Bundesrat **Drucksache** **527/1/17**

04.07.17

Empfehlungen R - AV
der Ausschüsse

zu **Punkt 97** der 959. Sitzung des Bundesrates am 7. Juli 2017

Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens

A.

1. Der **Ausschuss für Agrarpolitik und Verbraucherschutz**

empfiehlt dem Bundesrat,

zu dem Gesetz gemäß Artikel 77 Absatz 2 des Grundgesetzes die Einberufung des Vermittlungsausschusses mit dem Ziel zu verlangen, die Regelungen zur Online-Durchsuchung und Quellen-Telekommunikationsüberwachung zu streichen.

Begründung:

Der Bundesrat sieht mit Sorge, dass die im Gesetz vorgesehene weite Befugnis zur Online-Durchsuchung und Quellen-Telekommunikationsüberwachung zu einer massiven Schwächung der IT-Sicherheitsinfrastruktur und damit auch zu einer Gefährdung der Nutzerinnen und Nutzer informationstechnischer Systeme beitragen kann. Das Gesetz sieht vor, dass eine Überwachung von Messenger-Diensten durch den Einsatz eines sogenannten Staatstrojaners möglich sein soll, der tief in das Betriebssystem von Rechnern und Smartphones eindringt und eine umfangreiche Überwachung möglich macht. Der vorgeschlagene Einsatz von Spähsoftware kann dazu führen, dass die für die Installation dieser Software notwendigen Schwachstellen auf den informationstechnischen Geräten von Verbraucherinnen und Verbrauchern auch von Kriminellen entdeckt und missbraucht werden können. Die Ausnutzung von bisher unbekannten Sicherheitslücken eines informationstechnischen Systems zum Einsatz von

...

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

Überwachungsprogrammen kann erhebliche Sicherheitsinteressen der Verbraucherinnen und Verbraucher beeinträchtigen.

Das vorliegende Gesetz schafft ein Interesse für Sicherheitsbehörden, die Cyber-Sicherheit weltweit zu schwächen, um informationstechnische Systeme von Zielpersonen infiltrieren zu können. Die kalkulierte IT-Unsicherheit erscheint insbesondere vor dem Hintergrund der jüngsten Cyber-Angriffe mithilfe des globalen Erpressungstrojaners "WannaCry" und damit einhergehenden Aufforderungen staatlicher Sicherheitsbehörden an Verbraucherinnen und Verbraucher sowie Unternehmen, die IT-Systeme besser zu sichern, zumindest widersprüchlich.

Die Installation von Überwachungssoftware seitens staatlicher Stellen kann dazu führen, dass Dritte in das System mittels Nachladefunktion eindringen können, indem sie eine unzureichende Authentifizierung und Verschlüsselung ausnutzen. Je öfter die Schwachstelle ausgenutzt wird, desto eher können auch Kriminelle und andere Interessengruppen solche Lücken missbrauchen.

Dem Bundesrat war es nicht möglich, sich im Rahmen der Stellungnahme zu dem Gesetzentwurf der Bundesregierung, der bereits eine Vielzahl von Maßnahmen zur effektiveren und praxistauglichen Ausgestaltung des Strafverfahrens enthielt, hierzu zu positionieren. Das Gesetz bedarf jedoch zum Schutz der Rechte der Verbraucherinnen und Verbraucher einer entsprechenden Änderung.

B.

2. Der **federführende Rechtsausschuss**

empfiehlt dem Bundesrat,

zu dem Gesetz einen Antrag gemäß Artikel 77 Absatz 2 des Grundgesetzes nicht zu stellen.

C.

Der **Ausschuss für Agrarpolitik und Verbraucherschutz**

empfiehlt dem Bundesrat ferner folgende

E n t s c h l i e ß u n g

zu fassen:

3. Der Bundesrat sieht mit Sorge, dass die im Gesetz vorgesehene weite Befugnis zur Online-Durchsuchung und Quellen-Telekommunikationsüberwachung zu einer massiven Schwächung der IT-Sicherheitsinfrastruktur und damit auch zu einer Gefährdung der Nutzerinnen und Nutzer informationstechnischer Systeme beitragen kann. Das Gesetz sieht vor, dass eine Überwachung von Messenger-Diensten durch den Einsatz eines sogenannten Staatstrojaners möglich sein soll, der tief in das Betriebssystem von Rechnern und Smartphones eindringt und eine umfangreiche Überwachung möglich macht. Der vorgeschlagene Einsatz von Spähsoftware kann dazu führen, dass die für die Installation dieser Software notwendigen Schwachstellen auf den informationstechnischen Geräten von Verbraucherinnen und Verbrauchern auch von Kriminellen entdeckt und missbraucht werden können. Die Ausnutzung von bisher unbekannten Sicherheitslücken eines informationstechnischen Systems zum Einsatz von Überwachungsprogrammen kann erhebliche Sicherheitsinteressen der Verbraucherinnen und Verbraucher beeinträchtigen.

4. Der Bundesrat stellt fest, dass das Gesetz im Rahmen der Beratung im Deutschen Bundestag um die weiteren Regelungsbereiche der Online-Durchsuchung und Quellen-Telekommunikationsüberwachung ergänzt worden ist, die weit über den ursprünglichen Wesensgehalt des Gesetzes hinausgehen. Eine umfassende Beteiligung der Länder zu diesen Regelungsbereichen hat nicht stattgefunden. Der Bundesrat bedauert, dass es ihm nicht möglich

war, sich im Rahmen der Stellungnahme zu dem Gesetzentwurf der Bundesregierung, der bereits eine Vielzahl von Maßnahmen zur effektiveren und praxistauglichen Ausgestaltung des Strafverfahrens enthielt, hierzu zu positionieren. Bei einer Regelung dieser Tragweite, Eingriffstiefe und Auswirkung auf die Praxis sowie den Kernbereich privater Lebensgestaltung wäre dies jedoch angemessen gewesen.

5. Der Bundesrat stellt fest, dass mit den vorgelegten Änderungen für den Bereich der Strafverfolgung Rechtsgrundlagen für die Online-Durchsuchung und die Quellen-Telekommunikationsüberwachung geschaffen werden sollen. Nach einem Grundsatzurteil des Bundesverfassungsgerichts waren solche Eingriffe bisher auf Terrorismus-Ermittlungen im Bereich der Gefahrenabwehr beschränkt. Der Bundesrat merkt an, dass der Einsatz von Überwachungsprogrammen durch die Strafverfolgungsbehörden in Form einer Online-Durchsuchung und einer Quellen-Telekommunikationsüberwachung angesichts der Vielzahl damit zugänglicher personenbezogener Daten umfangreichere Rückschlüsse über die Zielperson zulässt als die akustische Wohnraumüberwachung. Dies bedeutet eine völlig neue Schwere des Grundrechtseingriffs und beinhaltet erhebliche datenschutzrechtliche Risiken.

   Der Bundesrat sieht die Gefahr, dass das vorliegende Gesetz das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sowie das Fernmeldegeheimnis verletzt, da es die diesbezüglich vom Bundesverfassungsgericht im Gefahrenabwehrbereich aufgestellten Voraussetzungen nicht erfüllen könnte. Das Bundesverfassungsgericht hat für den präventiven Bereich strenge Voraussetzungen an die Online-Überwachung geknüpft. Diese Maßstäbe müssen auch im Bereich der Strafverfolgung berücksichtigt werden. Das Gesetz begrenzt die Online-Überwachung aber weder auf schwerste Straftaten, noch beschränkt es die Quellen-Telekommunikationsüberwachung auf laufende Kommunikation. Der Bundesrat hat daher erhebliche Zweifel an der Verhältnismäßigkeit des Gesetzes.

Begründung (nur gegenüber dem Plenum):

Das Gesetz schafft ein Interesse für Sicherheitsbehörden, die Cyber-Sicherheit weltweit zu schwächen, um informationstechnische Systeme von Zielpersonen infiltrieren zu können. Die kalkulierte IT-Unsicherheit erscheint insbesondere vor dem Hintergrund der jüngsten Cyber-Angriffe mithilfe des globalen Erpressungstrojaners "WannaCry" und damit einhergehenden Aufforderungen staatlicher Sicherheitsbehörden an Verbraucherinnen und Verbraucher sowie Unternehmen, die IT-Systeme besser zu sichern, zumindest widersprüchlich. So kann die Installation von Überwachungssoftware seitens staatlicher Stellen dazu führen, dass Dritte in das System mittels Nachladefunktion eindringen können, indem sie eine unzureichende Authentifizierung und Verschlüsselung ausnutzen. Je öfter die Schwachstelle ausgenutzt wird, desto eher können auch Kriminelle und andere Interessengruppen solche Lücken missbrauchen.

Künftig sollen Rechner und Smartphones überwacht, deren Mikrofone aktiviert und deren Speicher ausgelesen werden können. Dies bedeutet eine völlig neue Schwere des Grundrechtseingriffs und beinhaltet erhebliche datenschutzrechtliche Risiken.

Das neue Gesetz ermöglicht die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung zu Strafverfolgungszwecken nicht nur im Fall von schweren Straftaten, sondern etwa auch bei Steuerdelikten, Computerbetrug, Hehlerei, Geld- und Wertzeichenfälschung oder der Verleitung zur missbräuchlichen Asylantragstellung. Dies kann langfristig zu einer ausufernden Anwendung der Online-Überwachung im Verhältnis zum geltenden Rechtszustand führen. Darüber hinaus erlaubt das vorliegende Gesetz den Behörden, gespeicherte Daten auszulesen, auch wenn diese Gegenstand früherer Kommunikation waren. Dies betrifft konkret die über Messenger-Dienste versandten Nachrichten. Die Quellen-Telekommunikationsüberwachung könnte dadurch zu einer Online-Durchsuchung werden.