BÜNDNIS 90
DIE GRÜNEN
LANDTAGSFRAKTION HESSEN

BÜNDNIS 90/DIE GRÜNEN SCHLOSSPLATZ 1-3 65183 WIESBADEN

An:
Parteirat
LAG-Demokratie und Recht
LAG-Medien und Netzpolitik

**Mathias Wagner MdL**
Fraktionsvorsitzender
Bildungspolitischer Sprecher

**Jürgen Frömmrich, MdL**
Innenpolitischer Sprecher

BÜNDNIS 90/DIE GRÜNEN
im Hessischen Landtag
Schlossplatz 1-3
65183 Wiesbaden

Tel: +49 (611) 350 746
Fax: +49 (611) 350 604
Email: m.wagner@ltg.hessen.de

Wiesbaden, den 21.November 2017

**LMV-Beschluss zur Quellen-TKÜ und Online-Durchsuchung im Verfassungsschutzgesetz**

Liebe Freundinnen und Freunde,

wir möchten Euch über den Stand der Dinge in Bezug auf den o.g. LMV-Beschluss informieren.

Zunächst für alle, die nicht bei der Landesmitgliederversammlung (LMV) sein konnten, ein kurzes „was bisher geschah": Die Landtagsfraktion hat im Oktober gemeinsam mit unserem Koalitionspartner einen Gesetzentwurf zur Reform des Verfassungsschutzes vorgestellt und für die in dieser Woche stattfindende November-Sitzung des Landtags in die parlamentarischen Beratungen eingebracht. Die meisten Regelungen in diesem Gesetzentwurf sind unter uns GRÜNEN unstrittig und teilweise die Umsetzung unserer langjährigen Forderungen.

Zwei der Regelungen in diesem Gesetzentwurf sind auf innerparteiliche Kritik gestoßen: die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und die Online-Durchsuchung. Zur LMV gab es zwei Anträge, die sich gegen diese beiden Maßnahmen ausgesprochen haben und einen Antrag des Landesvorstands, der sich unter bestimmten Voraussetzungen für beide Maßnahmen ausgesprochen hat. Alle drei Anträge haben wir Euch in der Anlage beigefügt.

Nach einer intensiven und fairen Debatte wurde der Antrag 5.6 „Digitale Gefahrenabwehr statt digitaler Gefahrenquellen", der maßgeblich von der LAG Medien und Netzpolitik erarbeitet wurde, mit knapper Mehrheit beschlossen.

Somit haben wir die Situation, dass die Landtagsfraktion einen Gesetzentwurf vorgestellt und in den Landtag eingebracht hat und die LMV sich gegen zwei der Regelungen in diesem Gesetzentwurf ausgesprochen hat. Weil über die sozialen Medien von der Opposition anderes verbreitet wird, eine Erläuterung: Die Einbringung des Gesetzentwurfs in die in dieser Woche stattfindende Plenarsitzung hatte nichts mit der LMV zu tun. Vielmehr hatten wir das bereits bei der Vorstellung des Gesetzentwurfs im Oktober angekündigt. Das kann man natürlich auch richtig oder falsch finden

und die LAGen Medien und Netzpolitik sowie Demokratie und Recht haben das auch kritisiert. Uns ist aber wichtig festzustellen, dass wir das Gesetz nicht wegen der LMV jetzt in den Landtag eingebracht haben.

Soweit zu dem, was bisher geschah.

In der Fraktion beraten wir jetzt darüber, wie wir mit dem Unterschied zwischen dem Gesetzentwurf und dem Votum der LMV umgehen. Das ist auch deshalb nicht einfach, weil es sich um einen gemeinsamen Gesetzentwurf mit unserem Koalitionspartner handelt. Unser Koalitionspartner ist natürlich erstmal nicht bereit, eine getroffene Vereinbarung über den Gesetzentwurf wieder zu ändern. Das wäre bei uns ja auch nicht anders, wenn ein CDU-Parteitag sich gegen eine getroffene Vereinbarung in unserem Sinne aussprechen würde.

Unmittelbar nach unserem LMV-Beschluss haben wir noch am Samstag Kontakt zu unserem Koalitionspartner aufgenommen. Am Sonntag gab es ein erstes Gespräch und auch am Montag in der Koalitionsrunde haben wir über die Situation beraten. Die schlechte Nachricht: Eine Lösung haben wir noch nicht. Die gute Nachricht: Wir müssen sie auch noch nicht haben. Der Gesetzentwurf geht jetzt in die parlamentarische Beratung. Eine abschließende Entscheidung wird es erst im nächsten Jahr geben. Zuvor wird eine Anhörung zu dem Gesetzentwurf stattfinden, die Gelegenheit bietet, weiteren Sachverstand einzubeziehen. Erst am Ende des Gesetzgebungsprozesses müssen die Abgeordneten die Entscheidung treffen, was sie für vertretbar halten.

Landtagsfraktion, Landesvorstand sowie LAG Medien und Netzpolitik haben vereinbart, dass wir eine Arbeitsgruppe bilden, die bei den beiden genannten Themen fachlich in die Tiefe geht.

Selbstverständlich halten wir Euch über die weitere Entwicklung auf dem Laufenden und stehen Euch auch gerne jederzeit für Rückfragen zur Verfügung.

Viele Grüße

Mathias Wagner
Fraktionsvorsitzender

Jürgen Frömmrich
Innenpolitischer Sprecher

Anlage:
3 Anträge zur LMV

BÜNDNIS 90
DIE GRÜNEN
HESSEN

**Landesmitgliederversammlung, 18.November 2017**
**Congress Park, Hanau**

Antragssteller: Peter Löwenstein (Darmstadt-Dieburg), u.w.

# „Bürgerrechte achten statt Gesetzen, die unsere Sicherheit gefährden“

Die Landesmitgliederversammlung Hessen möge beschließen, den „Gesetzentwurf der Fraktionen CDU und BÜNDNIS 90/ DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen“ (1 ) abzulehnen.
[Optionales Modul: Dieses soll auf der LMV getrennt abgestimmt werden, wenn so von der LMV gewünscht:] Die Landesmitgliederversammlung Hessen empfiehlt ihrer Fraktion BÜNDNIS 90/ DIE GRÜNEN diesem Beschluss im Hessischen Landtag zu folgen.

Begründung

Der obige Gesetzentwurf wurde Anfang Oktober zuerst der Öffentlichkeit vorgestellt ( 2 ). Die Landesarbeitsgemeinschaften Medien und Netzpolitik MuN und der Parteirat wurden vorher nicht über den finalen Entwurf fachlich informiert.

In der Sitzung der Landesgemeinschaft Medien und Netzpolitik am 25.10.2017 wurde der Gesetzentwurf von Abgeordneten der Grünenfraktion erstmals der LAG detailliert vorgestellt und von Vertretern des Chaos Computer Club Darmstadt und weiteren Mitgliedern sowie Gästen knapp 3 Stunden fachlich bewertet.

Die Landesarbeitsgemeinschaft lehnte schließlich den Gesetzentwurf in diesem Wortlaut mit einem Beschluss ab: „Die LAG MUN lehnt den Gesetzesentwurf für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen in der aktuellen Form ab. Die Quellen-TKÜ und die Onlinedurchsuchung halten wir für zu weitgehend.“ (3)

Die konkrete Kritik an dem Entwurf wurde Wochen zuvor mit einem Fragenkatalog den Abgeordneten auf der MuN Mailingliste bekannt gemacht. Die Bitte um eine Beantwortung vor der obigen Sitzung der MuN wurde von den Angeordneten abgelehnt mit Hinweis auf eine mündliche Beantwortung in der kommenden Sitzung am 25.10.2017. (4)

Da die in dem Fragenkatalog konkret dargestellte Kritik am Entwurf im Sitzungsverlauf am 25.10.2017 fachlich nicht zufriedenstellend aufgelöst werden konnte (5) und im weiteren Dialog mit den Abgeordneten als kritisch bewertete Sachverhalte sehr deutlich wurden,

wurde dem Antrag auf Ablehnung des Gesetzentwurfs in der Sitzung mit einer Enthaltung entsprochen.

Verschiedene NGOs aus Südhessen, die sich seitdem mit dem Entwurf befassten, lehnen den Gesetzentwurf ebenfalls nach fachlichen Beratungen ab (z.B. Chaos Computer Club (6), Bündnis „Demokratie statt Überwachung", „Datenschützer Rhein-Main"). Es haben sich Bündnisse aus netzpolitischen und bürgerrechtlichen NGOs gebildet, deren fachliche Kritik angehört werden muss.
Die Grüne Jugend hat sich in ihrer LMV Anfang November mit einem Antrag ebenfalls kritisch und fachlich ausgezeichnet begründet zu dem Gesetzentwurf positioniert. (7)

Deswegen: Wir Grünen lehnen Online-Durchsuchungen und Quellen-TKÜ aufgrund der hiermit einhergehenden Sicherheitsproblematik und dem Missbrauchspotenzial von Staatstrojanern entschieden ab.

Der Gesetzentwurf benötigt in der vorgestellten Form eine fachliche Überarbeitung, um die von der grünen LAG MuN, der Grünen Jugend Hessen und NGOs dargestellten erheblichen Mängel abzustellen.

Die notwendige Heilung des Gesetzentwurfs erscheint in der verbleibenden Zeit bis zur geplanten Befassung im Hessischen Parlament im November 2017 kaum möglich, wie von Abgeordneten auf der LAG Sitzung MuN im Oktober geäußert wurde.

Daher ist der Gesetzentwurf abzulehnen. [Die weitere Begründung erfolgt mündlich]
Antragsteller: Peter Löwenstein, KV Darmstadt-Dieburg

Anlagen:
1- Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen
http://www.gruenehessen.de/landtag/files/2017/10/HSVG.pdf
2- Frankfurter Rundschau: http://www.fr.de/rhein-main/verfassungsschuetzer-in-hessenverfassungsschutz-soll-computer-anzapfen-duerfen-a-1362365
3- Zitat aus Anlage „LAG MuN Beschlussprotokoll 25.10.2017"
4- Fragenkatalog und Dialoge dazu in Anlage Mailingliste LAG MuN Hessen „Beantwortung des Fragenkatalogs"
5- Ausführliches Protokoll der LAG MuN Sitzung 25.10.2017, wird nachgereicht von den Sprechern der MuN sobald von diesen fertiggestellt.
6- „Geplanter Staatstrojaner in Hessen gefährdet IT-Sicherheit weltweit"
https://ccc.de/de/updates/2017/hessentrojaner
7- Grüne Jugend LMV November 2017 - Antrag „A17: Sicherheit nicht gegen Datenschutz ausspielen"
https://gjhlmv.antragsgruen.de/gjhlmv/Sicherheit_nicht_gegen_Datenschutz_ausspielen_-60072

BÜNDNIS 90
DIE GRÜNEN
HESSEN

**Landesmitgliederversammlung, 18.November 2017**

**Congress Park, Hanau**

Antragssteller: Markus Drenger (KV Darmstadt), u.w.

# Digitale Gefahrenabwehr statt digitaler Gefahrenquellen

Die vielen IT-Forschungseinrichtungen in Hessen sind weltweit für ihre Kompetenzen im Bereich Cybersicherheit bekannt.

Zur Stärkung des Standortes und der IT-Sicherheit insgesamt soll auch das Land Hessen Vorreiter im Bereich Cybersicherheit werden und als vertrauenswürdiger Partner an der Seite von Wissenschaft, Wirtschaft und der Bevölkerung auftreten, um eine gut vernetzte hessische IT-Sicherheitslandschaft zu etablieren. IT-Angriffe auf Krankenhäuser, Verkehrsunternehmen und Stromnetze haben gezeigt, dass fehlende IT-Sicherheit auch ganz konkrete Gefahren für Bürgerinnen und Bürger bedeuten können.

Dazu soll das Land ausnahmslos sämtliche Erkenntnisse über Gefährdungen mit Herstellern von informationstechnischen Systemen teilen und so zeitnahe Updates zur digitalen Gefahrenabwehr ermöglichen. Die Sicherheitsbehörden des Landes sollen mit Unternehmen und anderen Organisationen der Zivilgesellschaft kooperieren, um durch den Aufbau von Digitalkompetenzen mehr Sicherheit für Hessen zu schaffen. Das eingerichtete CERT-Hessen ist im Land als „Computer Emergency Response Team“ zu stärken und entsprechend auszustatten.

Entwicklung, Einsatz und Proliferation digitaler Waffen wie eine Software zur "Onlinedurchsuchung" können keine Bestandteile einer verantwortungsvollen Sicherheitspolitiksein!

Die Landesmitgliederversammlung der hessischen Grünen fordert die grüne Landtagsfraktion auf, sich für eine offene und friedliche Cybersicherheitsstrategie des Landes einzusetzen und aufdie angedachte Einführung von digitalen Waffen für den hessischen Verfassungsschutz zur sog. "Onlinedurchsuchung" und zur Quellen-TKÜ zu verzichten.

Begründung

Die CDU-Fraktion hat gemeinsam mit der Grünen Landtagsfraktion einen Entwurf zur Neuausrichtung des hessischen Verfassungsschutzes entwickelt.

Unter anderem soll dem Verfassungsschutz die Möglichkeit gegeben werden, informationstechnische Systeme Dritter anzugreifen und zu auszuwerten. Dieser Art von staatlichem Hacking ist sehr umstritten und dessen Ablehnung ist seit Jahren Kernbestandteil grüner Digital- und Bürgerrechtspolitik im Bundestag wie auch in Europa, ähnlich wie eine anlasslose Vorratsdatenspeicherung.

Stattdessen braucht es eine kooperative, friedliche und zielgerichtete Cybersicherheitsstrategie des Landes zum Schutz von IT-Nutzerinnen und -Nutzern in Hessen, seien es Unternehmen, Kommunen, kritische Infrastrukturen oder private Systeme von Bürgerinnen und Bürgern. Eine Stärkung des CERT ( https://innen.hessen.de/sicherheit/cybersicherheit/cert ) und die Einführung

**Trennung von Polizei und Nachrichtendiensten**

Ein Eingriff in informationstechnische Systeme stellt einen erheblichen Grundrechtseingriff dar. Die EU-Kommission hält diese Maßnahme für vergleichbar mit einer Beschlagnahme (vgl. Report on the Democratic Oversight of the Security Service). Solch starke polizeiliche Befugnisse sollten dem Verfassungsschutz als Nachrichtendienst nicht gegeben werden. Mit einer herkömlichen Telekommunikationsüberwachung, etwa von SMS, ist ein Angriff und die Übernahme der Kontrolle eines Systems im Rahmen einer sogenannten "Quellen-TKÜ" nicht vergleichbar.

**Friedenspolitisches:**

Die Entwicklung von Trojanern und Cyberwaffen wird in der Regel durch private Unternehmen durchgeführt, staatlichen Stellen fehlt dafür das KnowHow und die Kapazitäten. Dies birgt das nachweisbare Risiko, dass die hier finanzierten Überwachungsinstrumente "zweitverwertet" und damit mißbraucht werden und auch anderen Staaten und fragwürdigen, zwielichtigen, aber lukrativ bezahlenden Unternehmen und Organisationen zum Kauf angeboten werden.

- bayrisches Produkt in Bahrain: http://www.sueddeutsche.de/digital/finfisher-entwickler-gamma-spam-vom-staat-1.1595253-3

- hessisches Unternehmen auf Verkaufstour: https://netzpolitik.org/2014/mitarbeit-des-us-geheimdienstpartners-csc-solutions-am-german-staatstrojaner-war-schon-letztes-jahr-bekannt/

- italienische Hacking-Firma verkaufte an Regime https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim

**Sicherheitspolitik:**

Der Begriff eines informationstechnischen Systems (IS) fasst so ziemlich alles, was als zusammenhängendes System betrachtet werden kann. Von Groß- und

Hochleistungsrechnern, über verteilte Systeme, Personalcomputer, Laptops, Smartphones, Navigationssysteme, SmartHome-Systemen und auch 'Embedded Systemen', in Autos oder Industriesteuerungsanlagen, wie auch Hörgeräte, Herzschrittmacher und neue digitale Insulinpumpen fallen unter diese Kategorie. Diese Systeme müssen bestmöglich geschützt sein und nicht durch den Staat in Gefahr gebracht werden.

Entdecken Sicherheitsforscher oder Bürgerinnen und Bürger Sicherheitslücken in IT-Systemen und Produkten, melden Sie diese in der Regel an die Hersteller, damit diese schnellmöglich Sicherheitsupdates bereitstellen können. Kriminelle und Staaten, die digitale Waffen entwickeln, bieten jedoch online viel Geld, damit ihnen das Wissen über Sicherheitslücken verkauft wird und keine Sicherheitsupdates entwickelt werden. Diese Art von Anreizsystem schadet der IT-Sicherheit weltweit und die Beispiele dafür sind zahlreich:

- Polizist nutzt Staatstrojaner, um Tochter auszuspionieren und liefert damit Daten für einen Angriff auf die Bundespolizei https://www.golem.de/1201/88870.html

- Leaks aus der NSA ermöglichen es Kriminellen, Millionen von Geräten weltweit mit Schadsoftware zu infizieren https://motherboard.vice.com/de/article/xye5pn/was-die-nsa-mit-der-wannacry-hacking-attacke-zu-tun-hat

- Skandal um verfassungswidrigen Bundestrojaner
https://www.heise.de/newsticker/meldung/Parteien-fordern-Aufklaerung-des-Skandals-um-Bundestrojaner-1357769.html

- Analyse des verfassungswidrigen Bundestrojaners:
https://www.ccc.de/de/updates/2011/staatstrojaner

Grüne Positionen:

Landtagsfraktion Bündnis90/Die Grünen Hessen

Konzeptpapier "Digitalpolitik", 2013, Kapitel 3 Gefahrenabwehr:

http://www.gruene-hessen.de/landtag/files/2013/01/KP24-NETZPOLITIK-web4.pdf#14

"Das Bundesverfassungsgericht hat die Online-Durchsuchung und die elektronische Telekommunikationsüberwachung unter Richtervorbehalt gestellt und unter engsten Voraussetzungen erlaubt:

„Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkteeiner konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen.

Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. (...)“

Die hessische Landesregierung muss sich auf Bundes- und Europa-Ebene engagiert gegen eine anlasslose Vorratsdatenspeicherung stellen. In der hessischen Gefahrenabwehr darf Online-Durchsuchung nicht eingesetzt werden. Hessen muss sich dafür einsetzen, dass auf Bundesebene die Durchsuchung privater Rechner ausgeschlossen wird."

**Grüne Bundestagsfraktion**, 22.06.2017

Konstantin von Notz und Hans-Christian Ströbele zur Online-Durchsuchung, der Quellen-TKÜ und dem Zugriff auf Messengerdienste

https://www.gruene-bundestag.de/presse/pressestatements/2017/juni/konstantin-von-notz-und-hans-christian-stroebele-zur-online-durchsuchung-der-quellen-tkue-und-dem-zugriff-auf-messengerdienste-22-06-2017.html

**Reinhard Bütikofer** zur Exportkontrolle von digitalen Überwachungsinstrumenten:

http://reinhardbuetikofer.eu/2011/12/05/dual-use-exportkontrolle-ohne-zahne/

**Internationale Stimmen:**

**Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174 (22 July 2015)**

"13. Taking into account existing and emerging threats, risks and vulnerabilities and building upon the assessments and recommendations contained in the 2010 and 2013 reports of the previous Groups, the present Group offers the following recommendations for consideration by States for voluntary, non-binding norms, rules or principles of responsible behaviour of States aimed at promoting and open, secure, stable, accessible and peaceful ICT environment: (a) Consistent with the purposes of the United nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security... (f) States should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public... (i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions; (j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure; (k) States should not conduct or knowingly support activity to harm the information systems of authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another

State. A State should not use authorized emergency response teams to engage in malicious international activity."

**Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, U.N. Doc. CCPR/C/ITA/CO/6 (28 March 2017)**

"36. The Committee is concerned about reports alleging a practice of intercepting personal communications by intelligence agencies and the employment of hacking techniques by them without explicit statutory authorization or clearly defined safeguards from abuse... 37. The State party should review the regime regulating the interception of personal communications, hacking of digital devices and the retention of communications data with a view to ensuring (a) that such activities conform with its obligations under article 17 including with the principles of legality, proportionality and necessity, (b) that robust independent oversight systems over surveillance, interception and hacking, including by providing for judicial involvement in the authorization of such measures in all cases and affording persons affected with effective remedies in cases of abuse, including, where possible, an ex post notification that they were subject to measures of surveillance or hacking"

**Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40 (17 April 2013)**

"62. ...Offensive intrusion software such as Trojans, or mass interception capabilities, constitute such serious challenges to traditional notions of surveillance that they cannot be reconciled with existing laws on surveillance and access to private information. There are not just new methods for conducting surveillance; they are new forms of surveillance. From a human rights perspective, the use of such technologies is extremely disturbing. Trojans, for example, not only enable a State to access devices, but also enable them to alter – inadvertently or purposefully – the information contained therein. This threatens not only the right to privacy but also procedural fairness rights with respect to the use of such evidence in legal proceedings."

**European Commission For Democracy Through Law (Venice Commission), Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies, Study No. 719/2013 CDL-AD(2015)006 (7 April 2015)**

"101. ...a signals intelligence agency, through agreement with ISPs, or even without this agreement, might be able to access stored data, e.g. in the "cloud". Here it should be stressed that even if the ISP gives its consent, for states bound by European principles of data protection, it is not possible to argue that such access does not involve an interference with privacy and/or freedom of correspondence. For such personal data, the interference thus occurs even if the legal "owner" or controller of the data gives its consent. Thus, it follows that statutory authority must also exist for such a power of access without consent. The same can be said for the even more controversial power of remotely hacking into computers, and planting malware. This is equivalent to a search and seizure, with the

difference that it is covert and continuouzus throughout the period of operation of the malware, rather than open and on one occasion only. Following the ECtHR's case law on search and seizure, if this is to be allowed at all, it can only be with a very limited list of offences, with clear statutory authority, judicial authorization, minimization and destruction requirements and, bearing in mind its covert nature, strong oversight."

BÜNDNIS 90
DIE GRÜNEN
HESSEN

**Landesmitgliederversammlung, 18.November 2017**

**Congress Park, Hanau**

Antragssteller: Landesvorstand

# Gesetzentwurf zur Neuordnung des Verfassungsschutzes in Hessen

1. Die LMV begrüßt, dass mit dem Gesetzentwurf zur Neuordnung des Verfassungsschutzes (https://www.gruene-hessen.de/landtag/files/2017/10/HSVG.pdf) umfassende Konsequenzen aus dem Versagen der Sicherheitsbehörden im Zusammenhang mit der Mordserie des sogenannten Nationalsozialistischen Untergrunds (NSU) gezogen werden. Der Gesetzentwurf greift damit die Empfehlungen des ersten NSU-Untersuchungsausschusses des Bundestags auf. Dazu gehören beispielsweise:

- Verbindlicher Meinungsaustausch zwischen Polizei und Justiz;
- Arbeitskultur „selbstkritisches Denken", Fehlerkultur;
- Gesetzliche Verankerung von Informationspflichten;
- Effiziente Abstimmung im Verfassungsschutzverbund;
- Übermittlung von Informationen an die Strafverfolgungsbehörden;
- Einsatz und Umgang mit „menschlichen Quellen";
- Stärkung der Parlamentarischen Kontrolle.

2. Mit dem Gesetzentwurf wird ebenso die langjährige grüne Forderung nach einer stärkeren parlamentarischen Kontrolle des Verfassungsschutzes umgesetzt. Erstmals gibt es ein eigenes Verfassungsschutzkontrollgesetz. Darin wird bspw. geregelt: die Pflicht der Landesregierung zur umfassenden Unterrichtung der Parlamentarischen Kontrollkommission für den Verfassungsschutz (PKV); Bericht über den Einsatz technischer Mittel zur Wohnraumüberwachung, den verdeckter Zugriff auf informationstechnische Systeme und die Ortung von Mobilfunkgeräten, den Einsatz von Verdeckten Mitarbeiterinnen und Mitarbeiter und Vertrauensleuten (V-Leuten); Berichtspflicht gegenüber dem Parlamentarischen Kontrollgremium des Bundes und dem Bundesamt für den Verfassungsschutz. Die Befugnisse der PKV wurden dahingehend erweitert, dass die

Einberufung sowie die Akteneinsicht verbessert wurden und es wurde geregelt, dass zur Wahrnehmung der Kontrollaufgaben sachverständige Personen herangezogen werden können. Eine Pflicht zur Berichterstattung gegenüber dem Parlament wurde eingeführt und die Mitglieder der Kommission können Mitarbeiterinnen und Mitarbeiter zur Unterstützung ihrer Arbeit heranziehen.

3. In den Gesetzentwurf sind auch die Erkenntnisse der von der Landesregierung eingerichteten überparteilichen Expertenkommission zur Umsetzung der einvernehmlichen Empfehlungen des NSU-Untersuchungsausschusses des Deutschen Bundestages eingeflossen. Die Expertenkommission hat auf 248 Seiten die Umsetzung der Handlungsempfehlungen begutachtet und auf 35 Seiten zum ursprünglichen Gesetzentwurf der Regierungsfraktionen von CDU und GRÜNEN Stellung genommen. Die Empfehlungen dieser Expertenkommission sind in den jetzt vorliegenden Gesetzentwurf eingearbeitet worden. Bei der Erarbeitung des Gesetzentwurfs wurden auch die Gesetzgebungsprozesse auf Bundes- und Länderebene berücksichtigt, um so eine weitestmögliche Harmonisierung auf der Ebene der Verfassungsschutzbehörden herzustellen. Einbezogen wurden außerdem die Rechtsprechung des Bundesverfassungsgerichts und insbesondere dessen Urteile zum Umgang mit der Antiterrordatei und zum BKA-Gesetz.

4. Neben den bereits genannten Punkten enthält der Gesetzentwurf auch Regelungen zu den Themen Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und Online-Durchsuchung. Beide Themen stellen Gesellschaft, Staat und Politik vor schwierige Abwägungsfragen. Auf der einen Seite steht der Schutz der Bevölkerung vor Terroranschlägen und schwersten Straftaten. Auf der anderen Seite steht der Schutz der Bevölkerung vor einem Ausspähen ihrer Daten, Handys und Computer. Im Gegensatz zur Vorratsdatenspeicherung richten sich beide Maßnahmen aber nur anhand konkreter Verdachtsmomente und mit hohen Hürden gegen einzelne Personen und nicht anlasslos gegen alle Bürgerinnen und Bürger.

5. Die Quellen-TKÜ ist prinzipiell kein neues Instrument. In Hessen besteht die Möglichkeit der Quellen-TKÜ im Polizeirecht bereits seit 2009. Schon heute dürfen die Sicherheitsbehörden im Bund und in allen Ländern zur Verhinderung schwerster Straftaten in begründeten Einzelfällen unter Beachtung hoher Hürden Telefone abhören sowie Briefe, E-Mails und SMS-Nachrichten mitlesen. Neu ist, dass diese Möglichkeit auch für Messenger-Dienste wie „WhatsApp“ u.a. bestehen soll. Die Bundesländer Thüringen, Rheinland-Pfalz,

Hamburg, Bayern und Baden-Württemberg haben diese Möglichkeit bereits in ihren Polizei- oder Verfassungsschutzgesetzen verankert bzw. entsprechende Gesetzentwürfe in der Beratung.

6. Die LMV sieht aufgrund der unterschiedlichen technischen Voraussetzungen dennoch einen erheblichen Unterschied zwischen dem Mitlesen von SMS und von Messenger-Diensten. Denn bei SMS kann das Mitlesen bei der Übertragung der Nachricht und somit ohne Zugriff auf das Handy erfolgen. Bei Messenger-Diensten ist durch eine Software ein Zugriff auf das versendende Gerät notwendig, da die Nachrichten verschlüsselt versendet werden. Sowohl der Zugriff auf das Gerät selbst als auch die dafür notwendige Software werfen Fragen in Bezug auf die Verhältnismäßigkeit der Maßnahme auf. In besonderem Maße stellen sich diese Fragen auch in Bezug auf die noch weitreichendere Online-Durchsuchung.

7. Im Kern geht es um eine äußerst schwierige Abwägung: Auf der einen Seite kann es nicht sein, dass die Wahl des Kommunikationsmediums (SMS oder Messenger-Dienst) darüber entscheidet, ob die Sicherheitsbehörden Informationen zum Schutz der Bürgerinnen und Bürger vor Terroranschlägen und schwersten Straftaten erlangen können oder nicht. Auf der anderen Seite stellt das Instrument zur Erlangung dieser Information (Trojaner-Software) einen sehr weitreichenden Eingriff in die Grundrechte von Bürgerinnen und Bürger dar. Auch nutzt die Software Schwachstellen in IT-Systemen, die für andere Zwecke missbraucht werden können.

8. Das Bundesverfassungsgericht hat sich mit dieser Abwägung beschäftigt und ist zu dem Ergebnis gelangt, dass Quellen-TKÜ und Online-Durchsuchung nur im begründeten Einzelfall unter Berücksichtigung hoher Hürden erfolgen dürfen.

9. Vor diesem Hintergrund hält die LMV es für erforderlich, dass bei der parlamentarischen Beratung und der Anhörung zum Gesetzentwurf zur Neuordnung des Verfassungsschutzes die Einhaltung der Kriterien des Bundesverfassungsgerichts geprüft werden:

- Für die Online-Durchsuchung muss angesichts der Schwere des Eingriffs eine konkrete Gefahr für ein überragend wichtiges Rechtsgut, wie etwa das Leben einer Person, bestehen.

- Der Eingriff ist grundsätzlich unter Vorbehalt einer richterlichen Anordnung zu stellen und es müssen hinreichende Vorkehrungen getroffen werden um Eingriffe in den Kernbereich der privaten Lebensgestaltung zu vermeiden.

- Für die Quellen-TKÜ muss sichergestellt werden, dass nur die laufende Kommunikation überwacht wird. Sollten zum gegenwärtigen Zeitpunkt diese Anforderungen nicht erfüllbar sein heißt das, dass die Vorschrift bis auf weiteres nicht angewendet werden darf.

- Bei der Quellen-TKÜ müssen die Maßgaben des G-10-Gesetzes gelten, d.h. der Eingriff bedarf der Genehmigung der G-10-Kommission. Die G-10-Kommission entscheidet als unabhängiges Organ über die Zulässigkeit von Eingriffsmaßnahmen des Verfassungsschutzes in das Brief-, Post- und Fernmeldegeheimnis.

Außerdem muss geprüft werden,

- welche Missbrauchsrisiken mit dem Einsatz der notwendigen Software verbunden sind;

- ob und gegebenenfalls wie der Missbrauch der Software ausgeschlossen werden kann; ob die Einschätzung der Sicherheitsbehörden, dass durch die Nutzung von Quellen-TKÜ und Online-Durchsuchung relevante Erkenntnisse zum Schutz der Bevölkerung vor Terroranschlägen und schwersten Straftaten gewonnen werden können, tatsächlich gerechtfertigt ist;

10. In diesen Prozess sollen auch die Landesarbeitsgemeinschaften Medien und Netzpolitik sowie Demokratie und Recht und weitere interessierte Mitglieder eingebunden werden. Ein vertiefender Austausch zu diesen Themen wurde im Rahmen der Sitzungen der beiden genannten LAGen am 26. bzw. 28. Oktober 2017 begonnen. Hierzu hatte der Landesvorstand in Absprache mit den LAG-Sprecherinnen und -Sprechern auch über den Verteiler des Parteirats eingeladen.