

## Stellungnahme

### **Zum Gesetzentwurf zur Änderung des Bayerischen Verfassungsschutzgesetzes, des Ausführungsgesetzes Art.10 Gesetz und des Parlamentarischen Kontrollgremium-Gesetzes**

11. März 2008

Seite 1

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.100 Unternehmen, davon 850 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien.

#### **Zusammenfassung**

Das Bayerische Staatsministerium des Inneren hat am 12. Februar 2008 einen Entwurf für ein Gesetz zur Änderung des Bayerischen Verfassungsschutzgesetzes, des Ausführungsgesetzes Art.10 Gesetz und des Parlamentarischen Kontrollgremium-Gesetzes vorgelegt. Das Gesetz betrifft die vom BITKOM vertretene ITK-Industrie durch die vorgesehenen Änderungen des Landesverfassungsschutzgesetzes (BayVSG), und zwar unmittelbar hinsichtlich der

- Auskunftsrechte (Bestands- und Verkehrsdaten) des BayVSG-E nach Art. 6c Abs. 1 und 2
- mangelnden Entschädigung für diese Auskünfte nach Art. 6c Abs. 1 und 2 BayVSG-E
- Pflicht zur Beauskunftung von Verkehrsdaten (Standorte) von Teilnehmern im sog. Idle-Mode (keine aktive Verbindung, sondern z.B. Location update) nach Art. 6c Abs. 2 Nr. 4 BayVSG-E
- Regelung zum Einsatz des IMSI-Catchers; Art. 6c Abs. 4 BayVSG-E

Hier sehen wir noch Überarbeitungsbedarf, weil die vorgesehenen Normen teilweise zu besonderen Belastungen auf Seiten der Unternehmen führen, die vermieden werden sollten.

Mittelbar betroffen ist die vom BITKOM repräsentierte Branche durch die vorgesehene Befugnis zur verdeckten „Online Durchsuchung“ insoweit, als die Befugnisnorm auch Maßnahmen gegen Nachrichtenmittler vorsieht und zwar bezogen auf jegliche Arten „informationstechnischer Systeme“. Da der Begriff des Nachrichtenmittlers auch in der Begründung nicht präzisiert wird, besteht die Gefahr, dass entsprechende Maßnahmen gegen Mail-Server und anderer Serverstrukturen von Unternehmen im Rahmen von Ermittlungen gegen Privatpersonen, die auf diese Strukturen Zugriff haben, gerichtet werden. Dies widerspricht aus Sicht des BITKOM dem Grundsatz der Verhältnismäßigkeit, weil gegenüber den Nachrichtenmittlern, anders als gegenüber dem Verdächtigen selbst keine Heimlichkeit der Maßnahme erforderlich ist. Überdies ist die weite Einbeziehung von informationstechnischen Systemen aller Art insgesamt geeignet, das allgemeine Nutzervertrauen in IT-Systeme zu unterminieren.

Bundesverband  
Informationswirtschaft,  
Telekommunikation und  
neue Medien e.V.

Albrechtstraße 10 A  
10117 Berlin-Mitte  
Tel. +49. 30. 27576-0  
Fax +49. 30. 27576-400  
bitkom@bitkom.org  
www.bitkom.org

#### **Ansprechpartner**

Dr. Guido Brinkel  
Bereichsleiter  
Telekommunikations- und  
Medienpolitik  
Tel. +49. 30. 27576-221  
Fax +49. 30. 27576-51-221  
g.brinkel@bitkom.org

#### **Präsident**

Prof. Dr. Dr. h. c. mult.  
August-Wilhelm Scheer

#### **Hauptgeschäftsführer**

Dr. Bernhard Rohleder

## **Stellungnahme**

Zur Änderung des Bayerischen Verfassungsschutzgesetzes

Seite 2

Dies führt mittelbar zu Wettbewerbsnachteilen für die deutsche ITK-Industrie, weil Nutzer zunehmend auf ausländische Angebote ausweichen werden.

Schließlich ist die derzeitige Ausgestaltung der Befugnisnorm aus mehreren Gründen nicht mit den vom Bundesverfassungsgericht in seiner Entscheidung vom 27. Februar herausgestellten Anforderungen in Einklang zu bringen.

## Stellungnahme

Zur Änderung des Bayerischen Verfassungsschutzgesetzes

Seite 3

Inhalt	Seite
1 Allgemeines .....	4
2 Prognose zum Umfang der künftig tatsächlich anfallenden Maßnahmen .....	4
3 Fehlende Entschädigungsregelung.....	4
4 Umfang der Beauskunftung nach Art. 6c Abs. 2 Nr. BayVSG-E.....	5
5 Regelung zum Einsatz des IMSI-Catchers; Art. 6c Abs. 4 BayVSG-E.....	6
6 Verdeckte „Online-Durchsuchung“; § 6e, f BayVSG-E .....	6
6.1 Verfassungsrechtliche Anforderungen .....	6
6.2 Begriff der informationstechnischen Systeme in Art. 6e BayVSG-E .....	7
6.3 Adressatenkreis – Einbeziehung von Nachrichtennetzwerk.....	8

## **Stellungnahme**

Zur Änderung des Bayerischen Verfassungsschutzgesetzes

Seite 4

### **1 Allgemeines**

BITKOM begrüßt die klare Struktur des novellierten BayVSG und die nunmehr eindeutige Identifizierung der Rechte des Landesamtes für Verfassungsschutz im Gesetzentwurf. Insbesondere ist durch Art. 6c BayVSG-E nunmehr eindeutig die Ermächtigung zur Erhebung von Bestands- und Verkehrsdaten geregelt. Desweiteren unterscheidet der Entwurf klar zwischen der Datenerhebung durch Inanspruchnahme Dritter und durch eigene Mittel. Dadurch ist die Zusammenarbeit der TK-Unternehmen mit dem Landesamt für Verfassungsschutz organisatorisch und technisch einfach umsetzbar. Wir begrüßen außerdem - mit Ausnahme der Regelungen zur verdeckten Online-Durchsuchung - die klare Regelung der Eingriffsvoraussetzungen sowie das vorgesehene hohe Maß an Kontrolle und Transparenz. Insbesondere die Anforderung, dass ein Tätigwerden in der Regel nur unter Anordnung der Behördenleitung und vorausgegangener Bestätigung der Kontrollgremien möglich sein soll, verstehen wir als Signal zum Schutz der grundgesetzlich geschützten Vertraulichkeit von früherer, aktueller oder zukünftiger Kommunikation.

### **2 Prognose zum Umfang der künftig tatsächlich anfallenden Maßnahmen**

Seitens der Telekommunikations-Industrie kann die in der Einleitung und Begründung vorgenommene Prognose der tatsächlich anfallenden Maßnahmen nicht geteilt werden. Auch wenn statistisch gesehen in den letzten Jahren die Anfragen der Verfassungsschutzbehörden bei den Telekommunikations-Unternehmen der Zahl nach gering waren muss für die Zukunft von einem erheblichen Anstieg ausgegangen werden. Insbesondere wird die gezielt angestrebte Absenkung der Eingriffsvoraussetzungen nach § 6 Abs. 2 BayVSG-E auf „schwerwiegende Gefahren“ zu diesem Anstieg beitragen, da ausweislich der Entwurfsbegründung zu § 6 Abs. 2 BayVSG-E kein konkreter Straftatenbezug gegeben sein muss.

### **3 Fehlende Entschädigungsregelung**

Der vorgelegte Entwurf zum BayVSG enthält keinerlei Entschädigungstatbestände hinsichtlich der statuierten Auskunftspflichten. Bereits mit der Novellierung des TKG 2004 wurde in § 110 Abs. 9 eine Pflicht des Gesetzgebers zur Regelung einer angemessenen Entschädigung für Auskunftersuchen und Überwachungsmaßnahmen statuiert. Diese Entschädigung soll nach dem eindeutigen Wortlaut auch Maßnahmen nach den landesrechtlichen Ermächtigungen in diesem Bereich umfassen. Eine Ausnahme für bestimmte Behörden wurde nicht aufgenommen. Auf Bundesebene wird aktuell das TKEntschNeuOG beraten, das insbesondere die Entschädigung für Maßnahmen nach der StPO nach dieser Maßgabe regelt. Es ist somit mittlerweile anerkannt, dass Telekommunikationsunternehmen, die für staatliche Maßnahmen in Anspruch genommen werden, eine angemessene Entschädigung für die erbrachten Leistungen zusteht.

Der BITKOM fordert daher, der aus § 110 Abs. 9 folgenden Verpflichtung zur Schaffung einer Rechtsgrundlage für Entschädigungen nachzukommen. Wir präferieren dabei im Sinne aller Beteiligten eine Pauschalregelung, wie sie etwa auch dem Ent-

## Stellungnahme

Zur Änderung des Bayerischen Verfassungsschutzgesetzes

Seite 5

wurf zum TKEntschNeuOG zugrunde liegt. Hierdurch könnten die Administrationskosten sowohl auf Seiten des Landesamtes für Verfassungsschutz als auch auf Seiten der Wirtschaft gering gehalten werden.

### 4 Umfang der Beauskunftung nach Art. 6c Abs. 2 Nr. BayVSG-E

Nach Art. 6c Abs. 2 Nr. 4 BayVSG-E sollen die Verpflichteten im Rahmen der Verkehrsdaten auch die "zum Aufbau und zur Aufrechterhaltung der Telekommunikation notwendigen" Daten beauskunften. Wie sich aus der Einleitung und Begründung zum Gesetzentwurf ergibt sind damit Daten gemeint, welche im Netz vorgehalten werden, um das Routing für einen Rufaufbau zu ermöglichen. Es geht somit um die Beauskunftung der sog. „Location Updates“ von Endgeräten außerhalb eines konkreten Telekommunikationsvorgangs oder der Daten über die letzte Einbuchung im VLR/HLR.<sup>1</sup>

Diese Daten sind bislang nicht Teil der Verkehrsdatenbeauskunftung, da gerade kein Telekommunikationsvorgang stattfindet. Auch von der Erhebungs- und Speicherverpflichtung des § 113a TKG sind diese Daten folgerichtig nicht umfasst.

Die vorgesehene Verpflichtung, diese Daten zu beauskunften kann seitens der Unternehmen nur auf zwei Arten umgesetzt werden:

- Entweder müssten auch Location-Updates als Datensätze geschrieben und mit den Verkehrsdaten gespeichert, also vollständig historisiert werden. Dann würden von allen Mobilfunkteilnehmern unabhängig von einer Nutzung des Endgeräts alle Standortinformationen erhoben und gespeichert. Die daraus resultierende Datenmenge würde eine erhebliche Erweiterung der Leitungsanbindungen zu den Basisstationen erforderlich machen. Dies hätte bei den Verpflichteten Investitionen in Millionenhöhe zur Folge. Auch das Datenvolumen der im Rahmen der Vorratsdatenspeicherung vorzuhaltenden Daten würde nochmals erheblich anwachsen mit der Folge, dass die Kosten für Speicher, Administration und Backups erheblich ansteigen. Datenschutzrechtlich ist die Erhebung dieser Daten äußerst bedenklich, da hierüber vollständige Bewegungsprofile sämtlicher Kunden generiert würden.
- Alternativ könnten seitens der Verpflichteten die noch in den HLR/VLR-Systemen vorhandenen Daten beauskunftet werden. Eine solche Beauskunftung ist jedoch nicht im Rahmen der normalen Prozesse bei der Beauskunftung von Verkehrsdaten realisierbar und bedeutet damit organisatorischen und technischen Zusatzaufwand. Je nach Netzstruktur erfordert die Beauskunftung dieser Daten einen Zugang zu dem, die Kernprozesse des Netzes steuernden Kontrollnetz. Dieser Zugang ist in jedem Unternehmen streng reglementiert. Die Schaffung eines reinen Lesezugriffs für die Bearbeitung von Auskunftersuchen wäre erforderlich.

---

<sup>1</sup> Das HLR bezeichnet das Home Location Register. In diesem sind alle Rufnummern hinterlegt, welche im jeweiligen Mobilfunknetz dazu berechtigt sind, zu telefonieren. Zusätzlich wird im HLR hinterlegt, in welchem VLR (Visitor Location Register) der Teilnehmer zuletzt eingebucht war. Das VLR hält alle Teilnehmer vor, die im Einzugsbereich eingebucht sind; zusätzlich wird die letzte bekannte BSC (Base Station Controller) vorgehalten.

## Stellungnahme

Zur Änderung des Bayerischen Verfassungsschutzgesetzes

Seite 6

Eine entsprechend sichere Realisierung würde ebenfalls immense Kosten verursachen.

Der Gesetzeswortlaut deutet derzeit darauf hin, dass eine Realisierung nach Alternative 1 verlangt wird. Die Verpflichtung zur Beauskunftung dieser Daten wurde auch im Rahmen des Gesetzes zur Einführung der Vorratsdatenspeicherung seitens aller beteiligten Gesetzgebungsorgane diskutiert und am Ende endgültig abgelehnt. Eine Durchsetzung der auf Bundesebene gescheiterten Forderungen der Ermittlungsbehörden auf dem Wege der Landesgesetzgebung sehen wir als verfassungsrechtlich sehr bedenklich an. Aus unserer Sicht muss § 113a TKG hinsichtlich der zu speichernden und zu beauskunftenden Datentypen die abschließende Norm darstellen. Zu einer Sonderregelung für einzelne Behörden, insbesondere wenn diese vortragen, weniger als 40 Maßnahmen im Jahr zu generieren, darf es nicht kommen.

Sollte nicht aus den dargelegten Gründen von der Verpflichtung vollends abgesehen werden, so ist im Gesetz jedenfalls unbedingt klarzustellen, dass

- keine generelle Erhebungsverpflichtung der Location Updates von Endgeräten im Idle Mode auf BSC-Ebene erforderlich ist.
- keine Verpflichtung zur Speicherung der Daten besteht.
- die Verpflichteten in der Gestaltung der Auskunftserteilung frei sind.

### 5 Regelung zum Einsatz des IMSI-Catchers; Art. 6c Abs. 4 BayVSG-E

Art. 6c Abs. 4 Satz 1 BayVSG-E regelt die Voraussetzungen des Einsatzes des IMSI-Catchers. Der Begründung ist auf Seite 23 zu entnehmen, dass der Einsatz von IMSI-Catchern nicht der Überwachung von Kommunikationsinhalten sondern nur zur Vorbereitung von G-10-Maßnahmen dienen soll. Diese wichtige Einschränkung sehen wir im Normtext noch nicht umgesetzt. Wir schlagen deshalb folgende Formulierung vor:

„(4) Das Landesamt für Verfassungsschutz darf im Einzelfall unter den Voraussetzungen des Abs. 2 auch technische Mittel ausschließlich zur Ermittlung des Standorts eines aktiv geschalteten Mobilfunkendgeräts oder zur Ermittlung der Geräte- und Kartennummern einsetzen.“

Im Übrigen weisen wir darauf hin, dass der Einsatz des IMSI-Catchers nach derzeitigem Stand kein zulässiges technisches Mittel für die in Art. 6c Abs. 4 BayVSG-E genannten Zwecke darstellt, da sein Einsatz die Frequenznutzung erheblich stört. Seine Nutzung wäre damit nur unter Einhaltung der Rahmenbedingungen gemäß §55 Abs. 1 Satz 5 TKG zulässig. Nach unserem Kenntnisstand hat die BNetzA die bis zum 01.07.2007 geltenden vorläufigen Rahmenbedingungen aber nicht verlängert.

### 6 Verdeckte „Online-Durchsuchung“; § 6e, f BayVSG-E

#### 6.1 Verfassungsrechtliche Anforderungen

Mit der Entscheidung vom 27. Februar 2008 1 (1 BvR 370/07; 1 BvR 595/07) hat das Bundesverfassungsgericht die verfassungsrechtlichen Mindestvoraussetzungen für

## Stellungnahme

Zur Änderung des Bayerischen Verfassungsschutzgesetzes

Seite 7

das heimliche Ausspähen informationstechnischer Systeme durch staatliche Behörden festgelegt.

BITKOM begrüßt, dass die bayerische Landesregierung bereits im Begleitschreiben zum Gesetzentwurf deutlich gemacht hat, die Konsequenzen des Urteils im Gesetzgebungsverfahren streng zu berücksichtigen. In Umsetzung dieser Ankündigung regen wir folgende Modifikationen an:

- Genaue Prüfung, ob die bislang vorgesehene Bezugnahme zu den materiellen Eingriffsvoraussetzungen der § 1 Abs. 1 und 3 Abs. 1 G 10 den vom BVerfG aufgestellten strengen Anforderungen gerecht wird.
- Wir halten es für notwendig, das vom Bundesverfassungsgericht als zentral herausgestellte Erfordernis tatsächlicher Anhaltspunkte für eine konkrete Gefahr für ein überragend wichtiges Rechtsgut unmittelbar in die Befugnisnorm aufzunehmen. Das Gericht hat hierzu explizit ausgeführt, dass eine reine Verweisung auf das G 10 nicht ausreicht.
- Ersetzung der in § 6f Abs. 1 BayVSG-E vorgesehenen Anordnungsbefugnis des Bayerischen Innenministeriums durch einen strengen Richtervorbehalt.
- Der vorgelegte Entwurf stellt nicht sicher, dass Inhalte die dem Kernbereich privater Lebensführung zuzuordnen sind, bereits nicht erhoben werden. Das Bundesverfassungsgericht fordert ein zweistufiges Schutzkonzept. Das in § 6 f. Abs. 5 Nr. 3 BayVSG-E vorgesehene Verwertungsverbot für entsprechende Informationen genügt dem insoweit nicht.

### 6.2 Begriff der informationstechnischen Systeme in Art. 6e BayVSG-E

Laut Begründung soll die Formulierung „informationstechnische Systeme“ sicherstellen, dass die notwendigen technischen Maßnahmen ergriffen werden dürfen, um eine Datenerhebung aus Speichermedien zu ermöglichen. Es wird weiterhin auf die zukünftige technische Entwicklungen hingewiesen sowie auf die Notwendigkeit, auch die Datenerhebung von Peripheriegeräten, wie etwa der Tastatur, zu ermöglichen. Gemessen an diesem Zweck ist nicht ersichtlich, warum mit dem Begriff der informationstechnischen Systeme ein äußerst weitreichender Anwendungsbereich gewählt worden ist. Dieser Begriff umfasst deutlich mehr als die in der Begründung beschriebenen Anwendungsfälle. Kritisch ist insbesondere, dass unter die Definition auch andere softwaregesteuerte Geräte eines Anwenders fallen können, insbesondere aber auch Server eines Internet-Providers.

Dass explizit auch Server von Internet-Providern unter diese Definition fallen, entspricht der offiziellen Auffassung des Bundesministeriums des Inneren, wie sie sich aus einer Antwort vom 22. August 2007 auf eine Anfrage des Bundesministeriums der Justiz ergibt. Danach sei unter einem informationstechnischem System ein System zu verstehen, „welches aus Hard- und Software sowie aus Daten besteht, das der Erfassung, Speicherung, Verarbeitung, Übertragung und Anzeige von Informationen und Daten dient“. Ausdrücklich beschränke sich die Definition nicht auf Personal Compu-

## Stellungnahme

Zur Änderung des Bayerischen Verfassungsschutzgesetzes

Seite 8

ter, also Einzelplatzrechner, die „im Gegensatz zu einem Großrechner/Server zu einem bestimmten Zeitpunkt von einer einzelnen Person bedient, genutzt und gesteuert werden kann“. Weiterhin heißt es, dass „je nach Fallkonstellation auch Server von der Online-Durchsuchung umfasst werden (können), die nach o.a. Definition „informationstechnische Systeme darstellen“.

### 6.3 Adressatenkreis – Einbeziehung von Nachrichtennetzwerkern

Schließlich sollte der zulässige Adressatenkreis der Maßnahme auf den Verdächtigen selbst beschränkt werden. Die unbeschränkte Einbeziehung von „Nachrichtennetzwerkern“ greift zu weit, weil es sich auch hierbei um einen Begriff mit einem nahezu unüberschaubaren Anwendungsbereich handelt, der in der Gesetzesbegründung bezeichnenderweise nicht präzisiert wird. Dies gilt insbesondere vor dem Hintergrund der Verwendung des generischen Begriffs „informationstechnisches System“ zur Festlegung des Untersuchungsobjekts (s. Punkt 6.2). Erfasst wären über die Einbeziehung der Nachrichtennetzwerke etwa Internet-Cafés, Mail-Server entsprechender Dienstleister, Unternehmen oder Universitäten sowie nahezu jede andere Serverstruktur, auf welche natürliche Personen potentiell Zugriff haben.

Die vorgesehene Befugnis könnte also beispielsweise eingesetzt werden, um ganze Unternehmensserver verdeckt aufgrund von Verdachtsmomenten gegen einen einzelnen Mitarbeiter zu durchforsten. Dies entspricht nicht dem Maßstab der Verhältnismäßigkeit, weil eine solche Maßnahme keine Heimlichkeit gegenüber solcherlei neutralen „Nachrichtennetzwerkern“, sondern allein gegenüber dem Verdächtigen erfordert. Hier stehen weniger einschneidende Maßnahmen zur Verfügung, z.B. Beschlagnahme oder Kopie von Serverinhalten. Damit müsste keine Schadsoftware eingebracht werden, die den Betrieb unabsehbar beeinträchtigen könnte. Auch der explizit in der Norm verankerte Einzelfallbezug schafft insoweit keine Abhilfe, da dieser nur abstrakt ausschließt, dass die Maßnahme zum Regelinstrument von Ermittlungen des Verfassungsschutzes wird.

Wir weisen außerdem darauf hin, dass die Einbeziehung von Servern sog. „Nachrichtennetzwerke“ das Vertrauen in IT-Sicherheit in Deutschland nachhaltig erschüttern und deutsche Unternehmen im internationalen Wettbewerb direkt benachteiligen würde. Kunden werden die Möglichkeit der Online-Durchsuchung auf deutschen Servern dadurch umgehen, dass sie auf entsprechende Angebote im Ausland zurückgreifen.