Deutscher Bundestag **Drucksache 19/25696**

19. Wahlperiode 22.01.2021

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jan Ralf Nolte, Martin Hess, Rüdiger Lucassen, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 19/25553 –

Einsatz der Quellen-Telekommunikationsüberwachung durch Geheimdienste

Vorbemerkung der Fragesteller

Die Quellen- Telekommunikationsüberwachung (TKÜ) ist nach Ansicht der Fragesteller wohl einer der repressivsten und meist umstrittenen behördlichen Maßnahmen in der Strafverfolgung. Daher ist eine dem Gebot der Gewaltenteilung folgende Kontrolle der exekutiven Maßnahmen durch die Judikative in der Demokratie essenziell.

Den ermittelnden Polizeibehörden ist gesetzlich nach § 100 der Strafprozessordnung (StPO) die Durchführung der Quellen-TKÜ erlaubt (https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html). Dies aber ausdrücklich erst nach richterlicher Anordnung (ebd.).

In Zukunft soll nach Beschluss der Bundesregierung der Einsatz von Überwachungssoftware auch durch die Geheimdienste, und das ohne richterliche Kontrolle, möglich sein (https://www.lto.de/recht/hintergruende/h/kabinett-staatstrojaner-geheimdienste-verfassungsschutz-bnd-mad-quellen-ueberwachung-messenger-bverfg-verfassungsbeschwerde/).

1. Welche Einstufung eines Betroffenen erlaubt den Einsatz der „Spionagesoftware“, im Sinne des Verfassungsschutzes ab der Einstufung Prüffall, Verdachtsfall oder Beobachtungsfall, im Sinne der Einstufung des Bundesamtes für den Militärischen Abschirmdienst (BAMAD) in die Kategorie Orange oder Rot?

Die Frage zur „Spionagesoftware“ wird im Zusammenhang der Vorbemerkung auf die Durchführung einer nachrichtendienstlichen Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) bezogen. Die tatbestandlichen Voraussetzungen einer Individualüberwachung nach dem Artikel 10-Gesetz (G 10) sind in dessen § 3 geregelt. Der Tatbestand der Befugnisnorm enthält einen enumerativen Straftatenkatalog und setzt einen entsprechenden individuellen Verdacht voraus.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 21. Januar 2021 übermittelt.

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

Bei Einstufung eines Personenzusammenschlusses als sogenannter „Prüffall“ des Bundesamts für Verfassungsschutz (BfV), wird zunächst geprüft, ob die Voraussetzungen einer nachrichtendienstlichen Beobachtung vorliegen. Nachrichtendienstliche Mittel werden dabei nicht eingesetzt, auch keine Telekommunikationsüberwachung.

Auch der Militärische Abschirmdienst (MAD) setzt keine nachrichtendienstlichen Mittel in sogenannten Prüffällen ein. Im Rahmen der Bearbeitung von Verdachtsfällen (Kategorie „Gelb“) kann auch der MAD unter den tatbestandlichen Voraussetzungen des § 3 G 10 von dem Mittel der Telekommunikationsüberwachung Gebrauch machen.

2. Wie viele Personen sind derzeit von der Verdachtsfallbeobachtung durch die Verfassungsschutzbehörden betroffen?

3. Nach welchen Kriterien werden Personen als Verdachtsfall geführt?

   a) Wie viele Personen werden wegen sogenannter Kennverhältnisse als Verdachtsfall geführt?

   b) Welche sind die juristischen Kriterien, die eine Beobachtung aufgrund von Kennverhältnissen erlauben?

Die Fragen 2 und 3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Einzelne Personen werden aktuell nicht als Beobachtungsobjekt mit Status Verdachtsfall geführt. Beobachtungobjekt sind nach § 4 Absatz 1 des Bundesverfassungsschutzgesetzes (BVerfSchG) vornehmlich Personenzusammenschlüsse. Die Kriterien für die Beobachtung von Einzelpersonen ergeben sich aus § 4 Absatz 1 Satz 4 BVerfSchG. Allgemeine Voraussetzung für die Informationssammlung zu Personen wegen Bestrebungen oder Tätigkeiten nach § 3 Absatz 1 BVerfSchG (auch in einem oder für einen Personenzusammenschluss) ist, dass tatsächliche Anhaltspunkte dafür vorliegen (§ 4 Absatz 1 Satz 3 BVerfSchG).

4. Wie viele Soldaten werden derzeit vom Bundesamt für Militärischen Abschirmdienst (BAMAD) als Kategorie Orange geführt?

   Nach welchen Kriterien werden Soldaten als Orange kategorisiert?

Mit Stand 31. Dezember 2020 waren 29 Soldaten in der Kategorie „Orange“ eingestuft. Die Kriterien für die Einstufung sind vorhaltbare Erkenntnisse, die Zweifel an der Verfassungstreue begründen. Die Frage, ob von der jeweiligen Person auch Bestrebungen gemäß § 1 Absatz 1 des MAD-Gesetzes (MADG) ausgehen, ist Gegenstand weiterer Ermittlungen.

5. Welcher Entscheidungsträger innerhalb der Nachrichtendienste soll den Einsatz der „Spionagesoftware“ billigen?

Gemäß § 9 Absatz 2 G 10 ist der Antrag durch den Behördenleiter oder seinen Stellvertreter zu stellen.

6. Welche Kriterien sind für den Einsatz der Software für die Nachrichtendienste vorgesehen?

Die Sachvoraussetzungen einer Individualüberwachung sind in § 3 G 10 geregelt. Speziell zur Quellen-TKÜ sieht der sich derzeit noch im parlamentarischen Verfahren befindliche Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts (Bundestagsdrucksache 19/24785) in einem in § 11 G 10 einzufügenden neuen Absatz 1a weitere Anforderungen ausdrücklich vor.

7. Soll es den Nachrichtendiensten erlaubt sein, alle Lebensbereiche zu durchleuchten und jede gesammelte Information zu verwerten, oder ist ausschließlich die Sammlung fallrelevanter Daten zulässig?

Die Nachrichtendienste des Bundes sammeln ausschließlich die für ihre gesetzliche Aufgabe erforderlichen Informationen. Es ist nicht ihre Aufgabe, alle Lebensbereiche zu durchleuchten.

8. Welche Kriterien sind für eine richterlich verfügte Quellen-TKÜ derzeit definiert?

Auf die Antwort zu Frage 6 wird verwiesen. An diesem gesetzlichen Maßstab erfolgt die unabhängige Prüfung einer Anordnung nach dem Artikel 10-Gesetz gemäß dessen § 15 durch die G 10-Kommission (die eine dem gerichtlichen Rechtsschutz gleichwertige Kontrolle ausübt, BVerfGE 143, 1 – Rn. 46).

9. Wie häufig wurde im Jahr 2019 eine Quellen-TKÜ beantragt?

   a) Wie oft wurde dieser stattgegeben?

   b) Wie oft wurde diese abgelehnt, und wie wurden die Ablehnungen begründet?

   c) Wie viele Quellen-TKÜ wurden nachträglich als unrechtmäßig getadelt?

Die Fragen 9 bis 9c werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Nach sorgfältiger Prüfung der Bundesregierung können hierzu keine (auch keine eingestuften) Auskünfte erfolgen.

Arbeitsmethoden und Vorgehensweisen der Sicherheitsbehörden des Bundes sind im Hinblick auf die künftige Aufgabenerfüllung besonders schutzwürdig. Bereits die Anzahl der Maßnahmen im sensiblen Computer Network Exploitation (CNE)-Umfeld lässt Rückschlüsse auf die Leistungsfähigkeit bzw. das Überwachungspotential zu.

Die erfragten Informationen zielen im Kern auf die Offenlegung bestimmter nachrichtendienstlicher Arbeitsmethoden und Vorgehensweisen im Bereich der technischen Aufklärung. Solche Arbeitsmethoden sind im Hinblick auf die künftige Erfüllung des gesetzlichen Auftrages der betroffenen Nachrichtendienste jedoch besonders schutzwürdig – der Schutz der technischen Aufklärungsfähigkeiten stellt für die Aufgabenerfüllung der Nachrichtendienste eine überragend wichtige Grundlage dar. Er dient der Aufrechterhaltung der Effektivität nachrichtendienstlicher Informationsbeschaffung durch den Einsatz spezifischer technischer Fähigkeiten und damit dem Staatswohl. Das Bekanntwerden der näheren Umstände der technischen Aufklärungsfähigkeiten, -tätigkeiten und Analysemethoden könnte das Wohl des Bundes gefährden.

Eine Antwort der Bundesregierung auf diese Frage würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik und den konkreten technischen Fähigkeiten der Sicherheitsbehörden einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Dabei würde die Gefahr entstehen, dass ihre bestehenden oder in der Entwicklung befindlichen operativen Fähigkeiten und Methoden aufgeklärt und damit der Einsatzerfolg gefährdet würde. Es könnten entsprechende Abwehrstrategien entwickelt werden. Dies könnte einen erheblichen Nachteil für die wirksame Aufgabenerfüllung der Sicherheitsbehörden und damit für die Interessen der Bundesrepublik Deutschland bedeuten. Vor diesem Hintergrund kann auch das geringe Risiko eines Bekanntwerdens bei einer eingestuften Antwort an die Geheimschutzstelle des Deutschen Bundestages nicht hingenommen werden.

Nach einer sorgfältigen Abwägung ist die Bundesregierung daher zu dem Ergebnis gekommen, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass ausnahmsweise das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

10. Welche Kontrollorgane überprüfen oder begleiten den Einsatz?

    Wie soll konkret das Parlamentarische Kontrollgremium eingebunden werden?

Eine besondere fachaufsichtliche Kontrolle ist durch die ministerielle Anordnungszuständigkeit eingerichtet (§ 10 Absatz 1 G 10). Anordnung und Durchführung von Maßnahmen nach dem Artikel 10-Gesetz sowie die nachfolgende Datenverarbeitung der erlangten personenbezogenen Daten und Betroffenenmitteilung bei den Nachrichtendiensten des Bundes unterliegen nach § 15 Absatz 5 (auch in Verbindung mit den Absätzen 6 und 7 sowie § 12 Absatz 1) einzelfallbezogen der umfassenden Kontrolle der unabhängigen G 10-Kommission, deren Mitglieder vom Parlamentarischen Kontrollgremium bestellt werden (§ 15 Absatz 1 Satz 4 G 10). Zudem erfolgt eine spezielle Kontrolle der Entwicklung der Verwaltungspraxis auch durch das Parlamentarische Kontrollgremium aufgrund des besonderen Berichtswesens nach § 14 Absatz 1 G 10.

11. Werden die Betroffenen über den Einsatz informiert?

Mitteilungen an Betroffene erfolgen gemäß § 12 G 10. Zur Durchführung wird auf die jährlichen Berichte des Parlamentarischen Kontrollgremiums nach § 14 Absatz 1 Satz 2 G 10 verwiesen (zuletzt: Bundestagsdrucksache 19/20376, S. 6).

12. Werden betroffene Dritte (wie bei Telefonüberwachungen) von dem Einsatz der „Spionagesoftware“ informiert?

Gemäß § 12 G 10 werden Betroffene im Sinne des § 3 Absatz 2 Satz 2 G 10 grundsätzlich über gegen sie gerichtete Maßnahmen informiert. Sonstige Personen werden über die verdeckte Maßnahme gegen den Betroffenen nicht informiert.

13. Ist für die Betroffenen ein Rechtsbehelf vorgesehen?

Personen, die annehmen, eine Maßnahme nach dem Artikel 10-Gesetz sei gegen sie gerichtet, können sich zur Prüfung des Sachverhalts an die G 10-

Kommission wenden, die von Amts wegen oder auf Grund von Beschwerden über die Zulässigkeit und Notwendigkeit von Beschränkungsmaßnahmen nach dem Artikel 10-Gesetz entscheidet. Ihrer Kontrolle unterliegen dabei sowohl Erhebung wie auch Weiterverarbeitung personenbezogener Daten durch die Nachrichtendienste des Bundes (§ 15 Absatz 5 G 10). Mit der Mitteilung an den Betroffenen wird zusätzlich der Rechtsweg zu den Verwaltungsgerichten eröffnet (vgl. § 13 G 10).

14. Wie lange werden die gesammelten Daten gespeichert?

15. Wo werden die gesammelten Daten gespeichert?

16. Wie wird sichergestellt, dass Dritten der Zugriff auf die Daten verwehrt wird?

17. Werden gesammelte Daten verbündeten Diensten zur Verfügung gestellt?

Die Fragen 14 bis 17 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Soweit Daten in Durchführung einer Quellen-TKÜ anfallen, werden diese entsprechend der gesetzlichen und untergesetzlichen Vorgaben behandelt. Zur Speicherdauer sind neben den allgemeinen gesetzlichen Regelungen die besonderen Prüfpflichten nach § 4 Absatz 1 G 10 maßgeblich. Die Übermittlung richtet sich nach § 4 Absatz 4 G 10. Die Datensicherheit ist bei den Nachrichtendiensten des Bundes bereits aufgrund des aufgabenprägenden Geheimschutzes generell durch effektive Vorkehrungen gewährleistet.

18. Wie soll die „Spionagesoftware“ auf Endgeräte aufgespielt werden?

Dazu bestehen gegenwärtig verschiedene Optionen, abhängig auch von den konkreten Umständen des Einzelfalls. Nach sorgfältiger Prüfung der Bundesregierung können dazu keine näheren Angaben gemacht werden, da die betreffenden Informationen beziehungsweise ihr Bekanntwerden in besonders hohem Maße das Staatswohl berühren und daher die Frage ausnahmsweise selbst in eingestufter Form nicht beantwortet werden kann.

Eine Offenlegung der angeforderten Informationen und Auskünfte birgt die konkrete Gefahr, dass Einzelheiten zu der Methodik und zu besonders schutzwürdigen spezifischen Fähigkeiten der Nachrichtendienste bekannt würden, infolgedessen sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf die konkreten Vorgehensweisen und Methoden der Nachrichtendienste ziehen könnten.

Dies könnte für die Nachrichtendienste eine höchst folgenschwere Einschränkung der Möglichkeiten der Informationsgewinnung bedeuten, wodurch die sachgerechte Erfüllung der gesetzlich festgelegten Aufgaben der Nachrichtendienste (Sammlung und Auswertung von Informationen) erheblich beeinträchtigt werden könnte. Sofern solche Informationen entfallen oder wesentlich zurückgehen, würden der Bundesrepublik Deutschland empfindliche Informations- und damit Sicherheitslücken drohen.

Auch eine VS-Einstufung und Hinterlegung der angefragten Informationen bei der Geheimschutzstelle des Deutschen Bundestages würde im vorliegenden Fall nicht ausreichen, um der erheblichen Sensibilität der angeforderten Informationen im Hinblick auf die Bedeutung für die Aufgabenerfüllung der Nachrichtendienste ausreichend Rechnung zu tragen. Die angefragten Inhalte be-

schreiben die Fähigkeiten und Arbeitsweisen der Nachrichtendienste so detailliert, dass eine Bekanntgabe auch gegenüber nur einem begrenzten Empfängerkreis ihrem besonderen Schutzbedürfnis nicht Rechnung tragen kann. Aufgrund dieses besonderen Schutzbedürfnisses kann hier auch ein geringfügiges Risiko des Bekanntwerdens nicht hingenommen werden.

Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass vorliegend das Staatswohl ausnahmsweise dem parlamentarischen Informationsrecht entgegensteht.

19. Wie hoch wird das Risiko von vorsätzlichen vorgehaltenen Sicherheitslücken in Systemen bewertet?

20. Sind der Bundesregierung Vorfälle von der Ausnutzung dieser Sicherheitslücken bekannt, und wenn ja, welche?

21. Mit welchen Mitteln soll der unberechtigte Zugriff über die Sicherheitslücken verhindert werden?

    Wer haftet im Schadensfall?

Die Fragen 19 bis 21 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Die Bundesregierung setzt sich inhaltlich mit dieser Thematik auseinander. Die Meinungsbildung innerhalb der Bundesregierung ist hierzu noch nicht abgeschlossen, daher kann insbesondere auch zur erfragten Risikobewertung keine Aussage getroffen werden. Grundsätzlich ist darauf hinzuwirken, dass eventuell bestehende Sicherheitslücken in IT-Systemen schnellstmöglich geschlossen werden.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.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