwesenheit der Fraktion der NPD diese Änderungen abgelehnt und dem Artikel 2 in der Fassung des Gesetzentwurfes zugestimmt.

**Zu Artikel 4 sowie zum Gesetzentwurf insgesamt**

Der Ausschuss hat jeweils mehrheitlich mit den Stimmen der Fraktionen der SPD und der CDU gegen die Stimmen der Fraktionen DIE LINKE und BÜNDNIS 90/DIE GRÜNEN bei Abwesenheit der Fraktion der NPD dem Artikel 4 unverändert zugestimmt und dem Landtag empfohlen, den Gesetzentwurf in der von ihm geänderten Fassung und im Übrigen unverändert anzunehmen.

Schwerin, den 6. Juni 2013

**Marc Reinhardt**  
Berichtersteller