Bundesrat **Drucksache 227/17**

21.03.17

Gesetzesantrag
des Freistaates Bayern

Entwurf eines ... Gesetzes zur Änderung des Bundesverfassungsschutzgesetzes - Befugnis zur Online-Datenerhebung

A. Problem

Deutschland wird in einer neuen Dimension durch den internationalen Terrorismus bedroht. Terroristen nutzen die Mittel der modernen Informationstechnik, um sich mit großer Geschwindigkeit über alle staatlichen Grenzen hinweg auszutauschen und ihre Pläne vor den Augen der Sicherheitsbehörden zu verbergen. Klassische nachrichtendienstliche Instrumente sind dieser geänderten Bedrohungslage nicht mehr gewachsen. Eine effektive Sicherheitsarchitektur erfordert, dass die dem Verfassungsschutz zur Verfügung stehenden Instrumente mit der technischen Entwicklung Schritt halten. Es ist daher geboten, dem Bundesamt für Verfassungsschutz auch die Befugnis zum verdeckten Eingriff in informationstechnische Systeme einzuräumen.

B. Lösung

Dem Bundesamt für Verfassungsschutz wird in Anlehnung an § 20k des Bundeskriminalamtgesetzes (BKAG) die Befugnis eingeräumt, mit technischen Mitteln verdeckt in informationstechnische Systeme einzugreifen.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0720-2946

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Keiner.

E.2 Erfüllungsaufwand für die Wirtschaft

Keiner.

E.3 Erfüllungsaufwand der Verwaltung

Keiner.

F. Weitere Kosten

Keine

Bundesrat **Drucksache 227/17**

21.03.17

Gesetzesantrag
des Freistaates Bayern

Entwurf eines ... Gesetzes zur Änderung des Bundesverfassungsschutzgesetzes - Befugnis zur Online-Datenerhebung

Der Bayerische Ministerpräsident München, 21. März 2017

An die
Präsidentin des Bundesrates
Frau Ministerpräsidentin
Malu Dreyer

Sehr geehrte Frau Präsidentin,

gemäß dem Beschluss der Bayerischen Staatsregierung übermittle ich den als Anlage mit Vorblatt und Begründung beigefügten

> Entwurf eines … Gesetzes zur Änderung des Bundesverfassungsschutzgesetzes – Befugnis zur Online-Datenerhebung

mit dem Antrag, dass der Bundesrat diesen gemäß Artikel 76 Absatz 1 GG im Bundestag einbringen möge.

Ich bitte, den Gesetzentwurf gemäß § 36 Absatz 2 GO BR auf die Tagesordnung der 956. Sitzung am 31. März 2017 zu setzen und anschließend den Ausschüssen zur Beratung zuzuweisen.

Mit freundlichen Grüßen
Horst Seehofer

Entwurf eines … Gesetzes zur Änderung des Bundesverfassungsschutzgesetzes - Befugnis zur Online-Datenerhebung

Vom …

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1
Änderung des Bundesverfassungsschutzgesetzes

§ 9 des Bundesverfassungsschutzgesetzes vom 20. Dezember 1990 (BGBl. I S. 2954), das zuletzt durch Artikel 4 des Gesetzes vom 4. November 2016 (BGBl. I S. 2473) geändert worden ist, wird wie folgt geändert:

1. Nach Absatz 2 wird folgender Absatz 2a eingefügt:

„(2a) [1]Das Bundesamt für Verfassungsschutz darf mit technischen Mitteln nur verdeckt auf informationstechnische Systeme zugreifen und aus ihnen Daten erheben, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraums eine zumindest nach ihrer Art oder der hierfür verantwortlichen Person konkretisierte Schädigung von

1. Leib, Leben oder Freiheit einer Person oder
2. solcher Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt,

eintritt und die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. [2]Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

[3]Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen.[4]Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen. [5]Bei jedem Einsatz des technischen Mittels sind zu protokollieren

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,
2. die Zielperson sowie die mitbetroffenen Personen,
3. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
4. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
5. die Organisationseinheit, die die Maßnahme durchführt.

[6]Die Protokolldaten dürfen nur verwendet werden, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach Satz 1 rechtmäßig durchgeführt worden ist. [7]Sie sind bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann automatisiert zu löschen, es sei denn, dass sie für den in Satz 6 genannten Zweck noch erforderlich sind. [8]Absatz 2 Satz 3 bis 8 gilt entsprechend.“

2. In Absatz 3 wird nach der Angabe „Absatz 2“ die Angabe „ , 2a“ eingefügt.

Artikel 2
Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

Deutschland wird in einer neuen Dimension durch den internationalen Terrorismus bedroht. Nicht mehr hierarchische Strukturen, sondern autonome Terrorzellen und radikalisierte Einzeltäter bedrohen das freiheitliche Zusammenleben der Menschen. Große Bedeutung für die veränderte Form der Bedrohung hat die moderne Informationstechnik. Geschwindigkeit und Reichweite der Kommunikation haben sich in den vergangenen zwei Jahrzehnten vervielfacht. Menschen gleicher Gesinnung vernetzen sich weltweit und knüpfen Kontakte zu Menschen, denen sie noch nie persönlich begegnet sind. Extremistische und terroristische Inhalte können ungefiltert eingestellt und verbreitet werden. Die zunehmende Vernetzung bietet terroristischen Strukturen neue Möglichkeiten zu arbeitsteiligem weltweitem Zusammenwirken.

Klassische nachrichtendienstliche Instrumente wie Telefonüberwachung, Observation oder Informanten sind dieser geänderten Bedrohungslage nicht mehr gewachsen. Es reicht nicht mehr aus, in bereits bekannte Organisationen einzudringen. Vielmehr müssen bislang unbekannte Gefährder identifiziert und an der Ausführung ihrer Pläne gehindert werden. Der Verfassungsschutz wird insoweit nicht nur tätig im Spannungsfeld zwischen den Grundrechten derer, die von seinen Maßnahmen betroffen sind und dem Sicherheitsinteresse der Allgemeinheit. Seine Befugnisse sind zugleich Ausdruck der Wehrhaftigkeit des demokratisch verfassten Rechtsstaats.

Eine effektive Sicherheitsarchitektur erfordert, dass die dem Verfassungsschutz zur Verfügung stehenden Instrumente mit der technischen Entwicklung Schritt halten. Es ist daher geboten, dem BfV auch die Befugnis zum verdeckten Eingriff in informationstechnische Systeme einzuräumen.

Das Bundesverfassungsgericht hat eine solche Maßnahme unter bestimmten strengen Voraussetzungen für verfassungsrechtlich zulässig gehalten (BVerfGE 120, 274/315 ff.; BVerfG, Urt. v. 20. April 2016, 1 BvR 966/09 u.a., Rn. 208 ff.). Es hat dabei hervorgehoben, dass das von ihm formulierte „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ nicht schrankenlos gewährleistet ist. Eingriffe in diese Rechtsposition können für den Bereich der Gefahrenabwehr zum Schutz für ein überragend wichtiges Rechtsgut gerechtfertigt werden. Überragend wichtig sind Leib, Leben, Freiheit der Person sowie solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staa-

tes oder die Grundlagen der Existenz der Menschen berührt. Dabei kann die Maßnahme schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen oder darauf zulassen, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann (BVerfG, Urt. v. 20. April 2016, 1 BvR 966/09 u.a., Rn. 112).

Es ist daher verfassungsrechtlich zulässig und zur Gewährleistung der inneren Sicherheit auch geboten, dem BfV die Befugnis zum verdeckten Eingriff in informationstechnische Systeme einzuräumen.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Bundesverfassungsschutzgesetzes)

Zu Nummer 1 (§ 9 Absatz 2a BVerfSchG)

Der neue Absatz 2a, der unmittelbar nach der ähnlich eingriffsintensiven Befugnis zur verdeckten Wohnraumüberwachung in Absatz 2 eingefügt wird, orientiert sich an § 20k des Bundeskriminalamtgesetzes (BKAG) und berücksichtigt auch die Vorgaben des hierzu ergangenen Urteils des Bundesverfassungsgerichts.

Satz 1 erlaubt dem BfV zum Schutz hochrangiger Rechtsgüter verdeckt durch technische Mittel in informationstechnische Systeme einzugreifen und aus ihnen Daten zu erheben. Umfasst ist dabei auch das Kopieren bestimmter Dateien von der Festplatte eines Rechners und deren elektronische Übertragung an das BfV sowie der Einsatz sogenannter Key-Logger, bei denen die Tastatureingaben erfasst werden, ohne dass notwendigerweise ein Zwischenspeichern auf der Festplatte erfolgt.

Der Begriff des informationstechnischen Systems ist bewusst weit gewählt, um alle nach der Rechtsprechung des Bundesverfassungsgerichts schutzbedürftigen informationstechnischen Systeme zu erfassen.

Die Rechtfertigung einer Maßnahme setzt nicht notwendigerweise voraus, dass eine Rechtsgutschädigung bereits unmittelbar bevorsteht. In Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts ist vielmehr eine Gefahrenprognose erforderlich, dass bestimmte Tatsachen auf eine im Einzelfall für die benannten Rechtsgüter bestehende Gefahr hinweisen. Maßgebliche Kriterien für die Gefahren-

schwelle sind: der Einzelfall, die zeitliche Nähe einer Rechtsgutschädigung und die Konkretisierung entweder nach der Art und Weise des schädigenden Ereignisses oder für die Gefährdung verantwortlichen Personen (BVerfG, Urt. v. 20. April 2016, 1 BvR 966/09 u.a., Rn. 112).

In Konkretisierung des Grundsatzes der Verhältnismäßigkeit darf die Maßnahme nur durchgeführt werden, wenn die Sachverhaltserforschung ansonsten aussichtslos oder wesentlich erschwert wäre.

Satz 2 verpflichtet das BfV bei der Durchführung der Maßnahme zu bestimmten technischen Schutzvorkehrungen, um den Eingriff in das infiltrierte System auf das unbedingt erforderliche Mindestmaß zu begrenzen und die Datensicherheit zu gewährleisten.

Satz 2 Nummer 1 bestimmt zunächst, dass beim Einsatz des technischen Mittels sicherzustellen ist, dass an dem IT-System nur solche Veränderungen vorgenommen werden, die für die Datenerhebung unbedingt erforderlich sind. Vor nicht unbedingt erforderlichen Veränderungen zu schützen sind nicht nur die von dem Nutzer des informationstechnischen Systems angelegten Anwenderdateien, sondern auch die für die Funktion des IT-Systems erforderlichen Systemdateien. Auch Beeinträchtigungen der Systemleistung sind auf das technisch Unvermeidbare zu begrenzen.

Satz 2 Nummer 2 schreibt vor, bei Beendigung der Maßnahme alle an dem infiltrierten System vorgenommenen Veränderungen rückgängig zu machen, soweit dies technisch möglich ist. Insbesondere ist die auf dem IT-System installierte Überwachungssoftware vollständig zu löschen und sind Veränderungen an den bei der Installation der Überwachungssoftware vorgefundenen Systemdateien – möglichst automatisiert, andernfalls manuell – rückgängig zu machen.

Satz 3 bestimmt in Anlehnung an § 14 Absatz 1 der Telekommunikations-Überwachungsverordnung (TKÜV), dass das eingesetzte technische Mittel gegen unbefugte Nutzung zu schützen ist. Insbesondere hat das BfV dafür Sorge zu tragen, dass die eingesetzte Software nicht durch Dritte (Hacker) zweckentfremdet werden kann. Insbesondere ist sicherzustellen, dass die Software nicht ohne erheblichen Aufwand dazu veranlasst werden kann, an einen anderen Server als den vom BfV verwendeten zurückzumelden, und dass die Software weder von Unbefugten erkannt noch angesprochen werden kann. Die Verpflichtung, das eingesetzte Mittel „nach dem Stand der Technik“ gegen unbefugte Nutzung zu schützen, bedeutet, dass sich

das BfV der fortschrittlichsten technischen Verfahren bedienen muss, die nach Auffassung führender Fachleute aus Wissenschaft und Technik auf der Grundlage neuester wissenschaftlicher Erkenntnisse erforderlich sind. Hierfür muss es die einschlägigen Aktivitäten auf den Gebieten der Wissenschaft und Technik umfassend und sorgfältig beobachten und auswerten.

Satz 4 schützt in Anlehnung an § 14 Absatz 2 Satz 1 TKÜV die Integrität und Authentizität der von dem technischen Mittel zum Zwecke der Ausleitung an das BfV bereitgestellten Daten vom Zeitpunkt der Bereitstellung für die Übertragung an das BfV an, während der Datenübertragung an das BfV sowie während ihrer Speicherung beim BfV. Die Daten sind vor ihrer Übertragung an das BfV zu verschlüsseln und beim BfV beweissicher zu speichern, insbesondere mit einer elektronischen Signatur und einem elektronischen Zeitstempel zu versehen.

Satz 5 bis 7 enthält Vorschriften über die Protokollierung der Maßnahme. Sie entsprechen § 20k Absatz 3 BKAG. Darüber hinausgehend wird auch die Protokollierung der Zielperson sowie der mitbetroffenen Personen vorgeschrieben.

Satz 8 erklärt hinsichtlich des einzuhaltenden Verfahrens die Vorschriften zur verdeckten Wohnraumüberwachung in § 9 Absatz 2 Satz 3 bis 8 BVerfSchG für entsprechend anwendbar. Ein solcher Gleichlauf des Verfahrens wird durch die Rechtsprechung des Bundesverfassungsgerichts nahe gelegt (BVerfG, Urt. v. 20. April 2016, 1 BvR 966/09 u.a., Rn. 108, 115, 117 f.). Demnach dürfen Maßnahmen zum verdeckten Eingriff in informationstechnische Systeme grundsätzlich nur durch den Richter angeordnet werden. In Eilfällen erfolgt die Anordnung durch den Präsidenten des BfV oder seinen Vertreter; die richterliche Entscheidung ist unverzüglich nachzuholen. Die gewonnenen Informationen unterliegen zudem besonderen Beschränkungen hinsichtlich der Übermittlung und weiteren Verwendung durch den Empfänger.

Zu Nummer 3 (§ 9 Absatz 3 BVerfSchG)

Verdeckte Maßnahmen, die in das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ eingreifen, weisen nach der Rechtsprechung des Bundesverfassungsgerichts eine der verdeckten Wohnraumüberwachung vergleichbare Eingriffsintensität auf (vgl. BVerfG, Urt. v. 20. April 2016, 1 BvR 966/09 u.a., Rn. 210). Wie bei der Wohnraumüberwachung bedarf es daher auch beim Zugriff auf informationstechnische Systeme grundrechtssichernder Verfahrensvorschriften in Form von Pflichten zur nachträglichen Benachrichtigung des

Betroffenen und zur Unterrichtung des Parlamentarischen Kontrollgremiums (vgl. BVerfG, Urt. v. 20. April 2016, 1 BvR 966/09 u.a., Rn. 136 und 143)

Zu Artikel 2 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten des Gesetzes (Artikel 82 Absatz 2 Satz 1 GG).