Deutscher Bundestag **Drucksache 19/1020**

19. Wahlperiode 28.02.2018

Kleine Anfrage

der Abgeordneten Konstantin Kuhle, Jimmy Schulz, Manuel Höferlin, Benjamin Strasser, Linda Teuteberg, Stephan Thomae, Grigorios Aggelidis, Christine Aschenberg-Dugnus, Jens Beeck, Nicola Beer, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg, Britta Katharina Dassler, Christian Dürr, Hartmut Ebbing, Dr. Marcus Faber, Daniel Föst, Thomas Hacker, Katrin Helling-Plahr, Katja Hessel, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Gyde Jensen, Thomas L. Kemmerich, Katharina Kloke, Daniela Kluckert, Pascal Kober, Dr. Lukas Köhler, Wolfgang Kubicki, Alexander Graf Lambsdorff, Ulrich Lechte, Oliver Luksic, Alexander Müller, Roman Müller-Böhm, Frank Müller-Rosentritt, Dr. Martin Neumann, Dr. h. c. Thomas Sattelberger, Dr. Wieland Schinnenburg, Matthias Seestern-Pauly, Frank Sitta, Bettina Stark-Watzinger, Katja Suding, Michael Theurer, Manfred Todtenhausen, Dr. Florian Toncar, Dr. Andrew Ullmann, Johannes Vogel, Nicole Westig und der Fraktion der FDP

Rechtsgrundlagen und Einsatz der Quellen-Telekommunikationsüberwachung

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 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 Kommunikationen 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.

Wir fragen die Bundesregierung:

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)?
3. Wie erfolgt die praktische Abgrenzung zwischen § 100a Absatz 1 Satz 2 und § 100a Absatz 1 Satz 3 StPO?
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)?
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)?
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)?
7. Wie vieler Versuche bedurfte es bei diesen Einsätzen für die erfolgreiche Installation der Software?

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

    Wenn ja, warum?

    Wenn nein, warum nicht?
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?
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?
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?

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?

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?

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?

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?

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?

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)?

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?

Berlin, den 27. Februar 2018

Christian Lindner und Fraktion

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