

Antwort der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Martina Renner,
Dr. André Hahn, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/316 –**

Einsätze von sogenannten stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen sowie Software zur Bildersuche im zweiten Halbjahr 2017

Vorbemerkung der Fragesteller

Halbjährlich fragen die Abgeordneten der Fraktion DIE LINKE. beim Bundesministerium des Innern, beim Bundesministerium der Finanzen und beim Bundeskanzleramt nach den Zahlen von Einsätzen digitaler Fahndungsmethoden (vgl. die Bundestagsdrucksachen 18/11041, 18/4130, 18/2257, 18/5645, 18/7285, 18/9366, 18/13205). Hintergrund ist die zunehmende Überwachung und Analyse digitaler Verkehre, die das Vertrauen in die Freiheit des Internet und der Telekommunikation untergraben. Aus Antworten aus früheren Anfragen geht hervor, dass dies vor allem den polizeilichen Bereich betrifft: Der Einsatz sogenannter stiller SMS, WLAN-Catcher und IMSI-Catcher nimmt zu, die Ausgaben für Analysesoftware steigen ebenfalls. Aus Sicht der Fragestellerinnen und Fragesteller sind diese Maßnahmen mitunter rechtlich gar nicht gestattet, etwa der Einsatz sogenannter stiller SMS. Denn Polizei und Geheimdienste dürfen nur passiv die Kommunikation von Telefonen abhören, die sogenannten stillen SMS werden aber von den Behörden erst erzeugt. Während die Bundesregierung zwar Angaben zu sogenannten stillen SMS des Bundeskriminalamtes und der Bundespolizei macht, bleiben Zahlen für den Zoll als Verschlusssache eingestuft. Hinsichtlich des Bundesnachrichtendienstes unterbleibt jede Mitteilung.

Vorbemerkung der Bundesregierung

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Fragen 1 bis 11 in offener Form ganz oder teilweise nicht erfolgen kann.

Die in den genannten 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 Aufklärungsaktivitäten und Analysemethoden stehen. Die Antworten auf die Kleine Anfrage beinhalten zum Teil detaillierte Einzelhei-

ten 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.

Eine Beantwortung der Fragen 1, 2, 4, 6, 7 und 9 bis 11 für den Bundesnachrichtendienst (BND) sowie der Fragen 7, 10 und 11 und eines Teils der Frage 4 für das Bundesamt für Verfassungsschutz (BfV) kann nicht in offener Form erfolgen. Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik von BND und BfV und insbesondere deren Aufklärungsaktivitäten und Analysemethoden stehen. Der Schutz vor allem der technischen Aufklärungsfähigkeiten des BND und des BfV im Bereich der Fernmeldeaufklärung stellt für deren Aufgabenerfüllung einen überragend wichtigen Grundsatz dar. Er dient der Aufrechterhaltung der Effektivität nachrichtendienstlicher Informationsbeschaffung durch den Einsatz spezifischer Fähigkeiten und damit dem Staatswohl. Eine Veröffentlichung von Einzelheiten betreffend solche Fähigkeiten würde zu einer wesentlichen Schwächung der den Nachrichtendiensten zur Verfügung stehenden Möglichkeiten zur Informationsgewinnung führen. Dies würde für die Auftragserfüllung des BND und des BfV erhebliche Nachteile zur Folge haben und kann für die Interessen der Bundesrepublik Deutschland schädlich sein. Insofern könnte die Offenlegung entsprechender Informationen die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen. Deshalb sind die entsprechenden Informationen als Verschlussache gemäß VSA mit dem VS-Grad „VS – Geheim“ bzw. „VS – Vertraulich“ eingestuft.

Darüber hinaus kann eine Beantwortung der Fragen 6 und 7 sowie eines Teils der Frage 9 für den Militärischen Abschirmdienst (MAD) sowie der Frage 6 für das militärische Nachrichtenwesen nicht in offener Form erfolgen. Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit Arbeitsweisen des MAD und des militärischen Nachrichtenwesens stehen bzw. Rückschlüsse auf technische und operative Einsatzmöglichkeiten sowie der Methodik der Datenanalyse zulassen. Ihr Schutz ist für die Aufgabenerfüllung des MAD bzw. des militärischen Nachrichtenwesens von überragender Bedeutung.

Die Abwägung des Aufklärungs- und Informationsrechts der Fragesteller mit den Sicherheitsinteressen der Bundesrepublik Deutschland bzw. dem Staatswohl führt insoweit zu einer höheren Gewichtung der Sicherheitsinteressen bzw. des Staatswohls.

Detaillierte Angaben zu den technischen Fähigkeiten und Methoden des MAD oder des militärischen Nachrichtenwesens sind lediglich für den parlamentarischen Bereich, nicht jedoch für die Kenntnisnahme einer breiten Öffentlichkeit bestimmt. Eine solche Bekanntgabe würde der Öffentlichkeit und damit möglicherweise fremden Nachrichtendiensten und Streitkräften Informationen über Fähigkeiten und Methoden des MAD oder des militärischen Nachrichtenwesens offenlegen. Das würde dem staatlichen Geheimhaltungsinteresse in diesen Bereichen evident widersprechen und erhebliche Nachteile für die Auftragserfüllung des MAD bzw. des militärischen Nachrichtenwesens haben.

Insofern würde die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland schädlich sein. Deshalb sind die entsprechenden Informationen als Verschlussache gemäß VSA mit dem VS-Grad „VS – Vertraulich“ eingestuft.*

1. Wie oft haben welche Bundesbehörden im zweiten Halbjahr 2017 von „WLAN-Catchern“ Gebrauch gemacht?
 - a) Welche Bundesbehörden haben zwar selbst keine „WLAN-Catcher“ eingesetzt, sich hierfür aber der Amtshilfe anderer Behörden oder Firmen bedient (bitte außer den Zahlen auch die beteiligten Behörden benennen)?
 - b) Wie viele Personen und Ermittlungsverfahren waren jeweils insgesamt betroffen (bitte nach Informationsgewinnung, Gefahrenabwehr und Strafverfolgung differenzieren)?
 - c) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?
 - e) Welche Hard- und Software wird für die „WLAN-Catcher“ genutzt, bzw. welche Änderungen haben sich hierzu gegenüber dem vorigen Halbjahr ergeben (vgl. die Bundestagsdrucksachen 17/14714, 18/2257, 18/4130, 18/7285)?

Die Fragen 1 bis 1c und 1e werden gemeinsam beantwortet.

Die Bundespolizei, das Bundeskriminalamt und der Zoll haben im zweiten Halbjahr 2017 keinen WLAN-Catcher eingesetzt. In den Ermittlungsverfahren des Generalbundesanwalts wurde ebenfalls kein „WLAN-Catcher“ eingesetzt. Im Übrigen wird auf die als „VS – Nur für den Dienstgebrauch“ sowie „VS – Geheim“ eingestuften Antwortteile gemäß der Vorbemerkung der Bundesregierung verwiesen.

- d) Wie viele Betroffene der Maßnahmen aus dem vorigen Halbjahr sind über die Maßnahmen mittlerweile nachträglich benachrichtigt worden?

Es wird auf die Antwort der Bundesregierung zu Frage 1 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/13205 vom 28. Juli 2017 verwiesen. Im Übrigen liegen der Bundesregierung hierzu keine Informationen vor.

- f) Inwiefern haben die Maßnahmen im zweiten Halbjahr 2017 aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitragen?

Es wird auf die Antwort der Bundesregierung zu Frage 1e der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/9366 vom 9. August 2016 verwiesen, deren Aussagen weiter gelten.

* Die vom Bundesministerium des Innern als „VS – Vertraulich“ und „VS – Geheim“ eingestuften Antwortteile sind in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und können dort nach Maßgabe der Geheimschutzordnung eingesehen werden. Die vom Bundesministerium des Innern als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteile sind im Parlamentssekretariat des Deutschen Bundestages hinterlegt und können dort von Berechtigten eingesehen werden.

2. Welche Bundesbehörden haben im zweiten Halbjahr 2017 wie oft „IMSI-Catcher“ eingesetzt?

Im fragegegenständlichen Zeitraum haben das Bundeskriminalamt in 13 Fällen und die Bundespolizei in 61 Fällen „IMSI-Catcher“ eingesetzt. In diesen Gesamtzahlen sind auch Unterstützungsmaßnahmen für andere Behörden enthalten.

Im Übrigen wird auf die als „VS – Nur für den Dienstgebrauch“ sowie „VS – Geheim“ eingestuften Antwortteile gemäß der Vorbemerkung der Bundesregierung verwiesen.

- a) Welche Bundesbehörden haben zwar selbst keine „IMSI-Catcher“ eingesetzt, sich hierfür aber der Amtshilfe anderer Behörden oder Firmen bedient (bitte außer den Zahlen auch die beteiligten Behörden benennen)?

Im zweiten Halbjahr 2017 wurden in den Ermittlungsverfahren des Generalbundesanwalts „IMSI-Catcher“ durch das Bundeskriminalamt sowie durch die Landeskriminalämter Berlin und Hessen eingesetzt.

Der Zoll verfügt über keine eigenen „IMSI-Catcher“. Für die Einsätze des Zolls wurde im Rahmen der Amtshilfe auf die Geräte des Bundeskriminalamtes, der Bundespolizei sowie verschiedener Landeskriminalämter zurückgegriffen. Eine statistische Erfassung erfolgt hierzu nicht.

- b) Wie viele Personen und Ermittlungsverfahren waren jeweils insgesamt betroffen (bitte nach Informationsgewinnung, Gefahrenabwehr und Strafverfolgung differenzieren)?

Im fragegegenständlichen Zeitraum wurden „IMSI-Catcher“ eingesetzt

- in Umsetzung entsprechender Beschlüsse des Ermittlungsrichters des Bundesgerichtshofs in 6 Ermittlungsverfahren des Generalbundesanwalts gegen 10 betroffene Personen,
- durch das Bundeskriminalamt in 13 strafprozessualen Ermittlungsverfahren mit 23 betroffenen Personen sowie
- durch die Bundespolizei in strafprozessualen Ermittlungsverfahren gegen 56 Beschuldigte, von denen 43 durch den Einsatz des „IMSI-Catchers“ betroffen waren.

Im Übrigen wird auf die als „VS – Nur für den Dienstgebrauch“ sowie „VS – Geheim“ eingestuften Antwortteile gemäß der Vorbemerkung der Bundesregierung verwiesen. Darüber hinaus liegen der Bundesregierung hierzu keine statistischen Informationen vor.

- c) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?

In den in der Antwort zu Frage 2b genannten Fällen, in denen in Umsetzung entsprechender Beschlüsse des Ermittlungsrichters des Bundesgerichtshofes „IMSI-Catcher“ in Ermittlungsverfahren des Generalbundesanwalts eingesetzt wurden, sind die Betroffenen bislang nicht benachrichtigt worden. In allen Fällen handelt es sich um laufende Ermittlungsverfahren, in denen die Gefährdung des Ermittlungszwecks einer Benachrichtigung derzeit noch entgegensteht.

Im Übrigen wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen. Darüber hinaus obliegt die fragegegenständliche Benachrichtigung von Betroffenen den

Landesstaatsanwaltschaften. Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

- d) Wie viele Betroffene der Maßnahmen aus dem vorigen Halbjahr sind über die Maßnahmen mittlerweile nachträglich benachrichtigt worden?

Betreffend die Maßnahmen aus dem vorigen Halbjahr, in denen „IMSI-Catcher“ in Umsetzung entsprechender Beschlüsse des Ermittlungsrichters des Bundesgerichtshofes in Ermittlungsverfahren des Generalbundesanwalts eingesetzt wurden, sind sechs Betroffene mittlerweile nachträglich hierüber benachrichtigt worden.

Darüber hinaus obliegt die fragegegenständliche Benachrichtigung von Betroffenen den Landesstaatsanwaltschaften. Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

- e) Inwiefern haben die Maßnahmen im zweiten Halbjahr 2017 aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitragen?

Soweit bereits abzusehen war, konnten durch den Einsatz des „IMSI-Catchers“ der weiteren Sachaufklärung dienende Erkenntnisse gewonnen werden, wie etwa Erkenntnisse zu weiteren Rufnummern. Im Übrigen wird auf die Antwort der Bundesregierung zu Frage 2c der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/4130 vom 26. Februar 2015 verwiesen, deren Aussagen weiter gelten.

- f) Für welche deutschen Firmen bzw. Lizenznehmer ausländischer Produkte wurden seitens der Bundesregierung im zweiten Halbjahr 2017 Ausfuhrgenehmigungen für „IMSI-Catcher“ in welche Bestimmungsländer erteilt?

Im fragegegenständlichen Zeitraum wurden Ausfuhrgenehmigungen für sogenannte „IMSI-Catcher“ in die Bestimmungsländer Jordanien, Rumänien und Schweiz erteilt. Zu einzelnen Unternehmen können zur Wahrung von Betriebs- und Geschäftsgeheimnissen keine Angaben gemacht werden.

3. Wie hat sich die Zahl der vom Bundesamt für Sicherheit in der Informationstechnik oder von anderen zuständigen Bundesbehörden (auch in deren Auftrag) aufgespürten IMSI-Catcher bzw. ähnlichen Abhöreranlagen für den Mobilfunkverkehr im Regierungsviertel oder in räumlicher Nähe zu anderen Bundesbehörden seit 2010 entwickelt, und in welchen Fällen konnten die Betreiber der Anlagen durch Bundesbehörden ausfindig gemacht werden (bitte diese Verantwortlichen jeweils benennen)?

Es wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuftem Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.

4. Welche Behörden des Bundesministeriums des Innern, des Bundesministeriums der Justiz und für Verbraucherschutz, des Bundesministeriums der Finanzen, des Bundeskanzleramtes und der Bundeswehr sind derzeit technisch und rechtlich in der Lage, an Mobiltelefone sogenannte Stille SMS zum Ausforschen des Standortes ihrer Besitzer/Besitzerinnen oder zum Erstellen von Bewegungsprofilen zu verschicken, bzw. welche Änderungen haben sich gegenüber dem vorigen Halbjahr ergeben?

Das Bundeskriminalamt, die Bundespolizei und der Zoll sind rechtlich und technisch in der Lage, sogenannte „Stille SMS“ an Mobiltelefone zu versenden. Das BfV setzt „Stille SMS“ ausschließlich im Rahmen angeordneter und durch die G10-Kommission des Deutschen Bundestages genehmigter Beschränkungsmaßnahmen ein. Gleiches gilt für den MAD.

Für die Bundeswehr im Übrigen wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil der Bundesregierung der Kleinen Anfrage der Fraktion DIE LINKE. zu Frage 2 auf Bundestagsdrucksache 18/5645 vom 24. Juli 2015 verwiesen.

- a) Welche Bundesbehörden haben zwar selbst keine „Stillen SMS“ eingesetzt, sich hierfür aber anderer Behörden oder Firmen bedient (bitte außer den Zahlen auch die beteiligten Behörden benennen)?

Auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung wird verwiesen.

- b) Wie viele „Stille SMS“ wurden von den jeweiligen Behörden im zweiten Halbjahr 2017 bzw. in deren Auftrag durch andere Behörden oder Firmen insgesamt jeweils versandt (bitte bezüglich des Zollkriminalamts nach den einzelnen Zollfahndungsämtern aufschlüsseln)?

Zeitraum	BfV	BKA	BPOL
2. Halbjahr 2017	179.258	21.932	33.645

Im Übrigen wird auf die als „VS – Nur für den Dienstgebrauch“ sowie „VS – Geheim“ eingestuften Antwortteile gemäß der Vorbemerkung der Bundesregierung verwiesen.

- c) Wie viele Personen und Ermittlungsverfahren waren jeweils betroffen (bitte nach Informationsgewinnung, Gefahrenabwehr und Strafverfolgung differenzieren)?

Es wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen. Darüber hinaus können weitere Angaben über die Anzahl betroffener Personen und Ermittlungsverfahren mangels entsprechender statistischer Erfassungen nicht gemacht werden.

- d) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?
 e) Wie viele Betroffene der Maßnahmen aus dem vorigen Halbjahr sind über die Maßnahmen mittlerweile nachträglich benachrichtigt worden?

Die Fragen 4d und 4e werden gemeinsam beantwortet.

Beim BfV erfolgt der Einsatz „Stiller SMS“ nur im Rahmen angeordneter G10-Beschränkungsmaßnahmen. Eine Mitteilung über die Durchführung erfolgt nach

§ 12 G10 (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses).

Darüber hinaus obliegt die fragegegenständliche Benachrichtigung von Betroffenen den Landesstaatsanwaltschaften. Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

- f) Welche Hard- und Software wird zum Versand und zur Auswertung von „Stillen SMS“ genutzt, bzw. welche Änderungen haben sich hierzu gegenüber dem vorigen Halbjahr ergeben (vgl. Bundestagsdrucksache 18/13205)?

Zur Beantwortung der Frage 4f wird hinsichtlich des Zolls auf die Antwort zu Frage 4a verwiesen. Im Übrigen wird auf den als „VS – Geheim“ eingestuften Antwortteil gemäß der Vorbemerkung sowie auf die Antwort der Bundesregierung zu Frage 4f der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/5645 vom 24. Juli 2015 verwiesen. Im fragegegenständlichen Zeitraum haben sich hierzu keine Änderungen ergeben.

- g) Inwiefern haben die Maßnahmen aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitragen?

Es wird auf die Antwort der Bundesregierung zu Frage 2c der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/4130 vom 26. Februar 2015 verwiesen, deren Aussagen weiter gelten.

5. Wie viele Maßnahmen der Funkzellenauswertung haben welche Behörden des Bundesministeriums des Innern, des Bundesministeriums der Justiz und für Verbraucherschutz, des Bundesministeriums der Finanzen, des Bundeskanzleramtes und der Bundeswehr im zweiten Halbjahr 2017 vorgenommen (bitte wie auf Bundestagsdrucksache 17/14714 beantworten)?

Im zweiten Halbjahr 2017 wurden durch das Bundeskriminalamt 376, durch die Bundespolizei 28 und von den Behörden des Zollfahndungsdienstes 12 Funkzellenauswertungen durchgeführt. Der Bundesnachrichtendienst hat im fragegegenständlichen Zeitraum keine Funkzellenauswertung vorgenommen. Im Übrigen wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.

- a) Welche Bundesbehörden haben zwar selbst keine Maßnahmen der Funkzellenauswertung eingesetzt, sich hierfür aber der Amtshilfe anderer Behörden bedient (bitte außer den Zahlen auch die beteiligten Behörden benennen)?

Im fragegegenständlichen Zeitraum wurden in den Ermittlungsverfahren des Generalbundesanwalts Funkzellenauswertungen durch das Bundeskriminalamt sowie die Landeskriminalämter Berlin und Hamburg durchgeführt.

- b) Wie viele Anschlüsse, Personen und Ermittlungsverfahren waren jeweils insgesamt betroffen?

In Umsetzung von Beschlüssen des Ermittlungsrichters des Bundesgerichtshofs wurden im fragegegenständlichen Zeitraum in drei Ermittlungsverfahren des Generalbundesanwalts Funkzellenabfragen durchgeführt. Weitere Angaben können mangels statistischer Erfassung nicht gemacht werden.

- c) Welche der Funkzellenabfragen wurden vom Ermittlungsrichter des Generalbundesanwalts beim Bundesgerichtshof gestattet, und im Zusammenhang mit welchen Ermittlungen fanden diese statt?

Auf die Antwort zu Frage 5b wird verwiesen. Die Ermittlungen betreffen den Tatvorwurf der Mitgliedschaft in einer terroristischen Vereinigung im Ausland und damit zusammenhängende Straftaten sowie den Tatvorwurf des Mordes. In einem weiteren Verfahren betreffen die Ermittlungen den Verdacht der verfassungsfeindlichen Sabotage, der Bildung einer kriminellen Vereinigung und anderer Delikte wegen Brandanschlägen auf Kabelschächte an Bahnanlagen in Leipzig, Köln, Hamburg, Dortmund, Berlin, Bremen und Bad Bevensen am 19. Juni 2017.

Bezogen auf das Bundeskriminalamt wurde ein Beschluss des Ermittlungsrichters beim Bundesgerichtshof in einem Ermittlungsverfahren des Generalbundesanwalts u. a. wegen Beteiligung an einer kriminellen Vereinigung gem. § 129 des Strafgesetzbuches (StGB) zur Funkzellendatenauswertung umgesetzt.

- d) Wie viele Betroffene sind über die Maßnahmen nachträglich benachrichtigt worden (bitte nach Informationsgewinnung, Gefahrenabwehr und Strafverfolgung differenzieren)?

Von den in den Ermittlungsverfahren des Generalbundesanwalts Betroffenen (Antwort zu Frage 5b) wurde bisher ein Betroffener nachträglich hierüber benachrichtigt.

Darüber hinaus obliegt die fragegegenständliche Benachrichtigung von Betroffenen den Landesstaatsanwaltschaften. Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

- e) Wie viele Betroffene der Maßnahmen aus dem vorigen Halbjahr sind über die Maßnahmen mittlerweile nachträglich benachrichtigt worden?

Soweit die Ermittlungsverfahren des Generalbundesanwalts dort noch anhängig sind, wurden die Betroffenen der Maßnahmen aus dem vorigen Halbjahr bisher nicht nachträglich über die Maßnahmen benachrichtigt. Darüber hinaus obliegt die fragegegenständliche Benachrichtigung von Betroffenen den Landesstaatsanwaltschaften. Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

- f) Inwiefern haben die Maßnahmen aus dem zweiten Halbjahr 2017 aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitrugen?

Der Einsatz der technischen Maßnahme hat in einem Fall wesentlich zur Aufklärung des Tatvorwurfs beigetragen. Im Übrigen handelt es sich um noch laufende Ermittlungsverfahren.

Im Übrigen wird auf die Antwort der Bundesregierung zu Frage 5d der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/4130 vom 26. Februar 2015 verwiesen, deren Aussagen weiter gelten.

6. Inwiefern sind Behörden des Bundesministeriums des Innern, des Bundesministeriums der Justiz und für Verbraucherschutz, des Bundesministeriums der Finanzen, des Bundeskanzleramtes und der Bundeswehr mittlerweile in der Lage, Mikrofone von Mobiltelefonen aus der Ferne zu aktivieren, um diese als Abhöreinrichtungen zu nutzen, in welchem Umfang wird dies bereits genutzt, und welche Soft- oder Hardware wird hierfür genutzt, bzw. welche Änderungen haben sich gegenüber dem vorigen Halbjahr ergeben?

Das in der Fragestellung beschriebene Verfahren wird vom Bundeskriminalamt nicht durchgeführt. Die Bundespolizei besitzt keine technischen Möglichkeiten zur Durchführung des beschriebenen Verfahrens.

Im Übrigen wird auf die als „VS – Nur für den Dienstgebrauch“, „VS – Vertraulich“ und „VS – Geheim“ eingestufteten Antwortteile gemäß der Vorbemerkung der Bundesregierung verwiesen.

7. Welche Software zur computergestützten Bildersuche bzw. zu Bildervergleichen haben polizeiliche oder geheimdienstliche Bundesbehörden im zweiten Halbjahr 2017 (auch testweise) beschafft, nach welchem Verfahren funktioniert diese, wo wird diese jeweils genutzt bzw. welche Nutzung ist anvisiert, welche konkreten Behörden bzw. welche von deren Abteilungen sind bzw. wären darauf zugriffsberechtigt, in welchen Ermittlungen kommen bzw. kämen diese im Einzel- oder Regelfall zur Anwendung, bzw. welche Änderungen haben sich gegenüber dem vorigen Halbjahr ergeben?

Im Bundeskriminalamt wurden im zweiten Halbjahr 2017 zwei Einzelplatzlizenzen für die Software „Videmo 360 Search“ beschafft. Hierbei handelt es sich um eine Software zum Durchsuchen von Videodateien mithilfe von maschineller Gesichtserkennung, die auf allgemeinen Verfahren zur biometrischen Gesichtserkennung basiert. Der Einsatz findet nur im repressiven Bereich im Rahmen von Ermittlungsverfahren statt.

Im Übrigen wird auf die als „VS – Vertraulich“ sowie „VS – Geheim“ eingestufteten Antwortteile gemäß der Vorbemerkung der Bundesregierung sowie auf die Antwort der Bundesregierung zu Frage 7 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/13205 vom 28. Juli 2017 verwiesen.

- a) Welche Kosten sind für Tests oder die Beschaffung entsprechender Software entstanden?

Für die Beschaffung der in der Antwort zu Frage 7 genannten Lizenzen für das Bundeskriminalamt sind im fragegegenständlichen Zeitraum Kosten i. H. v. 13 328 Euro entstanden.

Darüber hinaus wird auf die als „VS – Nur für den Dienstgebrauch“, „VS – Vertraulich“ sowie „VS – Geheim“ eingestufteten Antwortteile gemäß der Vorbemerkung der Bundesregierung sowie auf die Antwort der Bundesregierung zu Frage 7a der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/13205 vom 28. Juli 2017 verwiesen.

- b) Auf welche Datensätze kann die etwaige, neu beschaffte Software zugreifen, nach welchem Verfahren funktioniert diese, wo wird diese jeweils genutzt, und welche konkreten Behörden bzw. welche von deren Abteilungen sind darauf zugriffsberechtigt?

Im Bundeskriminalamt ist ein direkter oder automatisierter Zugriff auf bzw. Abgleich mit vorhandenen Datenbeständen durch die Software nicht möglich. Die zu untersuchenden Videodateien sind der Software durch vorherige Auswahl des Speicherortes bzw. der jeweiligen Videodatei zuzuweisen. Der Zugriff und die Bedienung der Software sind nur an Computersystemen bei und durch Mitarbeiter des Bundeskriminalamtes möglich und vorgesehen. Im Übrigen wird auf den als „VS – Vertraulich“ eingestuftem Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.

- c) Inwiefern kann die Bundesregierung mitteilen, ob die Anwendung von Software zur computergestützten Bildersuche bzw. zu Bildervergleichen im Vergleich zum vorigen Halbjahr zu- oder abnimmt (bitte auch die Zahlen der bundesweiten Erhebung der entsprechenden Daten für das Jahr 2016 mitteilen, siehe Bundestagsdrucksache 18/11041, Antwort zu Frage 7c)?

Beim Bundeskriminalamt wurden im Kalenderjahr 2017 insgesamt 26 879 Recherchen im zentralen Gesichtserkennungssystem (GES) durchgeführt. Die Anzahl der GES-Recherchen ist somit gegenüber dem Jahr 2016 um 16,5 Prozent (23 064) angestiegen. Darüber hinaus liegen der Bundesregierung keine Erkenntnisse vor.

- d) Inwiefern haben die Maßnahmen aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitragen, bzw. inwiefern lässt sich dies überhaupt rekonstruieren?

Es wird auf die Antwort der Bundesregierung zu Frage 7d der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/13205 vom 28. Juli 2017 verwiesen, deren Aussagen weiter gelten.

8. An welchen Forschungs- oder Pilotprojekten beteiligen sich welche Behörden des Bundesministeriums des Innern hinsichtlich der Entwicklung verbesserter Verfahren zur Gesichtserkennung (auch in temporär geschalteten Uploadportalen, siehe „G20-Gipfel: Polizei durchsucht zehntausende Dateien mit Gesichtserkennungssoftware“, NETZPOLITIK.ORG vom 28. September 2017), und welche Soft- und Hardware welcher Hersteller wird dabei genutzt?

Das Bundesamt für die Sicherheit in der Informationstechnik führt seit Dezember 2017 das Projekt FACETRUST durch. Das Projekt hat zum Ziel, die Erkennungsleistung von automatisierten gesichtsbiometrischen Grenzkontrollsystemen (eGates) weiterzuentwickeln. Dabei ist die zu nutzende Soft- und Hardware Gegenstand der Entwicklung und wird im Laufe des Projekts bestimmt.

Im Rahmen des gemeinsamen Pilotprojekts „Sicherheitsbahnhof Berlin Südkreuz“ von Bundesministerium des Innern, Bundespolizei, Bundeskriminalamt und Deutscher Bahn AG testet die Bundespolizei seit dem 1. August 2017 Systeme zur automatisierten Gesichtserkennung. Ziel der Erprobung ist es, die technische Funktionalität und Zuverlässigkeit aktueller Gesichtserkennungssysteme in Verbindung mit der vorhandenenameratechnik am Bahnhof Berlin Südkreuz zu erheben. Zum Einsatz kommen drei Gesichtserkennungssysteme der Firmen

IDEMIA Identity & Security Germany AG, DELL EMC mit der Software der Firma Herta Security sowie Elbex mit der Software der Firma Anyvision Face Recognition.

Im Übrigen wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.

9. Welche Software welcher Hersteller kommt bei Bundesbehörden zur kriminalpolizeilichen Vorgangsverwaltung und Fallbearbeitung zur Anwendung (bitte nach Vorgangsbearbeitung und kriminalistischer Fallbearbeitung aufschlüsseln), bzw. welche Änderungen haben sich gegenüber dem vorigen Halbjahr ergeben?

Es wird auf die Antwort der Bundesregierung zu Frage 8 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/13205 vom 28. Juli 2017 verwiesen. Hierzu haben sich im fragegegenständlichen Zeitraum keine Änderungen ergeben.

- a) Welche Kosten sind Bundesbehörden im Einzelfall und unter Berücksichtigung der Arbeitszeit innerhalb der Behörde für die Beschaffung, Anpassung, den Service und die Pflege der Software im zweiten Halbjahr 2017 entstanden?

Im fragegegenständlichen Zeitraum sind im Bundeskriminalamt für das Fallbearbeitungssystem „b-case“ Kosten i. H. v. 485 741,64 Euro entstanden (davon 340 941,64 Euro für die Pflege und 144 800 Euro für die Beschaffung von Erweiterungsmodulen).

Für die Weiterentwicklung und Fehlerbeseitigung des Fallbearbeitungssystems INPOL-Fall entstand ein Aufwand in Höhe von ca. 150 Personentagen (unter der Annahme einer Aufwandsverteilung auf interne und externe Mitarbeiter werden Kosten für externe Mitarbeiter in Höhe von 1 000 Euro pro Personentag veranschlagt), die Posten Wartung/Pflege und Testaufwand finden hierbei keine Berücksichtigung. Für externe IT-Dienstleistungen für das Vorgangsbearbeitungssystem (VBS) fielen im Leistungszeitraum Juli bis Oktober 2017 Kosten i. H. v. 355 340,11 Euro an (die Rechnungen für November und Dezember 2017 liegen noch nicht vor).

Im zweiten Halbjahr 2017 wurden Weiterentwicklungsmaßnahmen des Kriminaltechnischen Informationssystems KISS und der dazugehörigen KISS-Module i. H. v. 215 000,00 Euro bei der GFaI beauftragt. Davon wurden bereits Entwicklungsleistungen i. H. v. 45 000 Euro umgesetzt. Die restlichen Entwicklungsleistungen für KISS-Module werden 2018 von der GFaI erbracht. Weiterhin wurden Weiterentwicklungsmaßnahmen i. H. v. 75 000 Euro für FISH bei der GFaI beauftragt. Für die Evaluierung der Maßnahmen und Fachadministrationsaufgaben im laufenden Betrieb der Datenbankanwendungen können für das zweite Halbjahr 2017 ca. 5 000 Euro für Arbeitszeit veranschlagt werden.

Bei der Bundespolizei sind für das Fallbearbeitungssystem Kosten i. H. v. 230 000 Euro angefallen. Für das VBS@rtus-Bund entstanden für Service, Wartung, Pflege und Anpassungen Kosten i. H. v. 285 500 Euro.

Die Kosten für die Arbeitszeiten werden nicht gesondert erhoben.

In der Zollverwaltung sind für die Beschaffung, Anpassung, den Service und Pflege des IT-Systems „IN-ZOLL“ im zweiten Halbjahr 2017 Kosten i. H. v. 3 952 623,72 Euro angefallen, für das IT-Verfahren „ZenDa-ProFiS“ sind Kosten

i. H. v. 600 000 Euro angefallen. Die Kosten für die Arbeitszeit von Mitarbeitern der Zollverwaltung können mangels hierzu geführter Statistiken nicht erhoben werden.

- b) Welche weiteren Produkte der Firma rola Security Solutions GmbH (auch „Zusatzmodule“) wurden für welche Behörden und welche Einsatzzwecke beschafft, bzw. welche Änderungen haben sich gegenüber dem vorigen Halbjahr ergeben?

Im Bereich des Zolls, der Bundespolizei und des Bundeskriminalamtes wurden im fragegegenständlichen Zeitraum keine weiteren Produkte der Firma rola Security Solutions beschafft.

- c) Inwiefern und wofür werden Anwendungen von rola Security Solutions auch bei In- und Auslandsgeheimdiensten der Bundesregierung genutzt, bzw. welche Änderungen haben sich gegenüber dem vorigen Halbjahr ergeben?

Es wird auf die als „VS – Nur für den Dienstgebrauch“ und „VS – Vertraulich“ eingestuften Antwortteile gemäß der Vorbemerkung der Bundesregierung sowie auf die Antwort der Bundesregierung zu Frage 26 der Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 17/14714 vom 6. September 2013 verwiesen.

10. Wie oft haben Behörden des Bundesministeriums des Innern, des Bundesministeriums der Justiz und für Verbraucherschutz, des Bundesministeriums der Finanzen, des Bundeskanzleramtes und der Bundeswehr im zweiten Halbjahr 2017 Trojanerprogramme bzw. ähnliche Überwachungssoftware eingesetzt oder einsetzen lassen (bitte jeweils nach Polizei, Zoll und Geheimdiensten aufschlüsseln)?
- a) Welche der verfügbaren Programme (etwa „Übergangslösung“, Trojaner zur „Onlinedurchsuchung“, Trojaner zur „Quellen-TKÜ“) kamen dabei jeweils zur Anwendung?
- b) In welchem Umfang haben Bundesbehörden im vergangenen Halbjahr Trojaner auf mobilen Geräten platziert?
- c) Wie viele Personen und Ermittlungsverfahren waren von den Einsätzen der Trojaner insgesamt betroffen (bitte differenzieren nach Informationsgewinnung, Gefahrenabwehr und Strafverfolgung)?
- d) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?
- e) Inwiefern haben die Maßnahmen aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitrugen?

Die Fragen 10 bis 10e werden gemeinsam beantwortet.

Es wird auf die als „VS – Nur für den Dienstgebrauch“ und „VS – Geheim“ eingestuften Antwortteile gemäß der Vorbemerkung der Bundesregierung verwiesen.

11. In welchem Umfang haben die Behörden des Bundesministeriums des Innern, des Bundesministeriums der Justiz und für Verbraucherschutz, des Bundesministeriums der Finanzen, des Bundeskanzleramtes und der Bundeswehr im zweiten Halbjahr 2017 die Möglichkeit genutzt, sich Zugang zu Nutzeraccounts bei den Messengerdiensten Signal, WhatsApp, Telegram oder vergleichbaren Anwendungen zu verschaffen, indem sich Ermittlerinnen oder Ermittler dort mit einem weiteren Gerät zum Mitlesen einloggen?

Es wird auf die als „VS – Nur für den Dienstgebrauch“ sowie „VS – Geheim“ eingestufteten Antwortteile gemäß der Vorbemerkung der Bundesregierung verwiesen.

12. In welchem Umfang ist dieses Verfahren dabei misslungen bzw. wurde den Überwachten dieses sogar bekannt (sofern die Bundesregierung hierzu keine Statistiken führt, bitte angeben, ob dies selten oder häufig geschah)?

Zu den in der Fragestellung erbetenen Informationen zu den Erfolgsaussichten der Maßnahmen ist die Bundesregierung nach sorgfältiger Abwägung zu der Auffassung gelangt, dass die Frage nicht beantwortet werden kann.

Gegenstand der Frage sind solche Informationen, die in besonderem Maße das Staatswohl berühren und daher in einer zur Veröffentlichung vorgesehenen Fassung nicht behandelt werden können. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird durch gleichfalls Verfassungsrecht genießende schutzwürdige Interessen wie das Staatswohl begrenzt. Eine Bekanntgabe von Einzelheiten zu den Erfolgsaussichten bei der Ausleitung oder Lesbarmachung der über Messengerdienste erfolgenden elektronischen Kommunikation würde noch weitergehende Rückschlüsse auf die technischen Fähigkeiten und damit mittelbar auch auf die technische Ausstattung und das Aufklärungspotential der Sicherheitsbehörden zulassen als allein schon die Nennung von Fallzahlen. Selbst allgemein gehaltene Aussagen darüber, ob die Maßnahmen „selten“ oder „häufig“ misslingen oder den Überwachten bekannt werden, ließen Rückschlüsse über die technischen Möglichkeiten der Behörden zu und könnten zu einer Änderung des Kommunikationsverhaltens der beobachteten Personen führen. In der Folge wären eine weitere Aufklärung der von diesen verfolgten Bestrebungen und Planungen unmöglich oder stark gefährdet und ein Ersatz durch andere Instrumente nicht möglich. Dadurch könnten die Fähigkeiten, polizeiliche oder nachrichtendienstliche Erkenntnisse mittels Telekommunikationsüberwachung zu gewinnen, in erheblicher Weise negativ beeinflusst werden.

Die Gewinnung von Informationen mittels Telekommunikationsüberwachung ist für die Sicherheit der Bundesrepublik Deutschland und für die Aufgabenerfüllung der Sicherheitsbehörden jedoch unerlässlich.

Sofern solche Informationen entfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen. Dies betrifft insbesondere die Möglichkeiten zur Aufklärung nationaler und internationaler terroristischer Bestrebungen, bei denen derartige Kommunikationsmittel in besonderem Maße von den beobachteten Personen genutzt werden.

Auch eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der Entzifferung für die Aufgabenerfüllung der Sicherheitsbehörden nicht ausreichend Rechnung tragen, weil insoweit auch ein

geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann (vgl. BVerfGE 124, 78 [139]).

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 Sicherheitsbehörden zurückstehen.

13. Welche IT-Infrastruktur (inklusive Speicherkapazitäten) wurde für „Serviceleistungen“ eingerichtet oder vergrößert, die das BKA im Bereich der „Kommunikationsüberwachung“ den Polizeibehörden von Bund und Ländern anbietet (vgl. Bundestagsdrucksache 18/9366), bzw. welche Änderungen haben sich gegenüber dem vorigen Halbjahr ergeben?

Im fragegegenständlichen Zeitraum haben sich keine Änderungen gegenüber dem vorherigen Halbjahr ergeben.

