*die*Datenschützer Rhein Main

- keine Untaten mit Bürgerdaten -

eMail: kontakt@ddrm.de Internet: https://www.ddrm.de

Stellungnahme zum Gesetzesentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz der Neuausrichtung des Verfassungsschutzes in Hessen
LT-Drucksache 19/5412 vom 14.11.2017

EINLEITUNG

Nach Maßgabe des vorliegenden Gesetzentwurfs ist eine der wesentlichen Aufgaben des Landesamts für Verfassungsschutz (LfV) der Schutz des Landes Hessen und der Bundesrepublik Deutschland vor Bestrebungen gegen die freiheitlich demokratische Grundordnung. Zu dieser Grundordnung zählen insbesondere auch die im Grundgesetz konkretisierten Menschenrechte. Um ihrer Aufgabe gerecht zu werden, sollen die Verfassungsschutzbehörden in der Lage sein, umfangreiche Informationen zu erheben. Hierzu ist es teilweise erforderlich, dass den Behörden Mittel zur Verfügung stehen, die weit in die zu schützenden, verfassungsgemäßen Rechte Einzelner eingreifen. Der Gesetzgeber muss daher bei der Ermächtigung des LfV gründlich abwägen zwischen der Gefahr für die Grundordnung und der zu ihrer Verteidigung nötigen Mittel einerseits und der Wahrung der Rechte des Einzelnen und der Allgemeinheit andererseits. Die dem LfV zugestandenen Mittel müssen in ihrem Umfang stets verhältnismäßig sein und dürfen nicht ihrerseits zu einer Gefahr für die Menschen werden.

ZU ARTIKEL 1

Hessisches Verfassungsschutzgesetz (HVSG)

Dem LfV werden mit dem vorliegenden Gesetzentwurf zum einen weitere Aufgaben erteilt. Für *die*Datenschützer Rhein Main bleibt in diesem Zusammenhang unverständlich, weshalb die originär dem Landeskriminalamt zuzuordnende Bekämpfung der Organisierten Kriminalität ebenfalls nach § 2 Abs. 2 Nr. 5 eine Aufgabe des LfV sei. Zum anderen werden dem LfV weitreichende Möglichkeiten zum Eingriff in Grundrechte zugestanden. Die Spanne reicht hier von der Aufhebung des Brief- und Telekommunikationsgeheimnisses, über die optische und akustische Wohnraumüberwachung, die Ortung von Mobilfunkgeräten bis zu Eingriffen in Computer- und Kommunikationssysteme.

Auffällig ist hierbei, dass der Gesetzestext unbestimmt von „technischen Mitteln“ spricht, ohne diese einschränkend zu konkretisieren. Allgemein, besonders jedoch im Bereich der Wohnraumüberwachung, ist diese Eingriffsbefugnis einer staatlichen Behörde, beliebige Technik einzusetzen, zu weitreichend. Aber auch im Fall der Eingriffe in technische Systeme ist die fehlende Konkretisierung problematisch.

Bei den Eingriffen in Computersysteme (einschließlich Smartphones, Telekommunikationsanlagen, IoT-Geräte, Smart-Devices jeglicher Art,...) ist zu unterscheiden zwischen den Eingriffen zur heimlichen Durchsuchung dieser Geräte (der sogenannte "Hessentrojaner") und Eingriffen zum Abgriff einer laufenden Kommunikation (Quellen-Telekommunikationsüberwachung).

Unterschiede TKÜ & Quellen-TKÜ

Der Ermächtigung zur Quellen-TKÜ liegt der Wunsch zu Grunde, auf verschlüsselte und ggfs. dezentral organisierte Kommunikation über moderne Kommunikationsmittel genauso zugreifen zu können, wie dies bei klassischer Telefonie im Fest- oder Mobilfunknetz oder bei der SMS möglich ist. Hierbei ist zu beachten, dass es zwischen der klassischen TKÜ und der Quellen-TKÜ gravierende technische Unterschiede gibt. Bei der klassischen TKÜ erfolgt der Zugriff auf die Gesprächs- oder Textdaten der abzuhörenden Kommunikation an zentraler Stelle im Netzwerk des Kommunikationsanbieters. Ein Abgriff an dieser Stelle ermöglicht einen gezielten Zugriff auf die Kommunikation der überwachten Person und birgt zunächst keine Gefahr eines Zugriffs unberechtigter Dritter über die Abhöreinrichtung, da der Eingriff im geschützten Netzwerk des Anbieters stattfindet. Bei der Quellen-TKÜ ist dieser zentrale Zugriff auf die Kommunikation nicht möglich. Die Daten könnten ggfs. im Netz des Anbieters ausgeleitet werden, aufgrund der verschlüsselten Übermittlung sind sie aber in der Regel für die Behörden unbrauchbar. Die Schlüssel zur Ver- und Entschlüsselung der Nachrichten sind bei modernen Verfahren nur dem Sender und Empfänger bekannt (Ende zu Ende Verschlüsselung) und auch die Dienstanbieter und Hersteller der Kommunikationsverfahren haben meist keine Möglichkeit zur Entschlüsselung. Dies führt dazu, dass ein Zugriff auf den Klartext der Kommunikation lediglich auf dem Sendegerät, vor der Verschlüsselung, und dem Empfangsgerät, nach der Entschlüsselung, möglich ist. Diese Geräte befinden sich jedoch vollständig unter Kontrolle des Nutzers, so dass sie für einen Zugriff in der Regel kompromittiert/gehackt werden müssen.

Probleme der Quellen-TKÜ

Die wesentlichen Regelungen für die Quellen-TKÜ enthält § 6 des Gesetzentwurfs. In ihm ist festgeschrieben, das ein Eingriff in Geräte nur zulässig ist, wenn (1) durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird und (2) der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen. Punkt 2 regelt somit, dass die weniger invasive klassische TKÜ angewandt werden muss, sofern mit ihr ebenfalls ein Abhören der Kommunikation möglich ist.

Punkt 1 dürfte in der Praxis nicht realisierbar sein. Aktuell existiert eine Vielzahl verschlüsselter Kommunikationsverfahren, die in unterschiedlichen Versionsständen für unterschiedliche Plattformen/Betriebssystem mit ihrerseits vielzähligen unterschiedlichen Versionen angeboten werden. Zum abhören der Kommunikation muss eine Software auf den Geräten installiert werden, die die Daten abgreift und an die Behörden übermittelt. Da eine Anpassung der Abhörsoftware an all diese Versionskombinationen nicht realisierbar ist, wird ein Zugriff an zentraler Stelle im Betriebssystem erfolgen. Hier kann jedoch technisch nicht sichergestellt werden, dass ausschließlich laufende Kommunikation überwacht und aufgezeichnet wird. Ist es ggfs. noch möglich, z.B. die Audiodaten unterschiedlicher Programme/Apps zu unterscheiden, um lediglich die Daten des Kommunikationsprogramms zu erfassen, wird das Verfahren spätestens an der Feststellung der laufenden Kommunikation scheitern. Da die Daten vor der Verschlüsselung und vor dem Versand abgegriffen werden müssen, ist keine Zuordnung der aufgezeichneten Daten zu den gesendeten Daten möglich. Es ist daher nicht festzustellen, ob eine Kommunikation noch vor Versand der (Sprach-)Nachricht abgebrochen wurde. Viele aktuelle Kommunikation-Apps bieten zudem die Möglichkeit, alte Nachrichten nochmals anzuhören, so dass angehörte/gelesene Nachrichten ggfs. nicht zu laufender Kommunikation gehören. Auch hier ist eine Unterscheidung nicht zuverlässig realisierbar. Die Überwachung und Aufzeichnung von Daten, die nicht zur laufenden Kommunikation gehören, scheint daher unvermeidlich, womit ein gesetzestreuer Eingriff nicht möglich ist.

Hessentrojaner & Schutz des Kernbereichs privater Lebensgestaltung

Neben der Quellen-TKÜ wird mit § 8 auch der verdeckte Zugriff auf Computer, Handys,... erlaubt, um diese unbemerkt zu durchsuchen. Auch hier wird zur Realisierung des Zugriffs üblicherweise eine Software installiert werden müssen. Bei jeder (Online-)Durchsuchung muss gemäß § 7 und § 8 der Schutz des Kernbereichs privater Lebensgestaltung sichergestellt werden. Heutige Kommunikationsmittel sind jedoch oft ein digitales Spiegelbild des gesamten Lebens ihrer Besitzer. Auf Ihnen sind nicht selten intimste Informationen in Form von vertraulichen Kommunikationen, Fotos und Daten (z.B. auch Gesundheitsdaten) gespeichert. Eine zuverlässige Erkennung dieser Daten vor Einsichtnahme und/oder Übermittlung kann hier keineswegs sichergestellt werden, so dass der Schutz privatester Informationen nicht sicherzustellen ist.

Gefährdung der Zielsysteme und der Allgemeinheit

Sowohl die Abhörsoftware für eine Quellen-TKÜ als auch der "Hessentrojaner" müssen von den Behörden von außen ansprechbar sein. Dies ist erforderlich, um z.B. die Ausleitung von Daten zu starten und zu stoppen, um ggfs. Anpassungen bzgl. der abzuhörenden Kommunikationswege vorzunehmen oder um die Maßnahme zu beenden. Da sich die Zugriffsschnittstelle hierbei nicht wie bei der klassischen TKÜ im geschützten Netzwerk eines Netzbetreibers befindet, sondern direkt auf dem Gerät des Abzuhörenden, wird das Gerät der Gefahr eines unberechtigten Zugriffs durch Dritte ausgesetzt.

Zur Installation der Abhör- und Durchsuchungssoftware sind verschiedene Wege denkbar. Zum einen kann eine Installation direkt vorgenommen werden, wenn physischer Zugriff auf das Gerät besteht und dieses nicht durch Verschlüsselung und Authentisierungs- und Autorisierungsmethoden geschützt ist. Ggfs. kann ein Abzuhörender auch durch Social Engineering dazu gebracht werden, die Software selbst zu installieren. In den allermeisten Fällen werden jedoch Schwachstellen in den Betriebssystemen oder verwendeter Anwendungssoftware der betroffenen Geräte ausgenutzt werden müssen. Diese Lücken müssen von den Behörden selbst gefunden oder auf dem Schwarzmarkt gekauft werden. Da zur Erlangung aktueller Lücken, für die noch kein Patch des Herstellers vorliegt, große zeitliche und/oder finanzielle Aufwände betrieben werden müssen, entsteht für die Behörden ein großer Anreiz, diese Lücken nicht an die Hersteller der Geräte und Software zu melden. Dies wiederum führt zu einer großen Gefährdung der Allgemeinheit, da die Lücken so in allen betroffenen Geräten offen bleiben. Welche Auswirkungen dies haben kann, konnte gut am Beispiel der WannaCry-Ransomware beobachtet werden, die ab Mai 2017 weltweit eine große Anzahl von Computersystemen befallen und teilweise kritische Infrastruktur im Gesundheitswesen und im Verkehr lahmlegte.

Aber nicht nur das Zurückhalten von Informationen zu Sicherheitslücken gefährdet die IT-Sicherheit. Auch die Veränderung der Systeme zur Erlangung des Zugriffs kann sie für weitere Angriffe anfällig machen. Die Gefahr besteht hier nicht nur für den direkt Betroffenen in der Kompromittierung der enthaltenen Daten, sondern auch für die Allgemeinheit darin, dass das Gerät z.B. als Verteiler von SPAM und Computerviren fungieren oder im Rahmen eines Botnetzes missbraucht werden kann.

Auch Geräte unbeteiligter dürfen gehackt werden

Nochmals vergrößert wird die Gefahr für die Allgemeinheit, da nach § 8, Absatz 1, Punkt 2 nicht nur die Geräte des Abzuhörenden angegriffen werden dürfen, sondern auch alle weiteren Geräte, auf denen Zugangskennungen zu Accounts des Betroffenen oder Informationen über den Standort seiner informationstechnischen Geräte vermutet werden. Da die Ermittlung des Standortes z.B. über die IP-Adresse erfolgen kann, betrifft diese Regelung somit praktisch jedes System, das im weitesten Sinne in die Kommunikation des Abzuhörenden involviert war. Dies können im Zweifelsfall auch die Server großer (Kommunikations-)Provider oder ähnliche Systeme sein. Bzgl. der Reichweite der Regelung gibt es im Gesetz keine Einschränkungen. Gegen die Betreiber der betroffenen Geräte muss hierbei kein Verdacht bzgl. Bestrebungen gegen die freiheitlich demokratische Grundordnung o.Ä. vorliegen. Es reicht, das auf den Geräten die oben genannten Informationen vermutet werden. Von einer Verhältnismäßigkeit der Maßnahme kann hier keine Rede sein. *die*Datenschützer Rhein Main halten diesen Passus für offensichtlich verfassungswidrig und empfehlen dringend, ihn ersatzlos zu streichen.

Defizite bei Dokumentation und Rückbau

Der Gesetzentwurf schreibt vor, dass vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden müssen (§ 8,2,2). Dass ein automatisierter Rückbau aller Veränderungen jeweils möglich ist, erscheint mehr als fraglich. Hier ist daher zu befürchten, dass Geräte nach Abschluss der Maßnahmen mit gravierenden Sicherheitslücken zurückgelassen werden. Da, wie oben dargestellt, hiervon nicht nur die Systeme der Zielpersonen, sondern auch eine Vielzahl weiterer Systeme betroffen sein können, ergibt sich eine weitere, große Gefahr für die allgemeine IT-Sicherheit.

Die Dokumentationspflichten nach § 6 und § 8 sehen unter anderem vor, dass lediglich dauerhafte (also "nicht nur flüchtige") Veränderungen an angegriffenen Systemen dokumentiert werden müssen. Hier fehlt eine klare Definition des Begriffs "nicht nur flüchtig". Dies kann zu erheblichen Problemen in einer gerichtlichen Aufarbeitung eines solchen Eingriffs führen, da auch flüchtige Veränderungen erheblichen Einfluss auf die Sicherheit und Integrität eines IT-Systems haben können. Ggfs. fehlen daher wichtige Informationen über vorgenommene Veränderungen in den Akten. Gelten z.B. alle Veränderungen als flüchtig, die nur bis zum Neustart eines Systems greifen, können diese ggfs. für sehr lange Zeiträume aktiv sein. Viele Handys werden heute kaum noch aktiv ausgeschaltet und starten lediglich neu, wenn einmal versehentlich der Akku nicht rechtzeitig geladen wurde. Dies kann erst nach Monaten eintreten. Noch ausgeprägter gilt dies für Serversysteme, die häufig Uptimes (Laufzeit seit dem letzten Neustart) von vielen Monaten oder gar Jahren haben.

Maßnahmen ohne richterliche Genehmigung

Maßnahmen, die lediglich zum Schutz der für den Verfassungsschutz bei einem Einsatz in Wohnungen tätigen Personen dienen, unterliegen nach § 9 nicht dem Richtervorbehalt. In Anbetracht der Schwere der Eingriffe und der sich daraus ggfs. ergebenden Gefahren für die Allgemeinheit ist dies nicht nachvollziehbar.

Gleiches gilt für die Regelung bzgl. "Gefahr in Verzug". Gerade bei der zu erwartenden Dauer der Vorbereitung einer Maßnahme nach § 8 ist nicht nachvollziehbar, warum hier nicht vorab die Genehmigung eines Richters eingeholt werden kann.

Konzentration der richterlichen Genehmigungen an einem Gericht

§ 9 sieht vor, dass für sämtliche richterliche Entscheidungen zu Maßnahmen nach §§ 7 & 8 das Amtsgericht am Sitz des Landesamtes zuständig ist. Hier sehen wir die Gefahr, dass durch die Konzentration der Zuständigkeit, Prüfungen ggfs. nicht so gründlich erfolgen könnten, wie bei einer verteilten Zuständigkeit.

Schlussfolgerung zu Quellen-TKÜ & Hessentrojaner

Zusammenfassend kann gesagt werden, dass durch die im Gesetzentwurf vorgesehenen Berechtigungen für das LfV große Gefahren für die allgemeine IT-Sicherheit entstehen. Diese stehen in keinem angemessenen Verhältnis zu einem möglichen Erkenntnisgewinn durch die Maßnahmen. Die Berechtigungen sind in der beschriebenen Form daher nicht hinnehmbar.

Als absolute Mindestforderung muss eine Verpflichtung zur umgehenden Meldung bestehender Sicherheitslücken in IT-Systemen an die jeweiligen Hersteller und ein Verbot des Angriffs auf Informationssysteme gelten, die sich nicht unter direkter Kontrolle einer Zielperson befinden. Darüber hinaus muss für sämtliche Maßnahmen der Richtervorbehalt gelten.

Die Informationsübermittlung nach § 22, die ebenfalls für Daten nach §§ 7 und 8 möglich sein soll, lehnen *die*Datenschützer Rhein Main vollständig ab. Angesichts der zwar verpflichtenden, de facto jedoch nicht realisierbaren Verwendungsbeschränkung im Ausland, insbesondere in datenschutzrechtlich unsicheren Drittstaaten, ist von dieser Ermächtigung Abstand zu nehmen. Erschwerend kommt dabei hinzu, dass sich diese Daten weitestgehend der Kontrolle, auch und vor allem der parlamentarischen, entziehen.

Weiterhin ist nach unserer Ansicht § 7 Abs. 1 Nr. 3 verfassungswidrig. Im Urteil des Bundesverfassungsgerichts in Sachen Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen (1 BVR 370/07 und 1 BVR 595/07) werden die Grenzen einer heimlichen Infiltration eines informationstechnischen Geräts wesentlich enger begrenzt.

Hierzu führt das BVerfG aus:

„Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Hierzu zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen. Zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine existentielle Bedrohungslage nicht besteht, ist eine staatliche Maßnahme grundsätzlich nicht angemessen, durch die - wie hier - die Persönlichkeit des Betroffenen einer weitgehenden Ausspähung durch die Ermittlungsbehörde preisgegeben wird. Zum Schutz solcher Rechtsgüter hat sich der Staat auf andere Ermittlungsbefugnisse zu beschränken, die ihm das jeweils anwendbare Fachrecht im präventiven Bereich einräumt.“

ZU ARTIKEL 2

Gesetz zur parlamentarischen Kontrolle des Verfassungsschutzes in Hessen (Verfassungsschutzkontrollgesetz)

Die Kontrolle nachrichtendienstlicher Tätigkeiten bewegt sich naturgemäß auf dem schmalen Grad zwischen notwendiger Geheimhaltung einerseits und andererseits der Überprüfung durch das Parlament, die Öffentlichkeit und einzelner Betroffenen. In diesem Widerstreit ist dem Gesetzgeber auferlegt, die Geheimhaltung auf das absolut notwendige Maß zu beschränken, um die notwendige Überprüfung staatlichen Handelns zu ermöglichen. Ein Instrument dieser Aufsicht ist die Parlamentarische Kontrolle.

Mit der Novelle des PKGrG, zuletzt geändert am 5.1.2017 liegt ein Gesetzestext vor, der unmittelbar zum Vergleich herangezogen werden kann. Obwohl ebenfalls nicht frei von Kritik, muss sich der Gesetzentwurf der Fraktionen CDU und BÜNDNIS 89 / DIE GRÜNEN an diesem messen lassen auch in gerade in Hinsicht auf die Möglichkeiten der parlamentarischen Kontrolle.

Aus Sicht von *die*Datenschützer Rhein-Main ergeben sich vor allem, jedoch nicht ausschließlich im direkten Vergleich erhebliche Defizite:

1. Anders als im § 5 (1) PKGrG ist der Parlamentarischen Kontrollkommission in Hessen lediglich die Akteneinsicht nicht jedoch die Herausgabe, auch im Original oder die Übermittlung zugestanden. Obwohl dies eine Verbesserung auf niedrigem Niveau darstellt, da es sich nunmehr um ein Individualrecht handelt, bleibt es ohne Not hinter den Rechten auf Bundesebene zurück.

2. Nicht geregelt ist die Verpflichtung zur Rechts- und Amtshilfe von Gerichten und Behörden.

3. Auf Bundesebene wird der parlamentarischen Kontrolle in § 5 (2) PKGrG das Recht zugestanden, Angehörige des Nachrichtendienstes, Mitarbeiter und Mitglieder der Regierung und Beschäftigte anderer Behörden zu befragen. Dieser Passus fehlt im vorliegenden Gesetzesentwurf ebenfalls vollständig.

*die*Datenschützer Rhein Main empfehlen zu Punkt 1 - 3, § 4 des vorliegenden Gesetzesentwurfs entsprechend der Regelungen des § 5 Abs. 1-4 PKGrG neu zu fassen.

Ungeachtet der Messlatte PKGrG sind weitere spezifische Regelungen im vorliegenden Gesetzesentwurf zu hinterfragen und bedürfen einer kritischen Würdigung.

4. Zwar wird den Mitgliedern der Parlamentarischen Kontrollkommission gestattet, ihre Notizen im Nachhinein noch einmal einzusehen, jedoch ist lediglich der Begründung (Seite 64) zu entnehmen, dass diese zwei Wochen nach Ausfertigung des Protokolls vernichtet werden. Eine Notiz, die nicht Eingang in das Protokoll gefunden hat, ist damit nach unverhältnismäßig kurzer Zeit, gerade in Hinsicht auf die weiten Berichtszeiträume, unwiederbringlich verloren.

5. Die Regelung in § 3 (2), die es der Landesregierung vorbehält über Zeit, Art und Umfang der Unterrichtung zu bestimmen, stellt in unseren Augen eine unverhältnismäßige Einschränkung dar.

*die*Datenschützer Rhein Main empfehlen zu Punkt 4 die Nutzung moderner Hilfsmittel bei adäquater Sicherstellung der Geheimhaltung vollumfänglich zuzulassen und zu Punkt 5 die Einschränkung ersatzlos zu streichen.

Die Verfassung der Bundesrepublik Deutschland wie auch des Landes Hessens geht von der Annahme aus, dass das Parlament, also die Summe der in ihr vertretenden Abgeordneten unabhängig von der Fraktionszugehörigkeit die Regierung kontrolliert. Dieser hehre Grundsatz lässt sich in der Praxis bedauerlicherweise nur sehr selten beobachten. Vielmehr reduzieren sich die Regierungsfraktionen allzu häufig selbst auf einen verlängerten Arm der Regierung, wie auch schon das Bundesverfassungsgericht festgestellt hat.

Unter der Prämisse dieser Beobachtung ergibt sich zwingend, dass wirksame Instrumente zur Wahrung des Minderheitenschutzes zu implementieren sind, wie sie auch regelmäßig durch das Bundesverfassungsgericht gefordert werden. Auch ungeachtet dieser Betrachtung wäre eine Stärkung der Opposition, wie sie in den Untersuchungsausschlüssen bereits seit Jahrzehnten Einzug hält, ein folgerichtiger und konsequenter Schritt. Bedauerlicherweise fehlte den einreichenden Regierungsfraktionen hierzu die Entschlossenheit. Im gesamten Prozess der Parlamentarischen Kontrolle, beginnend mit der Einberufung bis zur Berichterstattung sind keine Ansätze des Minderheitenschutzes erkennbar.

So bleibt es unverständlich, warum

6. die Landesregierung zu konkrete Themen nur durch Mehrheitsentscheid der Kommission § 3 (1) berichten muss. Ein Individualrecht, zumindest jedoch ein Minderheitenrecht würde voraussichtlich die Kapazitäten der Landesregierung nicht überfordern, könnte aber erheblich zu Erkenntnisgewinnen beitragen.

7. die Möglichkeit eines Sondervotums, wie sie aus § 10 (2) PKGrG und den Untersuchungsausschüssen bekannt sind, nicht übernommen worden ist.

8. es den Fraktionen nicht selbst vorbehalten ist, nach beispielsweise einem Proporz Mitglieder und deren Mitarbeitenden in die Kommission zu entsenden.

*die*Datenschützer Rhein Main regen an, in den Fällen 6. und 7. ein Individualrecht einzuräumen, zumindest jedoch ein Minderheitenrecht zu implementieren, dass durch bereits zwei Fraktionen ausgelöst werden kann. Im Fall 8. empfehlen wir das Erfordernis einer Zustimmung durch Mehrheitsentschluss zu ersetzen durch die Möglichkeit einer Ablehnung einzelner Mitglieder oder Mitarbeitenden mit höherem Quorum. So entsteht ein Ausgleich zwischen angemessene Kontrolle des Parlament über die Entsendung und Eigenverantwortung der Fraktionen.

ZU ARTIKEL 3

Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung

A. STELLUNGNAHME ZUM GESETZENTWURF

Der vorliegende Gesetzesentwurf erweitert zum Teil erheblich die Befugnisse von Polizei und Verfassungsschutz. Hierbei ist insbesondere zu kritisieren:

1. Die Zuverlässigkeitsüberprüfung soll zukünftig durch die Erweiterung des § 13b auch dann möglich sein, wenn keine besondere Gefährdung der Veranstaltung vorliegt oder bekannt ist. Die Einschränkung, dass dies zum Schutz der Veranstaltung erforderlich sein muss, ist sehr allgemein gefasst und stellt in dieser Form eine Generalvollmacht dar.

*die*Datenschützer Rhein Main empfehlen zu 1., den Passus ersatzlos zu streichen. Liegen Erkenntnisse für eine besondere Gefährdung einer Veranstaltung vor, reichen die an anderer Stelle zur Verfügung stehenden Mittel aus.

In einem Rechtsstaat gilt ein Mensch solange als unschuldig, bis über seine Schuld befunden worden ist. Die elektronische Aufenthaltsüberwachung, gemeinhin “Fußfessel” genannt, wird mit § 31a eingeführt. Sie ist eine massive Einschränkung der Grundrechte einer Person, die keiner Straftat oder ihrer Vorbereitung überführt wurde.

Gilt dies allein schon für die ständige und lückenlose Aufzeichnung eines Bewegungsprofils, so ist dies erst recht einschlägig in Verbindung mit den weitreichenden Einschränkungen, zu denen die Polizeibehörden befugt werden sollen:

2. So kann neben dem Verbot, bestimmte Orte aufzusuchen, auch erlassen werden, bestimmte Bereiche nicht zu verlassen. Dabei stellt es der Gesetzesentwurf den Polizeibehörden vollkommen frei, wie weit diese Befugnisse auszudehnen sind. In der Theorie ist also selbst ein Hausarrest denkbar.

3. Vollkommen unerklärlich ist, warum im Zusammenhang mit der “Fußfessel” die Ermächtigungen notwendig ist, Personen aufzuerlegen, sich zu bestimmten Zeiten bei einer Polizeibehörde zu melden, da der Aufenthaltsort zum einen durch die "Fußfessel" bekannt ist und zum anderen Aufenthaltseinschränkungen ausgesprochen werden können.

4. Ebenso fragwürdig ist die in diesem Zusammenhang eingeräumte Ermächtigung, ein Kontaktverbot auszusprechen. Hierbei kann das technische Mittel der “Fußfessel” nur dann Wirkung entfalten, wenn auch die Personen, gegenüber denen ein Kontaktverbot ausgesprochen worden ist, diese Geräte tragen. Andernfalls ist eine automatisierte Verarbeitung, wie sie durch das Gesetz vorgeschrieben ist, nicht möglich, beziehungsweise nicht abzugrenzen von dem Verbot, sich an bestimmten Orten aufzuhalten.

5. Zwar ist der Einsatz grundsätzlich auf drei Monate beschränkt, kann jedoch beliebig oft für jeweils den gleichen Zeitraum verlängert werden.

Vor diesem Hintergrund empfehlen *die*Datenschützer Rhein Main, von der Einführung der elektronischen Aufenthaltsüberwachung Abstand zu nehmen.

B. STELLUNGNAHME ZUM ÄNDERUNGSANTRAG (LT-Drucksache 19/5785)

Mit dem Änderungsantrag werden weitere über die Gesetzesinitiative hinausgehenden Befugnisse der Gefahrenabwehrbehörden und Polizei eingeführt und neue Instrumentarien geschaffen.

Wir begrüßen den Willen der Regierungsfraktionen, der Kritik an der Umsetzung der Zuverlässigkeitsüberprüfung durch den vorliegenden Änderungsantrag zu begegnen. Leider kann uns der gewählte Ansatz nicht überzeugen. In § 13a HSOG wird bislang die Zuverlässigkeitsüberprüfung im Zusammenhang mit dem Zutritt oder Zugriff (auf Informationen) in Bezug auf den Vollzug geregelt.

1. Der Kreis der Betroffenen soll nun um Gruppen vergrößert werden, die dem Regelungsgehalt des § 13a bislang wesensfremd waren. Insbesondere die grundsätzliche Überprüfung in der Extremismusprävention wurde zwar gegenüber dem ursprünglichen Ansatz eingeschränkt, bleibt in dieser Form dennoch nicht erklärbar.

2. Hinzu kommt, dass die Prüfung weiterhin um Erkenntnisse des LfV erweitert werden soll, ohne dass hierfür hinreichender Anfangsverdacht bestehen muss.

3. Angesichts der Tatsache, dass das LfV lediglich übermittelt, ob sicherheitsrelevante Erkenntnisse vorliegen, ist die Möglichkeit zur Stellungnahme hier faktisch nicht anwendbar.

4. Dergleichen gilt für das teilweise schon heute vorhandene Erfordernis der Einwilligung. Grundsätzlich setzt eine Einwilligung die Freiwilligkeit voraus und somit das Fehlen von Repressionen bei Versagen derselben.

*die*Datenschützer Rhein Main empfehlen, in Bezug auf Punkt 1. die Überprüfung auf begründete Einzelfälle zu beschränken und in den Punkten 2 und 3 auf die Trennung von Polizei und Geheimdiensten zu bestehen und das LfV nicht in Zuverlässigkeitsüberprüfungen einzubeziehen. Hilfsweise ist zumindest im Punkt 2. die Einschränkung aufzunehmen, dass tatsächliche Anhaltspunkte vorliegen müssen, im Punkt 3. klar zu stellen, dass den Betroffenen ein Auskunftsrecht zusteht analog des Informationsfreiheitsgesetzes des Bundes. Letzteres ist notwendig, da in Hessen weder ein gleichartiges Recht gegenüber dem LfV besteht noch durch den aktuellen Gesetzentwurf geplant ist.

„Die Aufspaltung von Polizei und Ordnungsbehörden (in Hessen: Gefahrenabwehrbehörden) [ist zu verstehen] als Lehre aus dem [sogenannten] Dritten Reich, indem sich Geheime Staatspolizei (Gestapo) und der zum Teil mit der SS verschmolzenen Kriminalpolizei weitgehend „entstaatlicht" hatte." (Quelle: Rechtslexikon.net)

Durch die Änderungen in § 14 werden die Befugnisse der Gefahrenabwehrbehörden denen der Polizei gleichgestellt, die Einschränkung, dass zur Videoüberwachung öffentlicher Plätze zuvor bereits ein Kriminalitätsschwerpunkt vorliegen muss, entfällt. Die Aufspaltung zwischen Polizei und Gefahrenabwehrbehörden wird faktisch weiter zurückgedrängt.

In gleicher Weise steigen die Möglichkeiten zum Einsatz von Überwachungstechnik. Die Räume, in denen Bürgerinnen und Bürger von ihrem Recht auf informationelle Selbstbestimmung Gebrauch machen können und von der einst selbstverständlichen Annahme ausgehen dürfen, in der Öffentlichkeit von staatlicher Überwachung unbehelligt zu bleiben, schrumpfen in gravierender Weise.

Mittels § 14, Abs. 6 erhalten die Polizeibehörden die Option, unter gewissen Voraussetzungen Bodycams und andere Mittel zur Bild- und Tonaufzeichnung einzusetzen.

*die*Datenschützer Rhein Main empfehlen dringend, hier einen Passus aufzunehmen, dass die aufgenommene Person vor Beginn der Aufnahme auf den Umstand der Aufnahme hinzuweisen ist. Zudem fehlen jegliche Vorgaben bzgl. einer technischen Sicherung der Aufnahmen, z.B. mittels kryptographischer Verfahren, vor nachträglicher Veränderung.

Über § 25a sollen den Sicherheitsbehörden weitreichende Möglichkeiten zur automatisierten Analyse gespeicherter Daten, insbesondere in Bezug auf Beziehungsnetzwerke, eröffnet werden. Zwar sollen die Analysen nur im begründeten Einzelfall durchgeführt werden, jedoch sind keine Begrenzungen bzgl. ihrer Reichweite und keine Löschfristen vorgesehen.

Obwohl die Befugnisse und das Instrumentarium der Gefahrenabwehrbehörden und Polizei erweitert wurden, bleibt die parlamentarische Kontrolle unverändert. Insbesondere das neu eingeführte Element der automatisierten Anwendung zur Datenanalyse entzieht sich der notwendigen Überprüfung. *die*Datenschützer Rhein Main regen daher an, § 25a, wenn er beibehalten wird, um einen Abschnitt 4 analog zu § 15 (9) HSOG zu erweitern.

FAZIT

Die Eingangs dargestellte Verhältnismäßigkeit, die sicherzustellen hat, dass Schutzmaßnahmen zur Sicherung der freiheitlich-demokratischen Grundordnung und der Menschenrechte nicht zu deren größten Gefahr werden, wird durch den vorliegenden Gesetzentwurf nicht erreicht. Vielmehr werden die Befugnisse der Sicherheitsbehörden sehr stark ausgeweitet, ohne dass dem angemessene Schutzmöglichkeiten der Bürgerinnen und Bürger gegenüber stehen, oder auch nur ein wirksame Kontrolle entgegen gesetzt würde. Das Bekenntnis zur Unschuldsvermutung, eine tragende Säule unseres Rechtssystems und damit unabdingbarer Teil unserer Grundordnung, ist dem Vorstoß der Regierungskoalitionen nicht zu entnehmen. Vielmehr wird mit dem undefinierten Rechtsbegriff des „Gefährders“, der Ausweitung der Überprüfungen, der Datenübermittlungen und des Beobachtetens unbeteiligter Dritter der Kreis derer, die sich nicht mehr vorbehaltlos als „unbescholten“ erachten können, ausgeweitet.

Da hierbei auf Methoden zurück gegriffen wird, deren Wirksamkeit, abgesehen von einer vermeintlichen Steigerung der „gefühlten Sicherheit“, in keiner Weise belegt sind, halten *die*Datenschützer Rhein-Main es für sehr bedauerlich, dass der vorliegende Gesetzentwurf weder eine Befristung noch eine Evaluation der Wirksamkeit der mit ihm ermöglichten, umfangreichen Überwachungsmethoden vorsieht.

In der Gesamtschau und angesichts der kurzen Zeit, die für die Beratung noch verbleibt, müssen wir daher empfehlen, den Gesetzesentwurf fallen zu lassen.