Ausarbeitung

Zugriff auf vernetzte Geräte zum Zweck der Strafverfolgung

Strafverfahrensrechtliche Rahmenbedingungen

Zugriff auf vernetzte Geräte zum Zweck der Strafverfolgung
Strafverfahrensrechtliche Rahmenbedingungen

Aktenzeichen:	WD 7 - 3000 - 119/19
Abschluss der Arbeit:	19. August 2019
Fachbereich:	WD 7: Zivil-, Straf- und Verfahrensrecht, Bau und Stadtentwicklung

Inhaltsverzeichnis

1. Einleitung

Die bei der Nutzung so genannter „Smart-Home-Geräte“ in privaten Haushalten anfallenden Daten können im Zusammenhang mit einem Strafverfahren für Strafverfolgungsbehörden potentiell wertvolle Informationsquellen darstellen.[1] Vor diesem Hintergrund ist vorliegend von Interesse, ob und gegebenenfalls auf welcher Rechtsgrundlage und unter welchen Voraussetzungen Strafverfolgungsbehörden auf entsprechende Daten sowie insbesondere aktiv auf in entsprechenden Geräten enthaltene Mikrofone und Kameras zugreifen dürfen.

2. Offene Maßnahmen

2.1. Durchsicht (§ 110 StPO[2])

Im Rahmen der Durchsuchung einer Wohnung (§§ 102, 103 StPO) können die Strafverfolgungsbehörden verschiedene (potentielle) Beweismittel, wie etwa Datenträger, auffinden. Diese werden vor Ort oder nach einer vorläufigen Sicherstellung im Verfahren der Durchsicht nach § 110 StPO durch die Staatsanwaltschaft oder ihre Ermittlungspersonen auf ihr Beweispotenzial hin inhaltlich geprüft.[3] Die Durchsicht dient der Entscheidung, ob eine richterliche Beschlagnahme aufgrund der potenziellen Beweisbedeutung beantragt werden muss.[4] Die Durchsicht ist als Bestandteil einer Durchsuchung nur unter den Voraussetzungen des § 102 StPO bzw. § 103 StPO zulässig.[5]

Eine Durchsuchung im Sinne von §§ 102, 103 StPO setzt neben dem Anfangsverdacht die Vermutung voraus, dass Beweismittel oder der Tatverdächtige durch die Durchsuchung aufgefunden werden.[6] Das Verfahren ist in § 105 StPO geregelt, der unter anderem grundsätzlich eine richterliche Anordnung der Durchsuchung voraussetzt. Sämtliche Räume, die die private Lebensgestaltung schützen und in denen sich der Tatverdächtige aufhält oder die er benutzt, können durchsucht werden.[7]

Der Wortlaut des § 110 Absatz 1 StPO gestattet die „Durchsicht der Papiere des von der Durchsuchung Betroffenen“. Der Begriff „Papiere“ ist weit auszulegen, auch elektronische Daten auf Speichermedien und im Arbeitsspeicher eines Rechners sind von § 110 StPO erfasst – insofern ggf.

---

1 Gless, Wenn das Haus mithört: Beweisverbote im digitalen Zeitalter, Strafverteidiger (StV) 2018, 671.

2 Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 3 des Gesetzes vom 11. Juli 2019 (BGBl. I S. 1066) geändert worden ist.

3 Hegmann, in: Beck´scher Onlinekommentar zur Strafprozessordnung (BeckOK StPO), 34. Edition, Stand: 01.07.2019, § 110 Rn. 6.

4 BGH, Beschl. v. 05.08.2003, Az.: 2 BJs 11/03-5 - StB 7/03, Neue Zeitschrift für Strafrecht (NStZ) 2003, 670 (671).

5 Szesny, Durchsicht von Daten gem. § 110 StPO, Journal der Wirtschaftsstrafrechtlichen Vereinigung e.V. (WiJ) 4/2012, 228 (232).

6 Bruns, Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 102 Rn. 2 f.

7 BVerfG, Beschl. v. 13.10.1971, Az.: 1 BvR 280/66, BVerfGE 32, 54, 72 ff.

also auch vernetzte Geräte.[8] Es muss sich um Papiere bzw. Daten im Gewahrsam des von einer Durchsuchung Betroffenen, regelmäßig des Tatverdächtigen, handeln.[9] Die Durchsicht darf nur erfolgen, wenn Anhaltspunkte dafür existieren, dass unter den Papieren bzw. Daten Beweismittel sind, die im späteren Verfahren Verwendung finden können.[10] Da die Durchsicht den Betroffenen in seiner grundrechtlich geschützten Lebenssphäre und dem Grundrecht auf informationelle Selbstbestimmung aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG betrifft, ist bei der Durchführung insbesondere dem Verhältnismäßigkeitsgrundsatz Rechnung zu tragen.[11]

Hat der Betroffene Zugriff auf externe Speichermedien, können die Strafverfolgungsbehörden die Durchsicht auch auf die sich darauf befindlichen Daten erstrecken, wenn sonst der Verlust der gesuchten Daten zu besorgen ist (§ 110 Absatz 3 Satz 1 StPO). Nach § 110 Absatz 3 Satz 2 StPO dürfen Daten, die für die Ermittlung von Bedeutung sein können, gesichert werden.

Diese Maßnahme ist allerdings nur zulässig, wenn sich die entsprechenden Daten auf einem Server befinden, auf den die Strafverfolgungsbehörden zugreifen dürfen. Der Zugriff ist möglich, wenn sich der Server in Deutschland befindet oder der Betroffene dem Zugriff zustimmt.[12] Ist ein ausländischer Server öffentlich zugänglich und befindet er sich im Geltungsbereich des Übereinkommens des Europarats über Computerkriminalität[13], dürfen die Behörden auf die Daten nach Artikel 32 lit. a des Übereinkommens oder nach internationalem Gewohnheitsrecht auch darauf zugreifen.[14] Liegen die Daten auf einem nicht öffentlichen ausländischen Server, sind die deutschen Behörden im Rahmen eines förmlichen Rechtshilfeersuchens auf die Kooperation der ausländischen Behörden angewiesen.[15]

Sind unter den vorläufig sichergestellten Papieren im Sinne des § 110 StPO auch solche, die nicht die Voraussetzungen einer Beschlagnahme erfüllen, ist dies für die Rechtmäßigkeit der Durchsicht nicht entscheidend, da diese Maßnahme gerade der Feststellung dient, ob eine Beschlagnahme beantragt werden sollte.[16] Die Durchsicht nach § 110 StPO ist dagegen unzulässig,

---

8 BGH, Beschl. v. 05.08.2003 - Az.: 2 BJs 11/03-5 - StB 7/03, NStZ 2003, 670.

9 Bruns, Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 110 Rn. 3.

10 LG Stuttgart, Beschl. v. 26.03.2018, Az.: 6 Qs 1/18, BeckRS 2018, 8717 Rn. 20.

11 Hegmann, in: BeckOK StPO 34. Edition, Stand: 01.07.2019, § 110, Rn. 12.

12 Blechschmitt, Strafverfolgung im digitalen Zeitalter, MMR 2018, 361, 363.

13 Europarat-Übereinkommen über Computerkriminalität vom 23.11.2001, für die Bundesrepublik Deutschland in Kraft getreten am 01.07.2009, Bekanntmachung über das Inkrafttreten des Übereinkommens über Computerkriminalität vom 16.02.2010 (BGBl II S. 218), abrufbar unter: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008157a.

14 Bruns, Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 110 Rn. 8a.

15 Blechschmitt, „Strafverfolgung im digitalen Zeitalter“, MMR 2018, 361, 364.

16 LG Stuttgart, Beschl. v. 26.03.2018, Az.: 6 Qs 1/18, BeckRS 2018, 8717 Rn. 19.

wenn das betreffende Beweismittel offensichtlich vom Beschlagnahmeverbot nach § 97 StPO erfasst ist.[17]

Bei der Durchsicht können die Strafverfolgungsbehörden folglich unter den genannten Voraussetzungen Zugriff auf Smart-Home-Geräte und auf ihnen enthaltene Daten erlangen, um die Feststellung zu ermöglichen, ob diese Daten sichergestellt bzw. beschlagnahmt werden können.

2.2. Sicherstellung und Beschlagnahme (§§ 94 ff. StPO)

Nach § 94 Absatz 1 StPO sind „Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, … in Verwahrung zu nehmen oder in anderer Weise sicherzustellen." Unter einer Sicherstellung wird die Herstellung staatlicher Gewalt über den Gegenstand verstanden.[18] Auch wenn der Wortlaut nur Gegenstände umfasst, ist die Anwendbarkeit der Norm auf nichtkörperliche Informationen wie Daten anerkannt.[19] Auch vernetzte Geräte und die Inhalte einer Cloud sind also Gegenstände im Sinne von § 94 StPO.[20]

Damit eine (formlose) Sicherstellung erfolgen darf, müssen die Gegenstände im Sinne des § 94 StPO potentielle Beweisbedeutung haben.[21] Diese ist gegeben, wenn die Möglichkeit besteht, dass die Daten für die Beweisfrage – etwa bzgl. Tatbegehung, verfahrensrechtlicher Maßnahmen oder Strafzumessungsgründen – von gewisser Bedeutung sind.[22]

Weiterhin ist der Anfangsverdacht für eine Sicherstellung notwendig und ausreichend.[23] Ein Anfangsverdacht setzt die Kenntnis über tatsächliche Anhaltspunkte für eine Straftat voraus.[24] Auch die weiteren allgemeinen Verfahrensvoraussetzungen (z.B. ggf. der Strafantrag nach § 77 StGB[25])

---

17 BVerfG, Beschl. v. 27.06.2018, Az.: 2 BvR 1405/17, 2 BvR 1780/17, NJW 2018, 2385, 2388 Rn. 80.

18 Gerhold, in: BeckOK StPO, 34. Edition, Stand: 01.07.2019, § 94 Rn. 14.

19 BVerfG, Beschl. v. 12.04.2005, Az.: 2 BvR 1027/02, Neue Juristische Wochenschrift (NJW) 2005, 1917, 1920.

20 Blechschmitt, Strafverfolgung im digitalen Zeitalter, MMR 2018, 361, 364.

21 BVerfG, Beschl. v. 13.12.1994, Az.: 2 BvR 894/94, NJW 1995, 2839, 2840.

22 BVerfG, Beschl. v. 13.12.1994, Az.: 2 BvR 894/94, NJW 1995, 2839, 2840.

23 Greven, in: Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 94 Rn. 8.

24 Diemer, in: Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 152 Rn. 7.

25 Strafgesetzbuch (StGB) in der Fassung der Bekanntmachung vom 13.11.1998 (BGBl. I S. 3322), zuletzt geändert durch Art. 2 des Gesetzes zur Umsetzung der RL (EU) 2017/1371 vom 19.06.2019 (BGBl. I S. 844).

müssen gegeben oder noch zu beschaffen sein.[26] Können die Voraussetzungen für ein Strafverfahren nach einer erfolgten Sicherstellung nicht erfüllt werden, muss die Maßnahme unverzüglich aufgehoben werden.[27]

Bei der Anordnung der Sicherstellung muss aufgrund des Eingriffs in die Grundrechte des Betroffenen immer der Grundsatz der Verhältnismäßigkeit beachtet werden.[28] Demnach muss die für den Betroffenen am geringsten belastende Maßnahme, die den verfolgten Zweck erfüllt, gewählt werden.[29]

Werden die Gegenstände im Sinne von § 94 Absatz 1 StPO vom Gewahrsamsinhaber nicht freiwillig herausgegeben, können sie förmlich beschlagnahmt werden (§ 94 Absatz 2 StPO). Das Verfahren der Beschlagnahme ist in § 98 StPO normiert. Die dargestellten Voraussetzungen der Sicherstellung müssen auch für die Beschlagnahme vorliegen, insbesondere muss die Maßnahme also verhältnismäßig sein.[30] Zudem ist nach erfolgter Anhörung des Betroffenen grundsätzlich eine gerichtliche Anordnung notwendig (§§ 98 Absatz 1 Satz 1, 33 Absatz 3 StPO).

Außer der fehlenden Verhältnismäßigkeit sind in § 97 StPO weitere Gründe für das Verbot einer Beschlagnahme geregelt. Die Datensammlung kann von dem Beschlagnahmeverbot bzgl. Schriftstücken, die die Kommunikation zwischen dem Beschuldigten und einer (nach §§ 52, 53, 53a StPO) zeugnisverweigerungsberechtigten Person wiedergeben (§ 97 Absatz 1 StPO), erfasst sein. Andere Beschlagnahmeverbote können sich aus der Verfassung ergeben, beispielsweise bei schweren Verfahrensfehlern, die einen Grundrechtsverstoß darstellen.[31]

3. Verdeckte Maßnahmen

3.1. Telekommunikationsüberwachung (§ 100a StPO)

Gemäß § 100a Absatz 1 Satz 1 StPO darf auch ohne Wissen der Betroffenen ihre Telekommunikation überwacht und aufgezeichnet werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100a Absatz 2 StPO bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat, die Tat auch im Einzelfall schwer wiegt und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

---

26 Greven, in: Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 94 Rn. 10.

27 Greven, in: Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 94 Rn. 10.

28 BVerfG, Urt. v. 16.06.2009, Az.: 2 BvR 902/06, NJW 2009, 2431, 2437.

29 BVerfG, Beschl. v. 10.11.2017, Az.: 2 BvR 1775/16, NJW 2018, 1240, 1241.

30 Gerhold, in: BeckOK StPO, 34. Edition, Stand: 01.07.2019, § 94 Rn. 22.

31 BVerfG, Beschl. v. 12.04.2005, Az.: 2 BvR 1027/02, NJW 2005, 1917, 1922 bzgl. Berufsgeheimnisträgern.

3.1.1. Klassische Telekommunikationsüberwachung (§ 100a Absatz 1 Satz 1 StPO)

Der Begriff der Telekommunikation wird von der Strafprozessordnung nicht legaldefiniert, weshalb im rechtswissenschaftlichen Schrifttum im Detail unterschiedliche Interpretationen vertreten werden.[32] Der Bundesgerichtshof legt den Begriff unter Rückgriff auf die Definition in § 3 Nr. 22 TKG[33] aus.[34] Telekommunikation wird dort definiert als „der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen".

Im Kontext des § 100a StPO ist der Begriff, „weil das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG entwicklungsoffen ist und auch neuartige Übertragungstechniken umfassen soll (BVerfG NJW 1978, 313; 2006, 976 (978)), … dementsprechend auszulegen und damit gleichfalls entwicklungsoffen, jedoch auch zu berücksichtigen, dass Art. 10 Abs. 1 GG nicht dem rein technischen Telekommunikationsbegriff des Telekommunikationsgesetzes folgt, sondern an den Grundrechtsträger und dessen Schutzbedürftigkeit aufgrund der Einschaltung Dritter in den Kommunikationsvorgang anknüpft (vgl. BVerfGE 124, 43 (55 f.); BVerfGK 9, 62 (75); BVerfG Beschl. v. 6.7.2016 – 2 BvR 1454/13, BeckRS 2016, 50705)."[35]

Dem entsprechend werden erfasst nicht nur „Gespräche mittels Festnetztelefon, Mobiltelefon, Nachrichten in Form von Kurzmitteilungen (SMS), Multimediadaten (MMS), Fax und Fernschreiben"[36], sondern auch die Kommunikation mittels – verhältnismäßig – neuartiger Technologien über das Internet, etwa „E-Mails, Messenger-Systeme (insbes. ICQ, AIM, Yahoo, Windows Live Messenger) und sämtliche Arten der Internet-Telefonie."[37]

Erfasst ist dabei unabhängig vom Übertragungsmedium stets nur der Vorgang der Nachrichtenübermittlung oder funktionell gleichgestellter Daten.[38] Der Umfang der Telekommunikation wird mithin „begrenzt vom Absenden der Signale bis zu deren Empfang beim Adressaten, betrifft also nur den eigentlichen technischen Vorgang der Nachrichtenübermittlung."[39]

---

32 Vgl. Überblick bei Bruns, in: Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 100a Rn. 4.

33 Telekommunikationsgesetz (TKG) vom 22.06.2004 (BGBl. I S. 1190), zuletzt geändert durch Art. 12 des Gesetzes gegen illegale Beschäftigung und Sozialleistungsmissbrauch vom 11.07.2019 (BGBl. I S. 1066).

34 Günther, in: Münchener Kommentar zur StPO, 1. Auflage 2014, § 100a Rn. 29 m.w.N.

35 Graf, in: BeckOK StPO, 34. Edition, Stand: 01.07.2019, § 100a Rn. 18. So auch Bruns, in: Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 100a Rn. 4.

36 Bruns, in: Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 100a Rn. 16.

37 Graf, in: BeckOK StPO, 34. Edition, Stand: 01.07.2019, § 100a Rn. 19; Großmann, Telekommunikationsüberwachung und Online-Durchsuchung: Voraussetzungen und Beweisverbote, JA 2019, 241.

38 Bruns, in: Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 100a Rn. 16.

39 Graf, in: BeckOK StPO, 34. Edition, Stand: 01.07.2019, § 100a Rn. 21.

Im Ergebnis kann ein Abgreifen des Audio-/Videosignals an „Smart-Home-Geräten“ grundsätzlich durch § 100a Absatz 1 Satz 1 StPO gestattet sein, soweit hierbei ausschließlich laufende Telekommunikationsvorgänge erfasst sind.

Ganz grundsätzlich muss für die Anordnung einer TKÜ stets ein Tatverdacht vorliegen. Dieser erfordert, dass aufgrund der Lebenserfahrung oder der kriminalistischen Erfahrung fallbezogen aus sachlichen Beweisanzeichen auf das Vorliegen einer Straftat geschlossen werden kann.[40] Die dafür in Frage kommenden Straftaten sind im Katalog des § 100a Absatz 2 StPO aufgeführt. Weiterhin muss die Anlasstat nach § 100a Absatz 1 Satz 1 Nr. 2 StPO nicht nur abstrakt schwer wiegen, sondern auch im Einzelfall erheblich sein. Die Anordnung der Maßnahme setzt also eine Abwägung der Schwere der Straftat mit dem durch eine TKÜ verbundenen Eingriff in das Fernmeldegeheimnis im Einzelfall voraus.[41] Zudem muss bei jeder Maßnahme nach § 100a StPO der Subsidiaritätsgrundsatz[42] beachtet werden, der in § 100a Absatz 1 Satz 1 Nr. 3 StPO seinen Ausdruck findet. Nach § 100a Absatz 3 StPO darf die TKÜ zudem nur den Beschuldigten und Personen betreffen, deren Anschluss bzw. informationstechnische Systeme der Beschuldigte nutzt.

Weiterhin zu beachten sind die Einschränkungen durch § 100d StPO, der dem Schutz des Kernbereichs privater Lebensgestaltung dient. Gemäß § 100d Absatz 1 StPO ist eine TKÜ-Maßnahme unzulässig, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch eine Maßnahme nach § 100a StPO „allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden“. Werden Erkenntnisse aus dem Kernbereich privater Lebensgestaltung durch eine Maßnahme nach § 100a StPO erlangt, dürfen sie nicht verwertet werden; Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen (§ 100d Absatz 2 StPO).

3.1.2. Quellen-Telekommunikationsüberwachung (§ 100a Absatz 1 Sätze 2, 3 StPO)

Gemäß § 100a Absatz 1 Satz 2 StPO darf die Überwachung und Aufzeichnung der Telekommunikation auch in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. Hierbei handelt es sich um die so genannte Quellen-Telekommunikationsüberwachung (Quellen-TKÜ). Auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation dürfen dabei gemäß § 100a Absatz 1 Satz 3 StPO überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können. Bei der Quellen-TKÜ müssen stets auch die Voraussetzungen der normalen Telekommunikationsüberwachung vorliegen.[43]

---

40 BVerfG, Beschl. v. 30.04.2007, Az.: 2 BvR 2151/06, NJW 2007, 2752, 2753.

41 Graf, in: BeckOK StPO, 34. Edition, Stand: 01.07.2019, § 100a Rn. 102 f.

42 Graf, in: BeckOK StPO, 34. Edition, Stand: 01.07.2019, § 100a Rn. 104.

43 Freiling/Safferling/Rückert, Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen, JR 2018, 9, 10.

Die Quellen-TKÜ darf stets nur erfolgen, „wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen“ (§ 100a Absatz 1 Satz 2 StPO). Sie betrifft demnach vor allem den verschlüsselten Datenverkehr, der von einer „normalen“ TKÜ im Sinne von § 100a Absatz 1 Satz 1 StPO nur aufgrund der Verschlüsselung nicht erfasst werden kann, und ist subsidiär zur TKÜ.[44]

Die Vorschrift unterscheidet zwischen der Überwachung und Aufzeichnung laufender Telekommunikation (§ 100a Absatz 1 Satz 2 StPO) und gespeicherten Kommunikationsinhalten und -umständen (§ 100a Absatz 1 Satz 3 StPO). Beide Varianten setzen einen Eingriff mit technischen Mitteln voraus, womit der Zugriff auf das IT-System durch eine entsprechende Software gemeint ist.[45]

Bei der Überwachung und Aufzeichnung der in einer Anwendung gespeicherten Kommunikationsinhalte und -umstände einer abgeschlossenen Übertragung nach § 100a Absatz 1 Satz 3 StPO dürfen keine anderweitigen Daten des Endgeräts, die unabhängig von der Kommunikation sind, erfasst werden.[46] Neben Sprach- und Tastatureingaben können also nur Bild- oder Videodateien im Zusammenhang mit der gespeicherten Kommunikation durch eine Quellen-TKÜ ermittelt werden.[47] Zudem wird durch § 100a Absatz 1 Satz 3 StPO festgelegt, dass gespeicherte Inhalte nur erfasst werden dürfen, „wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können“.

Einen scharfen Sicherungsmechanismus bei der Vornahme von technischen Eingriffen in informationstechnische Systeme des Betroffenen sieht § 100a Absatz 5 StPO vor:

> „Bei Maßnahmen nach Absatz 1 Satz 2 und 3 ist technisch sicherzustellen, dass
>
> 1. ausschließlich überwacht und aufgezeichnet werden können:
>
> a) die laufende Telekommunikation (Absatz 1 Satz 2), oder
>
> b) Inhalte und Umstände der Kommunikation, die ab dem Zeitpunkt der Anordnung nach § 100e Absatz 1 auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können (Absatz 1 Satz 3),
>
> 2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

---

44 Freiling/Safferling/Rückert, Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen, JR 2018, 9, 10 f.

45 Freiling/Safferling/Rückert, Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen, JR 2018, 9, 10.

46 Graf, in: BeckOK StPO, 34. Edition, Stand: 01.07.2019, § 100a Rn. 115.

47 Bruns, in: Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 100a Rn. 44.

3. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden."

Aus § 100a Absatz 5 Nr. 1 StPO folgt, dass bereits jede Manipulation des informationstechnischen Systems, die auch nur die technische Möglichkeit beinhaltete, unabhängig von laufenden Telekommunikationsvorgängen etwa die Kamera und/oder das Mikrofon von Zielgeräten einzuschalten, von vornherein nicht auf § 100a StPO gestützt werden könnte und insofern unzulässig wäre.

Auch bei der Quellen-TKÜ gelten die Grenzziehungen zum Schutz des Kernbereichs privater Lebensgestaltung gemäß § 100d Absatz 1 und 2 StPO.[48]

3.2. Akustische Wohnraumüberwachung (§ 100c StPO)

§ 100c StPO normiert die „akustische Wohnraumüberwachung", unter der dem Wortlaut der Bestimmung zufolge das mit technischen Mitteln erfolgende Abhören und Aufzeichnen des in einer Wohnung nichtöffentlich gesprochenen Worts zu verstehen ist.

Voraussetzung dafür ist nach § 100c Absatz 1 Nr. 1 StPO, dass ein qualifizierter Verdacht bzgl. des Vorliegens einer Katalogtat im Sinne des § 100b Absatz 2 StPO besteht.[49] Erforderlich ist eine konkretisierte Verdachtslage, es muss also eine erhöhte Wahrscheinlichkeit für die Begehung der Katalogstraftat vorhanden sein.[50] Der Versuch einer Katalogtat ist bereits ausreichend, soweit dieser strafbar ist (§ 100c Absatz 1 Nr. 1 2. Halbsatz StPO).

Des Weiteren muss die Katalogtat im Einzelfall besonders schwer wiegen (§ 100c Absatz 1 Nr. 2 StPO). Dies ergibt sich bei den meisten Delikten im Katalog des § 100b Absatz 2 StPO bereits aus dem verletzten Rechtsgut.[51] In anderen Fällen kann die besondere Schwere bejaht werden, wenn die Tat mit anderen Katalogstraftaten im Zusammenhang steht oder wenn sie durch das Zusammenwirken mehrerer Straftäter begründet wird.[52]

Zielperson ist nach § 100c Absatz 1 Nr. 1 StPO, wer Beschuldigter einer Katalogtat gemäß § 100b Absatz 2 StPO ist. Die Maßnahme muss des Weiteren den Zweck verfolgen, Sachverhaltserforschung oder die Aufenthaltsermittlung eines Mitbeschuldigten zu betreiben (§ 100c Absatz 1 Nr. 4 StPO). Das primäre Ziel der Maßnahme muss darin bestehen, Kenntnis von Äußerungen des

48 S. o. bei Gliederungspunkt 3.1.1.

49 Vgl. BVerfG, Urt. v. 03.03.2004, Az.: 1 BvR 2378/98, NJW 2004, 999, 1012 ff.

50 Vgl. BVerfG, Urt. v. 03.03.2004, Az.: 1 BvR 2378/98, NJW 2004, 999, 1012 ff.

51 Soiné, Die strafprozessuale Online-Durchsuchung, NStZ 2018, 497, 498.

52 Bruns, in: Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 100c Rn. 12.

Beschuldigten zu erlangen – umfasst sind aber auch das Abhören und Aufzeichnen von Äußerungen sonstiger in der Wohnung anwesender Personen.[53]

Nach § 100e Absatz 2 StPO darf die akustische Wohnraumüberwachung nur auf Antrag der Staatsanwaltschaft durch das zuständige Landgericht angeordnet werden.

Liegen die genannten Voraussetzungen vor, darf nach § 100c Absatz 1 StPO in einer Wohnung das nichtöffentlich gesprochene Wort mit technischen Mitteln abgehört und aufgezeichnet werden. Der Wohnungsbegriff umfasst dabei alle von Artikel 13 GG geschützten Räumlichkeiten.[54] Über den engen Wortsinn hinausgehend erfasst der Wohnungsbegriff eine räumliche Sphäre, in der sich das Privat- und Geschäftsleben Dritter ungestört entfalten kann.[55] Somit sind auch allgemein nicht zugängliche Räume, welche zur Stätte des Aufenthalts und Wirkens von Menschen bestimmt sind, inbegriffen.[56]

Welche technischen Mittel zur Durchführung der Maßnahme eingesetzt werden, wurde bewusst nicht geregelt: „Um welche technischen Mittel es sich dabei handelt, hat der Gesetzgeber bewusst offen gelassen, um den Strafverfolgungsbehörden ebenso wie bei Maßnahmen nach § 100h die Möglichkeit zu geben, entsprechend der technologischen Entwicklung auf diejenige Technik zurückgreifen zu können, die für die konkrete Maßnahme am geeignetsten erscheint.“[57] Allerdings dürfen die technischen Mittel zum einen „allein zur Sprachaufzeichnung eingesetzt werden. Nicht statthaft ist der Einsatz technischer Mittel in Wohnungen zur Herstellung von Fotos oder Videoaufzeichnungen.“[58] Zum anderen ist zu berücksichtigen, dass § 100c StPO im Gegensatz zu den §§ 100a, 100b StPO gerade keine ausdrückliche Ermächtigung zum manipulativen Eingriff in fremde informationstechnische Systeme und zur Datenerhebung aus diesen aufführt[59]:

> „Ein Lauschangriff mittels Alexa dürfte aber von vornherein eher bei § 100b StPO, denn bei § 100c StPO zu verorten sein. Hierfür sprechen die Art und Weise des Zugangs – die Infiltration eines informationstechnischen Systems – und damit korrespondierend das betroffene Grundrecht. Maßnahmen, die mit einer heimlichen Infiltration eines informationstechnischen Systems verbunden sind, stellen nach Auffassung des BVerfG einen Eingriff in das Recht auf Vertraulichkeit und Integrität technischer Systeme und damit einen Eingriff in das sog. Computer- oder IT-Grundrecht dar. Dieses schützt als eigenständige Ausprägung des Rechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG den persönli-

53 Bruns, in: Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 100c Rn. 7.

54 Hegmann, in: BeckOK StPO, 34. Edition, Stand: 01.07.2019, § 100c Rn. 14.

55 Bruns, in: Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 100c Rn. 6.

56 Bruns, in: Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 100c Rn. 6.

57 Günther, in: Münchener Kommentar zur StPO, 1. Auflage 2014, § 100c Rn. 50.

58 Günther, in: Münchener Kommentar zur StPO, 1. Auflage 2014, § 100c Rn. 50.

59 Vgl. Eschelbach, in: Satzger/Schluckebier/Widmaier, StPO, 3. Aufl. 2018, § 100c Rn. 5.

chen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff, indem es Zugriffe auf informationstechnische Systeme insgesamt abwehrt und dabei nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten abstellt.“[60]

Aufgrunddessen dürfte § 100c StPO den Strafverfolgungsbehörden keine Befugnis dafür geben, auf die Mikrofone – geschweige denn Kameras – von Smart-Home-Geräten Betroffener mit dem Ziel der akustischen Wohnraumüberwachung zuzugreifen.[61]

Nach § 100c Absatz 1 Nr. 4 StPO darf die Überwachung zudem nur angeordnet werden, wenn die Erforschung des Sachverhalts auf andere Art und Weise „unverhältnismäßig erschwert oder aussichtlos wäre“. Damit sind Maßnahmen nach § 100c Absatz 1 StPO subsidiär gegenüber sämtlichen anderen Ermittlungsmaßnahmen.[62]

Auch bei der akustischen Wohnraumüberwachung gelten die Grenzziehungen zum Schutz des Kernbereichs privater Lebensgestaltung gemäß § 100d Absatz 1 und 2 StPO.[63] Zusätzlich gilt gemäß § 100d Absatz 4 StPO, dass Maßnahmen nach § 100c StPO nur angeordnet werden dürfen, soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Weiterhin gilt nach § 100d Absatz 4 StPO: Das Abhören und Aufzeichnen ist unverzüglich zu unterbrechen, wenn sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden.

3.3. Online-Durchsuchung (§ 100b StPO)

3.3.1. Grundsätzliches

Gemäß § 100b StPO darf auch ohne Wissen des Betroffenen mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und dürfen Daten daraus erhoben werden (Online-Durchsuchung), wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100b Absatz 2 StPO bezeichnete besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat, die Tat auch im Einzelfall besonders schwer wiegt und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

---

60 Blechschmitt, Strafverfolgung im digitalen Zeitalter, MMR 2018, 361, 365.

61 Blechschmitt, Strafverfolgung im digitalen Zeitalter, MMR 2018, 361, 365; Eschelbach, in: Satzger/Schluckebier/Widmaier, StPO, 3. Aufl. 2018, § 100c Rn. 5; zweifelnd Gless, Wenn das Haus mithört: Beweisverbote im digitalen Zeitalter, Strafverteidiger (StV) 2018, 671, 674.

62 Hegmann, in: BeckOK StPO, 34. Edition, Stand: 01.07.2019, § 100c Rn. 12.

63 S. o. bei Gliederungspunkt 3.1.1.

Unter den Begriff des informationstechnischen Systems in diesem Sinne fallen neben klassischen PCs „alle von einem Mikroprozessor gesteuerten Geräte, namentlich auch Mobiltelefone (Smartphones), Organizer oder Server und Router bis hin zu sog. smarten Haushaltsgeräten oder sog. Digitalen Assistenten (zB ‚Alexa' von Amazon, ‚Hello' von Google, ‚Cortana' von Microsoft, ‚Siri' von Apple …)."[64]

Zahlreiche Voraussetzungen des § 100b StPO entsprechen denjenigen für die akustische Wohnraumüberwachung nach § 100c StPO.[65] So bedarf es einer Katalogtat nach § 100b Absatz 2 StPO sowie eines Tatverdachts gegen die Zielperson der Maßnahme. Die Tat muss ebenso im Einzelfall besonders schwer wiegen. Des Weiteren darf keine Subsidiarität gemäß § 100b Absatz 1 Nr. 3 StPO vorliegen, folglich darf keine Ermittlungsmaßnahme mit geringerer Eingriffstiefe aber gleichen Erfolgsaussichten zur Verfügung stehen.[66]

Die Online-Durchsuchung muss sich gemäß § 100b Absatz 3 Satz 1 StPO gegen den Beschuldigten richten. Ein informationstechnisches System eines Dritten kann erfasst werden, soweit aufgrund bestimmter Tatsachen anzunehmen ist, dass es vom Beschuldigten benutzt wird und der alleinige Zugriff auf Geräte des Beschuldigten selbst zur Erreichung des Ermittlungsziels nicht genügt (§ 100b Absatz 3 Satz 2 StPO).

Des Weiteren ist die Verhältnismäßigkeit einer Anordnung bei deren Erlass sowie beim Andauern der Maßnahme zu überprüfen.[67] Gemäß § 100e Absatz 5 Satz 1 StPO ist eine Maßnahme abzubrechen, sobald der Eingriff nicht mehr im Verhältnis zu den erwarteten Ergebnissen oder zur Schuld des Beschuldigten steht.[68] Nach § 100e Absatz 2 StPO darf die Online-Durchsuchung nur auf Antrag der Staatsanwaltschaft durch das zuständige Landgericht angeordnet werden.

Liegen die Voraussetzungen des § 100b StPO vor, darf grundsätzlich mit technischen Mitteln in ein von dem Betroffenen der Maßnahme genutztes informationstechnisches System eingegriffen und Daten daraus erhoben werden. Es können nicht nur alle neu hinzukommenden Kommunikationsinhalte, sondern auch alle in dem IT-System gespeicherten Inhalte sowie das Nutzungsverhalten der Person überwacht werden.[69] Insofern ein Betroffener mithin über Smart-Home-Geräte Ton- und/oder Bildaufnahmen erstellt, sind diese von § 100b StPO grundsätzlich erfasst.

64 Bruns, in: Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 100b Rn. 4.

65 Braun/Roggenkamp, 0Zapftis v2.0 Repressive Staatstrojaner, Privacy in Germany (PinG) 7/2019, 53, 56.

66 Graf, in: BeckOK StPO, 34. Edition, Stand: 01.07.2019, § 100b Rn. 16.

67 Graf, in: BeckOK StPO, 34. Edition, Stand: 01.07.2019, § 100b Rn. 20.

68 Graf, in: BeckOK StPO, 34. Edition, Stand: 01.07.2019, § 100b Rn. 20.

69 Bruns, in: Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage 2019, § 100b Rn. 5.

Auch bei der Online-Durchsuchung gelten die Grenzziehungen zum Schutz des Kernbereichs privater Lebensgestaltung gemäß § 100d Absatz 1 und 2 StPO.[70] Zusätzlich ist gemäß § 100d Absatz 3 Satz 1 StPO, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach § 100b StPO erlangt wurden und den Kernbereich privater Lebensgestaltung betreffen, sind gemäß § 100d Absatz 3 Satz 2 StPO unverzüglich zu löschen oder von der Staatsanwaltschaft dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen.

3.3.2. Aktiv steuernder Zugriff auf Mikrofone/Kameras vernetzter Systeme

Im Schrifttum wird diskutiert, ob § 100b StPO so verstanden werden kann, dass er die Ermittlungsbehörden auch dazu ermächtigt, Mikrofone oder Kameras vernetzter Systeme selbst anzuschalten und hierdurch im Sinne eines „großen Spähangriffs“[71] Ton- und Bildsignale zu erfassen.

3.3.2.1. Meinungsstand

Zum Teil wird die Auffassung vertreten, § 100b StPO ermächtige aufgrund seines insoweit nicht ausdrücklich beschränkten Wortlauts Ermittlungsbehörden grundsätzlich auch dazu, vernetzte Systeme aktiv zum Ausspähen von Betroffenen einzusetzen. So vertritt *Beukelmann* die Auffassung, dass die „in § 100 b StPO nF vorgesehene Online-Durchsuchung … all jene Eingriffe (umfasst), die bisher bereits nach § 100 c StPO als akustische Raumüberwachung („Großer Lauschangriff“) zulässig waren. Es kommt dadurch zu erheblichen Eingriffen: der Zugriff auf die gespeicherten Daten, die heimliche Auswertung der aktuellen und gegebenenfalls früheren Kommunikation und – technisch möglich – ein „Großer Spähangriff“ auf die Umgebung des überwachten Systems dank dessen Kamera.“[72] Diese Auffassung hatte schon im Gesetzgebungsverfahren namentlich *Buermeyer* vertreten:

> „Durch Infektion der informationstechnischen Systeme von Beschuldigten soll nämlich ermöglicht werden (…) ein ‚Großer Spähangriff‘ auf die Umgebung des überwachten Systems, sofern es über eine Kamera-Funktion verfügt wie heute jedes Smartphone, jedes Tablet und nahezu jeder Laptop.“[73]

---

70 S. o. bei Gliederungspunkt 3.1.1.

71 Begrifflichkeit von Buermeyer, „Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur ‚Formulierungshilfe‘ des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess, Ausschuss-Drucksache 18(6)334, im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestags am 31. Mai 2017“, S. 4 (abrufbar als Teil des Wortprotokolls der Anhörung unter https://www.bundestag.de/resource/blob/530078/451e1a6aa6b77d7baf3e68e14e06cc3e/wortprotokoll-data.pdf).

72 Beukelmann, Online-Durchsuchung und Quellen-TKÜ, NJW-Spezial 2017, 440.

73 Buermeyer, „Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur ‚Formulierungshilfe‘ des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess, Ausschuss-Drucksache 18(6)334, im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestags am 31. Mai 2017“, S. 4.

Andere Stimmen schließen sich zwar grundsätzlich dem Befund an, dass der Wortlaut insofern offen sei, folgern hieraus jedoch nicht, dass die fraglichen technischen Maßnahmen von der Ermächtigung erfasst seien, sondern betonen, dass zweifelhaft und ungeklärt sei, ob die Maßnahmen einfachrechtlich erfolgen dürften. So führt *Eschelbach* unter Verweis auf *Buermeyer* aus:

> „Zumindest praktisch können auch Mikrofone oder Kameras aktiviert werden, die das informationstechnische System enthält und die akustische und optische Signale aus der Umgebung auffangen, welche dann als Daten ‚aus dem informationstechnischen System' an die Ermittlungsbehörden weitergeleitet werden können. Der Gesetzeswortlaut schließt dies nicht aus."[74] „Ob und wann mit der Maßnahme eine Totalüberwachung verbunden ist, bleibt im Gesetz ebenso wie in der Literatur und Rechtsprechung bisher ungeklärt."[75] „Für eine Online-Durchsuchung von Rechnern liefert § 100c keine Ermächtigung; diese ist in § 100b enthalten, wobei aber unklar bleibt, ob § 100b auch den Einsatz von Mikrophonen und Kameras infiltrierter informationstechnischer Systeme gestattet und so auch einen Lauschangriff ermöglicht…"[76]

Überwiegend wird demgegenüber die Auffassung vertreten, dass § 100b StPO nicht zu einem entsprechenden aktiv steuernden Zugriff auf Mikrofone bzw. Kameras von informationstechnischen Systemen zur Aufzeichnung des nichtöffentlich gesprochenen Wortes ermächtige.[77] So betont *Roggan*, dass trotz des weiten Wortlauts der Norm zu berücksichtigen sei,

> „dass die Regelung lediglich die Datenerhebung aus (»daraus«) einem infiltrierten System erlaubt. Auch spricht die Bezeichnung der Befugnis als (Online-)Durchsuchung für eine Beschränkung auf eine passive Kenntnisnahme von Datenbeständen, die sich bereits in dem System befinden und demnach (bereits) Gegenstand einer ziel- und zweckgerichteten Suche staatlicher Organe sein können. Das verböte eine Aktivierung bestimmter Handwarekomponenten des Systems zum Zwecke der Erlangung anders nicht ermittelbarer Sachverhalte (optische Erfassung der Umgebung durch die Inbetriebnahme einer Webcam etc.). (…) Auch das alleinige Mithören des gesprochenen Wortes in einer Wohnung durch die Mikrofonfunktion

74 Eschelbach, in: Satzger/Schluckebier/Widmaier, StPO, 3. Aufl. 2018, § 100b Rn. 4.

75 Eschelbach, in: Satzger/Schluckebier/Widmaier, StPO, 3. Aufl. 2018, § 100b Rn. 5.

76 Eschelbach, in: Satzger/Schluckebier/Widmaier, StPO, 3. Aufl. 2018, § 100c Rn. 5.

77 Singelnstein/Derin, Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, NJW 2017, 2646, 2647; Roggan, Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und die Allgemeinheit, StV 2017, 821, 826; Soiné, Die strafprozessuale Online-Durchsuchung, NStZ 2018, 497, 502; Gercke, in: Gercke/Julius/Temming/Zöller, StPO, 6. Auflage 2019, § 100b Rn. 11.

wäre schon deswegen verfassungswidrig, weil das § 100b StPO einführende Gesetz in Art. 17 das Wohnungsgrundrecht nicht als eingeschränkt bezeichnet."[78]

Dieser Auffassung sind auch *Singelnstein* und *Derin*: § 100b StPO gestatte lediglich,

„bereits gespeicherte Daten bzw. die während der Maßnahme erfolgende Nutzung des Systems für das Strafverfahren zu sichern. Unzulässig ist hingegen die Verwendung des gekaperten IT-Systems zur eigenständigen Erzeugung von Daten. Daher ist eine (heimliche) eigenständige Aktivierung von Mikrofon und Kamera ebenso wenig gestattet wie eine Veränderung der gespeicherten Daten. Dies macht der Name der Maßnahme deutlich („Durchsuchung") und wird durch die Legaldefinition in § 100 b I StPO geklärt. Danach darf in ein „System eingegriffen und dürfen Daten daraus erhoben werden". Die Befugnis gestattet also eine Erhebung aus dem System, nicht aber dessen manipulative Nutzung und Erhebung von Daten mittels desselben."[79]

Auch *Großmann* vertritt diese Auffassung:

„Da der Gesetzeswortlaut eine selbstständige Aktivierung von Kameras und Mikrofonen nicht ausdrücklich ausschließt, gehen manche Stimmen davon aus, dass die Norm auch hierzu eine Ermächtigungsgrundlage sein soll. Jenseits der zweifellos bestehenden technischen Realisierbarkeit solcher Eingriffe und des sich daraus ergebenden enormen Missbrauchspotentials derartiger Trojaner dürfte eine solche Maßnahme gleichwohl nicht von § 100 b StPO gedeckt sein: Der Gesetzeswortlaut spricht davon, dass aus dem infiltrierten System heraus Daten erhoben werden sollen. Eine ferngesteuerte Aktivierung von Kamera und Mikrofon und damit eine eigenständige Erzeugung neuen Datenmaterials durch Nutzung des informationstechnischen Geräts kann nicht unter den Wortlaut subsumiert werden. Zu berücksichtigen ist ferner, dass im geschützten Wohnbereich eine Aktivierung der Kamera zu repressiven Zwecken nach Art. 13 III GG gänzlich unzulässig wäre, da insoweit allenfalls eine akustische Überwachung durchgeführt werden kann. Aber auch eine „nur" akustische Überwachung im Wohnbereich des Betroffenen wäre nach der vorliegenden Regelung verfassungswidrig, da Art. 17 des § 100 b StPO einführenden Gesetzes Art. 13 GG nicht als eingeschränktes Grundrecht aufführt."[80]

78 Roggan, Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und die Allgemeinheit, StV 2017, 821, 826. Roggan kritisiert die Regelung gleichwohl, da aufgrund der „Befürchtung wegen zu besorgender Eingriffe in Art. 13 Abs. 1 GG" … schon „aus Gründen der Bestimmbarkeit des Befugnisumfangs für die Rechtsanwender … entgegenwirkende Kautelen ausdrücklich vorzusehen gewesen" wären (a.a.O. S. 826).

79 Singelnstein/Derin, Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, NJW 2017, 2646, 2647.

80 Großmann, Telekommunikationsüberwachung und Online-Durchsuchung: Voraussetzungen und Beweisverbote, JA 2019, 241, 244.

3.3.2.2. Bewertung

Die Auffassungen, wonach aus einem insofern angeblich nicht begrenzten Wortlaut von § 100b StPO zu folgern sei, dass auch das aktive Einschalten von Mikrofonen und Kameras fremder informationstechnischer Systeme und in der Folge das Ausspähen der Wohnung des Betroffenen durch die Norm gedeckt sein könnten, vermögen nicht zu überzeugen. Neben den bereits zitierten Argumenten der oben dargestellten gegenteiligen Auffassungen fällt vor allem ins Gewicht, dass schon aus dem Wortlaut von § 100b StPO, gerade auch in Zusammenschau mit dem von § 100c StPO, klar hervorgeht, dass Gegenstand der Datenabschöpfung gerade – und nur – das informationstechnische System ist: Nur „daraus" dürfen Daten ausweislich der Definition der Online-Durchsuchung in § 100b Absatz 1 Satz 1 StPO erhoben werden. Dem entsprechend lautet auch die Überschrift der Norm „Online-Durchsuchung", während § 100c StPO im Gegensatz hierzu von „Wohnraumüberwachung" spricht. Mit „Online-Durchsuchung" ist mithin nicht das Durchsuchen *des Wohnraums* bzw. der Wohnung des Betroffenen durch Online-Technik bezeichnet, sondern allein das Durchsuchen *der informationstechnischen Systeme* durch den Einsatz technischer Mittel.

Dies geht auch aus der Gesetzesbegründung hervor, in der es heißt, dass bei der „heimlichen Infiltration eines informationstechnischen Systems im Rahmen einer Online-Durchsuchung … die Nutzung *des Systems* umfassend überwacht und seine Speichermedien ausgelesen werden" können.[81] Es geht also ausdrücklich nur um die Überwachung der Nutzung *des Systems*, nicht etwa um die Überwachung der Nutzung *der Wohnung* des Betroffenen – eben nicht um „Wohnraumüberwachung". Also nur, wenn der Betroffene – oder ein Dritter – das System nutzt, eröffnet dies den Anwendungsbereich von § 100b StPO und damit den Ermittlungsbehörden im Rahmen des § 100b StPO die Möglichkeit, entsprechend anfallende Daten zu erheben.

Mit dieser Lesart im Einklang steht auch, dass sich die Gesetzesbegründung in diesem Zusammenhang ausführlich mit der Rechtsprechung des Bundesverfassungsgerichts zu Eingriffen in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auseinandersetzt, nicht aber mit Artikel 13 GG – bzw. zu letzterem gerade auf § 100c StPO verweist.[82] Aktive Eingriffe zur Wohnraumüberwachung sollen durch § 100b StPO mithin auch nach dem Willen des Gesetzgebers offenbar – dem Wortlaut entsprechend – gerade nicht ermöglicht werden. Damit im Einklang identifiziert die Gesetzesbegründung sprachlich klar durchweg das informationstechnische „System" als Gegenstand der Befugnisse von § 100b StPO, und nicht, davon unabhängig, das gesprochene Wort oder den Wohnraum.[83]

Im Ergebnis ermächtigt damit § 100b StPO die Strafverfolgungsbehörden nicht zum aktiven, steuernden Zugriff auf Mikrofon und/oder Kamera eines informationstechnischen Systems bzw.

---

81 Bericht und Beschlussempfehlung des Rechtsausschusses auf BT-Drs. 18/12785 vom 20.06.2017, S. 47 (Hervorhebung nicht im Original, d. Verf.).

82 Bericht und Beschlussempfehlung des Rechtsausschusses auf BT-Drs. 18/12785 vom 20.06.2017, S. 47 f.

83 Bericht und Beschlussempfehlung des Rechtsausschusses auf BT-Drs. 18/12785 vom 20.06.2017, S. 47 f.

Smart-Home-Gerätes, um hiermit Betroffene unabhängig von deren Nutzung des informationstechnischen Systems auszuspähen. Erfasst ist vielmehr lediglich das – passive[84] – Erheben einschlägiger Daten aus der Nutzung des Systems seitens des Betroffenen.

4. Ergebnis

Strafverfolgungsbehörden können nach geltendem Recht im Ermittlungsverfahren aufgrund unterschiedlicher Ermächtigungsgrundlagen in jeweils unterschiedlichen Konstellationen auch auf informationstechnische Systeme – darunter etwa auch Smart-Home-Hardware – von Verdächtigen zugreifen, wenn und soweit hierfür die jeweiligen Tatbestandsvoraussetzungen im Einzelfall vorliegen. Im Einzelnen gilt summarisch Folgendes:

- Im Wege einer „klassischen“ Durchsuchung (§§ 94 ff. StPO) können etwaige Geräte physisch sichergestellt sowie ggf. beschlagnahmt und gespeicherte Daten ausgelesen werden.

- Durch eine Telekommunikationsüberwachung (§ 100a Absatz 1 Satz 1 StPO) kann mittels entsprechender Systeme durchgeführte offene Telekommunikation überwacht und aufgezeichnet werden.

- Im Rahmen einer Quellen-Telekommunikationsüberwachung (§ 100a Absatz 1 Sätze 2, 3 StPO) kann mittels entsprechender Systeme durchgeführte Telekommunikation überwacht und aufgezeichnet werden, indem mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird; dies gilt auch für in diesen Systemen gespeicherte Kommunikationsinhalte. Durch § 100a StPO nicht gestattet wäre ein Erheben von Daten außerhalb eines Telekommunikationsvorgangs und mithin auch nicht ein aktives Ansteuern von Mikrofonen oder Kameras zum Zweck der Erzeugung und Speicherung von Ton- oder Bildaufnahmen in der betreffenden Wohnung.

- Die akustische Wohnraumüberwachung (§ 100c StPO) gestattet den Einsatz technischer Mittel – wie das Anbringen von Mikrofonen – in der Wohnung des Betroffenen; ein manipulativer Eingriff in die Integrität informationstechnischer Systeme des Betroffenen, etwa mit dem Ziel, Daten in Gestalt akustischer Signale aus Smart-Home-Geräten auszuleiten, dürfte von § 100c StPO nicht gedeckt sein.

- Mittels einer Online-Durchsuchung (§ 100b StPO) können auf entsprechenden informationstechnischen Systemen vorhandene Daten erhoben werden, indem mit technischen Mitteln in die Systeme eingegriffen wird, und hierbei auch Ton- und Bildsignale außerhalb von Telekommunikationszusammenhängen erfasst werden. Durch § 100b StPO nicht gestattet wäre jedoch das aktive Ansteuern von Mikrofonen oder Kameras informationstechnischer Systeme des Betroffenen zum Zweck der Erzeugung und Speicherung von Ton- oder Bildaufnahmen in der betreffenden Wohnung („Großer Spähangriff“).

***

84 Soiné, Die strafprozessuale Online-Durchsuchung, NStZ 2018, 497, 502.