06.06.13

Änderungsbedarf am schleswig-holsteinischen Entwurf eines Gesetzes zur Änderung des Landesverwaltungsgesetzes und des Landesverfassungsschutzgesetzes vom 10.04.2013 (Drs. 18/713)

Inhaltsverzeichnis

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
I. Landesverwaltungsgesetz		
I.1. Beschränkung auf Einzelfälle, konkrete Gefahr als Voraussetzung		
-	§ 180 a Bestandsdatenauskunft (1) Die Polizei darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), Auskunft über die nach §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten verlangen (§ 113 Abs. 1 Satz 1 des Telekommunikationsgesetzes), soweit dies zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für die öffentliche Sicherheit erforderlich ist. Das vom Telekommunikationsgesetz zum Inhalt und zur Übermittlung des Auskunftsverlangens an die Diensteanbieter vorgegebene Verfahren findet Anwendung (§ 113 Abs. 2 des Telekommunikationsgesetzes).	§ 180 a Bestandsdatenauskunft (1) Die Polizei darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), Auskunft über die nach §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten verlangen (§ 113 Abs. 1 Satz 1 des Telekommunikationsgesetzes), soweit dies **im Einzelfall** zur Abwehr einer ~~im einzelnen Falle bevorstehenden~~ Gefahr für die öffentliche Sicherheit erforderlich ist. Das vom Telekommunikationsgesetz zum Inhalt und zur Übermittlung des Auskunftsverlangens an die Diensteanbieter vorgegebene Verfahren findet Anwendung (§ 113 Abs. 2 des Telekommunikationsgesetzes).
Begründung: Die Änderung ist erforderlich, um entsprechend der Entschließung des Landtags vom 12.12.2012 (Drs. 18/370) sicher zu stellen, dass „die Auslieferung von Bestandsdaten (§ 113 Absatz 1 Satz 1 TKG) gesetzlich ausdrücklich auf Einzelfälle beschränkt bleibt“ (Drs. 18/370). Daneben wird der Rechtsprechung des Bundesverfassungsgerichts Rechnung getragen, wonach im Bereich der Gefahrenabwehr eine konkrete Gefahr zur Voraussetzung einer verhältnismäßigen staatlichen Bestandsdatenerhebung gemacht werden muss. 1. In § 180a Abs. 1 LVwG-RegE fehlt die in § 113 TKG a.F. enthaltene Bestimmung, dass Auskünfte über Telekommunikationsdaten nur „im Einzelfall“ erteilt werden dürfen und nicht routinemäßig oder massenhaft. Da die Beschränkung auf Einzelfälle fehlt, andererseits aber die ausufernd weiten Auskunftsrechte unverändert beibehalten werden sollen, wäre das Verhältnismäßigkeitsgebot verletzt und die Neufassung verfassungswidrig.		

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
Das Bundesverfassungsgericht hat § 113 TKG ausdrücklich nur deswegen als „verfassungsrechtlich noch hinnehmbar“ angesehen, weil „Auskünfte nach § 113 Abs. 1 Satz 1 TKG im Einzelfall angefordert werden und erforderlich sein müssen“ (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 177). Es hat die „Erfordernis der Erforderlichkeit auch im Einzelfall“ als Anforderung des Verhältnismäßigkeitsgrundsatzes eingeordnet (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 163). Dem Regierungsentwurf fehlt die verfassungsrechtlich gebotene Beschränkung von Auskünften auf Einzelfälle. Dass § 180a Abs. 1 LVwG-RegE eine „im einzelnen Falle bevorstehende Gefahr“ voraus setzt, besagt nichts darüber, ob aus Anlass solcher Gefahren nur im Einzelfall oder als Standardmaßnahme und massenhaft Auskünfte eingeholt werden dürfen. Rechtspolitisch unter dem Gesichtspunkt des Schutzes der Privatsphäre vorzugswürdig wäre es, Bestandsdaten ebenso gut zu schützen wie Telekommunikations-Verkehrsdaten. So ist es auch in dem rot-grün regierten Nordrhein-Westfalen vorgesehen (Drs. 16/2256). Wegen der verbreiteten rechtswidrigen Datenspeicherung wäre ferner wünschenswert, festzulegen, dass ausschließlich rechtmäßig gespeicherte Kommunikationsdaten erhoben werden dürfen. In der Vergangenheit sind immer wieder massive Verstöße von Telekommunikationsanbietern in Bezug auf Erhebung und Speicherung von personenbezogenen Daten festgestellt worden. 2. § 180a LVwG-RegE genügt auch seiner Ausgestaltung nach nicht den verfassungsrechtlichen Anforderungen. Nach der Rechtsprechung des Bundesverfassungsgerichts ist im Bereich der Gefahrenabwehr eine konkrete Gefahr Voraussetzung einer verhältnismäßigen staatlichen Bestandsdatenerhebung (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 177). § 180a Abs. 1 LVwG-RegE soll jedoch nur eine „bevorstehende“ und keine „bestehende“ Gefahr voraussetzen.		
I.2. Vorrang der Telekommunikationsüberwachung unter Mitwirkung des Anbieters vor dem unmittelbaren Zugriff mithilfe von Zugangssicherungscodes		
-	(2) [1]Bezieht sich das Auskunftsverlangen nach Absatz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Abs. 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vor-liegen	(2) [1]Bezieht sich das Auskunftsverlangen nach Absatz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Abs. 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
	1. zur Überwachung der Telekommunikation nach § 185 a oder 2. zur Sicherstellung von nicht mehr dem Schutz des Artikel 10 des Grundgesetzes unterliegenden in Endeinrichtungen oder auf Speichereinrichtungen abgelegten Daten nach § 210.	1. zur Überwachung der Telekommunikation nach § 185 a oder 2. zur Sicherstellung von nicht mehr dem Schutz des Artikel 10 des Grundgesetzes unterliegenden in Endeinrichtungen oder auf Speichereinrichtungen abgelegten Daten nach § 210 **und wenn die Maßnahme nach Nr. 1 oder 2 auf andere Weise nicht durchführbar ist**.
Begründung: Die Änderung ist erforderlich, um der Entschließung des Landtags vom 12.12.2012 (Drs. 18/370) Rechnung zu tragen, derzufolge „der Vorrang der Telekommunikationsüberwachung unter Mitwirkung des Anbieters vor dem unmittelbaren Zugriff mithilfe von Zugangssicherungscodes [...] festzuschreiben“ ist. Aufgenommen wird eine Subsidiaritätsklausel, derzufolge die Herausgabe eines Zugangssicherungscodes nur erfolgen darf, wenn eine Sicherstellung oder Telekommunikationsüberwachungsmaßnahme auf andere Weise nicht durchführbar ist. Die Erhebung von Zugangssicherungscodes wie Passwörter zu E-Mail-Postfächern oder Speicherdiensten stellt einen besonders tiefgreifenden Grundrechtseingriff dar, da sie der Schlüssel für die Nutzung weiterer Daten sind, die der Nutzer im Vertrauen auf den Zugangsschutz gespeichert hat. Die Herausgabe von Passwörtern ermöglicht den Zugriff auf Inhalte der Telekommunikation und weitere persönliche Inhalte wie Fotos, Tagebücher und Dokumente. Aus diesem Grund darf die behördliche Anforderung von Zugangssicherungscodes allenfalls als letztes Mittel zugelassen werden. Rechtspolitisch unter dem Gesichtspunkt des Schutzes der Privatsphäre vorzugswürdig wäre allerdings der gänzliche Verzicht auf die Herausgabe von Zugangssicherungscodes. So ist es auch in dem rot-grün regierten Nordrhein-Westfalen vorgesehen (Drs. 16/2256, S. 22).		
I.3. Schutz von IP-Adressen wie andere Verkehrsdaten		
	[2]Die Auskunft über die nach §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten nach Satz 1 und Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§	~~[2]Die Auskunft über die nach §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten nach Satz 1 und Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§~

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
	113 Abs. 1 Satz 3 des Telekommunikationsgesetzes). [3]Satz 2 gilt bei fest zugewiesenen Internetprotokoll-Adressen sinngemäß.	~~113 Abs. 1 Satz 3 des Telekommunikationsgesetzes). [3]Satz 2 gilt bei fest zugewiesenen Internetprotokoll-Adressen sinngemäß.~~ § 185 a Datenerhebung durch Überwachung der Telekommunikation (2) Eine Datenerhebung nach Absatz 1 kann sich beziehen auf 1. die Inhalte der Telekommunikation einschließlich der innerhalb des Telekommunikationsnetzes in Datenspeichern abgelegten Inhalte, 2. die Telekommunikationsverkehrsdaten (§ 96 Abs. 1 und § 113 a des Telekommunikationsgesetzes), 3. den Standort einer aktiv geschalteten Mobilfunkendeinrichtung ~~oder~~ 4. die Feststellung der Polizei nicht bekannter Telekommunikationsanschlüsse **oder** **5. die Feststellung des Inhabers eines Telekommunikationsanschlusses anhand einer Internetprotokoll-Adresse (§ 113 Abs. 1 Satz 3 des Telekommunikationsgesetzes)**.
Begründung: Die Änderung ist erforderlich, um der Entschließung des Landtags vom 12.12.2012 (Drs. 18/370) Rechnung zu tragen, derzufolge „für die Abfrage von IP-Adressen durch Behörden dieselben verfahrensrechtlichen und inhaltlichen Voraussetzungen eingeführt werden [sollen] wie für die Ausliefe-		

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
rung von Telekommunikations-Verkehrsdaten (z.B. Richtervorbehalt, Eingriffsschwellen)“. Die Identifizierung von Internetnutzern (§§ 180a LVwG-RegE und § 8a Abs. 1 S. 4 LVerfSchG-RegE) stellt einen besondern schwerwiegenden Grundrechtseingriff dar, weil sie die personenbezogene Nachverfolgung des Inhalts der abgerufenen oder geschriebenen Texte und Daten im Internet erlaubt. Anders als Auskünfte über Rufnummerninhaber geht die Identifizierung von Internetnutzern mit einem Eingriff in das grundrechtlich besonders geschützte Fernmeldegeheimnis einher. Die Begründung von behördlichen Auskunftsansprüchen ermöglicht es in Verbindung mit der Speicherung der Internetzugangsdaten nach § 100 TKG in weitem Umfang, die Identität von Internetnutzern zu ermitteln. Auch ist die mögliche Persönlichkeitsrelevanz einer Abfrage des Inhabers einer IP-Adresse eine andere als die des Inhabers einer Telefonnummer: Schon vom Umfang der Kontakte her, die jeweils durch das Aufrufen von Internetseiten neu hergestellt werden, ist sie aussagekräftiger als eine Telefonnummernabfrage. Auch hat die Kenntnis einer Kontaktaufnahme mit einer Internetseite eine andere inhaltliche Bedeutung: Da der Inhalt von Internetseiten anders als das beim Telefongespräch gesprochene Wort elektronisch fixiert und länger wieder aufrufbar ist, lässt sich mit ihr vielfach verlässlich rekonstruieren, mit welchem Gegenstand sich der Kommunizierende auseinander gesetzt hat. Die Individualisierung der IP-Adresse als der „Telefonnummer des Internet“ gibt damit zugleich Auskunft über den Inhalt der Kommunikation. Die für das Telefongespräch geltende Unterscheidung von äußerlichen Verbindungsdaten und Gesprächsinhalten löst sich hier auf. Wird der Besucher einer bestimmten Internetseite mittels der Auskunft über eine IP-Adresse individualisiert, weiß man nicht nur, mit wem er Kontakt hatte, sondern kennt in der Regel auch den Inhalt des Kontakts (BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 259). Die Identifizierung von dynamischen IP-Adressen ermöglicht in weitem Umfang eine Deanonymisierung von Kommunikationsvorgängen im Internet. Zwar hat sie eine gewisse Ähnlichkeit mit der Identifizierung einer Telefonnummer. Schon vom Umfang, vor allem aber vom Inhalt der Kontakte her, über die sie Auskunft geben kann, hat sie jedoch eine erheblich größere Persönlichkeitsrelevanz und kann mit ihr - so das Bundesverfassungsgericht ausdrücklich - nicht gleichgesetzt werden (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 174). Eben dies tut aber der Regierungsentwurf, was die Voraussetzung einer „bevorstehenden Gefahr“ jeglicher Art angeht. Die Identifizierung von Internetnutzern im selben weit reichenden Umfang zuzulassen wie Auskünfte über Rufnummerninhaber ist nicht hinnehmbar. Diese Gleichsetzung lehnen auch das Unabhängige Landesdatenschutzzentrum (Umdruck 18/1245) und die Neue Richtervereinigung (Umdruck 18/1250) in ihren Stellungnahmen zu dem Gesetzentwurf ab. Entsprechend der Entschließung des Landtags aus dem Jahr 2012 muss zumindest eine Gleichstellung mit der Verwendung sonstiger Verkehrsdaten nach § 185a LVwG erfolgen, also eine gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person zur Voraussetzung gemacht werden. Da IP-Adressen die Schnittstelle zwischen Bestands- und Verkehrsdaten darstellen, muss hier der höhere Standard zur Anwendung kommen. Dazu wird die Zuordnung von IP-Adressen in § 185a LVwG geregelt.		
-	**(3) Aufgrund eines Auskunftsverlangens nach Absatz 1 bis 2 hat der Diensteanbieter die zur Auskunftserteilung erforderlichen Daten un-**	*unverändert*

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
	verzüglich und vollständig zu übermitteln. Für seine Entschädigung ist § 23 des Justizvergütungs- und –entschädigungsgesetzes entsprechend anzuwenden.	
I.4. Keine Auskunftspflicht für Internet- und sonstige Telemediendienste		
-	**(4) Absatz 1 bis 3 gilt bei an die Telemedien-Diensteanbieter gerichteten Auskunftsverlangen auf Bestandsdaten nach § 14 des Telemediengesetzes sowie auf die Identifikation der Nutzer und auf das Datum und die Uhrzeit des Beginns und Endes der Nutzung beschränkte Daten im Sinne des § 15 des Telemediengesetzes entsprechend.**	~~(4) Absatz 1 bis 3 gilt bei an die Telemedien-Diensteanbieter gerichteten Auskunftsverlangen auf Bestandsdaten nach § 14 des Telemediengesetzes sowie auf die Identifikation der Nutzer und auf das Datum und die Uhrzeit des Beginns und Endes der Nutzung beschränkte Daten im Sinne des § 15 des Telemediengesetzes entsprechend.~~

Begründung:

Die Änderung ist erforderlich, um zu verhindern, dass die bundesgesetzliche Neuregelung der Bestandsdatenauskunft im Telekommunikationsgesetz zum Anlass genommen wird, um eine ganz andere Ermächtigung – nämlich zum Zugriff auf Internetdaten nach dem Telemediengesetz – einzuräumen.

Das vorliegende Gesetzgebungsverfahren wird mit großer Eile vorangetrieben, weil das Bundesverfassungsgericht die Anwendung der Bestandsdatenauskunft nach § 113 TKG befristet hat. In diesem Eilverfahren ist es keinesfalls angemessen, eine Befugnis neu einzuführen, die mit § 113 TKG und der diesbezüglichen Eilbedürftigkeit nichts zu tun hat. Dies gilt zumal deswegen, weil der Referentenentwurf, zu dem die Landesregierung noch eine schriftliche Anhörung durchführen konnte, die Einbeziehung von Telemediendiensten noch nicht vorsah. Überdies regelt auch das Bundesgesetz zur Bestandsdatenauskunft Telemedien nicht. Das Bundespolizeigesetz kennt eine entsprechende Befugnis nicht.

Die Datenerhebungsvorschriften des Landesverwaltungsgesetzes begründen bisher keine Auskunftspflicht über Informationen betreffend Internetnutzer. Eine Auskunftspflicht besteht nach der Rechtsprechung des Bundesverfassungsgerichts nur unter den Voraussetzungen, unter denen Datenträger sicher gestellt werden können. Bisher erlaubt § 210 LVwG der Polizei die zwangsweise Erhebung von Daten nur unter den Voraussetzungen der Sicherstellung von Sachen zulässig, also wenn dies erforderlich ist,

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag

1. zur Abwehr einer gegenwärtigen Gefahr für die öffentliche Sicherheit,

2. zur Verhinderung einer mißbräuchlichen Verwendung durch eine Person, die in Gewahrsam genommen worden ist, oder

3. um die Eigentümerin oder den Eigentümer oder die rechtmäßige Inhaberin oder den rechtmäßigen Inhaber der tatsächlichen Gewalt vor Verlust oder Beschädigung einer Sache zu schützen.

Diese Rechtslage genügt vollkommen, um dem im Regierungsentwurf beschriebenen Bedarf (Ankündigung von Amoktaten, Suiziden oder polizeilich relevanten Rechts-Rock-Konzerten) Rechnung zu tragen, soweit er legitim ist.

Der Regierungsentwurf will demgegenüber Anbieter sozialer Netzwerke und anderer Telemediendienste künftig verpflichten, zur Abwehr jeglicher (auch nicht gegenwärtiger) Gefahr ohne richterliche Anordnung Auskunft über Bestandsdaten der Nutzer, über „die Identifikation der Nutzer“ und über „das Datum und die Uhrzeit des Beginns und Endes der Nutzung“ zu erteilen. Was mit „Identifikation der Nutzer“ gemeint ist, ist unklar; da es sich nicht um Bestandsdaten handeln soll, ist möglicherweise die genutzte Internetkennung (IP-Adresse) gemeint. Auch bei Datum und Uhrzeit der Nutzung handelt es sich eindeutig nicht um Bestandsdaten, sondern um Daten über die Nutzung von Internetdiensten. Ob Passwörter erfasst werden sollen, ist unklar. Die Auskunft über Telemediendaten soll sich nach den Vorschriften über die Telekommunikations-Bestandsdatenauskunft richten. Welche dieser Vorschriften aber auf welche Anfragen Anwendung finden sollen, ist nicht normenklar geregelt.

Wer wann welche Informationen im Internet liest, schreibt oder sucht, ist eine äußerst sensible Information. Nach dem Telemediengesetz darf sie allenfalls zu Abrechnungszwecken erhoben werden; bei kostenfreien Diensten ist eine „Surfprotokollierung“ unzulässig. Dennoch erfolgt sie in der Praxis fast durchweg („Logfiles“).

Daten über die Nutzung von Telemedien sind nicht weniger sensibel als Daten über die Individualkommunikation der Bürger untereinander, die dem Fernmeldegeheimnis unterliegen. Nur unter den Voraussetzungen einer Telekommunikationsüberwachung ist es akzeptabel, auch auf dem Gebiet der Telemedien einen Anspruch der Behörden auf Auskunft über Nutzerdaten einzuräumen. Auch für Telemedien-Bestandsdaten dürfen keine geringeren Anforderungen gelten. Der Gesetzgeber hat zurecht betont, dass sie nicht weniger schutzwürdig sind als Nutzungsdaten (BT-Drs. 14/6098, 1 (29): „Hier besteht eine gleichwertige Interessenlage sowohl hinsichtlich der Nutzungsdaten als auch hinsichtlich der Bestandsdaten“). Erst Bestandsdaten ermöglichen es, Informationen über die Nutzung von Telemedien einer Person zuzuordnen. Bestandsdaten sind gerade auf dem Gebiet von Telemedien sehr sensibel, denn Telemedien haben das Angebot bestimmter Inhalte zum Gegenstand. Schon die Information, welche Telemedien eine bestimmte Person in Anspruch nimmt, kann weit reichende Rückschlüsse auf ihre politischen, finanziellen, sexuellen, weltanschaulichen, religiösen oder sonstigen persönlichen Interessen und Neigungen zulassen.

Bei der Anhörung im Innen- und Rechtsausschuss hat letztlich unter allen Sachverständigen (Unabhängiges Landesdatenschutzzentrum, Neue Richtervereinigung und Bund Deutscher Kriminalbeamte) Einigkeit bestanden, dass – zumal bis zur Klärung auf Bundesebene – eine landesgesetzliche Regelung zurückgestellt werden sollte.

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
Vor diesem Hintergrund ist die zweckfremde Regelung bezüglich Internet- und Telemediendiensten aus dem vorliegenden Gesetzentwurf zu streichen.		
I.5. Passwortabfrage nur mit richterlicher Anordnung		
-	§ 180 b Verfahren zur Bestandsdatenauskunft (1) Auskunftsverlangen nach § 180 a Abs. 2 dürfen nur auf Antrag der Polizei durch das nach § 186 Abs. 2 Satz 1 zuständige Gericht angeordnet werden. Für das Verfahren findet das Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechende Anwendung. Der Anhörung der betroffenen Person durch das Gericht bedarf es nicht. Bei Gefahr im Verzuge kann die Polizei die Anordnung treffen. In diesem Fall gelten die § 186 Abs. 1 Satz 3 bis 5, § 186 a Abs. 6 entsprechend. Satz 1 bis 4 findet 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 6 ist aktenkundig zu machen. Nach Abschluss der Maßnahmen nach § 180 a Abs. 2 ist die betroffene Person von der Polizei zu unterrichten und auf die Möglichkeit nachträglichen Rechtsschutzes hinzuweisen. Die Unterrichtung erfolgt, soweit und sobald der Zweck der Auskunft nicht vereitelt wird. Die Unterrichtung nach Satz 8 unterbleibt, wenn ihr überwiegende schutzwürdige Belange	§ 180 b Verfahren zur Bestandsdatenauskunft (1) Auskunftsverlangen nach § 180 a Abs. 2 dürfen nur auf Antrag der Polizei durch das nach § 186 Abs. 2 Satz 1 zuständige Gericht angeordnet werden. Für das Verfahren findet das Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechende Anwendung. Der Anhörung der betroffenen Person durch das Gericht bedarf es nicht. Bei Gefahr im Verzuge kann die Polizei die Anordnung treffen. In diesem Fall gelten die § 186 Abs. 1 Satz 3 bis 5, § 186 a Abs. 6 entsprechend. ~~Satz 1 bis 4 findet 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 6 ist aktenkundig zu machen.~~ Nach Abschluss der Maßnahmen nach § 180 a Abs. 2 ist die betroffene Person von der Polizei zu unterrichten und auf die Möglichkeit nachträglichen Rechtsschutzes hinzuweisen. Die Unterrichtung erfolgt, soweit und sobald der Zweck der Auskunft nicht vereitelt wird. Die Unterrichtung nach Satz 8 unterbleibt, wenn ihr überwiegende schutzwürdige Belange	§ 180 b Verfahren zur Bestandsdatenauskunft (1) Auskunftsverlangen nach § 180 a Abs. 2 dürfen nur auf Antrag der Polizei durch das nach § 186 Abs. 2 Satz 1 zuständige Gericht angeordnet werden. Für das Verfahren findet das Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechende Anwendung. Der Anhörung der betroffenen Person durch das Gericht bedarf es nicht. Bei Gefahr im Verzuge kann die Polizei die Anordnung treffen. In diesem Fall gelten die § 186 Abs. 1 Satz 3 bis 5, § 186 a Abs. 6 entsprechend. ~~Satz 1 bis 4 findet 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 6 ist aktenkundig zu machen.~~ Nach Abschluss der Maßnahmen nach § 180 a Abs. 2 ist die betroffene Person von der Polizei zu unterrichten und auf die Möglichkeit nachträglichen Rechtsschutzes hinzuweisen. Die Unterrichtung erfolgt, soweit und sobald der Zweck der Auskunft nicht vereitelt wird. Die Unterrichtung nach Satz 8 unterbleibt, wenn ihr überwiegende schutzwürdige Belange

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
	Dritter oder der betroffenen Person selbst entgegenstehen. Wird die Unterrichtung nach Satz 9 zurückgestellt oder nach Satz 10 von ihr abgesehen, gilt § 186 Abs. 4 Satz 5 bis 9 entsprechend.	Dritter oder der betroffenen Person selbst entgegenstehen. Wird die Unterrichtung nach Satz 9 zurückgestellt oder nach Satz 10 von ihr abgesehen, gilt § 186 Abs. 4 Satz 5 bis 9 entsprechend.

Begründung:

Die Änderung ist erforderlich, um der Entschließung des Landtags vom 12.12.2012 (Drs. 18/370) Rechnung zu tragen, die fordert, dass „eindeutig und restriktiv gesetzlich geregelt wird, unter welchen verfahrensrechtlichen (z.B. richterliche Anordnung oder Bestätigung und Dokumentationspflichten) und inhaltlichen Voraussetzungen Zugangssicherungscodes (wie Passwörter, PIN oder PUK), die den Zugang zu Endgeräten (z.B. Mobiltelefonen) und Speicherungseinrichtungen (z.B. E-Mail-Postfächer) sichern, gegenüber Staatsbehörden preiszugeben sind und deren Nutzung zugelassen wird“.

Die Erhebung von Zugangssicherungscodes wie Passwörter zu E-Mail-Postfächern oder Speicherdiensten stellt einen tiefgreifenden Grundrechtseingriff dar, da sie der Schlüssel für die Nutzung weiterer Daten sind, die der Nutzer im Vertrauen auf den Zugangsschutz gespeichert hat. Die Herausgabe von Passwörtern ermöglicht den Zugriff auf Inhalte der Telekommunikation und weitere persönliche Inhalte wie Fotos, Tagebücher und Dokumente.

Um von einer unabhängigen Instanz überprüfen zu lassen, dass die gesetzlichen Voraussetzungen des Zugriffs auf diese hochsensiblen Daten vorliegen, muss eine richterliche Anordnung durchgängig zur Voraussetzung der Herausgabe von Passwörtern gemacht werden. Dies fordern auch das Unabhängige Landesdatenschutzzentrum (Umdruck 18/1245) und die Neue Richtervereinigung (Umdruck 18/1250) in ihren Stellungnahmen zu dem Gesetzentwurf.

Wenn der Betroffene von einer beabsichtigten Passwortabfrage Kenntnis hat oder „haben muss“, ersetzt dies eine richterliche Prüfung der gesetzlichen Voraussetzungen des Zugriffs nicht. Die Kenntnis des Betroffenen hat mit der Erforderlichkeit einer richterlichen Anordnung nichts zu tun. Kein anderer Richtervorbehalt steht unter dem Vorbehalt einer Kenntnis durch den betroffenen.

Ebenso wenig ist einsichtig, warum die richterliche Anordnung einer Telekommunikationsüberwachung oder Handybeschlagnahme eine Entscheidung darüber entbehrlich machen soll, ob dazu die Anforderung eines Zugangssicherungscodes erforderlich ist. Oftmals ist eine Telekommunikationsüberwachung oder Auswertung eines Handyspeichers auch ohne Kenntnis von Passwörtern möglich. Über die Erforderlichkeit der Herausgabe persönlicher Zugangssicherungscodes muss aufgrund der Schwere des Grundrechtseingriffs der Richter entscheiden (vorbehaltlich Eilfällen).

Angemerkt werden soll, dass das rot-grün regierte Nordrhein-Westfalen der Polizei keinerlei Zugriff auf Zugangssicherungscodes erlaubt (Drs. 16/2256, S. 22).

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
I.6. Schutz von IP-Adressen wie andere Verkehrsdaten (Folgeänderung)		
-	(2) Absatz 1 gilt bei Auskunftsverlangen nach § 180 a Abs. 4 entsprechend.	~~(2) Absatz 1 gilt bei Auskunftsverlangen nach § 180 a Abs. 4 entsprechend.~~
I.7. Berichtspflicht und parlamentarische Kontrolle über IP-Auskünfte und Passwortabfragen		
§ 186 b Berichtspflicht der Landesregierung und parlamentarische Kontrolle (1) Die Landesregierung unterrichtet den Landtag jährlich über Anlass, Umfang, Dauer und Ergebnis nach § 185 Abs. 3 durchgeführter Maßnahmen und, soweit richterlich überprüfungsbedürftig, über durchgeführte Maßnahmen nach § 186 Abs. 1 Satz 7. Bei Maßnahmen nach § 185 a Abs. 1 gilt Satz 1 entsprechend. (2) Ein vom Landtag gewähltes Gremium übt auf der Grundlage dieses Berichtes die parlamentarische Kontrolle aus.	*unverändert*	§ 186 b Berichtspflicht der Landesregierung und parlamentarische Kontrolle (1) Die Landesregierung unterrichtet den Landtag jährlich über Anlass, Umfang, Dauer und Ergebnis nach § 185 Abs. 3 durchgeführter Maßnahmen und, soweit richterlich überprüfungsbedürftig, über durchgeführte Maßnahmen nach § 186 Abs. 1 Satz 7. Bei Maßnahmen nach **§ 180a Abs. 2 und nach** § 185 a Abs. 1 gilt Satz 1 entsprechend. (2) Ein vom Landtag gewähltes Gremium übt auf der Grundlage dieses Berichtes die parlamentarische Kontrolle aus.
Begründung: Die Änderung ist erforderlich, um dem Landtag zu ermöglichen, die Entwicklung der besonders tief in Grundrechte eingreifenden Auskünfte über Internetnutzer und Zugangssicherungscodes zu beobachten und erforderlichenfalls einzugreifen. Nach § 186b LVwG wird der Landtag bislang jährlich über Anlass, Umfang, Dauer und Ergebnis unter anderem von polizeilichen Zugriffen auf Verkehrsdaten unterrichtet. Die Identifizierung von Internetnutzern und auch die Erhebung von Zugangssicherungscodes greift so tief in die Grundrechte der Betroffenen ein, dass eine statistische Erfassung gleichfalls erforderlich ist. Dies gilt erst Recht mit Blick auf die bundesgesetzlich neu eingeführte		

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
automatisierte Datenschnittstelle, die eine erhebliche Vereinfachung und dadurch Vervielfachung der Datenzugriffe befürchten lässt. Eine umfassende statistische Erfassung der staatlichen Bestandsdatenabfragen ist für eine wissenschaftliche Überprüfung und öffentliche Kontrolle der getätigten Grundrechtseingriffe unerlässlich. Die Anzahl der getätigten Zugriffe muss der Öffentlichkeit zugänglich gemacht werden, damit das Ausmaß der getätigten Eingriffe und die damit verbundenen Grundrechtseinschränkungen für Betroffene für die Bürgerinnen und Bürger transparent nachvollziehbar sind. Die Entwicklung der tatsächlichen Nutzung der durch den Gesetzesentwurf vorgesehenen neuen Zugriffsbefugnisse durch Behörden kann so nachverfolgt und eine übergriffige Nutzung des Rechtsrahmens frühzeitig erkannt werden. Darüber hinaus ist es für eine wissenschaftliche Auseinandersetzung mit der Entwicklung von Abfragezahlen unerlässlich, derartige Daten genau nach Abfragegrund, abfragende Behörde, Zahl der Betroffenen und weiteren für die statistische Erfassung notwendigen Daten aufzuschlüsseln. Nur so kann eine auf wissenschaftlicher Faktenlage basierende unabhängige Evaluierung der Eingriffsbefugnisse durchgeführt werden.		
II. Landesverfassungsschutzgesetz		
II.1. Konkrete beobachtungsbedürftige Aktion oder Gruppierung als Voraussetzung von Bestandsdatenauskünften		
§ 8 a Besondere Auskunftsverlangen (1) [1]Die Verfassungsschutzbehörde darf im Einzelfall bei denjenigen, die geschäftsmäßig Postdienstleistungen, Telekommunikationsdienste oder Telemedien erbringen oder daran mitwirken, Auskunft über Daten einholen, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Postdienstleistungen oder Telemedien (Bestandsdaten) gespeichert worden sind, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist.	§ 8 a Besondere Auskunftsverlangen (1) [1]Die Verfassungsschutzbehörde darf im Einzelfall bei denjenigen, die geschäftsmäßig Postdienstleistungen oder Telemedien erbringen oder daran mitwirken, Auskunft über Daten einholen, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Postdienstleistungen oder Telemedien (Bestandsdaten) gespeichert worden sind, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. [2]**Bei denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, darf die Verfassungsschutzbehörde im Einzelfall Auskunft über**	§ 8 a Besondere Auskunftsverlangen (1) [1]Die Verfassungsschutzbehörde darf im Einzelfall bei denjenigen, die geschäftsmäßig Postdienstleistungen oder Telemedien erbringen oder daran mitwirken, Auskunft über Daten einholen, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Postdienstleistungen oder Telemedien (Bestandsdaten) gespeichert worden sind, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. [2]Bei denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, darf die Verfassungsschutzbehörde im Einzelfall Auskunft über die

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
	die nach den §§ 95 und 111 Telekommunikationsgesetz erhobenen Daten verlangen (§ 113 Abs. 1 Satz 1 des Telekommunikationsgesetzes), soweit dies zu ihrer Aufgabenerfüllung erforderlich ist.	nach den §§ 95 und 111 Telekommunikationsgesetz erhobenen Daten verlangen (§ 113 Abs. 1 Satz 1 des Telekommunikationsgesetzes), soweit dies ~~zu ihrer Aufgabenerfüllung~~ **zur Aufklärung einer bestimmten, nach diesem Gesetz beobachtungsbedürftigen Aktion oder Gruppierung** erforderlich ist.

Begründung:

Die Änderung ist erforderlich, um der Rechtsprechung des Bundesverfassungsgerichts Rechnung zu tragen, wonach eine Bestandsdatenauskunft gegenüber Nachrichtendiensten eine zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung geboten sein muss.

Nach der Rechtsprechung des Bundesverfassungsgerichts ist im Bereich der Nachrichtendienste Voraussetzung einer verhältnismäßigen staatlichen Bestandsdatenerhebung, dass diese „zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung geboten sein muss“ (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 177). Im Sinne der Normenklarheit, zur Erleichterung des Gesetzesvollzugs und zum Zwecke des Grundrechtsschutzes werden diese grundrechtlichen Anforderungen gesetzlich normiert.

Rechtspolitisch unter dem Gesichtspunkt des Schutzes der Privatsphäre vorzugswürdig wäre es, Bestandsdaten ebenso gut zu schützen wie Telekommunikations-Verkehrsdaten. So ist es auch in dem rot-grün regierten Nordrhein-Westfalen vorgesehen (Drs. 16/2256). Wegen der verbreiteten rechtswidrigen Datenspeicherung wäre ferner wünschenswert, festzulegen, dass ausschließlich rechtmäßig gespeicherte Kommunikationsdaten erhoben werden dürfen. In der Vergangenheit sind immer wieder massive Verstöße von Telekommunikationsanbietern in Bezug auf Erhebung und Speicherung von personenbezogenen Daten festgestellt worden.

II.2. Kein unbestimmter Zugriff auf Zugangssicherungscodes durch den Verfassungsschutz

-	[3]**Bezieht sich das Auskunftsverlangen nach Satz 2 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Abs. 1 Satz 2 des Telekommunika-**	[3]Bezieht sich das Auskunftsverlangen nach Satz 2 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Abs. 1 Satz 2 des Telekommunikationsgesetzes), darf

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
	tionsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.	die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten **zur Überwachung und Aufzeichnung der Telekommunikation nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses** vorliegen **und wenn die Maßnahme ohne die Auskunft nicht durchführbar ist**.

Begründung:

Die Änderung ist erforderlich, um entsprechend der Entschließung des Landtags vom 12.12.2012 (Drs. 18/370) sicher zu stellen, dass „eindeutig und restriktiv gesetzlich geregelt wird, unter welchen verfahrensrechtlichen (z.B. richterliche Anordnung oder Bestätigung und Dokumentationspflichten) und inhaltlichen Voraussetzungen Zugangssicherungscodes (wie Passwörter, PIN oder PUK), die den Zugang zu Endgeräten (z.B. Mobiltelefonen) und Speicherungseinrichtungen (z.B. E-Mail-Postfächer) sichern, gegenüber Staatsbehörden preiszugeben sind und deren Nutzung zugelassen wird; der Vorrang der Telekommunikationsüberwachung unter Mitwirkung des Anbieters vor dem unmittelbaren Zugriff mithilfe von Zugangssicherungscodes ist festzuschreiben“.

Zugangssicherungscodes (wie Passwörter, PIN oder PUK) sichern den Zugang zu Endgeräten und Speicherungseinrichtungen und damit die Betreffenden vor einem Zugriff auf die entsprechenden Daten beziehungsweise Telekommunikationsvorgänge. Das Bundesverfassungsgericht hat entschieden, dass Staatsbehörden PINs und Passwörter nur anfordern dürfen, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind. Diese Formulierung soll nun unverändert in das Gesetz aufgenommen werden.

Verfassungsrechtlich verletzt die lapidare Bezugnahme auf „die gesetzlichen Voraussetzungen für die Nutzung der Daten“ (§ 8a Abs. 1 S. 2 LVerfSchG-E) das Bestimmtheitsgebot. Sie ermöglicht weder der handelnden Behörde, noch dem verpflichteten Anbieter oder dem kontrollierenden Gericht, mit hinreichender Klarheit zu bestimmen, welche Voraussetzungen vorliegen müssen. Auch ist nicht gewährleistet, dass der Anbieter das Vorliegen der Zugriffsvoraussetzungen (z.B. richterliche Anordnung der Telekommunikationsüberwachung) anhand behördlich zur Verfügung gestellter Unterlagen kontrollieren kann. Wenn eine Behörde einen Zugriffscode anfordert, weiß der Anbieter nicht, ob dies zum Zweck der Telekommunikationsüberwachung oder zur Auswertung abgeschlossener Telekommunikation geschieht. Es ist nicht akzeptabel, die Kontrolle der gesetzlichen Voraussetzungen durch den Telekommunikationsanbieter bei der Anforderung von Zugriffscodes quasi ausfallen zu lassen, obwohl solche Codes besonders weitreichende und unkontrollierte Zugriffe ermöglichen.

Es ist aus diesen Gründen verfassungsrechtlich geboten, abschließend zu bestimmen, welche materiellen und formellen gesetzlichen Voraussetzungen für die Nutzung von Zugangscodes vorliegen müssen. Während § 180a LVwG-RegE eine solche Regelung vorsieht, ist im Fall des Verfassungsschut-

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
zes keine Regelung vorhanden, die dem Gebot der Normenklarheit genügte (so auch das Unabhängige Landesdatenschutzzentrum, siehe Umdruck 18/1245). Da der Verfassungsschutz die in § 180a LVwG-RegE angesprochene Sicherstellung nicht durchführen darf, bleibt nur der Fall der Telekommunikationsüberwachung nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses. Aufgenommen wird außerdem eine Subsidiaritätsklausel, derzufolge die Herausgabe eines Zugangssicherungscodes nur erfolgen darf, wenn eine Telekommunikationsüberwachungsmaßnahme auf andere Weise nicht durchführbar ist. Die Erhebung von Zugangssicherungscodes wie Passwörter zu E-Mail-Postfächern oder Speicherdiensten stellt einen besonders tiefgreifenden Grundrechtseingriff dar, da sie der Schlüssel für die Nutzung weiterer Daten sind, die der Nutzer im Vertrauen auf den Zugangsschutz gespeichert hat. Die Herausgabe von Passwörtern ermöglicht den Zugriff auf Inhalte der Telekommunikation und weitere persönliche Inhalte wie Fotos, Tagebücher und Dokumente. Aus diesem Grund darf die behördliche Anforderung von Zugangssicherungscodes allenfalls als letztes Mittel zugelassen werden. Rechtspolitisch unter dem Gesichtspunkt des Schutzes der Privatsphäre vorzugswürdig wäre allerdings der gänzliche Verzicht auf die Herausgabe von Zugangssicherungscodes an den Verfassungsschutz (so auch die Neue Richtervereinigung, Umdruck 18/1250). So ist es auch in dem rot-grün regierten Nordrhein-Westfalen vorgesehen (Drs. 16/2256, S. 22).		
II.3. Schutz von IP-Adressen wie andere Verkehrsdaten		
-	**[4]Die Auskunft darf auch anhand einer zu bestimmten Zeitpunkten zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Abs. 1 Satz 3 des Telekommunikationsgesetzes).**	[4]~~Die Auskunft darf auch anhand einer zu bestimmten Zeitpunkten zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Abs. 1 Satz 3 des Telekommunikationsgesetzes).~~
-	**[5]Aufgrund eines Auskunftsverlangens nach den Sätzen 2 bis 4 haben diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, die zur Auskunft erforderlichen Daten unverzüglich, vollständig und richtig zu übermitteln.**	[3]Aufgrund eines Auskunftsverlangens nach ~~den Sätzen~~ **Satz** 2 ~~bis 4~~ haben diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, die zur Auskunft erforderlichen Daten unverzüglich, vollständig und richtig zu übermitteln.
(2) Die Verfassungsschutzbehörde darf im Einzelfall Auskunft einholen bei 1. Luftfahrtunternehmen zu Namen und An-	(2) *unverändert*	(2) Die Verfassungsschutzbehörde darf im Einzelfall Auskunft einholen bei 1. Luftfahrtunternehmen zu Namen und An-

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
schriften der Kundin oder des Kunden sowie zur Inanspruchnahme und den Umständen von Transportleistungen, insbesondere zum Zeitpunkt von Abfertigung und Abflug und zum Buchungsweg, 2. Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen zu Konten, Konteninhaberinnen oder Konteninhabern und sonstigen Berechtigten sowie weiteren am Zahlungsverkehr Beteiligten und zu Geldbewegungen und Geldanlagen, insbesondere über Kontostand und Zahlungsein- und -ausgänge, 3. denjenigen, die geschäftsmäßig Postdienstleistungen erbringen oder daran mitwirken, zu den Umständen des Postverkehrs, 4. denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, zu Verkehrsdaten nach § 96 Abs. 1 Nr. 1 bis 4 des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 2 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198), und sonstigen zum Aufbau und zur Aufrechterhaltung der Telekommunikation notwendigen Verkehrsdaten und 5. denjenigen, die geschäftsmäßig Telemedien erbringen oder daran mitwirken, zu a) Merkmalen zur Identifikation der Nutzerin oder des Nutzers, b) Angaben über Beginn und Ende sowie		schriften der Kundin oder des Kunden sowie zur Inanspruchnahme und den Umständen von Transportleistungen, insbesondere zum Zeitpunkt von Abfertigung und Abflug und zum Buchungsweg, 2. Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen zu Konten, Konteninhaberinnen oder Konteninhabern und sonstigen Berechtigten sowie weiteren am Zahlungsverkehr Beteiligten und zu Geldbewegungen und Geldanlagen, insbesondere über Kontostand und Zahlungsein- und -ausgänge, 3. denjenigen, die geschäftsmäßig Postdienstleistungen erbringen oder daran mitwirken, zu den Umständen des Postverkehrs, 4. denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, zu Verkehrsdaten nach § 96 Abs. 1 Nr. 1 bis 4 des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 2 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198), ~~und~~ **zu** sonstigen zum Aufbau und zur Aufrechterhaltung der Telekommunikation notwendigen Verkehrsdaten **und zu Internetprotokoll-Adressen (§ 113 Abs. 1 Satz 3 des Telekommunikationsgesetzes)** und 5. denjenigen, die geschäftsmäßig Telemedien erbringen oder daran mitwirken, zu a) Merkmalen zur Identifikation der Nut-

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
über den Umfang der jeweiligen Nutzung und c) Angaben über die von der Nutzerin oder von dem Nutzer in Anspruch genommenen Telemedien, soweit dies zur Aufklärung von Bestrebungen oder Tätigkeiten erforderlich ist und tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die in § 5 Abs. 1 genannten Schutzgüter vorliegen. Im Falle des § 5 Abs. 1 Nr. 1 gilt dies nur für Bestrebungen, die bezwecken oder aufgrund ihrer Wirkungsweise geeignet sind, 1. zu Hass oder Willkürmaßnahmen gegen Teile der Bevölkerung aufzustacheln oder deren Menschenwürde durch Beschimpfen, böswilliges Verächtlichmachen oder Verleumden anzugreifen und dadurch die Bereitschaft zur Anwendung von Gewalt zu fördern und den öffentlichen Frieden zu stören oder 2. Gewalt anzuwenden oder vorzubereiten, einschließlich dem Befürworten, Hervorrufen oder Unterstützen von Gewaltanwendung, auch durch Unterstützen von Vereinigungen, die Anschläge gegen Personen oder Sachen veranlassen, befürworten oder androhen.		zerin oder des Nutzers, b) Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und c) Angaben über die von der Nutzerin oder von dem Nutzer in Anspruch genommenen Telemedien, soweit dies zur Aufklärung von Bestrebungen oder Tätigkeiten erforderlich ist und tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die in § 5 Abs. 1 genannten Schutzgüter vorliegen. Im Falle des § 5 Abs. 1 Nr. 1 gilt dies nur für Bestrebungen, die bezwecken oder aufgrund ihrer Wirkungsweise geeignet sind, 1. zu Hass oder Willkürmaßnahmen gegen Teile der Bevölkerung aufzustacheln oder deren Menschenwürde durch Beschimpfen, böswilliges Verächtlichmachen oder Verleumden anzugreifen und dadurch die Bereitschaft zur Anwendung von Gewalt zu fördern und den öffentlichen Frieden zu stören oder 2. Gewalt anzuwenden oder vorzubereiten, einschließlich dem Befürworten, Hervorrufen oder Unterstützen von Gewaltanwendung, auch durch Unterstützen von Vereinigungen, die Anschläge gegen Personen oder Sachen veranlassen, befürworten oder androhen.
Begründung:		

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
	Die Änderung ist erforderlich, um der Entschließung des Landtags vom 12.12.2012 (Drs. 18/370) Rechnung zu tragen, derzufolge „für die Abfrage von IP-Adressen durch Behörden dieselben verfahrensrechtlichen und inhaltlichen Voraussetzungen eingeführt werden [sollen] wie für die Ausliefe-rung von Telekommunikations-Verkehrsdaten (z.B. Richtervorbehalt, Eingriffsschwellen)“. Die Identifizierung von Internetnutzern (§ 8a Abs. 1 S. 4 LVerfSchG-RegE) stellt einen besondern schwerwiegenden Grundrechtseingriff dar, weil sie die personenbezogene Nachverfolgung des Inhalts der abgerufenen oder geschriebenen Texte und Daten im Internet erlaubt. Anders als Auskünfte über Rufnummerninhaber geht die Identifizierung von Internetnutzern mit einem Eingriff in das grundrechtlich besonders geschützte Fernmeldege-heimnis einher. Die Begründung von behördlichen Auskunftsansprüchen ermöglicht es in Verbindung mit der Speicherung der Internetzugangsdaten nach § 100 TKG in weitem Umfang, die Identität von Internetnutzern zu ermitteln. Auch ist die mögliche Persönlichkeitsrelevanz einer Abfrage des Inhabers einer IP-Adresse eine andere als die des Inhabers einer Telefonnummer: Schon vom Umfang der Kontakte her, die jeweils durch das Aufrufen von Internetsei-ten neu hergestellt werden, ist sie aussagekräftiger als eine Telefonnummernabfrage. Auch hat die Kenntnis einer Kontaktaufnahme mit einer Inter-netseite eine andere inhaltliche Bedeutung: Da der Inhalt von Internetseiten anders als das beim Telefongespräch gesprochene Wort elektronisch fi-xiert und länger wieder aufrufbar ist, lässt sich mit ihr vielfach verlässlich rekonstruieren, mit welchem Gegenstand sich der Kommunizierende aus-einander gesetzt hat. Die Individualisierung der IP-Adresse als der „Telefonnummer des Internet“ gibt damit zugleich Auskunft über den Inhalt der Kommunikation. Die für das Telefongespräch geltende Unterscheidung von äußerlichen Verbindungsdaten und Gesprächsinhalten löst sich hier auf. Wird der Besucher einer bestimmten Internetseite mittels der Auskunft über eine IP-Adresse individualisiert, weiß man nicht nur, mit wem er Kontakt hatte, sondern kennt in der Regel auch den Inhalt des Kontakts (BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 259). Die Identifizierung von dynamischen IP-Adressen ermöglicht in weitem Umfang eine Deanonymisierung von Kommunikationsvorgängen im Inter-net. Zwar hat sie eine gewisse Ähnlichkeit mit der Identifizierung einer Telefonnummer. Schon vom Umfang, vor allem aber vom Inhalt der Kontakte her, über die sie Auskunft geben kann, hat sie jedoch eine erheblich größere Persönlichkeitsrelevanz und kann mit ihr - so das Bundesverfassungsge-richt ausdrücklich - nicht gleichgesetzt werden (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 174). Eben dies tut aber der Regierungsentwurf, wenn er Auskunftsersuchen allgemein zur „Aufgabenerfüllung“ erlaubt. Die Identifizierung von Internetnutzern im selben weit reichenden Umfang zuzulassen wie Auskünfte über Rufnummerninhaber ist nicht hinnehmbar. Das Bundesverfassungsgericht hat für IP-Auskünfte an Nachrichtendienste ein „Erfordernis einer auf Anhaltspunkte im Tatsächlichen gestützten kon-kreten Gefahr“ aus dem Verhältnismäßigkeitsgebot abgeleitet (BVerfGE 125, 260, Absatz-Nr. 261). Eine bloße Bezugnahme auf die Aufgaben des Verfassungsschutzes genügt den verfassungsrechtlichen Vorgaben nicht. Dementsprechend hat der Landtag gefordert, IP-Auskünfte Verkehrsdatenaus-künften gleichzusetzen. Die für Verkehrsdatenauskünfte geltenden Voraussetzungen genügen den verfassungsrechtlichen Anforderungen. Hier werden nämlich „tatsächliche Anhaltspunkte für schwerwiegende Gefahren“ zur Voraussetzung gemacht. Deswegen wird die Auskunft über IP-Adressen im Absatz 2 geregelt, wo bisher Verkehrsdatenauskünfte geregelt sind.	

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
(7) Auskunftspflichten zu Post- und Telekommunikationsverkehrsdaten sowie zu Nutzungsdaten von Telemedien (Absatz 2 Satz 1 Nr. 3 bis 5) werden gemäß § 8 b Abs. 1 von der Innenministerin oder dem Innenminister angeordnet. Über die Anordnung unterrichtet die Verfassungsschutzbehörde die G 10-Kommission (§ 8 b Abs. 2). Ferner teilt sie die Anordnung der betroffenen Person mit; § 12 Abs. 1 und 3 des Artikel 10-Gesetzes findet entsprechende Anwendung. Nach der Mitteilung steht der betroffenen Person der Rechtsweg offen. Für die Verarbeitung der erhobenen Daten ist § 4 des Artikel 10-Gesetzes entsprechend anzuwenden. Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird insoweit eingeschränkt.	(7) Auskunftspflichten zu Post- und Telekommunikationsverkehrsdaten**, zu Telekommunikationsbestandsdaten nach Absatz 1 Satz 3 und 4** sowie zu Nutzungsdaten von Telemedien (Absatz 2 Satz 1 Nr. 3 bis 5) werden gemäß § 8 b Abs. 1 von der Innenministerin oder dem Innenminister angeordnet. Über die Anordnung unterrichtet die Verfassungsschutzbehörde die G 10-Kommission (§ 8 b Abs. 2). Ferner teilt sie die Anordnung der betroffenen Person mit; § 12 Abs. 1 und 3 des Artikel 10-Gesetzes findet entsprechende Anwendung. Nach der Mitteilung steht der betroffenen Person der Rechtsweg offen. Für die Verarbeitung der erhobenen Daten ist § 4 des Artikel 10-Gesetzes entsprechend anzuwenden. Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird insoweit eingeschränkt.	*unverändert*
II.4. Berichtspflicht und parlamentarische Kontrolle über IP-Auskünfte und Passwortabfragen		
(8) Über sämtliche Anordnungen nach Absatz 2 ist das Parlamentarische Kontrollgremium gemäß § 8 b Abs. 4 zu unterrichten. Das Innenministerium berichtet ferner dem Parlamentarischen Kontrollgremium des Bundes über Anordnungen nach Absatz 2; § 8 b Abs. 4 findet entsprechende Anwendung.	*unverändert*	(8) Über sämtliche Anordnungen nach **[Absatz 1 Satz 3 und 4 sowie nach]** Absatz 2 ist das Parlamentarische Kontrollgremium gemäß § 8 b Abs. 4 zu unterrichten. **Das Gremium erstattet dem Landtag jährlich einen Bericht über die Durchführung sowie Art, Umfang und Anordnungsgründe der Maßnahmen.** Das Innenministerium berichtet ferner dem Parlamentarischen Kontrollgremium des Bundes über Anordnungen nach Absatz 2; § 8 b Abs. 4 findet entsprechende

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
		Anwendung.

Begründung:

Diese Änderung ist erforderlich, um dem Landtag zu ermöglichen, die Entwicklung der besonders tief in Grundrechte eingreifenden Auskünfte über Internetnutzer und Zugangssicherungscodes zu beobachten und erforderlichenfalls einzugreifen.

Nach § 8a Abs. 8 LVerfSchG wird das Parlamentarische Kontrollgremium bislang unter anderem über Zugriffe auf Verkehrsdaten unterrichtet. Die Identifizierung von Internetnutzern und auch die Erhebung von Zugangssicherungscodes greift so tief in die Grundrechte der Betroffenen ein, dass eine Unterrichtung gleichfalls erforderlich ist. Dies gilt erst Recht mit Blick auf die bundesgesetzlich neu eingeführte automatisierte Datenschnittstelle, die eine erhebliche Vereinfachung und dadurch Vervielfachung der Datenzugriffe befürchten lässt.

Entsprechend § 8b Abs. 3 S. 2 Bundesverfassungsschutzgesetz ist daneben eine statistische Unterrichtung des Landtags und der Öffentlichkeit erforderlich. Dies ist für eine wissenschaftliche Überprüfung und öffentliche Kontrolle der getätigten Grundrechtseingriffe unerlässlich. Die Anzahl der getätigten Zugriffe muss der Öffentlichkeit zugänglich gemacht werden, damit das Ausmaß der getätigten Eingriffe und die damit verbundenen Grundrechtseinschränkungen für Betroffene für die Bürgerinnen und Bürger transparent nachvollziehbar sind. Die Entwicklung der tatsächlichen Nutzung der durch den Gesetzesentwurf vorgesehenen neuen Zugriffsbefugnisse durch Behörden kann so nachverfolgt und eine übergriffige Nutzung des Rechtsrahmens frühzeitig erkannt werden. Darüber hinaus ist es für eine wissenschaftliche Auseinandersetzung mit der Entwicklung von Abfragezahlen unerlässlich, derartige Daten genau nach Abfragegrund, abfragende Behörde, Zahl der Betroffenen und weiteren für die statistische Erfassung notwendigen Daten aufzuschlüsseln. Nur so kann eine auf wissenschaftlicher Faktenlage basierende unabhängige Evaluierung der Eingriffsbefugnisse durchgeführt werden.

Der Text in eckigen Klammern ist nur erforderlich, falls § 8a Abs. 1 S. 3 oder 4 LVerfSchG-RegE nicht – wie hier vorgesehen – gestrichen werden sollte.

II.5. IP-Auskünfte und Passwortabfragen (Folgeänderungen)

-	**(9) Für die Erteilung von Auskünften nach Absatz 1 Satz 2 bis 4 hat der Verpflichtete Anspruch auf eine Entschädigung entsprechend § 23 des Justizvergütungs- und -entschädigungsgesetzes.**	(9) Für die Erteilung von Auskünften nach Absatz 1 Satz 2 ~~bis 4~~ **und über Internet-Protokolladressen nach Absatz 2 Nr. 4** hat der Verpflichtete Anspruch auf eine Entschädigung entsprechend § 23 des Justizvergütungs- und -entschädigungsgesetzes.

Geltendes Recht	Regierungsentwurf	Änderungsvorschlag
§ 26 a G 10-Kommission (1) Die G 10-Kommission nimmt die Aufgaben des gleichnamigen Kontrollorgans nach § 15 des Artikel 10-Gesetzes wahr. § 15 Abs. 5 bis 7 des Artikel 10-Gesetzes gelten entsprechend. Sie ist ferner 1. beim Einsatz technischer Mittel zum Ausfindigmachen eines Mobilfunkendgerätes (§ 8 Abs. 8) und 2. bei der Anordnung von Auskunftspflichten zu Post- und Telekommunikationsverkehrsdaten sowie zu Nutzungsdaten von Telemedien (§ 8 a Abs. 2 Nr. 3 bis 5) zu beteiligen.	§ 26 a G 10-Kommission (1) Die G 10-Kommission nimmt die Aufgaben des gleichnamigen Kontrollorgans nach § 15 des Artikel 10-Gesetzes wahr. § 15 Abs. 5 bis 7 des Artikel 10-Gesetzes gelten entsprechend. Sie ist ferner 1. beim Einsatz technischer Mittel zum Ausfindigmachen eines Mobilfunkendgerätes (§ 8 Abs. 8) und 2. bei der Anordnung von Auskunftspflichten zu **Telekommunikationsbestandsdaten (§ 8 a Abs. 1 Satz 3 und 4),** zu Post- und Telekommunikationsverkehrsdaten (§ 8 a Abs. 2 Nr. 3 und 4) sowie zu Nutzungsdaten von Telemedien (§ 8 a Abs. 2 Nr. 5) zu beteiligen.	§ 26 a G 10-Kommission (1) Die G 10-Kommission nimmt die Aufgaben des gleichnamigen Kontrollorgans nach § 15 des Artikel 10-Gesetzes wahr. § 15 Abs. 5 bis 7 des Artikel 10-Gesetzes gelten entsprechend. Sie ist ferner 1. beim Einsatz technischer Mittel zum Ausfindigmachen eines Mobilfunkendgerätes (§ 8 Abs. 8) und 2. bei der Anordnung von Auskunftspflichten ~~zu Telekommunikationsbestandsdaten (§ 8 a Abs. 1 Satz 3 und 4),~~ zu Post- und Telekommunikationsverkehrsdaten **oder Internet-Protokoll-adressen** (§ 8 a Abs. 2 Nr. 3 und 4) sowie zu Nutzungsdaten von Telemedien (§ 8 a Abs. 2 Nr. 5) zu beteiligen.