

Antwort

der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Katja Keul, Dr. Konstantin von Notz, Luise Amtsberg, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 19/1810 –**

Einsatz von Spähsoftware bei der Strafverfolgung (Quellen-Telekommunikationsüberwachung und Online-Durchsuchung)

Vorbemerkung der Fragesteller

Das Straf- und Strafverfahrensrecht als schärfster Eingriff des Staates in das Freiheitsrecht erfordert strikte Wahrung von Rechtsstaatlichkeit und Grundrechten der Verfahrensbeteiligten wie aller Bürgerinnen und Bürger. Nur auf dieser Grundlage sind Effektivität, Praxistauglichkeit und Anpassung an moderne technische Möglichkeiten Maßstäbe der Modernisierung der Strafprozessordnung.

Die von der Großen Koalition 2017 in die Strafprozessordnung (StPO) eingefügte Regelung der Ermittlungsmaßnahmen Quellen-Telekommunikationsüberwachung (TKÜ) und Online-Durchsuchung werden nach Ansicht von Rechtswissenschaftlern und Sachverständigen für Informationstechnik den rechtsstaatlichen und grundrechtlichen Herausforderungen der Digitalisierung nicht gerecht und erscheinen bei Einhaltung der Vorgaben der StPO und des Grundgesetzes als praktisch unanwendbar (vgl. Buermeyer, Stellungnahme zur Anhörung des Ausschusses für Recht und Verbraucherschutz am 31. Mai 2017 (www.bundestag.de/ausschuesse/ausschuesse18/a06/anhoerungen/stellungnahmen/508846), Stellungnahme Chaos Computer Club (Neumann, Kurz, Rieger) ebenda, Blechschmitt, Zur Einführung von Quellen-TKÜ und Online-Durchsuchung, Strafverteidiger-Forum 2017 S. 361-365, Stellungnahme Chaos Computer Club vom 4. Februar 2018 zur Anhörung im Innenausschuss des Hessischen Landtages, Ausschussvorlage INA 19/63 Teil 3, S 290 ff. (<https://hessischer-landtag.de/content/innenausschuss-anh%C3%B6rung-zum-verfassungsschutz>)). Denn bislang ist es offenbar weder dem eine Quellen-TKÜ oder Online-Durchsuchung anordnenden Gericht noch der die Maßnahme beantragenden oder bei Gefahr im Verzug zunächst entscheidenden Staatsanwaltschaft sowie der durchführenden Behörde sicher möglich, sich Gewissheit über die Gesetzes- und Verfassungskonformität der für die informationstechnische Überwachung jeweils eingesetzten Software (im Folgenden abgekürzt: Spähsoftware) zu verschaffen. Sichere IT-Infrastrukturen und durchgehend hohe Verschlüsselungsstandards dürfen nicht gefährdet werden. Insbesondere nötig sind strikte Beachtung des

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 18. Mai 2018 übermittelt.

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

vom Bundesverfassungsgericht (BVerfG) aus dem allgemeinen Persönlichkeitsrecht hergeleiteten Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, des Grundsatzes der Verhältnismäßigkeit sowie der Nachrangigkeit solcher Ermittlungsmaßnahmen vor anderen Erkenntnismöglichkeiten.

Vorbemerkung der Bundesregierung

Die Bundesregierung beantwortet die im Rahmen des parlamentarischen Fragerechts angefragten Sachverhalte gegenüber dem Deutschen Bundestag grundsätzlich transparent und vollständig, um dem verfassungsrechtlich verbrieften Aufklärungs- und Informationsanspruch des Deutschen Bundestages zu entsprechen. Soweit Anfragen Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung aber zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann (BVerfGE 124, Seite 161, 189).

Bei der Abwägung ist auch zu berücksichtigen, ob durch die Bekanntgabe von Einzelaspekten der Sicherheitsbehörden Individualrechte Einzelner tangiert werden, insbesondere das durch Artikel 2 Absatz 1 des Grundgesetzes (GG) geschützte Recht auf Leben und körperliche Unversehrtheit. Die Abwägung kann dazu führen, dass die Bundesregierung nicht zur Arbeitsweise, Ausstattung und Methode der Sicherheitsbehörden Stellung nimmt.

Ergibt die im Einzelfall vorzunehmende Abwägung, dass lediglich die Veröffentlichung einer geheimhaltungsbedürftigen Information ausgeschlossen ist, wird die Antwort unter Beachtung des jeweils erforderlichen Grades der Verschlussache bei der Geheimschutzstelle des Deutschen Bundestages hinterlegt.

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Fragen 1, 2, 3, 4, 19, 20, 21 in offener Form ganz oder teilweise nicht erfolgen kann. Die in diesen Fragen 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 Ermittlungsaktivitäten und Analysemethoden stehen. 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 Verschlussachen (VS-Anweisung – VSA) als „VS – Nur für den Dienstgebrauch“ eingestuft und werden als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt.*

* Das Bundesministerium des Innern, für Bau und Heimat hat Teile der Antworten als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

1. In wie vielen Fällen haben Bundesbehörden bisher im Auftrag der Bundesanwaltschaft oder in Amtshilfe für Landesstrafverfolgungsbehörden und jeweiliger zugrunde liegender Anordnungen Spähsoftware
 - a) zur Quellen-TKÜ (§ 100a Absatz 1 Sätze 2 und 3 StPO) und
 - b) zur Online-Durchsuchung (§ 100b StPO),
 - c) bei der Verfolgung jeweils welcher Anlasstaten eingesetzt (bitte aufschlüsseln nach jeweiliger Rechtsgrundlage, Anlasstat, durchführender Bundesbehörde)?

Auf die Vorbemerkung der Bundesregierung sowie den als Verschlussache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil wird verwiesen.

2. In wie vielen Fällen richtete sich die Maßnahme gemäß Frage 1 gegen
 - a) Beschuldigte,
 - b) Angeschuldigte und
 - c) Angeklagte?

Auf die Vorbemerkung der Bundesregierung sowie den als Verschlussache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil wird verwiesen.

3. In wie vielen Fällen wurden Erkenntnisse, die aufgrund von Maßnahmen gemäß Frage 1 gewonnen wurden, in Verfahren berücksichtigt, die sich nicht gegen Personen gemäß Frage 2 richteten?

Auf die Vorbemerkung der Bundesregierung sowie den als Verschlussache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil wird verwiesen.

4. In wie vielen Fällen gemäß Frage 1 wurden Informationen nicht verwendet, da sie den Kernbereich privater Lebensführung betrafen, und in wie vielen Fällen wurden Informationen, die bereits Eingang in Ermittlungsakten gefunden hatten, aus diesem Grund später ausgeschlossen?

Auf die Vorbemerkung der Bundesregierung sowie den als Verschlussache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil wird verwiesen.

5. Wie können sich nach Kenntnis der Bundesregierung das eine Quellen-TKÜ anordnende Gericht und die die Maßnahme beantragende oder bei Gefahr im Verzug zunächst entscheidende Staatsanwaltschaft sowie die durchführenden Behörden Gewissheit darüber verschaffen, dass wie in der StPO vorgeschrieben technisch sichergestellt ist,
 - a) dass ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet werden kann (§ 100a Absatz 5 Satz 1 Nummer 1a StPO) oder dass ausschließlich gespeicherte Inhalte und Umstände der Kommunikation, die ab der TKÜ-Anordnung während des laufenden Übertragungsvorgangs hätten überwacht und aufgezeichnet werden können, überwacht und aufgezeichnet werden können (§ 100a Absatz 5 Satz 1 Nummer 1b StPO) und die Quellen-TKÜ nicht zu einem Vollzugriff auf Inhalte und Ressourcen des Zielsystems führt und damit faktisch eine rechtswidrige Online-Durchsuchung bedeutet;
 - b) dass am Zielsystem nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind (§ 100a Absatz 5 Satz 1 Nummer 2 StPO) und die vorgenommenen Veränderungen am Zielsystem soweit technisch automatisch rückgängig gemacht werden (§ 100a Absatz 5 Satz 1 Nummer 3 StPO)?

Die zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung (TKÜ) eingesetzten Softwareprodukte werden vor der Einsatzfreigabe umfassend hinsichtlich der Erfüllung der gesetzlichen Vorgaben überprüft. Die Ergebnisse dieser Prüfung stehen den in der Fragestellung genannten Stellen auf Anforderung zur Einsichtnahme zur Verfügung.

6. Wie können sich nach Kenntnis der Bundesregierung das eine Quellen-TKÜ anordnende Gericht und die die Maßnahme beantragende oder bei Gefahr im Verzug zunächst entscheidende Staatsanwaltschaft sowie die durchführenden Behörden Gewissheit darüber verschaffen, dass
 - a) die Spähsoftware („das eingesetzte Mittel“ in der Terminologie der StPO) nach dem Stand der Technik gegen unbefugte Nutzung geschützt ist (§ 100a Absatz 5 Satz 2 StPO) und

Auf die Antwort zu Frage 5 wird verwiesen.

- b) die Maßnahme nicht unzulässig ist, weil sie allein den Kernbereich privater Lebensgestaltung betrifft (§ 100d Absatz 1 StPO)?

Vor der Durchführung einer Quellen-TKÜ-Maßnahme wird der zugrundeliegende Sachverhalt gemäß der gesetzlichen Vorgaben dahingehend überprüft, ob Anhaltspunkte dafür bestehen, dass ausschließlich Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung gewonnen werden könnten. Im Einzelfall berücksichtigt die – soweit aufgrund der vorliegenden polizeilichen Erkenntnisse und ggf. schon vorliegenden einzelnen Ermittlungsergebnisse mögliche – Prognose die voraussichtliche Art der Nutzung des überwachten Anschlusses/der überwachten Kennung oder des erwartbaren Verhältnisses der möglichen Telekommunikationsteilnehmer. Die Staatsanwaltschaft prüft dies im Rahmen der Entscheidung über die Beantragung der Maßnahme ebenso wie das anordnende Gericht. Die Pflicht der durchgängigen Prüfung des Kernbereichsschutzes bei der Durchführung der Maßnahme selbst ist hiervon unberührt.

7. Wie können sich nach Kenntnis der Bundesregierung das eine Online-Durchsuchung anordnende Gericht und die die Maßnahme beantragende Staatsanwaltschaft sowie die durchführenden Behörden Gewissheit darüber verschaffen, dass wie in der StPO vorgeschrieben
 - a) soweit möglich technisch sichergestellt ist, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden (§ 100d Absatz 3 Satz 1 StPO),
 - b) technisch sichergestellt ist, dass am Zielsystem nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind (§ 100b Absatz 4 i. V. m. § 100a Absatz 5 Satz 1 Nummer 2 StPO),
 - c) die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisch rückgängig gemacht werden (§ 100b Absatz 4 i. V. m. § 100a Absatz 5 Satz 1 Nummer 3 StPO), und
 - d) die Spähsoftware („das eingesetzte Mittel“ in der Terminologie der StPO) nach dem Stand der Technik gegen unbefugte Nutzung geschützt ist (§ 100b i. V. m. § 100a Absatz 5 Satz 2 StPO)?

Die zur Durchführung von Maßnahmen der Online-Durchsuchung eingesetzten Softwareprodukte werden vor Einsatzfreigabe umfassend hinsichtlich der Erfüllung der gesetzlichen Vorgaben überprüft. Die Ergebnisse dieser Prüfung stehen den in der Fragestellung genannten Stellen auf Anforderung zur Einsichtnahme zur Verfügung.

8. Was bedeutet es für die bei Maßnahme-Antrag und Maßnahme-Anordnung vorzunehmenden Verhältnismäßigkeitsabwägungen, wenn eine Rückgängigmachung (siehe Fragen 5b und 7c) technisch nicht oder nicht vollständig möglich ist?

Die abschließende Beurteilung der Verhältnismäßigkeit einer Maßnahme obliegt der anordnenden Stelle. Die beantragende oder anordnende Stelle wird die genannten Aspekte im Einzelfall im Rahmen der Beantragung bzw. Anordnung der Maßnahme in die Abwägung einstellen.

9. Wenn eine von einer Privatfirma erstellte Spähsoftware eingesetzt werden soll, wie wird nach Kenntnis der Bundesregierung sichergestellt, dass die eingesetzte Spähsoftware die einzelnen Vorgaben der StPO (siehe Fragen 5 bis 7) einhält?

Auf die Antwort zu den Fragen 5 und 7 wird verwiesen.

10. Liegt nach Kenntnis der Bundesregierung einer die Maßnahme beantragenden Staatsanwaltschaft und einem die Maßnahme anordnenden Gericht sowie den durchführenden Behörden eine von unabhängiger Stelle erstellte Zertifizierung darüber vor, dass die eingesetzte Spähsoftware die einzelnen Vorgaben der StPO (siehe Fragen 5 bis 7) einhält?

Auf die Antwort zu den Fragen 5 und 7 wird verwiesen. Eine „von unabhängiger Stelle erstellte Zertifizierung“ sieht das Gesetz nicht vor.

11. Welche Stelle erstellt ggf. eine Zertifizierung (Frage 10) und ist diese Stelle aufgrund welcher Gestaltung unabhängig?

Auf die Antwort zu Frage 10 wird verwiesen.

12. Bedeutet die Antwort der Bundesregierung zu den Fragen 30 bis 32 der Kleinen Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 19/1434 (S. 11 und 12), dass die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die Quellcodes der Spähsoftware
- a) zugänglich waren oder sind,
 - b) nicht zugänglich waren oder sind,
- und im Falle b), warum nicht?

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat im Juni 2016 einen Kontrollbesuch hinsichtlich der beim Bundeskriminalamt entwickelten Software zur Durchführung von Quellen-TKÜ durchgeführt. Eine Anfrage zur Einsichtnahme in den Quellcode der beim Bundeskriminalamt entwickelten Software zur Durchführung von Quellen-TKÜ wurde durch die BfDI nicht gestellt. Im Übrigen wird auf die Antwort der Bundesregierung zu den Fragen 30 bis 32 der Kleinen Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 19/1434 vom 28. März 2018 verwiesen.

13. Ist die in der zu Frage 12 bezeichneten Antwort der Bundesregierung mehrfach erwähnte externe Überprüfung von Spähsoftware auf Gesetzeskonformität überhaupt geeignet und in der Lage, die Einhaltung der einzelnen Vorgaben der StPO (siehe Fragen 5 bis 7) festzustellen, oder handelt es sich um eine Überprüfung auf lediglich – wie in der vorgenannten Antwort formuliert – „Einhaltung der geforderten Rahmenbedingungen“ und damit um eine allgemeine und nicht im Hinblick auf die Vorgaben der StPO spezifische Überprüfung?

Auf die Antworten zu den Fragen 5 bis 7 wird verwiesen. Die von den Fragestellern angesprochenen „Rahmenbedingungen“ umfassen vollständig die Anforderungen der Strafprozessordnung (StPO).

14. Ist nach Kenntnis der Bundesregierung einer die Maßnahme beantragenden Staatsanwaltschaft und einem die Maßnahme anordnenden Gericht dabei eine eigene Prüfung der Spähsoftware möglich und ggf. anhand welcher Informationen?
- Oder müssen Staatsanwaltschaft und Gericht sich ausschließlich auf die Angaben der die Maßnahme durchführenden Behörden verlassen?

Der Umfang der Prüfung der Anregung oder des Antrags einer strafprozessualen Maßnahme wird von der Staatsanwaltschaft bzw. dem Gericht im Einzelfall festgelegt, wobei die notwendigen – auch technischen – Informationen für die Beurteilung der Recht- und Verhältnismäßigkeit der Maßnahme einbezogen werden.

Vor dem Hintergrund der eindeutigen Maßgabe des Artikels 20 Absatz 3 zweiter Halbsatz des Grundgesetzes können sich Staatsanwaltschaft und Gericht dabei aus Sicht der Bundesregierung auch auf die Angaben der die Maßnahme durchführenden Behörde verlassen.

15. Wird nach Kenntnis der Bundesregierung der die Maßnahme beantragenden Staatsanwaltschaft und dem die Maßnahme anordnenden Gericht, ggf. auf Verlangen, der Quellcode der Spähsoftware zur Verfügung gestellt, und wenn nein, warum nicht?

Auf die Antwort zu Frage 14 wird verwiesen.

16. Wenn zum Aufspielen der Spähsoftware – Fälle kriminalistischer List ausgenommen – bislang unbekannte Schutzlücken des Zielsystems genutzt werden, der Staat sich also als Hacker betätigt, wie wirken sich nach Kenntnis der Bundesregierung dann die vielfach beschriebene Gefährdung der IT-Sicherheit insgesamt durch dieses Vorgehen (etwa: Pohlmann/Riedel, Quellen-TKÜ als Gefahr für die allgemeine IT-Sicherheit, in: Deutsche Richterzeitung Heft 2/2018, S. 52 ff.) und die Schutzpflicht des Staates für die IT-Sicherheit auf die Rechtmäßigkeits- und Verhältnismäßigkeitsprüfung der die Maßnahme beantragenden Staatsanwaltschaft bzw. des anordnenden Gerichts aus?

Rechtfertigt zum Beispiel die Verfolgung eines Bandendiebstahls als möglicher Anlasst einer Online-TKÜ oder Online-Durchsuchung (§§ 100a Absatz 2 Nummer 1j, 100b Absatz 2 Nummer 1h StPO) eine Gefährdung der IT-Sicherheit insgesamt?

Die Prüfung der Verhältnismäßigkeit umfasst alle Umstände der jeweiligen Maßnahme und des jeweiligen Einzelfalls, also auch die Art und Weise der Durchführung. Ergänzend wird auf die Antwort zu Frage 8 verwiesen. Im Übrigen teilt die Bundesregierung nicht die Auffassung der Fragesteller, dass durch die Durchführung einer Quellen-TKÜ die IT-Sicherheit insgesamt gefährdet wird.

17. Umfasst die von der StPO geforderte gerichtliche Anordnung der Maßnahme jeweils das Aufspielen der Spähsoftware auf das Zielgerät zusammen mit dem Ausleiten der Daten, oder kann die Spähsoftware zum Zeitpunkt der Beantragung und/oder Anordnung der Maßnahme schon auf das Zielgerät aufgespielt sein und sich die Beantragung bzw. Anordnung auf das Zulassen des Ausleitens beschränken und so der Richtervorbehalt ausgehöhlt werden?

Wie sind die diesbezüglichen Ausführungen in der Gesetzesbegründung zu verstehen (Bundestagsdrucksache 18/12785, S. 51/52)?

In den Fällen des § 100a Absatz 1 Satz 3 StPO werden nur jene Inhalte und Umstände der Kommunikation erfasst, die zeitlich nach der Überwachungsanordnung gespeichert wurden und die – wären sie nicht verschlüsselt – auch im öffentlichen Telekommunikationsnetz hätten erhoben werden können. Die Vorschriften zu den technischen Anforderungen (§ 100a Absatz 5 Satz 1 Nummer 1 Buchstabe b StPO) stellen sicher, dass nicht auf sonstige Inhalte des informationstechnischen Systems des Betroffenen zugegriffen wird und insbesondere keine Kommunikationsinhalte erfasst werden, die zeitlich vor Erlass der Überwachungsanordnung gesendet wurden.

Auch für den rein theoretischen Fall, dass die Software bereits aufgespielt war, ändert das aber nichts an den Voraussetzungen einer rechtmäßigen strafprozessualen Maßnahme; insbesondere dürfte auf diesem Weg nicht der Richtervorbehalt umgangen werden (vgl. die Rechtsprechung des BVerfG zur zweckändernden Verwendung personenbezogener Daten nach dem Grundsatz der hypothetischen Datenneuerhebung, Entscheidung vom 20. April 2016 (1 BvR 966/09)).

18. Können (ggf. mit welchen Mitteln) – angesichts des Umstandes, dass sich auf insbesondere mobilelektronischen Geräten vielfachst Daten sozusagen des „ganzen Lebens“ der Zielpersonen und vieler anderer Personen (ggf. unbeteiligter Dritter) befinden –
- Kernbereich der Lebensgestaltung und sonstige Daten überhaupt voneinander klar getrennt werden,
 - dieser Kernbereich bei der Online-TKÜ und der Online-Durchsuchung überhaupt geschützt und
 - mithin insgesamt die Anforderung des BVerfG insoweit erfüllt werden (bitte ggf. Ablauf und Sicherung genau beschreiben)?

Für die Maßnahmen der Quellen-TKÜ als auch der Online-Durchsuchung wurden entsprechend der Rechtsprechung des BVerfG Erhebungs- und Verwertungsverbote gesetzlich geregelt. Beide Maßnahmen dürfen nicht durchgeführt werden, wenn tatsächliche Anhaltspunkte vorliegen, dass dadurch ausschließlich Erkenntnisse aus dem Bereich der privaten Lebensgestaltung erlangt werden (§ 100d Absatz 1 StPO). Dabei ist jeweils eine Subsumtion anhand der konkreten Einzelfallumstände vorzunehmen.

Werden im Rahmen der Durchführung der Maßnahmen Erkenntnisse über den Kernbereich der privaten Lebensgestaltung erlangt, dürfen diese nicht verwertet werden. Aufzeichnungen sind unverzüglich zu löschen.

Bei der Online-Durchsuchung ist, soweit wie möglich, technisch sicherzustellen, dass Daten aus dem Kernbereich der privaten Lebensgestaltung nicht erhoben werden (§ 100d Absatz 3 StPO). Sind solche Informationen dennoch erlangt worden, sind diese unverzüglich zu löschen oder von der Staatsanwaltschaft dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit vorzulegen, dessen Entscheidung für das weitere Verfahren bindend ist.

19. Inwiefern ist die u. a. im Fall der Oldschool Society angewandte Ermittlungsmethode, heimlich ein weiteres Smartphone zum Mithören anzumelden, aus kriminalistischer Sicht (ggf. nach Einschätzung der Bundesregierung) geeignet, eine Quellen-TKÜ-Maßnahme auf dem jeweiligen Zielgerät zu ersetzen?

Auf die Vorbemerkung der Bundesregierung sowie den als Verschlussache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuftem Antwortteil wird verwiesen.

20. In wie vielen Fällen wurde die Ermittlungsmethode in Frage 19 in den letzten drei Jahren nach Kenntnis der Bundesregierung angewandt?

Auf die Vorbemerkung der Bundesregierung sowie den als Verschlussache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuftem Antwortteil wird verwiesen.

21. Welche Kosten insgesamt sind seit 2015 für die Entwicklung und den Ankauf von Spähsoftware sowie den Ankauf von Sicherheitslücken entstanden?

Auf die Vorbemerkung der Bundesregierung sowie den als Verschlussache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuftem Antwortteil wird verwiesen.

22. Ist die Kostenangabe in www.sueddeutsche.de/digital/ueberwachung-polizeispioniert-handynutzer-mit-trojaner-aus-1.3842439 („In Haushaltsunterlagen für das Jahr 2017 beantragte das BKA Sachmittel im Umfang von 50 Millionen Euro, um die „operativen IT-Systeme“ zu verbessern. Der Smartphone-Trojaner wurde damals als „3. Produktlinie“ bezeichnet. Die erste und zweite Produktlinie galt Laptops und Desktop-Rechnern.“) zutreffend oder inwieweit unzutreffend, und welcher Betrag für operative IT-Systeme ist für den Haushalt 2018 angemeldet und mit welchen Jahresbeträgen in die Finanzplanung eingestellt?

Eine Aufschlüsselung bzw. Spezifizierung der Begrifflichkeit „[Verbesserung von] operative[n] IT-Systeme[n]“ i. S. d. haushalterischen Betrachtung ist dem Bundeskriminalamt nicht möglich. Zu diesem Oberbegriff liegen keine zweckgebundenen Haushaltsplanungen vor.

