**Deutscher Bundestag** **Drucksache 19/1505**

**19. Wahlperiode** 03.04.2018

# Antwort

## der Bundesregierung

### auf die Kleine Anfrage der Abgeordneten Konstantin Kuhle, Jimmy Schulz, Manuel Höferlin, weiterer Abgeordneter und der Fraktion der FDP
### – Drucksache 19/1020 –

## Rechtsgrundlagen und Einsatz der Quellen-Telekommunikationsüberwachung

Vorbemerkung der Fragesteller

Personen, die einer Straftat verdächtig sind, nutzen zunehmend standardmäßig verschlüsselte Kommunikationsmittel wie beispielsweise Skype, WhatsApp oder Telegram. Vor diesem Hintergrund hat der Deutsche Bundestag in der 18. Wahlperiode mit den Stimmen der Fraktionen der CDU/CSU und SPD den Einsatz der Onlinedurchsuchung und der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) durch die Strafverfolgungsbehörden ermöglicht. Ihre Rechtsgrundlage findet die Quellen-TKÜ zu repressiven Zwecken in § 100a Absatz 1 Satz 2 und 3 der Strafprozessordnung (StPO). Dabei soll § 100a Absatz 1 Satz 3 StPO eine spezifische Ermächtigungsgrundlage für verschlüsselte Kommunikationsmittel enthalten, während § 100a Absatz 1 Satz 2 StPO die Ermächtigungsgrundlage für unverschlüsselte Kommunikationsmittel enthalten soll (vgl. Formulierungshilfe der Bundesregierung für einen Änderungsantrag der Fraktionen der CDU/CSU und SPD zu dem Gesetzentwurf der Bundesregierung auf Bundestagsdrucksache 18/11272, Ausschussdrucksache 18(6)334).

Medienberichten zufolge hat das Bundeskriminalamt (BKA) nun damit begonnen, dieses Instrument zu nutzen, um so auch verschlüsselte Botschaften lesen zu können (vgl. www.sueddeutsche.de/digital/ueberwachung-polizei-spioniert-handynutzer-mit-trojaner-aus-1.3842439, letzter Abruf: 20. Februar 2018). Neben der eigens konzeptionierten Remote Communication Interception Software (RCIS) stehe dem BKA hierfür die von der FinFisher GmbH entwickelte Software FinSpy zur Verfügung. Unbekannt ist, wie oft und mit welchem Erfolg die Programme bereits zur Strafverfolgung eingesetzt wurden (vgl. https://netzpolitik.org/2018/breitseite-gegen-staatstrojaner-in-hessen-verfassungswidrig-und-gefaehrlich/, letzter Abruf: 20. Februar 2018).

Das Bundesverfassungsgericht (BVerfG) legte im Jahr 2008 für die Überwachung informationstechnischer Systeme zu präventiven Zwecken einen differenzierten Prüfungsmaßstab fest. Wenn und solange sich eine Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt, ist ihre Rechtsgrundlage nur an Artikel 10 des Grundgesetzes (GG) (Fernmeldegeheimnis) zu messen. Sind daneben weitere personenbezogene Daten umfasst, die einen Einblick in wesentliche Teile der Lebensgestaltung des

*Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 27. März 2018 übermittelt.*

*Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.*

Betroffenen oder gar ein aussagekräftiges Bild seiner Persönlichkeit geben, betrifft die Maßnahme zugleich das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG. Dieser spezifische Grundrechtsschutz erstrecke sich auch „auf solche Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können“ (vgl. BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07, Rn. 203).

In Bezug auf die Eingriffsermächtigung forderte das BVerfG, dass diese „tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut“ voraussetzen müsse, und stellte fest: „Zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine existenzielle Bedrohungslage nicht besteht, ist eine staatliche Maßnahme grundsätzlich nicht angemessen“ (vgl. BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07, Rn. 247 bis 248). Ferner seien – neben der Erforderlichkeit einer richterlichen Anordnung –Vorkehrungen für den Schutz des Kernbereichs privater Lebensgestaltung zu treffen.

In einer jüngeren Entscheidung zur präventiven Quellen-TKÜ nach § 20l Absatz 2 des Bundeskriminalamtgesetzes (BKAG) hob das BVerfG hervor, dass maßgeblich sei, dass „das Gesetz keinen Zweifel lasse, dass eine Quellen-TKÜ nur bei einer technisch sichergestellten Begrenzung der Überwachung auf die laufende Kommunikation erlaubt ist“. Anderenfalls käme nur ein Vorgehen in Form einer Online-Durchsuchung unter den Voraussetzungen von § 20k Absatz 1 BKAG in Betracht (vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 234).

Das BKA ist der Auffassung, dass die eingesetzte Quellen-TKÜ ausschließlich Inhalte der laufenden Kommunikation zugänglich mache (vgl. www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html, letzter Abruf: 20. Februar 2018). Demzufolge wären die vom BVerfG im Urteil vom 27. Februar 2008 geforderten Voraussetzungen zum Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht einschlägig (vgl. auch Bundestagsdrucksache 18/12785, S. 50).

Diese Annahme wurde im Rahmen der öffentlichen Anhörung zur Formulierungshilfe der Bundesregierung zum Änderungsantrag der Fraktionen der CDU/CSU und SPD zu dem Gesetzentwurf der Bundesregierung bezweifelt (vgl. Stellungnahme des Sachverständigen Dr. Ulf Buermeyer, S. 9, www.bundestag.de/blob/508848/bdf7512e32578b699819a5aa33dde93c/buermeyer-data.pdf, letzter Abruf 23. Februar 2018). Die systematische Einordnung der Quellen-TKÜ gemeinsam mit der konventionellen Telekommunikationsüberwachung in § 100a StPO suggeriere fälschlicherweise, dass es sich um einen vergleichbaren Eingriff handele. Bezogen auf die Eingriffsintensität stehe sie in Wahrheit der Online-Durchsuchung nahe, da beide Maßnahmen die Infiltration des Systems erforderten (vgl. auch Blechschmitt, Zur Einführung von Quellen-TKÜ und Online-Durchsuchung, StraFo 9/2017 S. 361 bis 365). Der Wortlaut des § 100a Absatz 1 Satz 3 StPO verdeutliche, dass technisch möglich sei, was rechtlich nicht möglich sein soll: „Auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.“

Diese Regelung zeige, dass die Ermittlungsbehörden auf sämtliche gespeicherten Kommunikationen zugreifen können. Zwar sehe § 100a Absatz 5 Nummer 1 Buchstabe b StPO vor, dass bei Maßnahmen nach Absatz 1 Satz 3 technisch sicherzustellen ist, dass ausschließlich solche gespeicherten Inhalte und Kom-

munikationen überwacht und aufgezeichnet werden können, die ab dem Zeitpunkt der Anordnung hätten überwacht und aufgezeichnet werden können. Um diese Prüfung aber ausführen zu können, müsse das Programm zunächst alle gespeicherten Kommunikationsinhalte auslesen und auswerten, um entscheiden zu können, welche davon nach dem Beginn der Maßnahme gespeichert wurden (vgl. Stellungnahme des Sachverständigen Dr. Ulf Buermeyer, S. 17, Link s. o., dies voraussetzend auch Bundestagsdrucksache 18/12785, S. 52). Das aber bedeute, dass technisch bereits die „entscheidende Hürde genommen ist, um das System insgesamt auszuspähen", mit der Folge, dass der Eingriff an Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG zu messen sei (vgl. BVerfG, Urteil von 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07, Rn. 188).

Vor diesem Hintergrund bestehen erhebliche praktische und verfassungsrechtliche Unsicherheiten im Zusammenhang mit den geltenden Regelungen zur Quellen-TKÜ.

## Vorbemerkung der Bundesregierung

Die vorliegend in den Fragen 11, 16, 17 und 18 erbetenen Auskünfte betreffen zum Teil geheimhaltungsbedürftige Informationen zur Arbeitsweise, Methodik und den Aufklärungsaktivitäten des Bundesnachrichtendienstes (BND) sowie im Hinblick auf Frage 11 und 18 des Bundesamts für Verfassungsschutz (BfV). Sie berühren in besonders hohem Maße das Wohl des Bundes und können deshalb im konkreten Fall selbst in eingestufter Form nicht erteilt werden. Zu dieser Entscheidung ist die Bundesregierung nach sorgfältiger Abwägung der widerstreitenden Interessen gelangt. In einen angemessenen Ausgleich zu bringen waren in diesem Fall einerseits das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Parlaments (Artikel 38 Absatz 1 Satz 2 und Artikel 20 Absatz 2 Satz 2 des Grundgesetzes) und andererseits das ebenfalls Verfassungsrang genießende schutzwürdige Interesse des Wohls des Bundes (Staatswohl) sowie das Interesse an einer funktionsgerechten Aufgabenwahrnehmung des BND als deutscher Auslandsnachrichtendienst.

Im Einzelnen:

Die Fragen 11 und 18 in Bezug auf den BND und das BfV sowie die Fragen 16 und 17 in Bezug auf den BND zielen auf solche Informationen, die in besonders hohem Maße das Staatswohl berühren und daher durch die Bundesregierung nicht beantwortet werden können. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung findet seine Grenzen durch das gleichfalls Verfassungsrang genießende schutzwürdige Interesse des Staatswohls. Mit einer Beantwortung dieser Fragen würden Einzelheiten zur Methodik des BND und des BfV offengelegt, welche die weitere Arbeitsfähigkeit und Aufgabenerfüllung auf dem spezifischen Gebiet der technischen Aufklärung gefährden würde. Die Offenlegung der konkreten nachrichtendienstlichen technischen Methoden birgt das Risiko der Kenntniserlangung dieser Maßnahmen durch beobachtete Akteure. Es bestünde die Gefahr, dass diese Mittel zur Informationsgewinnung unwirksam werden. Eine Auflistung der konkreten Verfahrensweisen beim Einsatz von IT-gestützten technischen Aufklärungsmitteln würde darüber hinaus weitgehende Rückschlüsse auf technische Ausstattungen und Möglichkeiten des BND und des BfV und somit mittelbar auch auf das Aufklärungsprofil des BND zulassen, so dass unmittelbare, schutzwürdige Geheimhaltungsinteressen berührt sind.

Des Weiteren könnten die Fähigkeiten des BND und des BfV, nachrichtendienstliche Erkenntnisse im Wege der technischen Aufklärung zu gewinnen, durch ein Bekanntwerden bei den Betreibern entsprechender Dienste in erheblicher Weise negativ beeinflusst werden.

Die Gewinnung von Informationen durch technische Aufklärung ist für die Sicherheit der Bundesrepublik Deutschland und für die sich aus § 1 Absatz 2 des BND-Gesetzes (BNDG) bzw. § 3 Absatz 1 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (BVerfSchG) ergebende Aufgabenerfüllung von BND und BfV jedoch unerlässlich. Sofern solche Informationen entfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen. Insbesondere ist das sonstige Informationsaufkommen des BND nicht ausreichend, um ein vollständiges Lagebild zu erhalten und Informationsdefizite im Bereich der technischen Aufklärung auszugleichen. Insofern birgt eine Offenlegung der angefragten Informationen die Gefahr, dass Einzelheiten zur konkreten Methodik und zu aus den vorgenannten Gründen im hohen Maße schutzwürdigen, spezifischen technischen Fähigkeiten des BND und des BfV bekannt würden. Infolgedessen könnten sowohl ausländische staatliche als auch nichtstaatliche Akteure Rückschlüsse auf spezifische Vorgehensweisen und technische Fähigkeiten des BND und des BfV ziehen. Dies würde folgenschwere Einschränkungen der Informationsgewinnung bedeuten, womit letztlich der gesetzliche Auftrag des BND – die Sammlung und Auswertung von Informationen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind (§ 1 Absatz 2 BNDG) – und des BfV – die Sammlung und Auswertung von Informationen insbesondere über Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind, sowie über sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht (§ 3 Absatz 1 BVerfSchG) – nicht mehr sachgerecht erfüllt werden könnten.

Eine VS-Einstufung und Weiterleitung der angefragten Informationen an die Geheimschutzstelle des Deutschen Bundestages kommt angesichts ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der technischen Aufklärung für die Aufgabenerfüllung des BND und des BfV und den zuvor benannten Gründen nicht in Betracht, weil insoweit auch ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann (vgl. BVerfGE 124, 78 [139]). Die angefragten Inhalte erfordern eine derart detaillierte Darstellung der technischen Fähigkeiten des BND und des BfV, dass eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen kann. Dies gilt umso mehr, als sie u. a. Spezifika betreffen, deren technische Umsetzung nur durch bestimmte Verfahren erfolgen kann. Bei einem Bekanntwerden der schutzbedürftigen Informationen wäre kein Ersatz durch andere Instrumente der Informationsbeschaffung möglich.

Aus dem Vorgesagten ergibt sich, dass die mit den Fragen 11 und 18 zu BND und BfV und den Fragen 16 und 17 zu BND erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht in diesem Fall wesentlich überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber den Geheimhaltungsinteressen des BND und des BfV zurückstehen.

Die in den Fragen 1, 2, 4, 5, 6, 7, 11, 12, 13, 16 und 17 erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik der von der Kleinen Anfrage betroffenen Dienststellen des Bundes und insbesondere deren technischen Fähigkeiten stehen und damit mittelbar Rückschlüsse auch auf die (geplante) technische Ausstattung und das Know-how der Dienststellen zulassen. Die Antworten auf die Kleine Anfrage beinhalten zum Teil detaillierte Einzelheiten zu ihren technischen Fähigkeiten und ermittlungstaktischen Verfahrensweisen. Aus ihrem Bekanntwerden könnten Rückschlüsse auf ihre Vorgehensweise, Fähigkeiten und Methoden gezogen werden. Deshalb sind einzelne Informationen gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) als „VS-Nur für den Dienstgebrauch“ eingestuft und werden als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt.*

Darüber hinaus kann die Bundesregierung die mit den Fragen 1, 2, 5, 7, 8, 9, 10, 16, 17, 18 und 22 erbetenen Auskünfte selbst in eingestufter Form nicht oder nicht vollständig erteilen. Zu dieser Entscheidung ist die Bundesregierung nach sorgfältiger Abwägung der widerstreitenden Interessen gelangt. In einen angemessenen Ausgleich zu bringen waren auch in diesem Fall einerseits das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Parlaments (Artikel 38 Absatz 1 Satz 2 und Artikel 20 Absatz 2 Satz 2 des Grundgesetzes) und andererseits das ebenfalls Verfassungsrang genießende schutzwürdige Interesse des Wohls des Bundes (Staatswohl) sowie das Interesse an einer funktionsgerechten Aufgabenwahrnehmung des BKA, der BPOL und des Zolls im Zusammenhang mit der (internationalen) Verbrechensbekämpfung.

Im Einzelnen:

Die Fragen zielen auf einen äußerst sensiblen Bereich der verdeckten informationstechnischen Informationsgewinnung und berühren daher in besonders hohem Maße das Wohl des Bundes.

Die Informationen sind besonders geheimhaltungsbedürftig, weil sie im Ergebnis weitgehende Rückschlüsse auf die technischen Fähigkeiten und damit mittelbar auch auf die (geplante) technische Ausstattung und das Know-how des BKA, der BPOL und des Zolls zulassen. Dadurch könnten die zur effektiven Strafverfolgung und Gefahrenabwehr notwendigen Fähigkeiten des BKA, der BPOL und des Zolls in erheblicher Weise negativ beeinflusst und somit auch zukünftige Maßnahmen der informationstechnischen Überwachung erheblich erschwert bzw. unmöglich werden.

Die Gewinnung von Informationen durch Maßnahmen der informationstechnischen Überwachung ist für die Aufgabenerfüllung des BKA, der BPOL und des Zolls sowie weiterer hierfür gesetzlich befugter Sicherheitsbehörden und damit für die Sicherheit der Bundesrepublik Deutschland unerlässlich.

Eine VS-Einstufung und Weiterleitung der angefragten Informationen an die Geheimschutzstelle des Deutschen Bundestages kommt angesichts ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der technischen Aufklärung für die Aufgabenerfüllung der betroffenen Behörden und den zuvor benannten Gründen nicht in Betracht, weil insoweit auch ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann (vgl. BVerfGE 124, 78

* Das Bundesministerium des Innern, für Bau und Heimat hat Teile der Antworten zu den Fragen 1, 2, 4 bis 7, 11 bis 13, 16 und 17 als „VS ‑ Nur für den Dienstgebrauch“ eingestuft.
Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

[139]). Bereits Angaben z. B. zu Installationsversuchen, Funktionsumfang oder konkreten Diensten bzw. Betriebssystemen seitens des BKA bei Maßnahmen der Informationstechnischen Überwachung könnte die weitere Gewinnung von Informationen durch Maßnahmen der informationstechnischen Überwachung erheblich erschweren bzw. gar unmöglich machen. In diesem Fall wäre ein Ersatz durch andere Instrumente nicht möglich. Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber den Geheimhaltungsinteressen der betroffenen Sicherheitsbehörden zurückstehen.

1. In wie vielen Fällen wurde vom BKA bereits Software zur Überwachung informationstechnischer Systeme zur Gefahrenabwehr eingesetzt, und in wie vielen Fällen erfolgt dies derzeit?

2. In wie vielen Fällen wurde vom BKA bereits Software zur Überwachung informationstechnischer Systeme zur Strafverfolgung eingesetzt, und in wie vielen Fällen erfolgt dies derzeit?

   In wie vielen Fällen wurde die Maßnahme dabei auf § 100a Absatz 1 Satz 3 und in wie vielen Fällen auf § 100a Absatz 1 Satz 2 StPO gestützt (bitte aufschlüsseln)?

Es wird auf die Vorbemerkung und den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil verwiesen.*

3. Wie erfolgt die praktische Abgrenzung zwischen § 100a Absatz 1 Satz 2 und § 100a Absatz 1 Satz 3 StPO?

Produkte zur Durchführung von Maßnahmen der Quellen-TKÜ nach § 100a Absatz 1 Satz 2 und 3 der Strafprozessordnung (StPO) sind entsprechend der rechtlichen Rahmenbedingungen ausgestaltet. Hinsichtlich der rechtlichen Voraussetzungen der Quellen-TKÜ in § 100a Absatz 1 Satz 2 und Satz 3 StPO wird auf die Antwort zu Frage 19 verwiesen.

4. Auf welche Arten informationstechnischer Systeme (Hardware) wurde bei der Überwachung informationstechnischer Systeme zur Strafverfolgung jeweils, d. h. nach beiden Rechtsgrundlagen § 100a Absatz 1 Satz 2 und 3 StPO, zugegriffen (Tablets, PCs, Smartphones) (bitte aufschlüsseln)?

Es wird auf die Vorbemerkung und im Übrigen auf den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil verwiesen.*

5. Auf welche konkreten Messenger-Dienste (Software wie z. B. Skype, WhatsApp) wurde in diesen Fällen jeweils zugegriffen?

   Auf welchen Betriebssystemen liefen die überwachten Dienste (Windows, Linux, Android etc.) (bitte aufschlüsseln)?

Auf den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil wird verwiesen. Im Übrigen kann die Bundesregierung unter Bezugnahme auf die Vorbemerkung hierzu keine weitere Aussage treffen.

6. Aufgrund des Verdachts welcher Straftatbestände wurde die Software zur Überwachung informationstechnischer Systeme bereits eingesetzt (bitte nach Straftatbeständen und Ermächtigungsgrundlagen § 100a Absatz 1 Satz 2 und Satz 3 StPO aufschlüsseln)?

Es wird auf den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil verwiesen.

7. Wie vieler Versuche bedurfte es bei diesen Einsätzen für die erfolgreiche Installation der Software?

Auf den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil wird verwiesen. Im Übrigen kann die Bundesregierung unter Bezugnahme auf die Vorbemerkung hierzu keine weitere Aussage treffen.

8. Wie lange dauert der durchschnittliche Einsatz von Software zur Überwachung informationstechnischer Systeme durch das BKA in diesen Fällen an?

9. Welche Unterschiede bestehen konkret zwischen den eingesetzten Programmen „RCIS“ und „FinSpy“?

10. Nach welchen Kriterien trifft das BKA die Entscheidung, welches Softwarepaket (z. B. „RCIS“ oder „FinSpy“) zur Überwachung informationstechnischer Systeme zum Einsatz kommt?

Unter Bezugnahme auf die Vorbemerkung kann die Bundesregierung hierzu keine Aussage treffen.

11. Verwenden neben dem BKA auch andere Behörden auf Bundesebene bereits Software zur Überwachung informationstechnischer Systeme nach den Regeln der Quellen-TKÜ?

    Wenn ja, welche Behörden sind dies, und in vielen Fällen erfolgte der Einsatz?

Für den BND und das BfV wird auf die Vorbemerkung verwiesen. Im Übrigen wird auf den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil verwiesen.

12. In wie vielen Strafverfahren sind die durch den Einsatz von Software zur Überwachung informationstechnischer Systeme nach den Regeln der Quellen-TKÜ gewonnenen Erkenntnisse bereits als Beweis eingebracht worden, und welche Straftatbestände wurden angeklagt (bitte aufschlüsseln)?

13. In wie vielen Strafverfahren und aufgrund welcher Straftatbestände, in denen durch den Einsatz von Software zur Überwachung informationstechnischer Systeme gewonnene Erkenntnisse als Beweis eingebracht wurden, erfolgte eine Verurteilung der Angeklagten?

Die Fragen 12 und 13 werden gemeinsam beantwortet.

In Strafverfahren des Generalbundesanwalts wurden bislang keine unter Anwendung des neuen § 100a Absatz 1 Satz 2 und 3 StPO erlangten Beweismittel in ein Strafverfahren eingebracht. Über den Einsatz im Bereich der Strafverfolgung auf Länderebene liegen der Bundesregierung keine Erkenntnisse vor.

Im Übrigen wird auf den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil verwiesen.

14. Entspricht es der Auffassung der Bundesregierung, dass die Quellen-TKÜ technisch mit einer Onlinedurchsuchung vergleichbar ist?

Wenn ja, warum?

Wenn nein, warum nicht?

Die technische Umsetzung richtet sich nach den rechtlichen Vorgaben. Auf die Antwort zu Frage 15 wird verwiesen.

15. Entspricht es der Auffassung der Bundesregierung, dass die Quellen-TKÜ hinsichtlich ihrer rechtlichen Anforderungen, insbesondere im Hinblick auf einen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG mit einer Onlinedurchsuchung vergleichbar ist?

Wenn ja, warum?

Wenn nein, warum nicht?

Die rechtlichen Anforderungen für die Quellen-TKÜ zu repressiven Zwecken ergeben sich aus § 100a StPO. Die rechtlichen Anforderungen für die Online-Durchsuchung sind dann in § 100b geregelt. Die rechtliche Ausgestaltung der Befugnisse ist entsprechend den Anforderungen des Bundesverfassungsgerichts für Eingriffe in das Fernmeldegeheimnis nach Artikel 10 Absatz 1 des Grundgesetz (GG) und in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nach Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG erfolgt. Auf die Ausführungen in der Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss – Bundestagsdrucksache 18/12785, S. 47 ff.) wird verwiesen.

16. Wird für die Onlinedurchsuchung und für die Quellen-TKÜ dieselbe Software eingesetzt?

17. Ist die zur Überwachung informationstechnischer Systeme verwandte Software grundsätzlich in der Lage, sowohl eine Quellen-TKÜ als auch eine Onlinedurchsuchung auszuführen, und wie unterscheiden sich die verwandten Programme diesbezüglich?

18. Wie kann nach Auffassung der Bundesregierung technisch sichergestellt werden, dass die zur Quellen-TKÜ eingesetzte Software ausschließlich auf Inhalte der laufenden Kommunikation zugreift, sie also „nicht mehr kann, als sie darf“?

    Wie geschieht dies in der Praxis?

Die Fragen 16 bis 18 werden gemeinsam beantwortet.

Gesetzlich befugte Sicherheitsbehörden nutzen zur Durchführung von Maßnahmen der Quellen-TKÜ und Online-Durchsuchung verschiedene Softwareprodukte, um die operativen Bedarfslagen abzudecken. Zum individuellen Funktionsumfang und den taktischen Einsatzmöglichkeiten können unter Bezugnahme auf die Vorbemerkung keine Aussagen getroffen werden.

Produkte zur Durchführung von Maßnahmen der informationstechnischen Überwachung werden vor ihrem Einsatz auf Konformität mit der aktuellen Rechtslage geprüft. Erst nach positivem Abschluss dieser Prüfungen werden die Produkte für den Einsatz freigegeben.

Im Übrigen wird bzgl. der Fragen 16 und 17 auf den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil verwiesen.

19. Welchen Anwendungsbereich hat § 100a Absatz 1 Satz 3 StPO für den Fall, dass die von deutschen Ermittlungsbehörden eingesetzte Software zur Überwachung informationstechnischer Systeme ausschließlich auf die laufende Kommunikation zugreifen kann?

Auf die Ausführungen in der Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss – Bundestagsdrucksache 18/12785, S. 47 ff.) wird verwiesen.

20. Erlaubt § 100a Absatz 1 Satz 3 StPO nach Ansicht der Bundesregierung auch den Zugriff auf gespeicherte Kommunikationsinhalte, wenn sie nicht in verschlüsselter Form übertragen worden sind?

    Wie kann technisch zwischen gespeicherten Kommunikationsinhalten unterschieden werden, die einerseits verschlüsselt und andererseits unverschlüsselt übermittelt worden sind?

Auf die Antwort zu Frage 19 wird verwiesen.

21. Erfasst die Überwachung nach § 100a Absatz 1 Satz 2 und 3 StPO auch den bloßen Datenaustausch zwischen digitalen Endgeräten oder den einseitigen Informationsabruf (z. B. beim Surfen im Internet, vgl. BVerfG, Beschluss vom 6. Juli 2016 – 2 BvR 1454/13, Rn. 32 ff., oder der Nutzung von Cloud-Inhalten), oder ist in diesen Fällen § 100b StPO anwendbar?

§ 100a Absatz 1 Satz 2 und 3 StPO erfasst die Überwachung und Aufzeichnung der Telekommunikation. Der Begriff der Telekommunikation umfasst alle Formen der Nachrichtenübermittlung unter Raumüberwindung in nichtkörperlicher

Weise mittels technischer Einrichtungen, auch von Maschine zu Maschine. § 100b StPO erlaubt die Erhebung von Daten, die sich auf einem von dem Betroffenen genutzten informationstechnischen System befinden.

22. Ist nach Ansicht der Bundesregierung mit der zur Verfügung stehenden Software ein Zugriff auf gespeicherte Kommunikationsinhalte im Sinne von § 100a Absatz 1 Satz 3 StPO möglich, ohne zugleich technisch auf sämtliche auf dem informationstechnischen System gespeicherte Kommunikationsinhalte zuzugreifen?

    Wenn ja, wie ist dies nach Ansicht der Bundesregierung möglich, und wie stellt sie es in der Praxis sicher?

Es wird auf die Antwort zu den Fragen 16 bis 18 verwiesen.

23. Ist der Zugriff auf Kommunikationsinhalte, die vor der Anordnung der Überwachung des informationstechnischen Systems übermittelt worden sind nach Auffassung der Bundesregierung rechtlich zulässig, und wenn ja, aufgrund welcher Rechtsgrundlage?

Eine Maßnahme nach § 100a Absatz 1 Satz 3 StPO ist zeitlich auf Kommunikationsinhalte begrenzt, die nach dem Ergehen des richterlichen Beschlusses abgesendet werden. Ältere Nachrichten, die vor Erlass des richterlichen Beschlusses versandt wurden, dürfen auf der Grundlage des § 100a Absatz 1 Satz 3 StPO nicht erhoben werden. Solche Kommunikationsinhalte können auf der Grundlage des § 100b StPO erhoben werden, soweit die Voraussetzungen im Übrigen vorliegen.

24. Wie kann nach Ansicht der Bundesregierung technisch und praktisch zwischen Kommunikationsinhalten unterschieden werden, die vor der Anordnung der Überwachungsmaßnahme übermittelt worden sind, und solchen, die erst danach übermittelt worden sind?

Produkte zur Durchführung von Maßnahmen einer Quellen-TKÜ durch Sicherheits- oder Strafverfolgungsbehörden des Bundes sind entsprechend der rechtlichen Rahmenbedingungen ausgestaltet und ermöglichen eine Anpassung der Produkte an die rechtlichen Anforderungen der Maßnahme.

25. Erlaubt § 100a Absatz 1 Satz 2 und 3 StPO nach Auffassung der Bundesregierung auch die Erhebung von Informationen, die erforderlich sind, um auf laufende oder gespeicherte Kommunikation zuzugreifen (z. B. die Erhebung von Passwörtern)?

Auf die Antworten zu den Fragen 19 und 21 wird verwiesen.

26. Wurden und werden im Rahmen der Quellen-TKÜ oder zu deren Vorbereitung auch andere Informationen als Kommunikationsinhalte vom informationstechnischen Gerät ausgelesen (z. B. Art und Version des Betriebssystems, Informationen zur Identifikation des Nutzers des informationstechnischen Systems, Existenz von Antivirensoftware, verwendete Kommunikationsprogramme, Speicherort)?

27. Sofern auch andere Informationen als Kommunikationsinhalte ausgelesen werden, was ist nach Ansicht der Bundesregierung hierfür die Rechtsgrundlage?

Die Fragen 26 und 27 werden gemeinsam beantwortet.

Der zulässige Umfang der Erhebung von Inhalten und Umständen der Kommunikation richtet sich nach den Vorgaben in § 100a Absatz 1 Satz 2 und 3 StPO. Die Erhebung anderer Informationen als Kommunikationsinhalte richtet sich nach den jeweiligen Befugnisnormen.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
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 0722-8333