



Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit RLP
Postfach 3040 | 55020 Mainz

Hintere Bleiche 34 | 55116 Mainz
Postfach 3040 | 55020 Mainz

Landtag Rheinland-Pfalz
- Innenausschuss
- Rechtsausschuss
Platz der Mainzer Republik 1
55116 Mainz

LANDTAG
Rheinland-Pfalz
17/6003
VORLAGE

Telefon +49 (0) 6131 208-2449
Telefax +49 (0) 6131 208-2497

poststelle@datenschutz.rlp.de
www.datenschutz.rlp.de

Ihr Zeichen	Ihre Nachricht vom	Geschäftszeichen	Telefondurchwahl	Datum
656-1-11/656-1-12	10. Dezember 2019	6.06.00.002	2449	20.01.2020

Beratung des Entwurfs eines Landesgesetzes zur Neufassung des Landesverfassungsschutzgesetzes und zur Änderung weiterer Gesetze (Drs. 17/10488) am 23. Januar 2020

Stellungnahme des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

Sehr geehrte Frau Direktorin,

gerne nehme ich die Möglichkeit in Anspruch, im Rahmen der gemeinsamen Sitzung des Innen- und Rechtsausschusses am 23. Januar 2020 zum Entwurf eines Landesgesetzes zur Neufassung des Landesverfassungsschutzgesetzes und zur Änderung weiterer Gesetze (Drs. 17/10488) Stellung zu nehmen.

Anbei finden Sie die Stellungnahme in schriftlicher Form mit der Bitte um Weiterleitung an die jeweiligen Ausschüsse.

Mit freundlichen Grüßen

Prof. Dr. Dieter Kugelmann



Stellungnahme

des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
zum **Gesetzentwurf der Fraktionen der SPD, FDP und BÜNDNIS 90/DIE GRÜNEN**

Landesgesetz zur Neufassung des Landesverfassungsschutzgesetzes und zur Änderung weiterer Gesetze (im Folgenden LVerfSchG-E)

I. Übergreifende Anmerkungen

Der Gesetzentwurf weist viel Licht auf, hat aber auch einige Schattenseiten. Zunächst ist positiv anzumerken, dass die Landesregierung die Verfassungsschutzbehörde zwar in ihren Befugnissen deutlich stärkt, dabei jedoch nicht die Regelung aller nach aktuellem Stand technisch möglicher Überwachungsmaßnahmen vorsieht, sondern anstrebt, die Befugnisse der Verfassungsschutzbehörde an den Stand der Technik anzupassen und dabei rechtsstaatliches bzw. verhältnismäßiges Maß zu wahren. Befugnisse zum Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation (Quellen-TKÜ) sowie zum Einsatz technischer Mittel in informationstechnischen Systemen (Online-Durchsuchung) haben keinen Einzug in das Landesverfassungsschutzgesetz genommen. Dies ist nachhaltig zu begrüßen. Des Weiteren wurde der Kernbereichsschutz betroffener Personen erweitert (§ 8 Abs. 2 LVerfSchG-E).

Der Gesetzesentwurf sieht allerdings nichtsdestotrotz erhebliche Erweiterungen der bisherigen sowie die Schaffung neuer Befugnisse vor. Auch die Datenverarbeitungsregelungen werden modifiziert und ermöglichen den Verfassungsschutzbehörden eine erweiterte zweckändernde Verarbeitung, insbesondere zur Übermittlung personenbezogener Daten. Die durch das Ministerium des Innern und für Sport erstellte hilfreiche Synopse gibt einen Überblick über die Änderungen im Vergleich zum Vorgängergesetz. Dies ist insbesondere vor dem Hintergrund hilfreich, dass die Gesetzesbegründung zu einigen der wesentlichen Änderungen keine Aussagen trifft. Auch wenn die Anwendung und Auslegung des Gesetzes sich grds. auf den Wortlaut des Gesetzes beschränkt, ist es im Rahmen des Gesetzgebungsverfahrens sinnvoll und erforderlich, zu kommunizieren, welche Änderungen – insbesondere solche, die die Grundrechtspositionen von Grundrechtsträgern schwächen – erfolgen und welche Intention der Gesetzgeber damit verfolgt. Nur so kann der demokratische, politische und rechtliche Diskurs im Rahmen des Gesetzgebungsverfahrens auf Augenhöhe und informiert erfolgen.

Der Gesetzentwurf stärkt die Parlamentarische Kontrollkommission erheblich und stattet sie mit neuen Kontrollbefugnissen aus. Aufgrund des § 34 Abs. 4 LVerfSchG-E ist gesichert, dass diese Kommission über ausreichende Sachkunde in Bezug auf die entscheidungserheblichen Sachverhalte verfügt. Die mit der starken parlamentarischen Kontrolle der Parlamentarischen Kontrollkommission und der Kontrolle durch die G 10-Kommission einhergehende eingeschränkte Kontrolle des LfDI ist vor diesem Hintergrund hinnehmbar. Den Möglichkeiten der Konsultation im Rahmen des § 30 Abs. 1 letzter Halbsatz LVerfSchG-E steht der LfDI aufgeschlossen gegenüber. Der LfDI teilt in diesem Zusammenhang gerne seine Sachkunde, die er im Rahmen seiner Kontrollzuständigkeit zu den Telekommunikations- und Wohnraumüberwachungsbefugnissen der Polizei des Landes Rheinland-Pfalz sammeln konnte.



II. Überwachungsbefugnisse des Verfassungsschutzbehörde

1. Eingriffsschwelle der Überwachungsbefugnisse

Die neu geschaffenen Befugnisse, insbesondere solche, die aufgrund ihrer Heimlichkeit (Wohnraumüberwachung) oder Streubreite (z.B. Funkzellenabfrage) besonders eingriffsintensiv sind, müssen den Anforderungen der Rechtsprechung des Bundesverfassungsgerichts standhalten, was die Eingriffsschwelle, die Transparenz der Maßnahme und die Kontrolle und Aufsicht anbelangt. Dazu habe ich folgende Anmerkungen:

a) Funkzellenabfrage

Hinsichtlich des Einsatzes der Funkzellenabfrage (§ 14 LVerfSchG-E) und des IMSI-Catchers (§ 15 LVerfSchG-E) wird die Eingriffsschwelle dadurch determiniert, dass zusätzlich zu § 5 LVerfSchG-E die Voraussetzungen des § 3 Abs. 1 des Art. 10-Gesetzes vorliegen müssen, also tatsächliche Anhaltspunkte für den Verdacht, dass eine der in dem Katalog aufgezählten Straftaten vorliegt. Nach der Rechtsprechung des Bundesverfassungsgerichts führt die Anforderung des Vorliegens tatsächlicher Anhaltspunkte dazu, dass Vermutungen oder allgemeine Erfahrungssätze allein nicht ausreichen, sondern bestimmte Tatsachen festgestellt werden, die eine Gefahrenprognose tragen (vgl. BVerfGE 120, 274; NJW 2008, 822 Rn. 250). Durch diesen Konkretisierungsgrad der Eingriffsschwelle wird der Einsatz der Instrumente auf das unbedingt Erforderliche beschränkt. Dies ist begrüßenswert und stellt einen wichtigen Punkt bei der Kontrolle dar.

b) Wohnraumüberwachung

Die Eingriffsschwelle der Wohnraumüberwachung ist demgegenüber niedriger. In der Gesetzesbegründung wird dazu ausgeführt, dass nach dem Polizei- und Ordnungsbehördengesetz erfolgende polizeiliche Überwachungsmaßnahmen bereits dann zulässig sind, wenn Tatsachen die Annahme rechtfertigen, dass eine Person mit hinreichender Wahrscheinlichkeit terroristische Straftaten begehen wird. Deswegen sollen für die Verfassungsschutzbehörde die bundesverfassungsgerichtlich zugestandenen Befugnisse im Vorfeld konkreter Terrorgefahren uneingeschränkt und erst recht gelten, da dem Wesen einer nachrichtendienstlichen Gefahrenforschungsbehörde entsprechend die Hauptaufgabe der Verfassungsschutzbehörde in der verdeckten Vorfeldaufklärung extremistischer und terroristischer Bestrebungen bestehe (vgl. Gesetzesbegründung S. 87). Die Überzeugungskraft dieses Erst-Recht-Schlusses soll dahin stehen. Jedenfalls kann dies nicht dazu führen, dass die Befugnisse, die der Polizei bereits weit im Vorfeld einer konkreten Gefahr zustehen, für die Verfassungsschutzbehörde noch weiter ins Vorfeld zu rücken. Im Gegenteil sind insbesondere bei solch überschneidenden Tätigkeitsfeldern zu prüfen, ob Mechanismen und Formen von Kooperationen gefunden werden, die eine doppelte Überwachung der betroffenen Person – die sich eingriffsintensivierend auswirkt – vermeiden. Das verfassungsrechtliche Trennungsgebot zielt auf eine Verringerung von Eingriffsintensität unter Wahrnehmung von Möglichkeiten der Kooperation. In diesem Zusammenhang wird angemerkt, dass das Land Niedersachsen die Wohnraumüberwachung aus dem Arsenal nachrichtendienstlicher Befugnisse gestrichen hat. Wenn die Landesregierung trotzdem an der Regelung festhalten möchte, sollte der Einsatz von Wohnraumüberwachung jedenfalls höherschwellig geregelt werden und eine Wohnraumüberwachung in § 18 Abs. 1 S. 2 erst dann zulassen, wenn aufgrund Tatsachen über das individuelle Verhalten einer



Person die konkrete Wahrscheinlichkeit besteht, dass sich eine von ihr ausgehende, in § 18 Abs. 1 S. 1 LVerfSchG-E genannte Gefahr unverzüglich realisieren wird.

2. Benachrichtigungspflichten

Überwachungsmaßnahmen müssen nach der Rspr. des Bundesverfassungsgerichts zum BKA-G (BVerfG, Urteil vom 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09) von verfahrenssichernden Maßnahmen, die Voraussetzung für die Verhältnismäßigkeit dieser Maßnahmen sind, flankiert werden. Dazu zählt insbesondere die Transparenz der Maßnahme. Insofern ist es erforderlich, Benachrichtigungspflichten zu regeln, um sicherzustellen, dass der Betroffene solcher Maßnahmen zumindest nachträglich von den Überwachungsmaßnahmen Kenntnis erlangt und ihm die Möglichkeit des subjektiven Rechtsschutzes nach Art. 19 Abs. 4 Grundgesetz (GG) eröffnet wird. (vgl. BVerfG, Urteil vom 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 Rn. 136). Es ist insbesondere im Bereich der Nachrichtendienste und damit auch der Verfassungsschutzbehörden nachvollziehbar, dass bestimmte Beobachtungen durch die Benachrichtigung und Offenlegung nicht kompromittiert werden dürfen. Für diesen Fall würde es dem Gesetzgeber – unterstützt durch die o.g. Rspr. – offenstehen, enge Ausnahmetatbestände von den Benachrichtigungspflichten zu schaffen. Wiegen die entgegenstehenden Gründe so schwer, dass eine nachträgliche Benachrichtigung auszuschließen ist, muss geregelt werden, dass dies richterlich bestätigt und in regelmäßigen Abständen überprüft wird (BVerfGE 125, 260 [336 f.] = NJW 2010, 833).

Diesem Auftrag ist der Gesetzgeber nur im Rahmen der Wohnraumüberwachung nachgekommen (vgl. § 19 Abs. 4 LVerfSchG-E). Andere heimliche Überwachungsmaßnahmen, zu denen auch die Funkzellenabfrage und die Nutzung des IMSI-Catchers zu zählen sind, sollen dagegen immer ohne jede Kenntnisnahme der betroffenen Personen erfolgen. Dies ist nicht tragbar vor dem Hintergrund der genannten bundesverfassungsrechtlichen Rechtsprechung.

Der LfDI teilt die Auffassung der Landesregierung, dass die Maßgaben, die das Bundesverfassungsgericht zum BKA-G zur Verfassungsmäßigkeit, insbesondere Verhältnismäßigkeit eingriffssintensiver Überwachungsmaßnahmen geschaffen hat, auch auf Nachrichtendienste und deren Datenverarbeitung entsprechend Anwendung finden. Dies kann aber nicht nur die Maßgaben betreffen, die die Regelung eingriffssintensiver Befugnisse oder die Erleichterung der zweckändernden Datenverarbeitung im Rahmen der hypothetischen Datenneuerhebung (dazu mehr unter Ziff. 5b) anbelangen, sondern muss nach hiesiger Auffassung in der Konsequenz auch die grundrechtsschützenden und rechtsstaatlich erforderlichen Anforderungen an Transparenz und aufsichtliche Kontrolle einschließen.

III. Neuregelung der Datenverarbeitungsgrundlagen

1. Allgemeine Befugnisse der Verfassungsschutzbehörde (§ 9 LVerfSchG)

a) Herabsenkung der Eingriffsschwellen und Lockerung des Subsidiaritätsgrundsatzes

Die Gesetzesbegründung führt zu § 9 LVerfSchG-E aus, dass das Bundesverfassungsgericht (BVerfG, Urteil v. 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07, Rn. 255 – juris, BVerfG, Beschluss v. 24. Januar 2012, 1 BvR 1299/05, Rn. 177 – juris; BVerfG, Urteil v. 24. April 2013, 1 BvR 1215/07, Rn. 117 – juris) „inzident“ zum Recht der Nachrichtendienste einen weniger detaillierten Regelungsansatz anerkannt habe und die Eingriffsschwellen für nachrichtendienstliche Gefahren-



erforschung in der Vergangenheit niedriger gesehen habe. Allerdings folgert das Bundesverfassungsgericht diese Anforderungen unmittelbar aus dem Verhältnismäßigkeitsgrundsatz, der generell gilt. Jedenfalls stellt sich die Frage, ob dies der Grund dafür sein soll, dass die Eingriffsschwellen in Bezug auf den Einsatz nachrichtendienstlicher Mittel herabgesenkt wurden. Zu dieser erheblichen Änderung schweigt die Gesetzesbegründung. Die Subsidiaritätsklausel des § 10 Abs. 4 S. 2 und S. 3 LVerfSchG soll sich – laut Synopse – nunmehr in § 5 S. 2 / § 8 Abs. 1 LVerfSchG-E wiederfinden. Die kritikwürdige Folge ist, dass der Subsidiaritätsgrundsatz als Ausdruck des Verhältnismäßigkeitsgrundsatzes im Vergleich zur vorherigen Rechtslage erheblich aufgeweicht wird. Dies führt insbesondere im Zusammenhang mit den abgesenkten Eingriffsschwellen zu einer deutlichen Steigerung der Grundrechtsintensität der Maßnahmen, die nach hiesiger Auffassung nicht gerechtfertigt ist. Es ist insoweit an den vorherigen Regelungen festzuhalten.

b) Der Einsatz nachrichtendienstlicher Mittel bei Minderjährigen

Der Minderjährigenschutz des § 17 LVerfSchG wurde im Rahmen der Novellierung gestrichen. Dafür wurde im Rahmen der allgemeinen Befugnisse nunmehr geregelt, dass der Einsatz nachrichtendienstlicher Mittel gegenüber Minderjährigen ab Vollendung des 10. Lebensjahres und bis zur Vollendung des 14. Lebensjahres ausnahmsweise zulässig ist, bei tatsächlichen Anhaltspunkten für die Planung, Begehung oder Verwirklichung einer der in § 3 Abs. 1 des Artikel 10-Gesetzes genannten Straftat (§ 9 Abs. 4 LVerfSchG-E).

Es steht zudem zu befürchten, dass die in der Gesetzesbegründung geäußerte Erwartung, dass die Regelung gewährleistet, dass sich die Beobachtung von unter 14-Jährigen mit nachrichtendienstlichen Mitteln nur auf Extremfälle der Planung, Begehung und Verwirklichung staatsgefährdender terroristischer Straftaten beschränkt, nicht bestätigt wird. In dem Straftatenkatalog des Art. 10-Gesetzes finden sich auch Straftaten, die bereits weit im Vorfeld einer möglichen Rechtsgutverletzung die Erfüllung des objektiven Tatbestandes ansetzen, insbesondere § 89a Strafgesetzbuch (StGB), der die Strafbarkeit der Vorbereitung einer schweren staatsgefährdenden Gewalttat normiert. Dieser ermöglicht die Bestrafung von Vorfeldhandlungen, insbes. solcher, die sich z.T. noch als Vorbereitungshandlung der Vorbereitungshandlung darstellen – vgl. z.B. nur das Sichverschaffen von Gegenständen gem. § 89a Abs. 2 Nr. 3 StGB, die für die Herstellung von Waffen usw. gem. Abs. 2 Nr. 2 wesentlich sind. Für die Natur dieses Straftatbestandes ist maßgeblich, dass die objektiven Kriterien nur in der Gesamtschau der subjektiven Voraussetzungen zu beurteilen sind (vgl. Paeffgen, in: Kindhäuser/Neumann (Hrsg.), Strafgesetzbuch, 5. Auflage 2017, § 89a Rn. 16). Wenn diese nicht bei der Einschätzung der Verfassungsschutzbehörde berücksichtigt werden, würde bereits der Baumarktbesuch eines 11jährigen, bei dem er Draht für den Bau seiner Martinslaterne kaufen möchte, geeignet sein, ihn mit nachrichtendienstlichen Mitteln zu beobachten. Mit diesem Beispiel soll an dieser Stelle der Verfassungsschutzbehörde nicht unterstellt werden, ohne Not Minderjährige überwachen zu wollen. Der Gesetzgeber muss sich jedoch bewusst sein, dass derartige Verweise in andere Gesetze wohl durchdacht werden sollten, insbesondere dann, wenn sie Rückwirkungen auf die Eingriffsschwelle der eigentlichen Befugnis haben, die die betroffenen Personen stärker belasten.

Auch wenn die Vorschrift flankiert wird von der in § 24 Abs. 4 LVerfSchG-E verkürzten Lösungsverpflichtung, reicht dies als verfahrenssichernde Maßnahme nicht aus. Derartige Maßnahmen sollten zumindest unter einem Amtsleitervorbehalt gestellt werden. Bestimmte Dokumentations-



verpflichtungen sollten die Entscheidungen, die einer Erhebung mit nachrichtendienstlichen Mitteln und Speicherung von personenbezogenen Daten von Minderjährigen zugrunde liegen, nachvollziehbar machen.

Auch die Altersgrenze ist im Vergleich zu ähnlich ausgerichteten Regelungsentwürfen sehr niedrig, so sieht z.B. § 10 des Entwurfs des vierten Gesetzes zur Änderung von Vorschriften auf den Gebiet des Verfassungsschutzrechts (HmbVerfSchG-E) die Schwelle der Ermöglichung eingriffsintensiver Maßnahmen bei 12 und nicht 10 Jahren vor.

2. Besondere Auskunftsverlangen (§ 13 LVerfSchG-E)

Die Möglichkeiten der Verfassungsschutzbehörde mittels besonderer Auskunftsverlangen Kreditinstitute, Telekommunikations- und Telemediendienste um Informationen und Auskünfte zu ersuchen, bestehen schon nach der derzeitigen Rechtslage. Insbesondere in Bezug auf Telekommunikations- und Telemediendienste wurden diese Befugnisse jedoch erweitert. Während zuvor die Daten, die beauskunftet werden müssen, in dem Gesetz selbst (§ 10 a Abs. 4 LVerfSchG) definiert und damit auch der Umfang bestimmt wurde, werden nunmehr dynamische Verweise auf Regelungen des Telekommunikationsgesetzes sowie auf das Telemediengesetzes gesetzt, die zur Folge haben, dass der Umfang der im Rahmen des Auskunftersuchen zur Verfügung gestellten Daten erweitert wird.

Eine weitere Änderung der Vorschrift betrifft den Adressatenkreis des zweiten Absatzes. Nach geltender Rechtslage war es der Verfassungsschutzbehörde möglich, im Einzelfall Auskünfte bei Luftfahrtunternehmen einzuholen. Nunmehr wurde dies auf alle "Verkehrsunternehmen" erweitert. Diese sollen nach der Gesetzesbegründung "u.a." auch Fernbus- und Eisenbahnunternehmen betreffen. Begründet werden diese Änderungen mit den Bedingungen eines globalisierten Fernreisemarkts. Zu den Auskünften sollen nunmehr Betreiber von Computerreservierungssystemen und globalen Distributionssystemen verpflichtet werden. Die Änderung hat eine Erweiterung der Befugnis dahingehend zur Folge, dass nunmehr eine nahezu durchgängige Kontrolle des individuellen Bewegungsverhaltens ermöglicht wird, was die Eingriffsintensität erheblich steigert (vgl. BVerfGE 120, 378 [Rn. 92]). Dieser Umstand wird durch die Formulierung "Absatz 2 S. 1 entspricht weitgehend der geltenden Regelung in § 10 a Abs. 2 LVerfSchG" bagatellisiert (Gesetzesbegründung S. 75).

3. Erhebung und Verarbeitung von Daten aus digitalen Medien (§ 20 LVerfSchG-E)

Die Regelung zur Erhebung und Verarbeitung von Daten aus digitalen Medien trägt dem Regelungsspielraum Rechnung, den das Bundesverfassungsgericht im Rahmen seiner Entscheidung zur Online-Durchsuchung eröffnet und zugleich begrenzt hat (vgl. BVerfG, Urteil vom 27. 2. 2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822). Insbesondere werden die eingriffsintensiveren Maßnahmen nach Abs. 2 unter einen Amtsleitervorbehalt als verfahrenssichernde Vorkehrung gestellt. Auf die Verhältnismäßigkeit derartiger Maßnahmen und ihre Einhegung ist besonderes Augenmerk zu richten. Entsprechende interne Anleitungen der Verfassungsschutzbehörde könnten hier hilfreich sein.



Der § 20 Absatz 3 regelt die Befugnis, verdeckt auf zugangsgesicherte digitale Medien oder Endgeräte zugreifen zu können. Dies soll "auf dem technisch vorgesehenen Weg" erfolgen. Diese unbestimmte und nicht normenklare Regelung greift in das Telekommunikationsgeheimnis nach Art. 10 GG ein, sieht jedoch keine der Eingriffsintensität entsprechenden verfahrenssichernde Vorkehrungen vor abseits von allgemeinen dynamischen Verweisungen in das Artikel 10-Gesetz sowie das Landesgesetz zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses. In dieser Form begegnet die Vorschrift verfassungsrechtlichen Zweifeln.

4. Zugriff auf Videoüberwachungsanlagen des öffentlich zugänglichen Raums (§ 21 LVerfSchG-E)

Besonders kritisch ist die neu geschaffene Möglichkeit des Zugriffes auf Videoüberwachungsanlagen des öffentlich zugänglichen Raums zu bewerten. Die Regelung entspricht nicht dem Bestimmtheitsgebot und dem Gebot der Normenklarheit, ist vor dem Hintergrund des Trennungsgabotes verfassungsrechtlich zweifelhaft und auch sicherheitspolitisch nicht überzeugend.

Die Videoüberwachung öffentlich zugänglicher Plätze und Bereiche nimmt stetig zu. Im Rahmen von zahlreichen Entschlüssen sprechen sich die Datenschutzaufsichtsbehörden des Bundes und der Länder mehrfach gegen Videoüberwachung und deren Ausweitung aus (z.B. "[Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken](#)" vom 30.3.2017 oder "[Videoüberwachungsverbesserungsgesetz](#)" zurückziehen!" vom 10.11.2016). Der Grund liegt unter anderem darin, dass mittels Videoüberwachung unzählige Daten Unbeteiligter, die keinerlei Anlass zur Überwachung gegeben haben, verarbeitet werden.

Des Weiteren ist Videoüberwachung ein Bereich, der stark vom technischen Fortschritt geprägt wird. Ein Fortschritt der zu schnell voranschreitet, als dass legislativ die technischen Möglichkeiten angemessen und auf ein erforderliches Maß beschränkt werden können. Dies zeigt eindrucksvoll die bereits seit drei Jahren geführte Diskussion, ob die polizeirechtlichen Videoüberwachungsbefugnisse (u.a. der Bundespolizei) den Einsatz von Kameras ermöglichen können, die mittels biometrischer Gesichtserkennung eine Identifizierung und Verfolgung und den Abgleich von betroffenen Personen zulassen.

Dabei ist anzumerken, dass im Bereich der Kontrolle der Videoüberwachung ein aufsichtliches Vollzugsdefizit besteht. Angesichts der erheblichen Anzahl von privaten und öffentlichen Betreibern, die den öffentlich zugänglichen Raum überwachen, ist es dem LfDI und auch den anderen Datenschutzaufsichtsbehörden kaum möglich, durch eine flächendeckende Kontrolle sicherzustellen, dass die Videoüberwachungsanlagen im Einklang mit geltendem Recht betrieben werden. Der von diesen unzulässigen Anlagen ausgehende ungerechtfertigte Eingriff in die Persönlichkeitsrechte der betroffenen Personen würde durch die Verwendung der Daten durch die Verfassungsschutzbehörde perpetuiert und vertieft.

Die in § 21 LVerfSchG-E geregelten Befugnisse nach Abs. 1 zur allgemeinen Aufgabenerfüllung nach § 5 LVerfSchG-E, also unter geringen Voraussetzungen auf verfügbare Einrichtungen zur Videoüberwachung zugreifen zu können und nach Abs. 2 auf gespeicherte Bild- und Tonaufzeichnungen aus dem öffentlichen Raum zugreifen zu können, eröffnen der Landesverfassungsschutz-



behörde damit den Zugang zu einer nicht bezifferbaren Anzahl von Datenverarbeitungsanlagen, ohne dass dies hinreichend bestimmt und rechtsstaatlich angemessen geregelt wird. Hier wird nicht klar, ob ein Zugriff in Echtzeit oder auch ein Zugriff auf vorhandene Aufzeichnungen gemeint ist.

Es ist zum einen nicht klar, ob die Regelung sich an private oder öffentliche Betreiber richtet, insbesondere auch an solche Videoüberwachungsanlagen von den Polizeibehörden. Dazu ist anzumerken, dass nach § 2 Abs.2 LVerfSchG-E der Verfassungsschutzbehörde als Ausprägung des Trennungsgebotes keine exekutiven polizeilichen Befugnisse, insbesondere keine Zwangsbefugnisse zustehen. Die Verfassungsschutzbehörde darf in der Folge die Polizeibehörde auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen, die sie selbst nicht durchführen darf (Gesetzesbegründung S. 56). Ein Zugriff auf vorhandene Daten der Polizei fällt unter Kooperation. Ein Zugriff auf Daten privater Betreiber, z.B. Einkaufszentren, wäre eine Befugnis der Verfassungsschutzbehörde unmittelbar gegenüber privaten Rechtssubjekten. Da der Begriff des öffentlichen Raumes fluid ist, wie auch die Fraport Entscheidung des Bundesverfassungsgerichts gezeigt hat, bedarf eine Eingriffsbefugnis der Verfassungsschutzbehörde konkreter Umgrenzungen. Der Vorschrift in der vorliegenden Form mangelt es an der verfassungsrechtlich erforderlichen Bestimmtheit.

Neben den Eingriffsschwellen fallen auch die Lösungsregelungen hinter denen des Landesdatenschutzgesetzes oder des Polizei- und Ordnungsbehördengesetzes weit zurück.

Wenn die Gesetzesbegründung anführt, dass die Auswertung von Videoüberwachung dem positiven Sicherheitsempfinden der Bürgerinnen und Bürger dienen kann, muss darauf hingewiesen werden, dass keinerlei Nachweis darüber geführt werden kann, dass Videoüberwachung objektiv die öffentliche Sicherheit verbessert. Im Gegenteil ist in Bezug auf das Sicherheitsempfinden der Bürgerinnen und Bürger zu berücksichtigen, dass sich bei diesen der Überwachungsdruck nicht nur in horizontaler Dimension verstärkt, sondern auch in vertikaler, wenn nunmehr die Befürchtung bestehen muss, neben Unternehmen und der Polizei auch nachrichtendienstlich erfasst zu werden, ohne dass dazu Anlass gegeben wurde und ohne dass es eine Möglichkeit gibt, sich dem zu entziehen. Empirische Belege, dass das Sicherheitsempfinden von Bürgerinnen und Bürgern durch einen Zugriff der Verfassungsschutzbehörde auf Videoüberwachungen des öffentlichen Raumes gesteigert würde, sind nicht ersichtlich.

Die Regelung ist ersatzlos zu streichen.

5. Verarbeitung personenbezogener Daten

a) Einwilligung als Verarbeitungsgrundlage (§ 23 Abs. 1 Nr. 6)

Die Einwilligung ist ein wichtiges Instrument des Datenschutzrechtes. Mittels einer Einwilligung können Datenverarbeitungen legitimiert werden, wenn keine Rechtsgrundlage die Datenverarbeitung trägt. Dabei ist die Einwilligung u.a. Ausdruck des Rechts auf informationelle Selbstbestimmung, welches jedermann das Recht verleiht, über die Verarbeitung seiner personenbezogenen Daten selbst zu bestimmen, also auch bestimmen zu können, dass seine Daten verarbeitet werden (BVerfGE 65, 1). Diese Entscheidung ist jedoch nur dann selbstbestimmt, wenn sie freiwillig, abseits von Zwang, sondern auf Augenhöhe und unter größtmöglicher Transparenz – also informiert – erfolgt. Das Element der Freiwilligkeit ist konstituierendes Element der Selbstbestimmung.



In einem Über- /Unterordnungsverhältnis, welches zwischen Sicherheitsbehörden und den betroffenen Bürgerinnen und Bürgern besteht, liegt es nahe, dass die betroffene Person nicht über eine Wahlmöglichkeit verfügt. Dies ist insbesondere dann nicht der Fall, wenn weitere Belange, wie etwa Jobsicherheit (z.B. im Anwendungsfeld von Zuverlässigkeitsüberprüfungen bei Akkreditierungsverfahren) hinzutreten. Des Weiteren dürften die Aufgaben der Verfassungsschutzbehörde und ihre größtenteils verdeckt erfolgende Beobachtungstätigkeit einer umfassenden Informierung der betroffenen Person entgegenstehen.

Des Weiteren verfügt die Verfassungsschutzbehörde spätestens nach diesem Gesetzesentwurf über umfangreiche Datenerhebungsbefugnisse. Dabei ist fraglich, welcher Anwendungsbereich für die Einwilligung als Datenverarbeitungsbefugnis überhaupt verbleibt. Es sollte im jeden Fall vermieden werden, eine unecht freiwillige Legitimation von Datenverarbeitungen der Verfassungsschutzbehörde zu schaffen, auf die zurückgegriffen werden kann, wenn die Voraussetzungen einer gesetzlichen Grundlage zur Datenverarbeitung nicht vorliegen. Die Regelung sollte gestrichen werden, wenn sie angesichts ihres Anwendungsbereiches für die praktische Durchführung der Aufgaben nicht erforderlich ist.

b) Befugnisse der zweckändernden Datenverarbeitung (§ 23 Abs. 4 LVerfSchG-E)

Im Rahmen des Urteils des Bundesverfassungsgerichts zum BKA-G wurden zudem Aussagen zur modifizierten Zweckbindung – der sog. hypothetischen Datenneuerhebung – geschaffen. Diese Neuerungen haben eine Modifikation des Zweckbindungsgrundsatzes zur Folge. Diese Modifikation, die zu Lasten des Rechts auf informationelle Selbstbestimmung gehen, wurde durch das Bundesverfassungsgericht insbesondere in Bezug auf heimliche und eingriffsintensive Überwachungsmaßnahmen geschaffen. Gerechtfertigt ist die Absenkung der Hürden für eine Zweckänderung in diesem Zusammenhang dadurch, dass die zweckändernde Nutzung bereits gewonnener Informationen zwar einen Eingriff in das Recht auf informationelle Selbstbestimmung und ggfs. das Telekommunikationsgeheimnis für sich begründet, diese jedoch nicht so tief sind, wie die Eingriffswirkung, die von einer theoretischen Datenneuerhebung ausgehen würde.

Vor diesem Hintergrund kann es jedoch nicht die Intention des Bundesverfassungsgerichts gewesen sein, jedwede Weiterverarbeitung und Übermittlung von personenbezogenen Daten zu erleichtern, sofern eine entsprechende Gleichwertigkeit in Bezug auf die Rechtsgüter besteht.

Falls die Landesregierung jedoch diese Möglichkeiten eröffnen möchte, müssen auch die weiteren Anforderungen des Bundesverfassungsgerichts, die an die Verarbeitung im Wege der hypothetischen Datenneuerhebung bestehen, umgesetzt werden. Dies betrifft insbesondere die Kennzeichnung der betreffenden Daten. Die Kennzeichnungspflichten sind verfahrensrechtliche Sicherungen, um die verfassungsrechtlichen Anforderungen an eine verhältnismäßige zweckändernde Verarbeitung zu gewährleisten (vgl. bereits BVerfG, Urt. v. 24. 4. 2013 – 1 BvR 1215/07 NJW 2013, 1499, Rn. 114 - unter Bezugnahme auf ständige Rechtsprechung). In diesem Zusammenhang sind in dem Entwurf eines Landesgesetzes zur Änderung des Polizei- und Ordnungsbehördengesetzes (POG-E) sowie beamtenrechtlicher Vorschriften umfassende Kennzeichnungspflichten vorgesehen, um die Einhaltung des Grundsatzes der hypothetischen Datenneuerhebung im Rahmen der polizeilichen Datenverarbeitung sicherzustellen (siehe die Gesetzesbegründung S. 138).



Eine entsprechende Regelung ist im Landesverfassungsschutzgesetz zwingend zu ergänzen.

6. Datenübermittlungen durch und an die Verfassungsschutzbehörde

a) Informationsübermittlungen an die Verfassungsschutzbehörde (§ 25 LVerfSchG-E)

Die in § 25 LVerfSchG-E geregelte Verpflichtung der öffentlichen Stellen des Landes Rheinland-Pfalz, der Verfassungsschutzbehörde von sich aus Informationen zu übermitteln, die für die Erfüllung der Aufgaben nach § 5 LVerfSchG-E erforderlich sind, wird im Gegensatz zu der vorherigen Regelung unter keine weitere eingrenzende Bedingung (wie ein Gewaltbezug) gestellt. Der Begründung nach soll die fachliche Einschätzung, ob diese Informationen sachdienlich sind, von der Verfassungsschutzbehörde vorgenommen werden.

Es wird klarstellend darauf hingewiesen, dass diese Übermittlungsverpflichtung keine für sich genommene Rechtsgrundlage zur Datenübermittlung für die jeweilige Stelle darstellt. Entsprechend des sog. "Doppeltürmodells" (BVerfGE 130, 151 [199 f., 201]) benötigen die betreffenden öffentlichen Stellen weiterhin eine eigene präzise und bereichsspezifische Ermächtigungsgrundlage, die eine entsprechende Datenübermittlung legitimiert.

Weitere datenschutzrechtliche und verfassungsrechtliche Bedenken bestehen in Bezug auf die Regelung in Abs. 6, die die Verfassungsschutzbehörde dazu ermächtigt, Personen und die von diesen benutzten oder eingesetzten Kraftfahrzeuge zur Mitteilung über das Antreffen in dem polizeilichen Informationssystem auszuschreiben. In der Gesetzesbegründung wird dazu ausgeführt, dass durch die Ausschreibung keine polizeiliche Aufgabenwahrnehmung veranlasst werde. Dem nachrichtendienstlichen Erkenntnisbedarf wird lediglich bei Gelegenheit polizeilicher Aufgabenwahrnehmung Rechnung getragen, ohne dass polizeiliche Befugnisse für nachrichtendienstliche Aufgaben ausgeübt werden.

Dem ist entgegenzusetzen, dass diese "Gelegenheiten" sich nicht nur auf Zufallsfunde im Rahmen von Verkehrskontrollen beziehen, sondern darüber hinaus durch die Befugnis der rheinland-pfälzischen Polizei zur automatisierten Kennzeichenerfassung (§ 27c PolG) und den darin erfolgenden Abgleich mit dem Fahndungsbestand der Polizei sich weitere Gelegenheiten eröffnen.

Auch wenn durch die Ausschreibung keine polizeiliche Aufgabenwahrnehmung veranlasst wird, führt die Ausübung eingriffsintensiver Befugnisse der Polizei doch zur Erfüllung nachrichtendienstlicher Aufgaben. Dies ist vor dem Hintergrund des Trennungsgebotes nicht tragbar und steht nicht im Einklang mit § 2 Abs. 2 LVerfSchG-E.

Die Erweiterung der Ausschreibungen um solche der Nachrichtendienste ist darüber hinaus vor dem Hintergrund der derzeitigen Überlegungen des Landes und des Bundes zur Schaffung eines länderübergreifenden Informationsverbundes sehr bedenklich, da etwaige Zugriffe auf die personenbezogenen Daten erweitert werden würden.

b) Informationsübermittlungen durch die Verfassungsschutzbehörde

In Bezug auf die Informationsübermittlungen durch die Verfassungsschutzbehörden gilt die Kritik zu den Befugnissen der zweckändernden Datenverarbeitung (§ 23 Abs. 4 LVerfSchG-E) entsprechend (s.o.).



Die Übermittlungsbefugnis in § 26 Abs. 4 LVerfSchG-E betrifft die Mitwirkung der Verfassungsschutzbehörden gem. § 6 Abs. 2 LVerfSchG-E. Angesichts der bereits bestehenden Praxis sowohl im Rahmen von Einstellungsverfahren Bediensteter im Sicherheitsbereich, insbesondere im Rahmen des Einstellungsverfahrens der Polizei des Landes Rheinland-Pfalz als auch im Rahmen von Akkreditierungsverfahren bei Großveranstaltungen, anlassbezogen die Verfassungsschutzbehörde zu involvieren, ist es begrüßenswert, dass nunmehr eine normenklare Regelung erfolgt, welche die Datenübermittlungen legitimiert. Dies war seitens des LfDI mehrfach gefordert worden. Die Bedenken, die gegen den Umfang und den zu niedrighschwelligem Anlass solcher Zuverlässigkeitsüberprüfungen im Rahmen der Stellungnahme des LfDI im Gesetzgebungsverfahren zur Novellierung des Polizei- und Ordnungsbehördengesetzes gem. §§ 27, 28 GGO am 16. September 2019 geäußert wurden, werden aufrechterhalten. Die Mitwirkung sowie die Datenübermittlungen zum Zwecke der Zuverlässigkeitsüberprüfungen sollten angesichts der erheblichen Bindung von Ressourcen der Verfassungsschutzbehörde in Ausnahmefällen angezeigt sein und sich nicht zu einer Regelabfrage steigern.

IV . Datenschutzkontrolle des LfDI

1. Abhilfebefugnisse des LfDI

Grundsätzlich ist begrüßenswert, dass die Datenschutzkontrolle durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz gesondert in § 30 LVerfSchG-E geregelt wurde sowie bestimmte Regelungen des Landesdatenschutzgesetzes durch § 39 LVerfSchG-E für anwendbar erklärt wurden. Des Weiteren ist die Funktion des Landesbeauftragten aufrechterhalten worden, im Rahmen von Betroffenenrechten, insbesondere dem Auskunftsrecht als Instanz des individuellen Rechtsschutzes die Verweigerung einer Auskunft nach § 29 Abs. 2 LVerfSchG-E überprüfen zu können (§ 29 Abs. 3 LVerfSchG-E). Die datenschutzrechtlichen Bestimmungen, die in § 30 Abs. 1 Satz 1 LVerfSchG-E angesprochen sind, umfassen insbesondere Regelungen zur Erhebung und Übermittlung von Daten durch die Verfassungsschutzbehörde.

Diese Möglichkeit und Befugnis des Landesbeauftragten zur Kontrolle der Verfassungsschutzbehörde ist jedoch nur dann zielführend, wenn dieser entsprechende Abhilfebefugnisse erhält, um Datenschutzverstößen abhelfen zu können. Die datenschutzrechtliche Kontrolle kann nur dann im Rahmen des kompensatorischen Grundrechtsschutzes eingriffsintensive Maßnahmen rechtfertigen, wenn sie entsprechend effektiv ist. Nach der Rechtsprechung des Bundesverfassungsgericht setzt die Gewährleistung einer wirksamen aufsichtlichen Kontrolle eine mit wirksamen Befugnissen ausgestattete Stelle voraus (vgl. grundlegend BVerfGE 65, 1 [46] = NJW 1984, 419) NJW 2016, 1781, beck-online). In diesem Zusammenhang ist begrüßenswert, dass der LfDI zumindest das Recht zur Beanstandung gem. § 42 Abs. 1 LDSG hat.

Mit Blick auf die Synopse ist jedoch auffällig, dass in vielen Ländern die Befugnisse der Datenschutzaufsichtsbehörde weiter gehen. Da dieser Gesetzesentwurf im Vergleich zu denen anderer Bundesländer anstreben sollte, die Freiheitsrechte der betroffenen Personen bei größtmöglicher Funktionalität der Verfassungsschutzbehörde zu gewährleisten, sollte die Datenschutz-



aufsicht als Institution des kompensatorischen Grundrechtsschutzes entsprechend stark ausgestattet werden.

2. Einschränkungen der Sicherheit des Bundes oder eines Landes

Das infolge der datenschutzrechtlichen Kontrolle bestehende Auskunfts- und Einsichtsrecht des LfDI kann dann eingeschränkt werden, wenn das fachlich zuständige Ministerium im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet werden würde. Wie bereits im Landesdatenschutzgesetz als auch dem Polizei- und Ordnungsbehördengesetz stößt diese Vorschrift auf Bedenken. Angesichts des Ausnahmecharakters der Vorschrift ist eine restriktive Auslegung angezeigt, die eine Auskunftsverweigerung nur in engen Grenzen rechtfertigt. Die Verweigerung kann indes nicht auf die generelle Geheimhaltungsbedürftigkeit gestützt werden. Der LfDI ist zur Verschwiegenheit verpflichtet und er stellt sicher, dass die zuständigen Mitarbeiter und Mitarbeiterinnen ausreichend sicherheitsüberprüft sind.

Angesichts des Eingriffs in die Rechtspositionen des LfDI sollte die Entscheidung dokumentiert werden, um im Zweifel einer gerichtlichen Entscheidung Stand zu halten. Diese Voraussetzung wurde in den ähnlichen Vorschriften des Landesdatenschutzgesetzes und des Polizei- und Ordnungsbehördengesetzes implementiert und sollte auch hier geregelt werden.

3. Sicherheitsüberprüfung

Die Regelung in § 30 Abs. 3 LVerfSchG-E, dass die datenschutzrechtliche Kontrolle nur durch Be dienstete des LfDI ausgeübt werden kann, die nach § 12 Landessicherheitsüberprüfungsgesetz ermächtigt sind, ist zu weitgehend. Es ist den Regelungen des Landessicherheitsüberprüfungsgesetzes immanent, dass nur die Personen Zugriff auf bzw. Zugang zu besonders geheimhaltungsbedürftigen Daten haben dürfen, die entsprechend sicherheitsüberprüft sind. Beim LfDI sind entsprechend bestimmte Mitarbeiter nach dem Landessicherheitsüberprüfungsgesetz verpflichtet und berechtigt. Die Einhaltung dieser Vorgaben wird durch den Geheimschutzbeauftragten des LfDI gewährleistet. Es ist nicht nachvollziehbar, warum die Mitarbeiter pauschal der eingriffsintensiven Sicherheitsüberprüfung unterzogen werden sollen, obwohl die gesetzlichen Vorgaben sich nach anlassbezogenen Geheimhaltungsbedürfnissen richten und der LfDI dafür Sorge trägt, dass die Vorgaben des Landessicherheitsüberprüfungsgesetzes eingehalten werden.

Vergleichbare Regelungen sind weder im Bundesverfassungsschutzgesetz noch in entsprechenden Gesetzen der Länder geregelt. Die Regelung ist ersatzlos zu streichen.

4. Verweis auf das Landesdatenschutzgesetz

Es fehlen Verweise auf Regelungen des technisch-organisatorischen Datenschutzes. Angesichts der Regelung zum automatisierten Datenabruf gem. § 25 Abs. 5 LVerfSchG-E sind zum einen Protokollierungsregelungen entsprechend denen des § 60 LDSG aufzunehmen. Des Weiteren sollten zudem auch seitens der Verfassungsschutzbehörde die Pflicht zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten (nach alter Rechtslage Verfahrensverzeichnis § 10 LDSG a.F.) sowie zur Datenschutz-Folgenabschätzung (ähnlich zur nach alter Rechtslage bestehenden Vorabkontrolle gem. § 9 Abs. 5 LDSG a.F.) bestehen. Die Bereichsausnahme der Verfassungsschutzbehörde aus dem Anwendungsbereich der Datenschutz-Grundverordnung und damit auch aus weiten



Teilen des Landesdatenschutzgesetzes darf nicht dazu führen, dass das Datenschutzniveau der Datenverarbeitung der Verfassungsschutzbehörde im Vergleich zur alten Rechtslage herabgesenkt wird. Entsprechend sind in den Verweis die Regelungen des § 53 LDSG (Anforderungen an die Sicherheit der Verarbeitung), des § 56 (Durchführung einer Datenschutz-Folgenabschätzung) sowie des § 58 (Verzeichnis von Verarbeitungstätigkeiten) aufzunehmen.

V. Fazit

Der Gesetzesentwurf hat zum Ziel, der Verfassungsschutzbehörde eine effektivere Aufgabenerfüllung zu ermöglichen. Dazu führt er neue und erweiterte Befugnisse ein. Dem Grunde nach ist diese Zielrichtung nachvollziehbar. Die Änderungen führen jedoch teils zu einer Absenkung der Eingriffsschwellen und zu zahlreichen – teilweise erweiterten – Datenverarbeitungsbefugnissen der Verfassungsschutzbehörde, die zu Lasten der Freiheitsrechte Einzelner gehen.

Deutlich wird dies insbesondere durch die Schaffung eingriffsintensiver Überwachungsbefugnisse, wie z.B. der Funkzellenabfrage (§ 14 LVerfSch-G) und der Erweiterung der Verkehrs- und Bestandsdatenauskunft (§ 13 LVerfSch-G), durch Erweiterung der allgemeinen Befugnisse (§ 9 LVerfSchG-E), durch die Herabsenkung des Minderjährigenschutzes und durch die geschaffenen Befugnisse zum Zugriff auf digitale Medien (§ 20 LVerfSch-G) und dem Zugriff auf Einrichtungen der Videoüberwachung, die den öffentlich zugänglichen Raum überwachen (§ 21 LVerfSchG-E). Darüber hinaus fallen zudem die erweiterten zweckändernden Datenverarbeitungsgrundlagen und Rechtsgrundlagen zur Datenübermittlung ins Gewicht bei der Beurteilung der Verhältnismäßigkeit des Gesetzesentwurfs im Ganzen.

Auch wenn diese Maßnahmen von einer umfangreichen Aufsicht und Kontrolle durch die parlamentarische Kontrollkommission sowie die nach dem Landesgesetz zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses gebildete Kommission und nicht zuletzt durch den LfDI flankiert werden, sollten weitere Regelungen geschaffen werden, die den Grundrechtsschutz durch Verfahren gewährleisten. Dazu zählen neben Benachrichtigungspflichten auch Vorkehrungen zur Ermöglichung einer effektiven Kontrolle im Wege von Kennzeichnungs- und Protokollierungspflichten.

Erweiterte Aufgaben der Verfassungsschutzbehörde müssen mit der Einräumung der dazu erforderlichen Befugnisse einhergehen. Jedoch ist angesichts des verfassungsrechtlichen Trennungsgebotes an die Bewertung der Erforderlichkeit ein strenger Maßstab anzulegen. Dieser betrifft nicht nur das „Ob“, sondern auch das „Wie“ der Befugnisse. Dazu ist die Bestimmtheit und Normenklarheit ein wesentlicher Gesichtspunkt, dem in dem Entwurf nicht hinreichend Rechnung getragen ist. Je mehr Befugnisse zu Eingriffen in Grundrechte die Verfassungsbehörde erhält, desto stärker wirkt auch der Grundrechtsschutz durch Verfahren. Dies begründet Nachbesserungsbedarf an dem Entwurf.