§ 4 Zugriffsmöglichkeiten zur Gewinnung elektronischer Daten

In der Strafprozessordnung finden sich eine Vielzahl an heimlichen und offenen Ermittlungsmaßnahmen, die in ihrer Intensität für den Betroffenen ganz unterschiedlich ausgeformt sind. Im Folgenden Kapitel sollen diese Ermächtigungsgrundlagen näher betrachtet werden und sodann unter Beachtung der hierzu ergangenen höchstrichterlichen Rechtsprechung und der sich hierzu in der Literatur entwickelten Strömungen untersucht werden, inwiefern nach aktueller Gesetzeslage auf die durch Sprachassistenten gespeicherten Informationen zugegriffen werden kann.

A. Allgemeines

I) Grundsatz

Das Strafprozessrecht ist zwingend an den verfassungsrechtlich normierten Gesetzesvorbehalt gebunden, da nur dessen Beachtung ein „faires Verfahren" garantieren kann. Es bedarf daher nach der vom BVerfG entwickelten Wesentlichkeitstheorie für jegliche Maßnahmen, die den Betroffenen in seinen verfassungsrechtlich garantierten Rechten zu verletzen drohen, einer gesetzlichen Ermächtigungsgrundlage.[262] Je nach Gewichtung der betroffenen Grundrechte sind an die Erhebung der Daten unterschiedliche Anforderungen zu stellen.[263] Die Bedeutung von Daten und damit auch deren Grundrechtsrelevanz ist ferner abhängig von der Datenart, die terminologisch in TKG und TMG näher beschrieben werden.[264]

262 BVerfG, Beschluss v. 01.03.2000 – 2 BvR 2017/94, Rn. 9.
263 *Trüg/Mansdörfer* in: Hilber, Handbuch Cloud Computing, Teil 7, Rn. 7.
264 *Darby*, Strafverfolgung im Internet, S. 25.

II) Datenarten

Im Zusammenhang mit den bei Telekommunikationsvorgängen relevant werdenden Telekommunikationsdaten wird klassischerweise zwischen Verkehrs-, Bestands- und Inhaltsdaten unterschieden.

1) Bestandsdaten

Gem. § 3 Nr. 3 TGK sind Bestandsdaten die zur Begründung, inhaltlichen Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhobenen Daten, wie den Namen, die Anschrift, die Rufnummer, den Vertragsbeginn oder die Kontodaten. Bestandsdaten geben damit Aufschluss über das Vertragsverhältnis zwischen dem Anbieter der Telekommunikationsdienstleistung und dem Nutzer. Sie sagen noch nichts darüber aus, ob einzelne Leistungen an den Nutzer erbracht wurden. Sie betreffen vielmehr das vertragliche „Grundverhältnis“[265].

2) Verkehrsdaten

Die Verkehrsdaten betreffen die Art des genutzten Kommunikationsdienstes, Anfang Ende und Dauer der Verbindung, das genutzte Datenvolumen, an der Kommunikation beteiligte Personen sowie deren Standorte.[266] Nicht von den Verkehrsdaten erfasst ist der konkrete Inhalt der Kommunikation.[267] In der nahen Vergangenheit sind die Verkehrsdaten im Zuge der Diskussion um die Vorratsdatenspeicherung rechtspolitisch in den Fokus gerückt. Mit den auf diesem Wege erhobenen Daten lassen sich Persönlichkeitsprofile erstellen und das Nutzerverhalten analysieren. Dies soll – so die Befürworter der gesetzlich umstrittenen Regelung[268] – der

265 *Darby*, Strafverfolgung im Internet, S. 25.
266 *Günther* in: MüKo-StPO, G10 § 1, Rn. 22; vgl. im Übrigen die Aufzählung in § 96 TKG.
267 *Günther* in: MüKo-StPO, G10 § 1, Rn. 22.
268 Problematisch ist dabei vor allen Dingen die anlasslose Speicherung der Daten. Vielfach wird bezweifelt, ob die verdachtslose Vorratsspeicherung sämtlicher Verbindungs- und Bewegungsdaten mit den Anforderungen des europäischen Gerichtshofs vereinbar ist. Der Europäische Gerichtshof erklärte 2016 schwedische und britische Gesetze zur verdachtslosen Vorratsdatenspeicherung für

Verhinderung und Aufklärung schwerer Straftaten dienen. Die Erhebung der Verkehrsdaten ist in den §§ 100g StPO, 96 TKG gesetzlich normiert.

3) Inhaltsdaten

Wenngleich sich keine gesetzliche Definition für Inhaltsdaten finden lässt, fällt hierunter jedenfalls der eigentliche Inhalt der ablaufenden Kommunikation.[269] Dabei wird keine Beschränkung auf den klassischen Fall eines Telefongespräches vorgenommen, vielmehr sind auch die konkreten Inhalte einer E-Mail oder eines Messenger-Chats hierunter zu fassen.

4) Zusammenfassung

Anhand dieser Definitionen wird bereits die unterschiedliche Wertigkeit von Daten für die Strafverfolgungsbehörden ersichtlich. Während Bestandsdaten eher von untergeordnetem Interesse sind und zur finalen Aufklärung eines Verbrechens nur selten beitragen können, stellen sich Verkehrs- und vor allem Inhaltsdaten in dieser Hinsicht vielversprechender dar. Gleichwohl sind Bestandsdaten zu Beginn des Ermittlungsverfahren oftmals von Nöten, um erste Anhaltspunkte zur Identifikation einer Person zu erhalten.[270] Während durch die Erhebung von Verkehrsdaten bestimmt werden kann, wo sich eine Person zum Tatzeitpunkt befand, kann nach Erlangen der Inhaltsdaten die komplette Kommunikation zwischen den Betroffenen unter Beachtung der gesetzlichen Grenzen zum Beweis herangezogen werden.

Unter Heranziehung der Verkehrsdaten seines Mobiltelefons verurteilte beispielsweise das LG Hannover einen Angeklagten wegen schwerer

---

nicht mit dem Unionsrecht vereinbar, vgl. EuGH, NJW 2017, 717 ff. Auf nationaler Ebene entschied das Oberverwaltungsgericht Nordrhein-Westfalen, dass das deutsche Gesetz zur Vorratsdatenspeicherung nicht mit Art. 15 Abs. 1 der Datenschutzrichtlinie (2002/58/EG v. 12.07.2002) und damit nicht mit EU-Recht vereinbar sei, vgl. OVG Münster, NVwZ-RR 2018, 43 ff. Die Richter forderten Regelungen, die den betroffenen Personenkreis auf Fälle beschränkten, bei denen ein zumindest mittelbarer Zusammenhang mit der gesetzlich bezweckten Verfolgung und Abwehr schwerer Straftaten bestehe.

269 *Bruns* in: KK-StPO, § 100a StPO, Rn. 15.

270 *Darby*, Strafverfolgung im Internet, S. 25.

Brandstiftung.[271] Dem Angeklagten wurde vorgeworfen, die Wohnung seines Freundes, bei dem er bis zum vorherigen Tag gewohnt hatte, durch Brandlegung zerstört zu haben. Zu seiner Verteidigung führte der Angeklagte aus, dass er den Brand um 19.00 Uhr nicht gelegt haben könne, da er erst die Bahn um 18:55 Uhr ab Hannover zurückgenommen habe und daher um 19:00 Uhr noch gar nicht am Tatort sein konnte. Nach Auswertung der Verkehrsdaten seines Mobiltelefons zeigte sich jedoch, dass der Angeklagte bereits ab 19.00 Uhr mehrfach an einem Funkmast zwischen dem Tatort und dem Bahnhof am Ort des Tatorts eingeloggt war.[272] In einem anderen Fall wurde der Angeklagte wegen Diebstahls und Beihilfe zum Diebstahl verurteilt. Die Überzeugung von der Tatbeteiligung des Angeklagten gewann das urteilende Gericht insbesondere aus den Verbindungsdaten des Mobiltelefons des Angeklagten, die Aufschluss über den jeweiligen Standort des Telefons, Zeitpunkt und Dauer der geführten Telefongespräche und zu den daran beteiligten Anschlüssen gaben.[273] Auf die während eines abgehörten Telefongesprächs gewonnen Inhaltsdaten wurde beispielsweise in einem Fall vor dem LG Stuttgart maßgeblich die Verurteilung wegen unerlaubten Handeltreibens mit Betäubungsmitteln in nicht geringer Menge gestützt.[274] Die Wichtigkeit dieser Daten kann daher aufsteigend von den Bestandsdaten über die Verkehrsdaten hin zu den Inhaltsdaten zusammengefasst werden. Während erstere in der Regel nur zu Beginn des Ermittlungsverfahrens eine Hilfe darstellen, geraten Bestandsdaten und vor allen Dingen Inhaltsdaten im Rahmen der gerichtlichen Beweisführung stärker in den Mittelpunkt. Bei den durch Sprachassistenten gefertigten Audioaufzeichnungen handelt es sich hieran anknüpfend um Inhaltsdaten. Die Aufzeichnungen beinhalten zuvörderst den Inhalt erfolgter Informationsabfragen.

271 LG Hannover, Urteil vom 23.04.2010 – 46 KLs 31/09; die Vorgehensweise zur Beweisgewinnung bestätigend BGHSt 56, 127.
272 BGH, MMR 2011, 412 f.
273 BGHSt 56, 138 (LG Stuttgart, 20.07.2010 – 19 KLs (b) 201 Js 102639/09).
274 BGH, NStZ 2008, 473, 473 (LG Stuttgart).

B. Ermächtigungsgrundlagen

I) § 100a StPO

Der Zugriff auf Telekommunikationsvorgänge erfolgt nach §§ 100a, 100e StPO. Die Normen ermächtigen zu einem Eingriff in das Fernmeldegeheimnis aus Art. 10 GG und das allgemeine Persönlichkeitsrecht, Art 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG.[275] Ob ein Zugriff auch auf die bei der Nutzung eines Smart Speakers ablaufenden Vorgänge möglich ist, richtet sich maßgeblich danach, ob in diesem Vorgang Telekommunikation im Sinne des § 100a StPO gesehen werden kann.

1) Tatbestandsmerkmal der Kommunikation

Eine Legaldefinition der „Telekommunikation" findet sich in der Strafprozessordnung nicht. Gerade in Anbetracht dessen, dass Cloud Computing nicht den Anwendungsfall darstellt, den der Gesetzgeber bei Schaffung des § 100a StPO vor Augen hatte, ist auch bis heute nicht hinreichend geklärt, inwiefern bei einer Verbindung des Nutzers mit dem Cloud-Dienst von Telekommunikation gesprochen werden kann. Entscheidend ist insofern auch, wie der Telekommunikationsbegriff aus § 100a StPO zu verstehen ist.

a) Weiter technischer Telekommunikationsbegriff

Allem voran in der Rechtsprechung entwickelte sich ab Mitte der 90er Jahre ein technisch geprägter Telekommunikationsbegriff.[276] Einfach gesetzlich wird dabei an § 3 Nr. 22 TKG angeknüpft, nach dessen Legaldefinition unter Kommunikation „der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen" zu verstehen ist. Argumente für diese Sichtweise werden vor allem mit Blick auf den gesetzgeberischen Willen vorgebracht. So soll im Zuge der Änderung des Wortlauts des § 100a StPO von „Fernmeldeverkehr" zu „Telekommunikation" zum Ausdruck gebracht worden sein, dass mit dieser Angleichung an die Terminologie des TKG die Begriffe auch inhaltlich

275 *Trüg/Mansdörfer* in: Hilber, Handbuch Cloud Computing, Teil 7, Rn. 24.
276 BGH, NJW 2003, 2034 f.; BGH, NJW 2007, 930, 931 f.

gleich auszulegen seien.[277] Wenngleich in diesem Lager Einigkeit herrscht, den Kommunikationsbegriff im Einklang mit dem TKG zu bestimmen, so können dennoch unterschiedliche Ausprägungen dieser weiten Sichtweise erkannt werden.[278]

aa) Technische Auslegung

Anhänger der rein technischen Auffassung greifen zur Bestimmung der Kommunikation ausschließlich und ohne etwaige Einschränkungen auf § 3 Nr. 22 TKG zurück. Ausweislich der hierfür einschlägigen Definition kann Telekommunikation auch zwischen bloßen Maschinen stattfinden; eine menschliche Teilhabe ist an dem Kommunikationsprozess überhaupt nicht erforderlich. Dies wird damit begründet, dass letztlich selbst die Kommunikation zwischen zwei Maschinen auf einen menschlichen Ursprung zurückgehe. Durch einen Befehl zur Ausführung oder das anfängliche Programmieren der Maschinen beruhe auch die durch Maschinen ablaufende Kommunikation mittelbar auf menschlichem Handeln.[279]

bb) Technikorientierte Auslegung

In die gleiche Richtung gehen die Rechtsprechung des Bundesgerichtshofs und große Teile der Literatur, die sich ebenfalls an der Legaldefinition des TKG orientieren.[280] Fortlaufend wird dabei betont, dass die Begriffe Telekommunikation in § 100a StPO und § 3 Nr. 22 TKG inhaltsgleich zu verstehen sein sollen.[281] Gleichwohl soll nicht jeder technische Vorgang des Aussendens, Übermittelns oder Empfanges von § 100a StPO erfasst sein. Dies solle nur für solche Vorgänge gelten, die mit der Nachrichtenübermittlung mittels Telekommunikationsanlagen im Zusammenhang

277 *Meininghaus*, Der Zugriff auf E-Mails im strafrechtlichen Ermittlungsverfahren, S. 79.
278 Ähnlich bereits *Grözinger*, Die Überwachung von Cloud-Storage, S. 182.
279 *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 266; *Meininghaus*, Der Zugriff auf E-Mails im strafrechtlichen Ermittlungsverfahren, S. 79.
280 *Klesczewski*, ZStW 2011, 737, 741; *Schmitt* in: Meyer-Goßner/Schmitt, § 100a StPO, Rn. 6.
281 BGH, StV 2003, 370, 371; *Hauck* in: LR-StPO, § 100a StPO, Rn. 29; *Graf* in: BeckOK-StPO, § 100a StPO, Rn. 3; *Eschelbach* in: SSW-StPO, § 100a StPO, Rn. 2; *Schmitt* in: Meyer-Goßner/Schmitt, § 100a StPO, Rn. 6.

stehen.[282] Dabei wird auch der Begriff der Telekommunikationsanlage anhand der Legaldefinition aus § 3 Nr. 23 TKG abgeleitet. „Telekommunikationsanlagen" sind technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können. Damit ein Vorgang daher unter § 100a StPO fallen könne, ist Voraussetzung, dass wenigstens eine Person mittels einer solchen Telekommunikationsanlage kommuniziere. Bei dieser Person soll jedoch wiederum nicht von Relevanz sein, ob sich der aktuelle Kommunikationsvorgang mit Wissen und Willen des Betroffen vollzieht.[283]

b) Grundrechtsanaloger Telekommunikationsbegriff

Eine andere Strömung will den Telekommunikationsbegriff analog zu Art. 10 Abs. 1 Var. 3 GG verstanden wissen.[284] Durch diese Auslegung der Ermächtigungsgrundlage soll ein möglichst umfassender Schutz des Fernmeldegeheimnisses aus Art. 10 GG gewährleistet werden.[285] Ihre Berechtigung soll diese Sichtweise darin finden, dass § 100a StPO in seiner ursprünglichen Fassung von der Überwachung des „Telekommunikationsverkehrs" ausgegangen ist, nun aber die gleiche Terminologie wie Art. 10 Abs. 1 Var. 3 GG, der vom „Telekommunikationsgeheimnis" spricht, nutzt.[286] Dadurch komme zum Vorschein, dass der Gesetzgeber eine Ermächtigung für die Überwachung sämtlicher von Art. 10 Abs. 1 Var. 3 GG geschützter Verhaltensweisen schaffen wollte.[287] Zudem sei zu beachten, dass auch bei einer solchen extensiven Auslegung der Ermächtigungsgrundlage der Schutz vor staatlichen Eingriffen nicht leelaufen würde. Denn gem. § 100a Abs. 1 StPO darf eine Überwachung und Aufzeichnung der Kommunikation nur dann erfolgen, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen hat. Ein notwendiges Anordnungserfordernis ist demnach der Verdacht, dass eine der hier abschlie-

282 BGH, StV 2003, 370, 371.
283 BGH, StV 2003, 370, 372.
284 *Wölm*, Schutz der Internetkommunikation und heimliche Internetaufklärung, S. 243; *Bruns* in: KK-StPO, § 100a StPO, Rn. 4; *Dalby*, Strafverfolgung im Internet, S. 93; Gaede, StV 2009, 96, 100.
285 LG Aachen, StV 1999, 590.
286 *Grözinger*, Die Überwachung von Cloud-Storage, S. 211.
287 *Grözinger*, Die Überwachung von Cloud-Storage, S. 211.

ßend aufgeführten Straftaten vorliegen könnte. Dabei ist es ausreichend, dass es nach kriminalistischer Erfahrung möglich erscheint, dass eine verfolgbare Straftat vorliegt (Anfangsverdacht)[288]. Es bedarf weder eines hinreichenden Tatverdachts[289], daher der einfachen Wahrscheinlichkeit einer Verurteilung,[290] noch eines dringenden Tatverdachts,[291] in Form einer hohen Wahrscheinlichkeit, dass der Beschuldigte als Täter oder Teilnehmer rechtswidrig und schuldhaft eine Straftat begangen hat[292]. Als weitere Einschränkung muss die Tat gem. § 100a Abs. 1 Nr. 2 StPO auch im Einzelfall schwer wiegen und die Erforschung des Sachverhalts muss auf andere Weise wesentlich erschwert oder aussichtslos wäre (sog. Subsidiaritätsklausel).

c) Enger strafverfahrensrechtlicher Telekommunikationsbegriff

Zuletzt wird für ein Lossagen von Einflüssen aus dem Grundgesetz oder dem TKG plädiert und eine eigenständige strafprozessuale Auslegung des Telekommunikationsbegriffes favorisiert.[293] Erstmalig aufgekommen ist die Frage nach einem genuin zu bestimmenden Telekommunikationsbegriff im Anschluss an den Beschluss eines BGH-Ermittlungsrichters betreffend den staatlichen Zugriff auf die in einer Mailbox gespeicherten Computerdaten.[294] In dem Beschluss vom 31.07.1995 erlaubte der zuständige Ermittlungsrichter über § 100a StPO den Zugriff auf die Mailbox des Betroffenen, ohne nähere Ausführungen zu der Frage, inwiefern bei den auf der Mailbox gespeicherten Daten noch von Fernmeldeverkehr i.S.d. § 100a a.F. StPO gesprochen werden kann.[295] Dadurch kam die Befürchtung auf, dass in der Entscheidung von der Eröffnung des grundrechtlichen Schutzbereich auf das Vorliegen einer tatbestandlichen Voraussetzung des Gesetzesvorbehalts geschlossen wurde.[296] Die sich sodann entwickelnde Strö-

288 *Beulke/Swoboda*, Strafprozessrecht, Rn. 172.
289 Vgl. §§ 170 Abs. 1, 203 StPO.
290 *Schmitt* in: Meyer-Goßner/Schmitt, § 203 StPO, Rn. 2.
291 Vgl. §§ 111a Abs. 1, 112 StPO.
292 *Roxin/Schünemann*, Strafverfahrensrecht, § 30, Rn. 5.
293 *Gercke* in: HK-StPO, § 100a StPO, Rn. 10; *ders.*, Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren, S. 98 f.; *Hiéramente,* HRRS 2016, 448, 450; *Demko*, NStZ 2004, 57, 61; *Roggan*, NJW 2015, 1995, 1996; *Bernsmann/Jansen*, StV 1999, 591; *Eschelbach* in: SSW-StPO, § 100a StPO, Rn. 5.
294 *Kudlich*, JuS 1998, 209, 213 f.
295 BGH (Beschluss des Ermittlungsrichter), NJW 1997, 1934.
296 *Kudlich*, JuS 1998, 209, 213 f.

mung war sich insofern einig, den Telekommunikationsbegriff anhand der gängigen Auslegungsmethoden unter Berücksichtigung der strafprozessualen Besonderheiten zu bestimmen.[297] Eine genauere Darstellung wie ein solcher Telekommunikationsbegriff sodann auszuformulieren wäre, findet sich jedoch nur selten. *Hiéramente* stellt im Zuge dieser Definitionsentwicklung das Erfordernis einer sozialen Interaktion in den Mittelpunkt.[298] Nur so könne dem Umstand Rechnung getragen werden, dass der Betroffene auch unter den Schutz des Art. 10 GG fallende Tätigkeiten verüben könne, ohne dabei freiwillig auf seine Privatsphäre zu verzichten. Beispielhaft dafür sei die gerade nicht öffentlich ablaufende Nutzung des Internets zur Informationsgewinnung, bei welcher – im Unterschied zur klassischen Telekommunikation im Rahmen eines Telefongesprächs – keine soziale Interaktion stattfinde. Bei der klassischen Telekommunikation offenbare der Betroffene im Rahmen eines Telefongesprächs, einer E-Mail oder im Chat bewusst und freiwillig Wissen gegenüber einem Dritten.[299] Die Nutzung des Internets zum Zwecke der reinen Informationsgewinnung erfordert hingegen keine Interaktion mit Dritten und ist, jedenfalls solange die Informationen nicht in öffentlichen frei zugänglichen Foren oder Chats geteilt werden, seiner Natur nach ein privater Vorgang. Andere wiederum stellen entscheidend darauf ab, dass die Kommunikation mit einem Mitteilungswillen erfolgen müsse.[300]

2) Nutzung eines Smart Speakers als Kommunikation i.S.d. § 100a Abs. 1 S. 1 StPO

Zur Beantwortung der Frage, ob die Nutzung eines Smart Speakers Telekommunikation i.S.d. § 100a StPO darstellt, ist entscheidend zu welchem Zeitpunkt die Nutzung des Sprachassistenten überwacht wird.[301] Dabei kann in das Stadium vor der Datenübertragung, während der Übertragung und nach der Übertragung der Daten unterschieden werden. Eine ähnliche Unterscheidung wurde grundlegend bereits zur Bestimmung der

297 *Gercke* in: HK-StPO, § 100a StPO, Rn. 10; *Fezer*, NstZ 2003, 625, 627.
298 *Hiéramente,* StraFo 2013, 96, 99.
299 *Hiéramente,* HRRS 2016, 448, 451.
300 *Wicker*, Cloud Computing und staatlicher Strafanspruch, S. 380.
301 Diese zutreffende Differenzierung bzgl. der Nutzung von Cloud-Speichern wie Dropbox, iCloud oder Google Drive bereits bei *Grözinger*, Die Überwachung von Cloud-Storage, S. 188 ff.

Ermächtigungsgrundlage hinsichtlich des Zugriffs auf den E-Mail-Verkehr herangezogen.[302]

a) Vor der Übertragung

Vor der Übertragung der aufgezeichneten Sprachnachricht scheidet ein Zugriff auf das Endgerät des Nutzers nach § 100a StPO sowohl nach der rein technischen als auch nach der technikorientierten Auffassung aus. Dem Aussenden, Übermitteln und Empfangen wie es in § 3 Nr. 22 TKG heißt, ist ein dynamischer Übermittlungsvorgang immanent. An einem solchen fehlt es, wenn sich die Audioaufzeichnungen bildlich gesprochenen noch nicht auf dem Weg zum Server des Sprachassistenten befinden, sodass keine Telekommunikation i.S.d. § 22 Nr. 3 TKG vorliegt. Auch ist zu diesem Zeitpunkt der Schutzbereich des Art. 10 GG noch nicht eröffnet. Die Daten befinden sich noch auf dem Gerät des Nutzers und damit noch in dessen Herrschaftssphäre. Vor Beginn des Übertragungsvorgangs ist vielmehr der Schutzbereich des Art. 2 Abs. 1 GG i.V.m. Art. 1 GG betroffen.[303] Zu einer Übertragung aufgrund oder infolge derer einfacher auf die Daten zugegriffen werden könnte, kam es zu diesem frühen Zeitpunkt noch nicht. Insofern ist Art. 10 GG, dem nur die Vertraulichkeit des zur Nachrichtenübermittlung eingesetzten Übertragungsmediums unterfällt[304], in diesem Stadium noch nicht einschlägig. Auch im Sinne eines strafprozessualen Telekommunikationsbegriffes liegt zu diesem Zeitpunkt noch keine Telekommunikation vor. Als Mindestanforderung verlangt auch dieser einen dynamischen Übermittlungsvorgang.

b) Während des Übertragungsweges

Deutlich interessanter erscheint aus dem Blickwinkel des § 100a StPO der zeitliche Teil der Übermittlung der Audioaufzeichnungen zum Server, bevor dort mittels Algorithmen die Spracheingaben in – für den Sprachassistenten – verwertbare Daten umgewandelt werden.

---

302 Vgl. bzgl. der aufgestellten Phasen *Schlegel*, HRRS 2007, 44, 47; *Beulke/Swoboda*, Strafprozessrecht, Rn. 392; *Graf* in: BeckOK-StPO, § 100a StPO, Rn. 55; *Klesczewski*, ZStW 2011, 737, 744 ff.; *Zimmermann*, JA 2014, 321 f.

303 BT-Drs. 18/12785, S. 49.

304 BVerfG, NJW 2002, 3619, 3621.

aa) Rein technische Auslegung

Im Lichte eines rein technischen Verständnisses des Telekommunikationsbegriffes wäre die Nutzung eines Sprachassistenten als Kommunikation i.S.d. § 100a StPO aufzufassen, sofern diese unter § 3 Nr. 22 TKG subsumierbar ist. Das Aussenden, Übermitteln und Empfangen beziehen sich auf jegliche Signale. Auf den Inhalt oder den Zweck der Signale kommt es nicht an. Entscheidend ist damit ausschließlich, ob eine technische Übertragungsleistung vorliegt, was unabhängig vom Übertragungsdienst und dem Inhalt der Übertragung zu beurteilen ist.[305] Den Signalen muss lediglich ein beliebiger Informationsgehalt zukommen, die sie als Nachricht identifizierbar machen und als solche Daten transportieren.[306] Der Übertragungsvorgang müsste wie sich aus § 3 Nr. 22 TKG ergibt mittels einer Telekommunikationsanlage i.S.d. § 3 Nr. 23 TKG erfolgen.

Das Endgerät eines Sprachassistenten zeichnet das gesprochene Wort auf, sodass dieses als gespeicherte Audiodatei via Internet an das Rechenzentrum bzw. die Cloud des Anbieters übermittelt werden kann. In dieser Übermittlung ist zweifelsohne eine Übertragungsleistung zu sehen, weshalb die transportierten Audioaufzeichnungen als Kommunikation i.S.d. §§ 22, 23 TKG einzuordnen sind, sofern auf den Datenstrom zwischen dem Nutzer des Sprachassistenten und dem verarbeitenden Server zugegriffen wird.

bb) Technikorientierter Telekommunikationsbegriff

Unabhängig davon, dass während des Übertragungsweges bei der Nutzung eines Sprachassistenten von Kommunikation i.S.d. §§ 22, 23 TKG gesprochen werden kann, müsste im Sinne der technikorientierten Auffassung der Betroffene einschränkend gerade mittels einer Telekommunikationsanlage kommunizieren wollen. Es ist daher zu klären, ob der Nutzer eines Sprachassistenten mittels diesem kommunizieren will oder durch die Aktivierung des Sprachassistenten lediglich eine Datenübermittlung von technischem Gerät zu technischem Gerät stattfindet. Zur Beantwortung dieser Frage eignet sich ein Blick auf einem ähnlich gelagerten Fall und die hierzu ergangene Rechtsprechung. Die bei der Nutzung eines Sprachassistenten ablaufende „Kommunikation im weitesten Sinne“ ist in

305 *Fetzer* in: Arndt/Fetzer/Scherer/Graulich-TKG, § 3, Rn. 100.
306 *Lünenberger/Stamm* in: Scheurle/Mayen-TKG, § 3, Rn. 61.

der Regel darauf gerichtet eine Antwort auf eine dem Sprachassistenten gestellte Frage zu erhalten. Der gleiche Ablauf findet sich in der Sache beim Surfen im Internet und der Nutzung einer Suchmaschine zur Informationsbeschaffung. Nach Ansicht des LG Ellwangen, stellt auch die Nutzung des Internets durch Abruf von Web-Seiten im World Wide Web mittels eines Web-Browsers eine Internetkommunikation und damit eine Telekommunikation im Sinne strafprozessualer Vorschriften dar.[307] Die Vertreter dieser Sichtweise argumentieren, dass es beim Abruf von Informationen im Internet im Rahmen des Googelns gerade nicht lediglich zu einem bloßen technischen Austausch von Datenpaketen zwischen informationstechnischen Systemen komme, sondern es sich bei den gewonnen Daten um bewusst von Personen zu Kommunikationszwecken eingegebene und abgerufene Informationen handle.[308] In der Eingabe von Suchbegriffen in einer Internetsuchmaschine wie Google könne daher Telekommunikation im Sinne des § 100a StPO liegen. Überträgt man diese Rechtsprechung auf den hiesigen Fall so müsste auch die Nutzung eines Sprachassistenten als Kommunikation i.S.d. § 100a StPO anzusehen sein.[309]

cc) Grundrechtsanaloger Telekommunikationsbegriff

Um aus Sicht eines grundrechtsanalogen Telekommunikationsbegriffes zu bestimmen, ob während des Übermittlungsvorgangs Telekommunikation vorliegt, ist bereits an dieser Stelle näher auf den sachlichen Schutzbereich des Art. 10 GG einzugehen und sodann zu fragen, ob die Nutzung eines Sprachassistenten während des Übermittlungsvorganges hierunter fällt.

(1) Grundsätzliches

In der Sache schützt Art. 10 Abs. 1 Var. 3 GG die unkörperliche Übermittlung von Informationen an individualisierte Empfänger mit Hilfe des Telekommunikationsverkehrs.[310] Der Schutzzweck des Art. 10 GG liegt

307 LG Ellwangen, Beschl. v. 28.05.2013, Az.: 1 Qs 130/12.
308 *Bär*, ZD 2017, 132, 137.
309 Im Ergebnis *Graf* in: BeckOK-StPO, § 100a StPO, Rn. 99; offenlassend, ob dabei Telekommunikation vorliegt BT-Drs. 19/11478, S. 3.
310 BVerfGE 115, 166, 182; *Hermes* in: Dreier-GG, Art. 10 GG, Rn. 37; *Schoch*, JURA 2011, 194, 197.

darin begründet, dass bei einer Kommunikation über eine räumliche Distanz die Gesprächspartner – im Gegenteil zu einem Gespräch unter Anwesenden – nicht die Möglichkeit haben, den äußeren Rahmen der Kommunikation alleine zu bestimmen und über die Privatheit und die Gesprächsbeteiligten selbst zu wachen.[311] Vielmehr ist aufgrund der räumlichen Distanz ein technischer Übermittlungsvorgang erforderlich, auf den der zu schützende Bürger keinen Einfluss hat. Der dabei bestehenden Gefahr, dass sich Dritte aufgrund technischer Möglichkeiten, Zugang zu den Inhalten und Übermittlungsdaten der Kommunikation verschaffen, soll so entgegengewirkt werden.[312] Als Abwehrrecht schützt Art. 10 GG vor einer staatlichen Kenntnisnahme des Inhalts und der näheren Umstände der Telekommunikation und so vor Gefahren für die Vertraulichkeit von Mitteilungen, die aus dem Übermittlungsvorgang einschließlich der Einschaltung fremder Übermittler entstehen.[313] Dabei kommt es weder auf die konkrete Übermittlungsart (Kabel, Funk, analoge oder digitale Vermittlung) noch die gewählte Ausdrucksform (Sprache, Bilder, Töne oder sonstige Daten) an.[314] Zu Recht wurde bezüglich des Schutzbereichs aus Art. 10 GG höchstrichterlich festgestellt, dass der Schutzbereich zum Schutz der Bürgerinnen und Bürger gegenüber neuen technischen Entwicklungen offen ist. Der sachliche Schutzbereich findet seine Grenze also nicht in den zu einem bestimmten Zeitpunkt bekannten und sich im Einsatz befindlichen Arten elektronischer Informationsvermittlung. Insofern wird von einer dynamischen und entwicklungsoffenen Grundrechtsgewährleistung gesprochen.[315] Beispielsweise werden E-Mails, SMS, Messenger-Dienste und Chats dem Fernmeldegeheimnis und nicht dem Briefgeheimnis zugeordnet.[316]

311 BverfGE 106, 28, 36.
312 BverfGE 106, 28, 36.
313 BverfGE 106, 28, 36 f.
314 BverfGE 115, 166, 182 f.; *Sodan* in: Sodan-GG, Art. 10 GG, Rn. 5; *Hermes* in: Dreier-GG, Art. 10 GG, Rn. 36; *Guckelberger* in: SHH, Art. 10 GG, Rn. 22.
315 BverfGE 115, 166, 182; *Durner* in: Maunz/Dürig-GG, Art. 10 GG, Rn. 64; *Pagenkopf* in: Sachs-GG, Art. 10 GG, Rn. 14b; *Sodan* in: Sodan-GG, Art. 10 GG, Rn. 5; *Guckelberger* in: SHH, Art. 10 GG, Rn. 21 f.; *Martini* in: v. Münch/Kunig, Art. 10 GG, Rn. 63.
316 *Morlok*, Grundrechte, Rn. 324.

(2) Sinn und Zweck der Grundrechte

Für die stets wiederkehrende Frage, inwiefern ein bestimmtes Verhalten unter den Schutz eines Grundrechts fällt, wird im Folgenden Sinn und Zweck der Grundrechte bemüht. Daher ist fraglich, was eigentlich Sinn und Zweck der Grundrechte darstellt. Eine richtungsweisende Antwort auf diese Frage findet sich bereits in der Lüth-Entscheidung aus dem Jahre 1958. Dort heißt es *„ohne Zweifel sind die Grundrechte in erster Linie dazu bestimmt, die Freiheitssphäre des einzelnen vor Eingriffen der öffentlichen Gewalt zu sichern*“[317]. In der Folge entwickelte sich eine Differenzierung in Freiheitsgrundrechte bzw. Abwehrgrundrechte, zur Abwehr eines staatlichen Handelns und Leistungsgrundrechte mit deren Hilfe ein staatliches Handeln erzwingbar werden sollte. Bei dem hier in Rede stehenden Art. 10 GG handelt es sich um ein sog. Freiheitsgrundrecht, mit der Zielsetzung, dass der Staat es unterlässt, auf den Fernmeldeverkehr bzw. die Telekommunikation zuzugreifen. Ein solches Abwehrgrundrecht hat das Ziel, die Freiheit vor staatlichen Zugriffen zu gewährleisten, stellt also den sog. status negativus dar.[318] Sofern es bereits zu einem staatlichen Eingriff gekommen ist wird der abwehrende Charakter der Freiheitsgrundrechte dadurch deutlich, dass sich aus dem Grundrecht ein Beseitigungsanspruch ergibt.[319] Hinsichtlich Art. 10 GG hat das BVerfG mehrfach betont, dass das Grundrecht zur Bestimmung seines Schutzgehalts an den Grundrechtsträger und dessen Schutzbedürftigkeit anknüpfen muss.[320] Daher ist für die Bestimmung der Reichweite von Art. 10 GG stets zu fragen, wovor der Grundrechtsträger geschützt werden soll und ob dieser in einer konkreten Situation aufgrund seiner Machtlosigkeit gegenüber dem Staat verfassungsrechtlich garantierten Schutz bedarf.

(3) Massen- oder Individualkommunikation

Eine grobe Unterteilung, ob ein Verhalten unter den Schutz des Art. 10 GG fällt, kann durch eine Unterscheidung zwischen Massen- und Individualkommunikation vorgenommen werden. Nur im Falle von Indi-

317 BverfGE 7, 198, 204.
318 *Hufen*, Grundrechte, § 5, Rn. 1.
319 *Jarass* in: Handbuch der Grundrechte, § 38, Rn. 16.
320 BverfGE 124, 43, 56; BVerfG, NJW 2007, 351, 354; *Hartmann* in: HK-GS, § 100a StPO, Rn. 2.

vidualkommunikation soll der Schutzbereich eröffnet sein. Hinsichtlich der Massenkommunikation, die an einen unbestimmten Rezipientenkreis gerichtet ist, wird angenommen, dass solche öffentliche Kommunikationsvorgänge nicht als vertraulich eingestuft werden können und damit nicht dem Schutz des Fernmeldegeheimnisses unterfallen.[321] Ursprünglich sollte diese Abgrenzung vor allem den Unterschied zwischen Rundfunk- und Telekommunikationsfreiheit verdeutlichen.[322] Gleichfalls wird sie aber auch zur Differenzierung innerhalb einer möglichen Betroffenheit des Art. 10 GG genutzt. Vor allen Dingen in der neueren Literatur wird zur Abgrenzung zwischen Individual- und Massenkommunikation auf die Art der Anwendung[323] oder auf das Vorhandensein etwaiger Zugangshindernisse abgestellt[324]. Während die Nutzung des World Wide Web aufgrund des ungehinderten Zugangs eher der Massenkommunikation zuzuordnen wäre, würde es sich bei der Versendung einer E-Mail vielfach um Individualkommunikation handeln. Eine solche Abgrenzung ist angesichts der technischen Gegebenheiten der über das Internet ablaufenden Telekommunikation jedoch ohnehin nicht zielführend, da ihr handfeste Abgrenzungskriterien fehlen.[325] So kann die E-Mail tatsächlich als Äquivalent postalischer Fernkommunikation und damit als Individualkommunikation angesehen werden, gleichzeitig bei Verwendung zur Versendung eines Newsletters aber auch der Massenkommunikation zuzuordnen sein.[326] Es würde sich unmittelbar die Frage anschließen, ab welcher Personenanzahl von einem unbestimmten Rezipientenkreis auszugehen wäre. Letztlich findet sich selbst im Falle der Versendung eines Newsletters mittels einer E-Mail ein in sich abgeschlossener Personenkreis als Empfänger der Nachricht wieder. Klarer wird diese Abgrenzung auch nicht durch Heranziehung des Kriteriums eines „Zugangshindernisses". Es bleibt unklar, wie ein solches Zugangshindernis praktisch ausgestaltet sein muss. Ist es lediglich die Eintragung in eine Maillingsliste zum Erhalt eines Newsletters, die aus der Massen- eine Individualkommunikation macht? Muss es sich bei offen einsehbaren Kommentierungen in sozialen Netzwerken, die ersichtlich mit Verzicht auf Vertraulichkeit getätigt wurden, dennoch um Individualkommunikation handeln, da schließlich für diese Netzwerke eine

321 *Gusy* in: v. Mangoldt/Klein/Stark, Art. 10 GG, Rn. 62; *Sankol*, MMR 2006, 361, 364.
322 *Gusy* in: v. Mangoldt/Klein/Stark, Art. 10 GG, Rn. 62.
323 *Sievers*, Der Schutz der Kommunikation im Internet, S. 129, m.w.N.
324 *Hermes* in: Dreier-GG, Art. 10 GG, Rn. 39.
325 *Guckelberger* in: SHH, Art. 10 GG, Rn. 23.
326 *Greve*, Acces-Blocking, S. 293.

Registrierung erforderlich ist und mithin ein Zugangshindernis besteht? Aus praktischen Gesichtspunkten schon gar nicht durchsetzbar ist diese Abgrenzung nicht zuletzt deswegen, da die zur Abgrenzung benötigten Informationen gewonnen werden müssten, ohne den Inhalt der übermittelten Nachricht einzusehen.[327] Hinzu kommt, dass selbst der Abruf frei zugänglicher Internetseiten die Herstellung einer individuellen Verbindung verursacht.[328]

In die gleiche Kerbe schlägt das BVerfG, wenn es auf diese Differenzierung verzichtet und vielmehr eine den konkreten Einzelfall betrachtende Sichtweise anlegt, die für entscheidend hält, ob die Kommunizierenden die ablaufende Kommunikation vertraulich wissen wollten.[329] Es ist festzuhalten, dass wenngleich es sich bei der Nutzung eines Sprachassistenten keineswegs um Massenkommunikation handelt, die dessen Nutzung aus dem Schutzbereich des Art. 10 GG herausnehmen würde, diese Abgrenzung bei den vielfältigen Kommunikationsmöglichkeiten über das Internet nur schwerlich anzuwenden ist.

(4) Teilnehmer an einem Kommunikationsvorgang

Fraglich ist, ob für einen Telekommunikationsvorgang im Sinne des Art. 10 GG hieran mindestens zwei Personen beteiligt sein müssen.

(4.1) Entwicklung der Rechtsprechung

Zwar hat sich das BVerfG in seiner Rechtsprechung zu Art. 10 GG noch nicht ausdrücklich hinsichtlich der Frage, ob es für die Schutzbereichseröffnung mindestens zweier Personen bedarf, geäußert. Aus diversen Entscheidungen, die im Nachfolgenden genauer betrachtet werden sollen, lassen sich jedoch Anknüpfungspunkte und Tendenzen erkennen.

327 *Sievers*, Der Schutz der Kommunikation im Internet, S. 130.
328 *Sievers*, Der Schutz der Kommunikation im Internet, S. 130.
329 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13 -, Rn. 37 = teilweise in NJW 2016, 3508 ff.

(4.1.1) Auslesen eines Endgerätespeichers

In einer Entscheidung, das Auslesen einer SIM-Karte betreffend, hat das BVerfG entschieden, dass auch die auf einer SIM-Karte des eigenen Handys gespeicherten Informationen dem Schutzbereich des Art. 10 GG zuzuordnen sind.[330] Einleitend betonte das Bundesverfassungsgericht, dass das Grundrecht aus Art. 10 GG neuen technischen Entwicklungen gegenüber offen sei und sich auf sämtliche Übermittlungen beziehe, die unter Zuhilfenahme der verfügbaren Telekommunikationstechniken vonstattengehen.[331] Gleichwohl finden sich in der Entscheidung Passagen, die auf die Beteiligung zweier miteinander Kommunizierender Personen schließen lassen: "[…] *wenn diese wegen der räumlichen Distanz zwischen den Beteiligten* […]"[332] oder „*die Kommunizierenden müssen sich auf die technischen Besonderheiten eines Kommunikationsmediums einlassen und sich dem eingeschalteten Kommunikationsmittler anvertrauen* […]"[333]. Neben dem Erfordernis eines Kommunikationsmittlers scheint das Bundesverfassungsgericht daher auch die Notwendigkeit von „Beteiligten" bzw. „Kommunizierenden" für eine Schutzbereichseröffnung für erforderlich zu halten. Relativiert wird die vermeintliche Betonung der personalen Komponente jedoch durch die Formulierung, dass der Schutz durch Art. 10 GG gerade einen Ausgleich für die technikbedingt notwendigerweise in Kauf genommene Einbuße an Privatheit schaffe, um den Gefahren zu begegnen, die sich gerade aus dem technischen Übermittlungsvorgang ergeben.[334] Darüber hinaus knüpfe das Fernmeldegeheimnis an das verwendete Kommunikationsmedium an.[335] Daraus könnte zu schließen sein, dass es der Intention des Bundesverfassungsgerichts entspricht, unabhängig von der Anzahl der konkret am Telekommunikationsvorgang beteiligten Personen, die Gefahr abzuwenden, die sich speziell aufgrund der Einschaltung eines Nachrichtenmittlers ergibt.[336]

330 BverfGE 115, 166.
331 BverfGE 115, 166, 182 f.
332 BverfGE 115, 166, 182.
333 BverfGE 115, 166, 184.
334 BverfGE 115, 166, 184; BVerfG, NJW 2007, 351, 353.
335 BverfGE 100, 313, 363; BverfGE 115, 166, 184.
336 *Kleih*, Die strafprozessuale Überwachung der Telekommunikation, S. 113.

(4.1.2) IMSI-Catcher Beschluss

In der genannten Entscheidung befasste sich das Bundesverfassungsgericht mit der Frage, ob die durch einen IMSI-Catcher erlangten Daten dem Schutzbereich des Art. 10 GG unterfallen. In technischer Hinsicht ist es allen Mobiltelefonen immanent, dass sich diese, sofern sie sich im empfangsbereiten Zustand befinden, in kurzen Abständen immer wieder in die für sie zuständige Basisstation des Mobilfunknetzwerkes einwählen. Diesen Umstand können sich gem. § 100i StPO die Strafverfolgungsbehörden durch den Einsatz eines IMSI-Catchers zu Nutze machen. Durch dessen Einsatz wird ein solches Mobilfunknetzwerk simuliert, in welches sich alle Mobiltelefone in einem gewissen Umkreis aufgrund des von dem Netzwerk ausgehenden Signals einwählen.[337] Indem nun sämtliche eingeschalteten Mobiletelefone ihre Daten an dieses simulierte Netzwerk senden, kann die auf der SIM-Karte gespeicherte International Mobile Subscriber Identity (IMSI) ausgelesen und der Standort eines Mobiltelefons innerhalb einer Funkzelle näher bestimmt werden.[338] Die Beschwerdeführer brachten dabei vor, dass das Telekommunikationsgeheimnis nicht nur den Inhalt einer Kommunikation, sondern darüber hinaus auch alle weiteren Umstände, wie Gerätenummer oder Standortdaten, die mit einer solchen Kommunikation in Zusammenhang stünden, schütze.[339] Dieser Sichtweise ist das BVerfG entgegengetreten. Art. 10 GG schütze gerade die individuelle Kommunikation zwischen den Beteiligten in den Fällen, in denen aufgrund der räumlichen Distanz eine Übermittlung durch Dritte erforderlich ist.[340] Beim Einsatz eines IMSI-Catchers fehle es jedoch an diesen Voraussetzungen, da in dieser Situation ausschließlich technische Geräte miteinander kommunizieren. Es fehle folglich an einem menschlich veranlassten Kommunikationsvorgang.[341] Der Umstand, dass Mobiltelefone Daten aussenden, die sich die Strafverfolgungsbehörden im vorliegenden Fall zu Nutze machten, erfolgte unabhängig von einem konkreten Kom-

337 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 13 f. = teilweise in NJW 2007, 351 ff.
338 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 14 = teilweise in NJW 2007, 351 ff.
339 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 23 = teilweise in NJW 2007, 351 ff.
340 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 51 = teilweise in NJW 2007, 351 ff.
341 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 57 = teilweise in NJW 2007, 351 ff.

munikationsvorgang. Da erst die tatsächliche Nutzung eines Mobiltelefons zum Informationsaustausch die übertragenen Daten als Kommunikationsinhalt qualifiziere, hat das BVerfG entschieden, dass der reine technische Datenaustausch zwischen Mobilfunkendgeräten nicht dem Schutzbereich des Art. 10 GG unterfallen.[342]

Vergleicht man diese Fallgestaltung mit der Nutzung eines Smart Speakers, ist zu erkennen, dass durch die Übermittlung, der durch das Gerät vor Ort aufgenommenen Audiodatei an den Sprachassistenten letztlich auch ein bloßer Austausch von Datenpaketen stattfindet. Jedoch ist für die Eröffnung des Schutzbereiches zu beachten, dass der Betroffene bei der Nutzung eines Sprachassistenten ebenso wie bei einem Telefonat, der Versendung einer E-Mail oder der Beteiligung an einem Chat aktiv Informationen aus seiner Privatsphäre offenbart, sodass auch hier ein besonderes Gefährdungspotenzial für die Privatheit dieser durch Telemedien übermittelten Informationen besteht. Dennoch lassen sich diesem Urteil des BVerfG jedenfalls Tendenzen erkennen, die einen zwischenmenschlichen Bezug in Form einer Beteiligung von mindestens zwei Menschen für den Schutz durch das Telekommunikationsgeheimnis fordern.[343] Denn das Gericht spricht im Zusammenhang mit der Eröffnung des Schutzbereiches von der *„räumlichen Distanz zwischen den Beteiligten"*[344] und einer individuellen Kommunikation und einem Kommunikationsvorgang *„zwischen Menschen"*[345]. Der gewählte Plural ließe somit auf das Erfordernis einer Kommunikation zwischen mindestens zwei Menschen schließen.

Allerdings betont das BVerfG gleichfalls, dass für den Schutz durch Art. 10 GG ein menschlich veranlasster Informationsaustausch stattfinden müsse. Bei der Informationsgewinnung durch einen IMSI-Catcher im Falle der gesprächsunabhängigen Erhebung von Standortdaten im „standby"-Modus eines Mobiltelefons, fehlt es jedoch gerade an einem solchen Austausch, der individuelle Züge aufweist.[346] Für die hier zu klärende Frage bedeutet dies jedoch, dass aus dem Beschluss folglich nicht eindeutig gefolgert werden, dass die Eröffnung des Schutzbereiches des Art. 10 GG

342 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 57 = teilweise in NJW 2007, 351 ff.

343 So *Grözinger*, Die Überwachung von Cloud-Storage, S. 79 f.

344 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 51.

345 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 57.

346 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 57; *Krüger*, ZJS 2012, 606, 610; *Harnisch/Pohlmann*, HRRS 2009, 202, 211 f.; a.A.: *Nachbaur*, NJW 2007, 335, 337; *Roggan*, KritV 2003, 76, 89 f.; *Schenke*, AöR 2000, 1, 20; *Wolter* in: SK-StPO, § 100i StPO Rn. 12.

gerade an der fehlenden Beteiligung zweier menschlicher Personen scheiterte. Ginge man davon aus, dass das Bundesverfassungsgericht die Schutzbereichseröffnung allein aufgrund des nicht menschlich veranlassten Informationsaustausches ablehnte, so erscheint es auch unter Berücksichtigung dieses Beschlusses möglich, die Nutzung eines Sprachassistenten unter den Schutz des Art. 10 GG zu fassen. Denn die Datenübertragung und damit auch die Informationsvermittlung bei der Nutzung eines Sprachassistenten ist gerade menschlich veranlasst. Ferner ist sie auch hinreichend individualisiert, da ein konkreter Betroffener Informationen preisgibt. In Anbetracht des Schutzzweckes des Art. 10 GG, der gerade dem Schutz vor der Gefahr eines Zugriffs durch staatliche Stellen auf räumlich distanzierte Nachrichtenübermittlung und der damit einhergehenden Einbuße an Privatsphäre dient,[347] könnte zu schließen sein, dass die durch eine Person veranlasste Übertragung von Daten zum Sprachassistenten durch Art. 10 GG geschützt ist. Ob das BVerfG die Kommunikation zwischen zwei Personen als zwingend erforderlich für die Gewährung des Schutzes aus Art. 10 GG erachtet, kann aus der vorliegenden Entscheidung jedenfalls nicht abschließend gefolgert werden.

(4.1.3) Surfen im Internet-Beschluss

Für eine Bestimmung der Telekommunikation i.S.d. Art. 10 GG ist darüber hinaus die oben bereits angeführte Entscheidung des BVerfG zum „Surfen im Internet" von Interesse. Die Entscheidung geht auf einen Beschluss des LG Ellwangen zurück, wonach die Überwachung der Websitennutzung durch § 100a StPO erfolgen könne. Das Landgericht stellte fest, dass es sich beim Surfen im Internet um Telekommunikation i.S.d. § 100a StPO handelt.[348] Während die Entscheidung des LG Ellwangen zunächst zur Vergleichbarkeit der Situation mit der bei der Nutzung eines Sprachassistenten im Rahmen einer technikorientierten Auslegung des Telekommunikationsbegriffes des § 100a StPO bemüht wurde, soll sie hier primär zur weiteren Klärung der Ausformung des Schutzbereichs aus Art. 10 GG herangezogen werden. Die Beschwerdeführer rügten in ihrer Beschwerdebegründung, dass das LG Ellwangen, indem es einer technikorientierten Auslegung des Telekommunikationsbegriffes gefolgt ist, verkannt habe, dass sich die Auslegung des § 100a StPO an Art. 10 GG

347 *Durner* in: Maunz/Dürig-GG, Art. 10 GG, Rn. 69.
348 LG Ellwangen, Beschl. V. 28.05.2013, Az.: 1 Qs 130/12.

orientiere müsse.[349] Für die Eröffnung des Schutzbereichs des Art. 10 GG sei nach dem Verständnis der Beschwerdeführer entscheidend, dass ein Informationsaustausch zwischen Menschen stattfinde. Bei der Informationsabfrage über das Internet finde allerdings ein bloßer Datenaustausch mit dem Netzwerk, jedoch keine zwischenmenschliche Kommunikation statt.[350] Der gesamte Vorgang der Informationsbeschaffung sei ein einseitiger Vorgang des Benutzers und daher Art. 10 GG nicht einschlägig, womit folglich auch keine Telekommunikation i.S.d. § 100a StPO vorliegen könne.[351] Ohne an dieser Stelle bereits den vielfach gezogenen Schluss von Schutzumfang auf Eingriffsermächtigung näher zu thematisieren, kann die im Anschluss an das LG Ellwangen vom BVerfG überprüfte Entscheidung dahingehend beleuchtet werden, ob das BVerfG „Surfen im Internet", der Argumentation der Beschwerdeführer folgend, unter Art. 10 GG fassen würde. Zunächst legte das Gericht unter strenger Beachtung des eigenen Prüfungsmaßstabs dar, dass die Auslegung und Anwendung strafprozessualer Normen, sofern in der fachgerichtlichen Entscheidung keine Willkür liegt oder spezifisches Verfassungsrecht verletzt wird, nicht Aufgabe des Bundesverfassungsgerichts sei.[352] Demzufolge sei die Auffassung des LG Ellwangen einem technikorientierten Telekommunikationsbegriff zu folgen nicht zu beanstanden.[353] Gleichwohl unternahm das Gericht Ausführungen zu der Frage, inwiefern das Surfen im Internet dem Schutzbereiches des Art. 10 GG unterfallen könne. Entscheidend für eine Eröffnung des Schutzbereiches streitet nach den Ausführungen des Bundesverfassungsgerichts, dass der Betroffene die Internetnutzung in dem Glauben an deren Vertraulichkeit vornahm.[354] Zudem findet im Gegensatz zum Einsatz eines IMSI-Catchers gerade nicht lediglich ein bloßer Datenaustausch statt, sondern es liegt ein konkretes Gefährdungspotential für die

349 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 16 = teilweise in NJW 2016, 3508 ff.
350 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 17 = teilweise in NJW 2016, 3508 ff.
351 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 10 = teilweise in NJW 2016, 3508 ff.
352 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 24 = teilweise in NJW 2016, 3508 ff.
353 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 24 = teilweise in NJW 2016, 3508 ff.
354 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 37 = teilweise in NJW 2016, 3508 ff.

Vertraulichkeit der Kommunikation vor.[355] Eben auf dieses Gefährdungspotential rekurrierte das Bundesverfassungsgericht bereits im Rahmen der – auch im Laufe dieser Arbeit noch relevant werdende – Entscheidung zur Beschlagnahme von E-Mails. Bereits in der damaligen Entscheidung war die spezifische Gefährdungslage aufgrund eines technisch bedingten Mangels an Beherrschbarkeit des gewählten Übermittlungsvorgangs das entscheidendes Kriterium für die Schutzbereichseröffnung des Art. 10 Abs. 1 Var. 3 GG.[356] Daher kann der Aspekt, ob der Nutzer die Daten beherrschen und ausreichende Schutzvorkehrungen treffen kann, als ein zentrales Kriterium bezüglich der Frage, ob eine telekommunikationsspezifische Gefährdungslage vorliegt, herangezogen werden.[357] Überhaupt knüpfe der Schutz durch das Telekommunikationsgeheimnis nicht an die Beteiligten einer Kommunikation, sondern an den Übermittlungsvorgang als solchen und das dabei genutzt Medium an.[358] Zuletzt stelle ein Informationsabruf im Internet auch eine körperlose Informationsübermittlung an einen individuellen Rezipienten dar.[359] Entscheidend ist allein die Individualität des Empfängers, der keinen unüberschaubaren Adressatenkreis darstellen darf.[360]

Insofern verhält sich die Entscheidung zwar auch nicht ausdrücklich zur Frage ob an einem Kommunikationsvorgang zwei Menschen beteiligt sein müssen. Sie gibt allerdings ein starkes Indiz, dass dies – sofern eine grundrechtstypische Gefährdungssituation besteht – von untergeordneter Bedeutung ist. Ferner klingt in der Entscheidung an, dass es im Lichte des Art. 10 GG nicht eines menschlichen Kommunikationspartner bedarf, solange eine Informationsabfrage auf Veranlassung des Betroffenen geschieht und dieser als Empfänger der Abfrage individualisierbar ist. Der Frage, ob ein Verhalten Telekommunikation i.S.d. Art. 10 GG darstellt, legt das BVerfG daher weniger ein personales Verständnis, sondern vielmehr ein durch Sinn und Zweck der Grundrechte als bürgerschützendes Recht geleitetes formal technisches Verständnis zu Grunde.

---

355 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 38 = teilweise in NJW 2016, 3508 ff.

356 BverfGE 124, 43, 55.

357 *Brodowski/Eisenmenger*, ZD 2014, 119, 121; *Schwabenbauer*, AöR 2012, 1, 34; *Martini* in: v. Münch/Kunig, Art. 10 GG, Rn. 76.

358 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 36 = teilweise in NJW 2016, 3508 ff.

359 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 38 = teilweise in NJW 2016, 3508 ff.

360 BverfGE 115, 166, 182; *Durner* in: Maunz/Dürig-GG, Art. 10 GG, Rn. 70.

(4.1.4) Zwischenergebnis

Die höchstrichterliche Rechtsprechung des Bundesverfassungsgerichts zeigt, dass für die Eröffnung des sachlichen Schutzbereiches nicht zwingend ein zwischenmenschlicher Informationsaustausch erforderlich ist. Vielmehr genügt es, wenn zur Nachrichtenübermittlung ein während der Übertragungsphase nicht beherrschbares Medium benutzt wird. Eine Einschränkung dahingehend, dass zwei natürliche Personen handeln müssen, ist Art. 10 GG auch im Übrigen fremd, sodass es für die Gewährleistung des Schutzgehalts gleich ist, ob eine Information lediglich an einen Server oder einen Menschen übermittelt wird. Maßgeblich ist vielmehr, dass der Vorgang auf Veranlassung des Betroffenen geschieht und dieser dabei der typischen Gefährdungslage, die mit der Nutzung eines technischen Kommunikationsmediums einhergehen, ausgesetzt ist. Dem folgend ist auch der Nutzer eines Sprachassistenten einer für Art. 10 GG typischen Gefährdungssituation ausgesetzt. Im Zuge der über die Server des Sprachassistenten durchgeführten Informationsabfrage besteht die Gefahr, dass Dritte auf diese Daten zugreifen. Diese Einschaltung des Servers in die Informationsabfrage führt dazu, dass sich die Daten nicht im ausschließlichen Herrschaftsbereich des Nutzers befinden und sie daher einem staatlichen Zugriff leichter ausgesetzt sind als eine direkte Kommunikation unter Anwesenden.[361] Ferner erfolgt die Informationsabfrage jedenfalls im klassischen Anwendungsfall auch auf Veranlassung des Nutzers, der den Sprachassistenten über das Codewort aktiviert. Der Entwicklung der Rechtsprechung folgend ist daher anzunehmen, dass diese die Nutzung eines Sprachassistenten unter Art. 10 GG fassen würde.

(4.2) Ansichten in der Literatur

(4.2.1) Multipersonale Strömung

Teilweise werden für die Schutzbereichseröffnung des Art. 10 GG zwingend zwei menschliche Kommunikationspartner gefordert.[362] Die fehlende Beteiligung einer zweiten Person bei der Nutzung eines Sprachassis-

361 Vgl. BverfGE 124, 43, 55.

362 *Grözinger*, Die Überwachung von Cloud-Storage, S. 98; *Soiné*, MMR 2015, 22, 23; *Martini* in: v. Münch/Kunig, Art. 10 GG, Rn. 73.

tenten würde diesen Vorgang hiernach nicht in den Schutzbereich der Telekommunikationsfreiheit fallen lassen.

(4.2.2) Differenzierende Ansicht

Eine differenzierende Strömung will bereits bei der Frage der Schutzbereichseröffnung des Art. 10 GG an ein materielles Kommunikationsverständnis anknüpfen.[363] Hinsichtlich der Internetnutzung sei bereits bei der Frage der Schutzbereichseröffnung des Art. 10 GG zwischen einer „kommunikativen" und einer „nicht kommunikativen" Internetnutzung zu unterscheiden.[364] Der Schutzbereich solle nur Kommunikationsdienste des Internets, wie E-Mail, Messenger-Systeme oder der Internet-Telefonie einbeziehen, während die nicht-kommunikative Nutzung des Internets, wie etwa der Besuch bestimmter Web-Seiten zur einseitigen Informationserlangung, nicht dem Schutzbereich unterfallen solle. In diesen Fällen soll vielmehr der Schutzbereich der informationellen Selbstbestimmung eröffnet sein.[365] Will man den Telekommunikationsbegriff in § 100a StPO analog zum verfassungsrechtlichen Telekommunikationsbegriff verstehen, so wäre aufgrund der dargestellten Vergleichbarkeit der Fälle des Surfens im Internet und der Nutzung eines Sprachassistenten zur Informationserlangung nach Ansicht von *Braun* und *Eschelbach* bereits der Schutzbereich des Art. 10 GG nicht eröffnet.[366] Analog hierzu bestünde dann auch keine Telekommunikation i.S.d. § 100a StPO.

(4.2.3) Unipersonale Strömung

Die wohl herrschende Ansicht innerhalb dieser Strömung erachtet es für die Schutzbereichseröffnung für ausreichend, wenn eine Person am Kom-

---

363 Insofern sind die Ausführungen durchaus vergleichbar mit einem materiellen Telekommunikationsverständnis im Rahmen des § 100a StPO, jedoch nimmt die hier angeführte Auffassung diese materiellen Einschränkungen nicht erst bei der Eingriffsermächtigung, sondern bereits auf Verfassungsebene im Rahmen des Grundrechts vor.

364 *Braun*, jurisPR-ITR 18/2013 Anm. 5; *ders*. HRRS 2013, 500, 503, *Eschelbach* in: SSW-StPO, § 100a StPO, Rn. 5.

365 *Braun*, jurisPR-ITR 18/2013 Anm. 5.

366 Vgl. *Braun*, jurisPR-ITR 18/2013 Anm. 5; *ders*. HRRS 2013, 500, 503, *Eschelbach* in: SSW-StPO, § 100a StPO, Rn. 5.

munikationsvorgang beteiligt ist. Nur so könne der bestehenden grundrechtstypischen Gefährdungslage Rechnung getragen werden, die eben auch in diesen Situationen bestehe. Daher wäre es mit dem anerkannten Grundsatz nicht in Einklang zu bringen einem unipersonal stattfindenden Vorgang den Schutz durch Art. 10 GG zu verwehren.[367] Demnach käme diese Ansicht für die Nutzung eines Sprachassistenten zur Eröffnung des Schutzbereichs aus Art. 10 GG.

(4.3) Stellungnahme

Nur durch ein formal technisches Schutzbereichsverständnis, das sich von einer strikt personalen Betrachtung des Fernmeldegeheimnisses löst und damit einhergehend einen weiten Schutzbereich garantiert, kann der Sinn und Zweck der Grundrechte in Gänze erfüllt werden. Unter Beachtung dessen, dass die technologische Entwicklung im heutigen Zeitalter eben die Nachrichtenübermittlung zwischen Menschen und Maschine ermöglicht, streitet hierfür auch die vielfach zitierte Entwicklungsoffenheit der Grundrechte.[368] Um diesem Grundsatz nachkommen zu können, muss gerade ein weites Schutzbereichsverständnis angelegt werden. Andernfalls würde in Anbetracht der Dynamisierung der verschiedensten Arten von Kommunikation, Informationsbeschaffung oder Übertragungstechniken kein hinreichender Grundrechtsschutz bestehen. Daher darf es für die Eröffnung des Schutzbereiches nicht von Belang sein, ob ein oder zwei Personen an einem Telekommunikationsvorgang beteiligt sind. Auch derjenige der eine Kommunikation mit einer technischen Maschine führt und so Informationen erhält oder die Ausführung einer Aktion befiehlt, übermittelt eine „Nachricht" mittels der Fernmeldetechnik. Entscheidend ist stets, ob sich der Nutzer durch die Verwendung der Telekommunikationstechnik in die Gefahr begibt, dass auf seine übermittelten Informationen leichter zugegriffen werden könnte.[369] In Anbetracht dessen, dass der Nutzer bei Verwendung eines Sprachassistenten zudem gerade davon ausgeht, dass seine Informationen nicht an einen menschlichen Kommunikations-

---

367 *Wolff* in: Hömig/Wolff-GG, Art. 10 GG, Rn. 6; *Brodowski/Eisenmenger,* ZD 2014, 119, 121; *Singelnstein*, NStZ 2012, 593, 595; *Sievers*, Der Schutz der Kommunikation im Internet, S. 106; die Schutzbedürftigkeit des Grundrechtsträger in den Vordergrund stellend auch BverfGE 124, 43, 56; BVerfG, NJW 2007, 351, 354.

368 Hierzu nur BVerfG, Urt. v. 02.03.2006, 2 BvR 2099/04; *Durner* in: Maunz/Dürig-GG, Art. 10 GG, Rn. 64.

369 BverfGE 124, 43, 55.

partner gelangen, sondern lediglich von einem technischen System beantwortet oder ausgeführt werden, steigt im Wege eines Erst-Recht-Schlusses die Vertraulichkeit dieser übermittelten Informationen. Der Schutz dieses Sachverhalts durch Art. 10 GG muss daher erst recht bestehen. Für das Erfordernis zweier Personen zur Schutzbereichseröffnung bringt vor allem *Grözinger* vor, dass in den Fällen einer nur einseitigen Telemediennutzung ein Schutz durch das IT-Grundrecht näher liege, da ein solch „einseitiger Vorgang" wesensverschieden zu den klassischen Telekommunikationsvorgängen sei.[370] Allerdings trifft *Grözinger* diese Aussage im Zusammenhang mit der Frage, ob das Ablegen von Dateien in Clouds, auf die lediglich der Nutzer selbst Zugriff hat, Kommunikation darstellen kann. Diese Situation ist nicht vergleichbar mit der Nutzung eines Sprachassistenten. Denn bei dessen Nutzung steht der kommunikative Aspekt deutlich mehr im Vordergrund. So wäre es beispielsweise für eine Dritte Person, die sich außerhalb eines Raumes aufhält, nicht sofort erkennbar, ob der Nutzer eines Sprachassistenten bloß mit einer Maschine oder einem Menschen spricht. Auch ansonsten ist die lediglich einseitige Nutzung einer Fernmeldetechnik nicht vom Schutzumfang des Art. 10 GG ausgeschlossen. Dem widerspricht auch nicht, dass das BVerfG in seiner alten Definition den Schutzbereich des Art. 10 GG derart verstand, dass hierunter der Austausch von Nachrichten, Meinungen oder Gedanken fiel. Aus dieser Definition ist keineswegs zu folgern, dass ein Austausch denklogisch nur zwischen zwei Personen möglich sei, weshalb eben auch zwei Personen für einen Kommunikationsvorgang vorhanden sein müssten.[371] Gerade das Beispiel eines Sprachassistenten zeigt, dass Nachrichten auch zwischen einer Person und einem technischen System ausgetauscht werden können. Denn der Sprachassistent reagiert jeweils individuell auf die Aussage des Nutzers, sodass dadurch durchaus ein Austausch von Nachrichten stattfindet. Ob der Nutzer eine reale Person oder einen virtuellen Assistenten zu einem bestimmten Sachverhalt befragt, hat auf das Vorliegen eines Austausches von Informationen keinen Einfluss. In die gleiche Richtung verlief bereits die Argumentation des BVerfG als dieses klarstellte, dass auch bei der Internetnutzung durch eine natürliche Person nicht ausschließlich technische Geräte miteinander kommunizieren und daher gerade nicht wie beim Einsatz „IMSI-Catchers" – lediglich ein Datenaustausch zur Sicherung

370 *Grözinger*, Die Überwachung von Cloud-Storage, S. 97.
371 So aber *Grözinger*, Die Überwachung von Cloud-Storage, S. 93.

der Betriebsbereitschaft stattfindet.[372] Sofern also auch nach dem Urteil des BVerfG zur Überwachung der Internetnutzung unter Rückgriff auf das Urteil des BVerfG zum Einsatz eines IMSI-Catchers gefolgert wird, dass das BVerfG zwingend zwei Personen für einen Telekommunikationsvorgang im Rahmen des Art. 10 GG für erforderlich halten würde, fußt dies auf einer unvollständigen Auswertung der höchstrichterlichen Rechtsprechung. Mittlerweile wird der Schutzbereich zudem durch das BVerfG dahingehend modifiziert, dass bereits die unkörperliche Informationsübermittlung an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs schützenswert ist.[373] Vom Begriff des klassischen Austausches hat sich auch diese Definition hin zur Übermittlung entwickelt. Jedenfalls eine Übermittlung von Informationen findet aber auch statt wenn ein technisches Gerät einem Menschen Informationen zukommen lässt. Für eine Informationsübermittlung sind daher keine zwei Menschen erforderlich.

Für die differenzierende Auffassung *Brauns* und *Eschelbachs* ergeben sich aus Art. 10 GG keine Anhaltspunkte, um bereits auf der Stufe der Schutzbereichseröffnung zwischen einer kommunikativen und einer nicht kommunikativen Internetnutzung zu unterscheiden. Vielmehr folgt aus dem Wortlaut „Fernmeldegeheimnis", dass sobald sich eine Person der Fernmeldetechnik bedient, der hierdurch übermittelte Inhalt „geheim" bleiben soll und daher durch Art. 10 GG geschützt ist, gleich ob es sich dabei um eine kommunikative oder nicht-kommunikative Internetnutzung handelt. Um den Wortlaut aus Art. 10 GG[374] jedoch nicht überzustrapazieren, kann der bloße Datenaustausch zwischen Maschinen, der gerade nicht menschlich veranlasst wurde, nicht unter den Schutz des Art. 10 GG fallen.[375] Dies würde den gesetzgeberischen Willen, mit Grundrechten stets die menschlich veranlasste Kommunikation zu schützen, missachten.

372 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13 -, Rn. 38 = teilweise in NJW 2016, 3508 ff.

373 BVerfGE 115, 166, 182; BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 33 = teilweise in NJW 2016, 3508 ff.

374 Dieser spricht streng genommen nur vom sog. Fernmeldegeheimnis. Allerdings ist zu Recht allgemein anerkannt, dass hierunter auch das Telekommunikationsgeheimnis fällt, vgl. nur BVerfG, NJW 2002, 3619, 3620. Auch in der Literatur ist umfassend nicht mehr von dem Fernmeldegeheimnis, sondern dem Telekommunikationsgeheimnis die Rede, vgl. m.w.N *Ogorek* in: BeckOK-GG, Art. 10 GG, Rn. 35.

375 A.A. wohl *Gähler*, HRRS 2016, 340, 343.

Vielmehr würde dann ein bloßes, dem Informationsaustausch dienliches maschinelles System geschützt.[376]

Zuletzt wird in der Literatur vorgebracht, dass sich die Entwicklungsoffenheit der Grundrechte lediglich auf die neuartigen technischen Formen der Übertragung beziehe, nicht aber auf die Frage, was Kommunikation im Sinne des Kommunikationsgeheimnisses darstellt.[377] Eine solche isolierte Betrachtung kann jedoch nicht trennscharf vorgenommen werden. Dies zeigt sich bereits am Beispiel der Mailbox oder des E-Mail-Verkehrs, deren Nutzung unter das Telekommunikationsgeheimnis fällt[378].[379] Mit der technischen Schaffung der Möglichkeit eine Nachricht zu speichern und später abzurufen, entstand eine neue technische Form der Nachrichtenübertragung, die aufgrund der Entwicklungsoffenheit des Grundrechts in den Schutzbereich fällt. Gleichsam entwickelte sich dadurch aber auch das Kommunikationsverständnis als solches weiter. Unter Kommunikation fällt nicht mehr nur der unmittelbare Austausch von Informationen wie in einem Telefongespräch, sondern auch die Speicherung und der zeitlich verzögerte Abruf einer Nachricht.[380] Insbesondere entschied das BVerfG in der Entscheidung hinsichtlich der Speicherung von E-Mails, dass der E-Mail-Verkehr gerade auch deswegen unter den Schutz des Art. 10 GG fallen, da der Nutzer während die E-Mail beim Provider gespeichert ist, keine Möglichkeit hat, diese gegen unbefugten Zugriff durch den Staat oder den Provider selbst zu schützen.[381] Aus diesem Mangel an Beherrschbarkeit folgt wiederum die grundrechtstypische Gefährdungssituation, die eine besondere Schutzbedürftigkeit durch das Fernmeldegeheimnis erfordere.[382] Um einen hinreichenden Schutz in dieser Gefährdungssituation auch in neu entstehenden Fällen – wie dem der Nutzung eines Sprachassistenten zu gewährleisten – ist es daher erforderlich, auch den verfassungsrechtlichen Kommunikationsbegriff als solchen ebenso wie die Frage nach technischen Formen der Nachrichtenübermittlung im Wandel

376 So bzgl. der Nichteröffnung des Schutzbereichs aus Art. 10 GG hinsichtlich solcher Vorgänge ohne menschliche Beteiligung auch *Grözinger*, Die Überwachung von Cloud-Storage, S. 93.
377 *Grözinge*r, Die Überwachung von Cloud-Storage, S. 94.
378 *Durner* in: Maunz/Dürig-GG, Art. 10, Rn. 107.
379 Hinsichtlich der E-Mail-Nutzung fällt jedenfalls der Abschnitt solange die E-Mail auf dem Server des Providers gespeichert und noch nicht abgerufen wurde unter den Schutz des Art. 10 GG.
380 BVerfGE 124, 43, 55.
381 BVerfGE 124, 43, 55.
382 BVerfGE 124, 43, 55.

der Zeit entwicklungsoffen zu betrachten. Nur dadurch kann der Schutzgehalt aus Art. 10 GG vollumfänglich gewahrt werden.

(5) Zwischenergebnis

Kommunikation im Sinne von Art. 10 GG setzt somit keine Beteiligung zweier Personen voraus. Die Nutzung eines Sprachassistenten fällt demnach unter den Schutzbereich des Art. 10 GG. Sofern der Telekommunikationsbegriff aus § 100a StPO analog zu Art. 10 GG ausgelegt werden soll, handelt es sich daher bei der Sprachassistentennutzung um Telekommunikation i.S.d. § 100a StPO.

dd) Strafprozessualer Telekommunikationsbegriff

Den verschiedenen Ausgestaltungen eines strafprozessualen Telekommunikationsbegriffs folgend, stellt sich ebenfalls die Frage, inwiefern während des Übertragungsweges zum Server von Kommunikation gesprochen werden kann. Sofern eine soziale Interaktion gefordert wird, könnte diese im hiesigen Beispiel lediglich mit dem Server erfolgen. Dies erscheint jedoch befremdlich. Soziale Interaktion beinhaltet bereits nach dem allgemeinen Wortsinn eine bewusst ablaufende zwischenmenschliche Interaktion. Daher kann dem Telekommunikationsbegriffsverständnis *Hiéramentes* folgend, bei der Nutzung eines Sprachassistenten während der Übertragung nicht von Telekommunikation i.S.d. § 100a StPO gesprochen werden. Dieses Ergebnis untermauern auch die Ausführungen *Hiéramentes*, der das Surfen oder Googeln im Internet zur Informationsgewinnung eher einem Selbstgespräch- oder Tagebucheintrag zuordnen will, hierin aber jedenfalls keine Kommunikation i.S.d. § 100a StPO sieht.[383] Die Konstellation der Nutzung eines Sprachassistenten ist mit dem bloßen Surfen im Internet durchaus vergleichbar. In beiden Konstellationen erhofft sich der Nutzer Antworten oder Informationen auf Fragen und dergleichen. Auch wer mit *Wicker* einen Mitteilungswillen in den Telekommunikationsbegriff nach § 100a StPO hineinlesen will[384], kommt zu keinem anderen Ergebnis. Im Unterschied zur klassischen Kommunikation bei der welcher sich der Äußernde per E-Mail, Telefonat oder Chat seinem Gegenüber

383 *Hiéramente*, HRRS 2016, 448, 451.
384 *Wicker*, Cloud Computing und staatlicher Strafanspruch, S. 380 f.

mitzuteilen vermag, ist bei der Nutzung eines Sprachassistenten primäres Hauptziel nicht die zwischenmenschliche Kommunikation gepaart mit einem Mitteilungswillen, sondern die bloße Informationsgewinnung. Genau genommen kann daher nicht von einem Mitteilungswillen, sondern (lediglich) von einem Informationswillen gesprochen werden. Es kommt dem Nutzer hier gerade nicht darauf an, dem Server etwas um der Mitteilung willen mitzuteilen, sondern lediglich, um eine korrekte Antwort auf die gestellte Frage zu erhalten.

c) Auf der Cloud des Diensteanbieters

Es bleibt zu klären, ob ein Zugriff über § 100a StPO auch noch möglich ist, wenn sich die Daten auf der Cloud des Dienstleistungsanbieters befinden.

aa) Technischer Kommunikationsbegriff

Aus Sicht des technischen Kommunikationsbegriffes ist festzuhalten, dass die Audioaufzeichnungen nach deren Bearbeitung auf der Cloud des Diensteanbieters ruhen. Ein „Aussenden, Übermitteln, oder Empfangen", liegt wie von § 22 Nr. 3 TKG gefordert nicht mehr vor. Somit würde nach dem rein technischen Telekommunikationsbegriff in diesem Stadium keine Telekommunikation i.S.d. § 100a StPO mehr vorliegen.

bb) Technikorientierter Telekommunikationsbegriff

Anders könnte diese Frage zu beantworten sein, sofern der technikorientierten Auslegung gefolgt werden soll. Bei konsequenter Vorgehensweise und Beachtung des Umstandes, dass diese Sichtweise die rein technikorientierte Sichtweise weiter einschränken soll, kann, wenn schon nach der rein technischen Ansicht in diesem Stadium keine Telekommunikation i.S.d. § 100a StPO mehr vorliegt, nach technikorientierten Telekommunikationsbegriff erst recht keine Telekommunikation vorliegen. Widersprüchlich hierzu ist jedoch die Entscheidung eines Ermittlungsrichters, des dieser Ansicht grundsätzlich zugewandten Bundesgerichtshofs. Der Ermittlungsrichter am BGH entschied, dass auch auf bereits auf einer Mailbox ruhende Nachrichten noch mittels § 100a StPO zugegriffen wer-

den könnte.[385] In einer späteren Entscheidung zur Online-Durchsuchung und dem Zugriff auf die auf einem Computer gespeicherten Daten, stellte der BGH ohne Begründung fest, dass § 100a StPO nicht als Ermächtigungsgrundlage in Frage komme.[386] Auf die frühere Entscheidung des Ermittlungsrichters wurde lediglich derart hingewiesen, dass diese den einmaligen heimlichen Zugriff auf eine passwortgeschützte Mailbox unter Heranziehung des § 100a StPO legitimierte.[387] Aus der Art und Weise der Verweisung lässt sich jedoch schlussfolgern, dass der Bundesgerichtshof diese Entscheidung heute so nicht mehr treffen würde. Schließlich wird in der Begründung der neueren BGH-Entscheidung ausgeführt, dass der damalige Ermittlungsrichter einen ähnlichen Sachverhalt „anders" bewertet habe.[388] Diese Formulierung wird im juristischen Sprachgebrauch in der Regel dann benutzt, wenn auf eine andere abweichende Meinung hingewiesen werden soll. Zudem zitiert der Bundesgerichtshof in seinen Urteilsbegründungen, sofern er seine Zustimmung zu einem früheren Urteil zum Ausdruck bringen will und sich hieran anschließt in der Regel mit Worten „so auch" oder „zuvor bereits".[389] Daher dürfte die Entscheidung des Ermittlungsrichters als einmalige Fehlinterpretation zu werten sein und der Bundesgerichtshof würde in Einklang mit der technikorientierten Auffassung zum Ergebnis kommen, dass die auf den Server des Sprachassistenten gespeicherten und dort ruhenden Informationen keine Telekommunikation i.S.d. § 100a StPO darstellen.

cc) Grundrechtsanaloger Telekommunikationsbegriff

Aus Sicht der grundrechtsanalogen Ansicht ist nicht entscheidend, ob die Daten noch in Bewegung sind oder bereits auf dem Speichermedium ruhen. Ein dynamischer Übermittlungsvorgang ist nicht notwendige Voraussetzung für die Schutzbereichseröffnung, sofern die von der Übermittlung ausgehende grundrechtstypische Gefährdungslage auch bei ruhenden Daten weiter fortbesteht.[390] Eine gegenteilige Schlussfolgerung lässt sich ferner auch nicht aus der Entscheidung zur "Online-Durchsuchung" des

385 BGH, NStZ 1997, 247.
386 BGH, MMR 2007, 237, 239.
387 BGH, MMR 2007, 237, 239.
388 BGH, MMR 2007, 237, 239.
389 Vgl. nur BGH, MMR 2015, 839, 840; BGH, NStZ 2016, 741, 743.
390 BverfGE 124, 43, 55 f.

BVerfG ableiten. Zwar betont das Gericht dort mehrfach, dass Art. 10 Abs. 1 GG die Inhalte und Umstände des "laufenden" Kommunikationsvorgangs umfasse.[391] Dagegen muss im Falle der virtuellen Speicherung einer Audioaufzeichnung berücksichtigt werden, dass die Beendigung eines laufenden Kommunikationsvorgangs nicht ebenso trennscharf bestimmt werden kann, wie dies beispielsweise im Rahmen einer Postsendung oder eines Telefonanrufes möglich ist. Während in den dortigen Fällen der Telekommunikationsvorgang mit dem Verlauten der Nachrichten am Telefonhörer als Endgerät oder mit Übergabe der Postsendung abgeschlossen ist, bleibt bei der virtuellen Speicherung der Audioaufzeichnung das dem Telekommunikationsvorgang immanente Risiko eines vereinfacht durchführbareren Zugriff Dritter weiter fortbestehen. Daher erscheint es folgerichtig, dass das Gericht einem weiteren Kriterium zur Bejahung oder Verneinung der Schutzbereichseröffnung des Art. 10 GG eine wohl noch gewichtigere Bedeutung beimisst. Die nach Abschluss eines Kommunikationsvorgangs vorhandenen Daten werden durch das Gericht nicht primär vom Schutzbereich des Art. 10 GG ausgenommen, weil diese nicht mehr in Bewegung sind, sondern weil diese im Herrschaftsbereich eines Kommunikationsteilnehmers gespeichert sind, der seinerseits auch eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff hätte treffen können.[392] Ausschlaggebend ist daher nicht, ob sich die Daten in einem laufenden Übermittlungsvorgang befinden, sondern vielmehr, ob der Nutzer weiterhin über diese Daten herrscht und er ausreichende Schutzvorkehrungen gegen eine unbefugte Verwendung treffen kann.[393] Daher können Cloud-Speicher auch nicht mit lokalen Speichermedien gleichgesetzt werden.[394] Zutreffend ist diese Sichtweise, da Cloud-Speicher – ähnlich wie E-Mail-Server – durch den Dienstleistungsanbieter fremdbeherrscht sind.[395] Dem Dienstleistungsanbieter sind die Daten zum einen technisch zugänglich und zum anderen kommt ihm die Hoheitsmacht zu, dem Nutzer den Zugriff auf die gespeicherten Daten vollständig vorent-

391 BverfGE 120, 274, 308 ff.; BverfGE 120, 274, 340.
392 BverfGE 120, 274, 308; BverfGE 124, 43, 55 f.
393 So auch *Gähler*, HRRS 2016, 340, 345; *Gersdorf* in: BeckOK-InfoMedienR, Art. 10 GG, Rn. 17 f.; *Brodowski/Eisenmenger*, ZD 2014, 119, 121; *Schwabenbauer*, AöR 2012, 1, 34.
394 Vgl. BverfGE 124, 43, 56.
395 BGH, NJW 2021, 1252, 1254; *Gersdorf* in: BeckOK-InfoMedienR, Art. 10 GG, Rn. 18.

halten zu können.[396] Dadurch wird auch der grundsätzliche Unterschied zur klassischen Online-Durchsuchung deutlich, bei der die Überwachung eines bestimmten Systems, das sich in der Herrschaftssphäre des Betroffenen befindet, im Vordergrund steht. Eine solche Konstellation lag auch der Entscheidung des BVerfG zur Online-Durchsuchung zugrunde, da die Online-Durchsuchung den Zugriff auf ein Zielsystem ermöglichen sollte, das sich in der Herrschaftssphäre des Nutzers befand. Das BVerfG legte seinen Überlegungen zur nicht vorhandenen Einschlägigkeit des Art. 10 GG daher ausschließlich die Situation zugrunde in der sich das Zielgerät im physischen Herrschaftsbereich des Nutzers befand, jedoch gerade nicht die Situation eines räumlich getrennten Cloud-Servers.[397] Auf einen räumlich getrennten Server bezog sich dagegen der Zugriff der Strafverfolgungsbehörden, mit welchem sich das BVerfG in der IMAP-Entscheidung befasste. In dieser Entscheidung hielt das BVerfG fest, dass die Beschlagnahme von E-Mails aus einem E-Mail-Postfach, auf das der Nutzer nur über eine Internetverbindung zugreifen kann, an Art. 10 GG zu messen ist.[398] Die beschlagnahmten Daten befinden sich hier gerade nicht im Herrschaftsbereich des Nutzers, sondern ruhen fremdbeherrscht auf den Servern des Dienstleistungsanbieters.[399] Insofern stehen die Entscheidungen des BVerfG zur Online-Durchsuchung und zur E-Mail Beschlagnahme hinsichtlich Art. 10 GG auch nicht in Widerspruch, sondern verdeutlichen vielmehr, dass die vorhandene Herrschaftsmacht des Nutzers über die Daten das entscheidende Kriterium für die Einschlägigkeit des Art. 10 GG darstellt. Folgerichtig ist der Schutzbereich des Art. 10 GG nur im Fall der E-Mail Beschlagnahme von einem fremden Server, nicht aber im Falle der Online-Durchsuchung eines physischen Endgeräts im Sinne eines lokalen Speichermediums eröffnet.

Folgt man innerhalb dieser Strömung der zutreffenden Ansicht, dass für die Schutzbereichseröffnung eine Person ausreichend ist, so unterfällt der Cloud-Speicher auch dann dem Schutzbereich des Art. 10 GG[400], wenn die Daten bereits auf dem Server des Sprachassistenten ruhen. Hinsichtlich

396 *Gersdorf* in: BeckOK-InfoMedienR, Art. 10 GG, Rn. 18; *Herrmann/Soiné*, NJW 2011, 2922, 2923; *Wicker*, DSRITB 2013, 981, 988.

397 So auch *Brodowski/Eisenmenger*, ZD 2014, 119, 121; *Gähler*, HRRS 2016, 340 346.

398 BverfGE 124, 43, 55 f. Dieser Maßstab gilt unabhängig davon, ob der Zugriff auf E-Mails im Rahmen des § 100a StPO oder im Rahmen anderer Ermächtigungsgrundlagen, wie beispielsweise § 94 StPO erfolgt, vgl. BverfGE 124, 43, 58 f.

399 BverfGE 124, 43, 55 f.

400 *Brodowski/Eisenmenger*, ZD 2014, 119, 121; *Gaede*, StV 2009, 96, 97.

§ 100a StPO würde dies bedeuten, dass sofern neben dem Merkmal der Telekommunikation auch die weiteren Voraussetzungen vorliegen, mittels dieser Norm auf die gespeicherten Daten zugegriffen werden könnte.[401]

dd) Strafprozessualer Telekommunikationsbegriff

Nach dem genuin strafprozessual bestimmten Telekommunikationsbegriff liegt bei einem Zugriff auf den Server keine Telekommunikation mehr vor. Weder findet in diesem Stadium eine soziale Interaktion statt, noch liegt bei Zugrundelegung dessen, dass die Dienstleister alte Sprachnachrichten abspeichern, um die Qualität der Spracherkennung zu erhöhen, ein Mitteilungswillen des Nutzers vor.

d) Zwischenergebnis

Vor der internetbasierten Übertragung der Audioaufzeichnungen zum Sprachassistenten scheidet ein Zugriff unter Heranziehung des § 100a StPO nach allen Ansichten aus. Hinsichtlich des Stadiums während des Übermittlungsvorgangs an die Server des Sprachassistenten bleibt festzuhalten, dass sowohl die rein technische Strömung als auch die lediglich technikorientierte Auffassung das Vorliegen eines Telekommunikationsvorgangs bejahen. Im Lager der grundrechtsanalogen Auffassung, die den Telekommunikationsbegriff in § 100a StPO grundrechtsanalog zu Art. 10 GG auslegen will, kommen die unipersonale sowie die differenzierende Auffassung aufgrund einer restriktiven Schutzbereichsauffassung

401 So vgl. BGH, NJW 2021, 1252, 1554. Äußerst kritisch zu dieser Begründung, vgl. *Grözinger*, NStZ 2021, 358 f.; *Hiéramente*, WiJ 2021, 19, 21 f.; *Trüg*, JZ 2021, 560, 564 f., die mit guten Argumenten darauf hinweisen, dass ein in Zugriff auf Datenbestände, die vor Anordnung einer Telekommunikationsüberwachung entstanden sind, nach § 100a Abs. 1 S. 1 StPO – unabhängig von dem Vorliegen von Telekommunikation – unzulässig ist. Denn eine Überwachung im Sinne des § 100a StPO könne bereits – nach dem Wortsinn – nur bei heimlicher Kenntnisnahme des Inhalts einer *laufenden* Kommunikation vorliegen. Hierfür spricht auch ein systematischer Vergleich mit den §§ 100a, 100b StPO. § 100b StPO, der von Online-Durchsuchung spricht, schließt gerade auch in der Vergangenheit generierte und damit ruhende Datenbestände mit ein. Für § 100c StPO – der wie § 100a Abs. 1 S. 1 StPO von Überwachung spricht - ist unumstrittenes Verständnis, dass denklogisch nur laufende Kommunikation überwacht werden kann.

nicht zu dessen Eröffnung, womit keine Telekommunikation vorläge. Die wohl herrschende Ansicht in diesem Lager bejaht jedoch zurecht auch bei nur einer involvierten Person die Eröffnung des Schutzbereiches, womit auch Telekommunikation i.S.d. § 100a StPO vorläge. Aus einer eigenständigen strafprozessualen Auslegung des Telekommunikationsbegriffes folgt, dass bei der Nutzung eines Sprachassistenten während des Übermittlungsvorgangs an die Server keine Telekommunikation i.S.d. § 100a StPO vorliegt.[402] Sobald die Daten auf dem Server des Sprachassistenten ruhen, verneinen sämtliche Ansichten, mit Ausnahme der unipersonalen Strömung, die den Schutzbereich des Art. 10 GG auch in diesem Fall für eröffnet erachten würde, das Vorliegen von Telekommunikation im Sinne des § 100a StPO.

e) Stellungnahme

Es bleibt die Frage, welcher Strömung zur Bestimmung des Telekommunikationsbegriffes in § 100a StPO der Vorzug zu geben ist.

aa) Kritik an den technischen Auffassungen

Den technischen Auffassungen ist entgegenzuhalten, dass es keineswegs unproblematisch erscheint, § 3 des TKG zur näheren Auslegung des § 100a StPO heranzuziehen. Dies gründet zum einen auf den divergierenden Normzwecken. Während die Eingriffsbefugnisse des TKG lediglich einen Eingriff in das Fernmeldegeheimnis aus Art. 10 GG gestatten, erlaubt das strafprozessuale Pendant hierzu auch solche in das aus dem allgemeine Persönlichkeitsrecht des Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG entstammende Recht auf informationelle Selbstbestimmung.[403] Das extensive Verständnis des § 3 TKG für die Leseart des § 100a StPO zu Grunde gelegt, würde daher den grundrechtlich durch Art. 2 Abs. 1 i.V.m. Art. 1 GG garantierten Schutz ohne Not einschränken.[404] Zum anderen verweist

402 Anders zu beurteilen sind Fälle in denen der Smart Speaker lediglich als zwischengeschaltetes Gerät verwendet wird. Daher könnte unproblematisch die Telekommunikation nach § 100a StPO überwacht werden, sofern über den Smart Speaker ein Telefonat geführt wird.

403 *Hauck* in: LR-StPO, § 100a StPO, Rn. 35; *Trüg/Mansdörfer* in: Hilber, Handbuch Cloud Computing, Teil 7, Rn. 24.

404 *Trüg/Mansdörfer* in: Hilber, Handbuch Cloud Computing, Teil 7, Rn. 24.

§ 100a StPO im Unterschied zu beispielsweise § 100g Abs. 1 S. 1 StPO gerade nicht ausdrücklich auf das TKG. Sofern der Gesetzgeber auch im Rahmen des § 100a StPO eine Heranziehung der im TKG normierten Legaldefinition gewollte hätte, hätte er auch in § 100a StPO eine entsprechende Verweisung verankert.[405] Hinzu kommt, dass das TKG nach Sinn und Zweck ein intaktes Telekommunikationswesen garantieren soll, vgl. § 1 TKG[406], wohingegen Zweck des § 100a StPO die Beweisgewinnung zur Wahrheitsfindung ist. Im Unterschied zur StPO sind die Begrifflichkeiten des TKG offensichtlich technikorientiert; mit der Wahrung der öffentlichen Sicherheit und dem Schutz der Gesellschaft, dem die StPO dient, hat das TKG keine Berührungspunkte.[407] Gegen einen Rückgriff auf die Normen des TKG spricht ferner die Existenz des § 99 StPO, der zeigt, dass zumindest einzelne Telekommunikationsformen eigenständigen Ermächtigungsgrundlagen unterfallen und daher nicht unter § 100a StPO gefasst werden sollen.[408] Durch den Versuch, mittels der Definition aus dem TKG auch die Voraussetzung in § 100a StPO mit Leben zu füllen, wird einmal mehr deutlich, dass es in der juristischen Praxis keine Seltenheit darstellt, die Auslegung eines Wortes, unterschiedliche Regelungszusammenhänge ignorierend, durch Bezugnahme auf Begriffsbildungen aus fremden Normen auszugestalten.[409] Diese Vorgehensweise ist methodisch stark zu kritisieren und kann deswegen nicht der Maßstab zur Auslegung des § 100a StPO darstellen.

Gegen ein rein technisches und damit sehr extensives Verständnis des Telekommunikationsbegriffes, welches dazu führen würde, dass auch der bloße Datentransfer zwischen Maschinen unter diesen Begriff zu subsumieren wäre, bestehen zudem bereits in Anbetracht des Wortsinns bzw. dem allgemeinen Sprachverständnis des Begriffes „Kommunikation" Bedenken.[410] Als Mindestvoraussetzung bedarf Kommunikation als Form der Verständigung die menschliche Veranlassung. Der bloße Datenaustausch zwischen elektronischen Geräten kann mit dem allgemeinem Sprachgebrauch nicht derart vereinbart werden, dass darunter eine Form der

405 So bereits *Grözinger,* Die Überwachung von Cloud-Storage, S. 207; *Günther* in: MüKo-StPO, § 100a StPO, Rn. 33.
406 *Eisenberg/Nischan*, JZ 1997, 74, 77.
407 *Günther* in: MüKo-StPO, § 100a StPO, Rn. 33.
408 *Gercke,* Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren, S. 94 f.
409 So auch *Demko*, NStZ 2004, 57, 60.
410 A.A.: *Graf* in: BeckOK-StPO, § 100a StPO, Rn. 6.

kommunikativen Verständigung verstanden werden könnte.[411] Es kann wenn ausschließlich technische Geräte miteinander in Verbindung stehen und es an einem menschlich veranlassten auf Kommunikationsinhalte bezogenen Informationsaustausch fehlt, daher keine Kommunikation i.S.d. § 100a StPO vorliegen.[412]

Selbst das LG Ellwangen, das den zur Nutzung eines Sprachassistenten ähnlich gelagerten Fall des Abrufens von Websites als Telekommunikation einstufte, dürfte hiervon nicht restlos überzeugt gewesen sein. Anders sind die Ausführungen der Kammer, wonach eine Subsumtion unter § 100a StPO auch erforderlich gewesen sei, um den Bürger zu schützen[413], nicht zu verstehen. Es wäre „fatal"[414] gewesen, wenn auf das Surfen im Internet ansonsten über die Generalklausel des § 161 StPO zugegriffen werden könnte. Dem Gericht ist insofern zuzustimmen, dass ein solches Verhalten keine schutzlose öffentliche Kommunikation darstellen darf. Die Schlussfolgerung des Gerichts dieses Problem dadurch zu lösen, das entsprechende Verhalten unter § 100a StPO zu subsumieren, ist jedoch nicht überzeugend. Denn selbst sofern § 100a StPO für nicht einschlägig befunden worden wäre, würde dies nicht bedeuten, dass auf eine spezielle Ermächtigungsgrundlage verzichtet werden kann und der Grundrechtseingriff auf die Generalklausel des § 161 StPO gestützt werden kann. Dies wäre nur dann möglich, wenn es sich bei den auf Grundlage des § 161 StPO erfolgten Grundrechtseingriff um einen nur wenig grundrechtsintensiven Eingriffe handeln würde.[415] Sowohl bei der Sichtung abgerufener Websites als auch bei dem Zugriff auf die durch Sprachassistenten vernommenen Aussagen handelt es sich allerdings um Tätigkeiten, die Einblicke in Handlungen geben, die der Betroffene im Schein absoluter Privatheit vornimmt. Solche Eingriffe in die Privatsphäre sind nicht vergleichbar mit dem kurzzeitigen Einsatz eines V-Mannes oder einer kurzzeitigen Observation, die immer wieder auf die Generalklausel gestützt werden.[416] Bei diesen Maßnahmen wird der Betroffene nicht in privaten Rückzugsräumen überwacht, sondern erst nachdem er sich in die Öffentlichkeit

411 Bernsmann, NStZ 2002, 103, 104.
412 BVerfG, MMR 2006, 805, 807.
413 LG Ellwangen, Beschluss v. 28.05.2013, Az.: 1 Qs 130/12.
414 LG Ellwangen, Beschluss v. 28.05.2013, Az.: 1 Qs 130/12.
415 *Kölbel* in: MüKo-StPO, § 161 StPO, Rn. 9; *Grießbaum* in: KK-StPO, § 161 StPO, Rn. 1.
416 Solche Maßnahmen können auf die Ermittlungsgeneralklausel, § 161 StPO, gestützt werden, vgl. *Grießbaum* in: KK-StPO, § 161 StPO, Rn. 1; *Sackreuther* in: BeckOK-StPO, § 161 StPO, Rn. 11.

begeben hat oder im Falle des Einsatzes eines V-Mannes nachdem sich der Betroffene freiwillig einer ihm Unbekannten Person offenbart hat. Die Eingriffsintensität ist daher deutlich geringer. Die richtige Schlussfolgerung des LG Ellwangen wäre daher gewesen, das Abrufen der Websites unter Heranziehung des § 100a StPO zu verbieten und sodann weitere mögliche Ermächtigungsgrundlagen der §§ 100a ff. StPO zu prüfen. Sofern keine weitere Ermächtigungsgrundlage als einschlägig befunden worden wäre, hätte der erfolgte Grundrechtseingriff aufgrund eines Verstoßes gegen den Gesetzesvorbehalt als rechtswidrig beurteilt werden müssen.

bb) Kritik an der grundrechtsanalogen Auffassung

Einem grundrechtsanalogen Verständnis des § 100a StPO ist kritisch entgegenzuhalten, dass von der Reichweite des Grundrechtsschutzes aus Art. 10 GG nicht auf die Reichweite einer grundrechtstangierenden Ermächtigungsgrundlage geschlossen werden darf.[417] Würde bei der Auslegung des einfachen Gesetzes lediglich auf den grundrechtlichen Schutzbereich zurückgegriffen, würde der Grundrechtsschutz ausgehöhlt. Sofern also eine Ermächtigungsgrundlage, auf den ersten Blick um des Grundrechtsschutzes Willen, grundrechtsanalog extensiv ausgelegt wird, führt dies letztlich die Schutzfunktion der Grundrechte ad absurdum.[418] Während Grundrechte gerade nicht den Staat berechtigen, sondern dessen Bürger schützen sollen, stellt § 100a StPO eine Berechtigung für den Staat dar, in die Rechte seiner Bürger verfassungsgemäß eingreifen zu können. Will man nun trotz dieses diametralen Unterschieds die dem Staat einfach gesetzlich zugesprochenen Eingriffsbefugnisse aus dem Schutzinhalt, den die Verfassung dem Bürger gerade zu dessen Schutz zuerkennt, ableiten, verfängt sich dies in einem Zirkelschluss zu Lasten des Bürgers. Dessen verfassungsrechtlich durch Art. 10 GG garantiertes Schutzniveau würde dadurch leerlaufen, dass dem Staat durch den inhaltlichen Gleichlauf zwischen Schutzniveau und Eingriffsermächtigung solch weite Eingriffsbefugnisse zukämen, dass der weite Schutzbereich wertlos erscheinen würde[419] Dass für einen rechtmäßigen staatlichen Eingriff dabei – wie auch im Falle

417 So auch *Hilgendorf/Valerius*, Internetstrafrecht, Rn. 783; *Roggan*, KritV 2003, 76, 80 und 89; *Grözinger, NStZ 2021, 358*.

418 *Bernsmann*, NStZ 2002, 103, 103; *Bernsmann/Jansen*, StV 1999, 591, 591; *Gercke*, GA 2012, 474, 488; *Hiéramente* WiJ 2021, 19, 21.

419 Zutreffend auch *Hiéramente/Fenina*, StraFo 2015, 365, 371.

des § 100a StPO – noch weitere tatbestandliche Voraussetzungen vorliegen müssen, vermag hieran nichts zu ändern.[420] Denn über das Vorliegen dieser weiteren Voraussetzungen ist stets losgelöst von der Frage zu entscheiden, ob das Tatbestandsmerkmal der Telekommunikation im konkreten Einzelfall gegeben ist. Ein Zusammenhang, dass sofern Art. 10 GG tangiert ist, auch das Tatbestandsmerkmal der Telekommunikation in § 100a StPO erfüllt ist, ist dem Gesetz fremd. Der Inhalt der Ermächtigungsgrundlage kann daher gerade nicht durch den Schutzbereich des Grundrechts bestimmt werden, in welches ein Eingriff unter Heranziehung eben dieser Ermächtigungsgrundlage legitimiert werden soll.[421] Insofern sind das den Bürger schützende Grundrecht und die den Staat berechtigende Ermächtigung strikt zu trennen. Wenn das BVerfG betont, dass das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG entwicklungsoffen ist und auch neuartige Übertragungstechniken umfassen soll,[422] so bedeutet das gerade nicht, dass der Begriff der Telekommunikation im Rahmen des § 100a StPO synonym hierzu auszulegen ist, sondern lediglich ebenso – aber stets in Anbetracht seines strafprozessualen Zweckes – entwicklungsoffen ist[423]. Insbesondere ist es nicht widersprüchlich Art. 10 GG entwicklungsoffen auszulegen, während dies für § 100a StPO restriktiver gehandhabt wird. Dabei ist unstreitig, dass § 100a StPO dem technischen Fortschritt dergestalt Rechnung tragen muss, dass neben dem klassischen Telefongespräch auch neuere Kommunikationsformen wie SMS, E-Mails, oder Chatnachrichten mittels § 100a StPO überwacht werden dürfen. Dieser Wechsel des Kommunikationsmediums ändert jedoch nichts an der Zielrichtung des § 100a StPO und seiner restriktiveren Auslegung im Lichte seiner selbst.[424] Es ist einmal mehr zu beachten, dass Art. 10 GG dem Schutz der Bürger dient[425] und, um dem verfassungsrechtlichen Schutzauftrag nachzukommen, eben dieser verfassungsrechtlich garantierte Schutz im Gleichschritt mit der technischen Entwicklung ausgeweitet werden muss. Hierfür sprechen nicht zuletzt auch praktische Erwägungen. Denn andernfalls müsste für neue Entwicklungen das Grundgesetz permanent geändert oder modifiziert werden. Zudem wäre der Bürger bei neuen Entwicklungen bei deren Nutzung der Bürger vor staatlichem Zugriff geschützt werden

420 A.A. *Wölm*, Schutz der Internetkommunikation und heimliche Internetaufklärung, S. 244.
421 *Wolter/Greco* in: SK-StPO, § 100a StPO, Rn. 13.
422 BVerfG NJW 2006, 976, 978.
423 A.A. *Graf* in: BeckOK-StPO, § 100a StPO, Rn. 20.
424 Zutreffend *Hiéramente/Fenina*, StraFo 2015, 365, 370, m.w.N.
425 *Schoch*, Jura 2011, 194, 195.

muss, bis zur Schaffung eines neuen Grundrechts schutzlos gestellt. Bei den Eingriffsermächtigungen der StPO handelt es sich jedoch um formelle Gesetze. Formellen Gesetze ist es seit jeher immanent, dass sie durch zahlreiche Modifizierung ständig an die Entwicklung angepasst oder gar neu geschaffen werden.[426] Letzteres zeigt nicht zuletzt die Existenz der §§ 100a, 100b, 100c StPO selbst.

Auch wenn Art. 10 GG nach den Ausführungen des BVerfG den „verfassungsrechtlichen Maßstab"[427] für die Eingriffsermächtigung aus § 100a StPO darstellt und sich die Auslegung des Telekommunikationsbegriffes in § 100a StPO auch an dem grundrechtlichen Schutz des Betroffenen aus Art. 10 GG orientieren müsse,[428] so ist daraus keinesfalls der nur vermeintlich logische Schluss zu ziehen, dass das BVerfG für eine grundrechtsanaloge Anwendung des Telekommunikationsbegriffes in § 100a StPO streitet. Vielmehr ist dies so zu verstehen, dass die Begriffsauslegung in § 100a StPO nicht weiter gehen darf als der durch Art. 10 GG normierte Schutz des Bürgers. Der Maßstab aus Art. 10 GG deckelt daher die Weite der durch § 100a StPO statuierten Eingriffsbefugnis. Dieses Verständnis wird dadurch gestützt, dass das BVerfG ausführte, dass die vom LG Ellwangen hinsichtlich § 100a StPO vorgenommene Auslegung auch dem Bedeutungsinhalt des eröffneten Art. 10 GG hinreichend gerecht werde und hiermit nicht in Widerspruch stehe[429], da der für rechtmäßig befundene Eingriff auf Grundlage des § 100a StPO sich in den durch Art. 10 GG normierten Grenzen halte. Ein solcher Widerspruch hätte dann bestanden, wenn der Schutzbereich des Art. 10 GG so eng ausgelegt würde, dass das gegenständliche Verhalten nicht hierunter, aber gleichwohl unter die Eingriffsermächtigung des § 100a StPO fallen würde. Aus der Systematik zwischen Grundrechtsschutz und Eingriffsbefugnis und dem Grundsatz des Gesetzesvorbehalts muss daher folgen, dass eine Eingriffsermächtigung nicht zu einem Eingriff ermächtigen darf, dem der Betroffene mangels Einschlägigkeit eines grundrechtlichen Schutzbereichs schutzlos ausgeliefert wäre. Der umgekehrte Schluss, dass die Auslegung im Lichte eines strafprozessualen materiellen Telekommunikationsbegriffes in § 100a StPO nicht restriktiver als in Art. 10 GG erfolgen dürfe bzw. hiermit

426 Vgl. *Durner* in: Maunz/Dürig-GG, Art. 10, Rn. 66; *Nicolai*, HRRS 2021, 365, 368.
427 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 32 = teilweise in NJW 2016, 3508 ff.
428 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 32 = teilweise in NJW 2016, 3508 ff.
429 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 38 = teilweise in NJW 2016, 3508 ff.

im Einklang grundrechtsanalog erfolgen müsse, kann mit Verweis auf die verfassungsgerichtliche Rechtsprechung allerdings nicht geführt werden. Vielmehr entspricht es gängiger Systematik, dass der Schutzbereich im Sinne eines möglichst weiten Grundrechtsschutzes weit zu verstehen ist, während staatliche Eingriffsbefugnisse für einen konkreten Einzelfall gelten und damit eng auszulegen sind.[430] Dass Art. 10 GG als Maßstab für die Auslegung des § 100a StPO ebenfalls herangezogen werden soll, kann daher nur bedeuten, dass der Umfang des Schutzbereichs aus Art. 10 GG den Telekommunikationsbegriff in § 100a StPO in seiner Weite eingrenzt, einer engeren Auslegung als sie in Art. 10 GG stattfindet aber nicht entgegensteht. Im Übrigen führt die Betroffenheit eines Grundrechts lediglich dazu, den diese Betroffenheit auslösenden Eingriff überhaupt an einer Befugnisnorm zu messen, es ist aber allein durch die Betroffenheit eines Grundrechts noch nichts darüber ausgesagt, ob dieser Eingriff auch von der Befugnisnorm gedeckt ist.[431]

cc) Lösung

Es bleibt daher festzuhalten, dass bei zutreffender Zugrundelegung eines strafprozessualen Telekommunikationsbegriffes die passive Informationsgewinnung in Form einer einseitigen Nutzung informationstechnischer Kommunikationsanlagen keine Kommunikation i.S.d. § 100a StPO darstellen kann. Allein aufgrund des Umstandes, dass Informationen bewusst preisgegeben werden, kann noch keine Kommunikation vorliegen. Das bloße Abrufen von Websites oder die Inanspruchnahme der ausgegliederten Rechenleistung des Sprachassistenten zur Informationsbeschaffung kann – selbst, wenn eine mögliche Straffälligkeit dabei evident erscheint (beispielsweise durch den Inhalt der Informationsanfrage: „Wie baue ich eine Bombe?“) keine Telekommunikation im Sinne des § 100a StPO darstellen.[432]

430 ähnlich auch *Wolter/Greco* in: SK-StPO, § 100a StPO, Rn. 13.
431 Zutreffend auch *Kudlich*, JuS 2001, 1165, 1167; *Eckhard*, CR 2001, 385, 387.
432 Zutreffend auch *Trüg/Mansdörfer* in: Hilber, Handbuch Cloud Computing, Teil 7, Rn. 27, die darauf hinweisen, dass Prozesse der Auslagerung von Rechenleistung, Speicher und Arbeitsspeicher oder von Anwendungen wie der Textverarbeitung in der Cloud keine Telekommunikation i.S.d. § 100a StPO darstellen; im Ergebnis auch *Böckenförde*, JZ 2008, 925, 937.

3) Eigener Vorschlag eines strafprozessualen Telekommunikationsbegriffes

Da jedoch nähere Ausführungen zur Ausgestaltung eines genuin strafprozessualen Telekommunikationsbegriffes nur vereinzelt zu finden sind, soll im Folgenden ein weiterer Vorschlag zur Lesart der umstrittenen Voraussetzung des § 100a StPO gemacht werden. Zur Bestimmung eines tauglichen strafprozessualen Telekommunikationsbegriffes ist § 100a StPO im Lichte der gängigen juristischen Auslegungsmethoden zu untersuchen.

a) Erforderliche Personenanzahl

Dabei ist zunächst die Frage zu klären, wie viele Personen an einem Vorgang beteiligt sein müssen, um von Telekommunikation i.S.d. § 100a StPO sprechen zu können.

aa) Auslegung nach Wortsinn

Nach allgemeinem Sprachgebrauch handelt es sich bei Kommunikation um eine Art der Verständigung. Eine tiefergehende Auseinandersetzung anhand des Wortlautes erfordert ebenso einen Blick auf den Wortursprung. Während „Tele" etwa „in die Ferne" bedeutet und dabei die räumliche Distanz des Vorgangs beschreibt, fällt unter den Begriff Kommunikation jede Form der Verständigung durch Informationsübermittlung.[433] Kennzeichnend für eine Verständigung ist, dass die jeweiligen Aussagen aufeinander Bezug nehmen. Dabei handelt es sich stets um eine beliebig weite Art der Informationsvermittlung, ohne Einschränkung auf bestimmte Arten der Informationsübermittlung. Aussagen können allerdings nur dann aufeinander Bezug nehmen, wenn diese durch mindestens zwei Personen abgegeben werden. Ansonsten ähnelt der Akt der Kommunikation eher einem Selbstgespräch, jedoch keiner klassischen Kommunikation in Form einer Verständigung.[434]

433 *Gercke*, Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren S. 100.

434 So auch *Roxin/Schünemann*, Strafverfahrensrecht, § 36, Rn. 5.

bb) Historische Auslegung

Eine historische Auslegung stellt die Entstehungsgeschichte des Gesetzgebers in den Vordergrund. Unter Zugrundelegung dessen wollte der Gesetzgeber mit der Schaffung des § 100a StPO im Jahr 1968 das Abhören des Fernsprechverkehrs und das Aufzeichnen der dadurch gewonnen Erkenntnisse sicherstellen.[435] Explizit verweist die Gesetzesbegründung darauf, dass den Strafverfolgungsbehörden die Befugnis zum „Telefongespräche abhören"[436] zuteilwerden soll. Es sollte eine Norm geschaffen werden, die es ermöglichte den Informationsaustausch der Täter, den diese infolge des technischen Fortschritts ohne Verlassen der Wohnung und ohne Niederschrift vornehmen konnten, zur Beweisgewinnung verwertbar zu machen.[437] Im Zuge der Neufassung des § 100a StPO durch das Poststrukturgesetz vom 08.06.1989 modifizierte der Gesetzgeber die Befugnis hin zur „Aufzeichnung des Fernmeldeverkehrs". Der Gesetzgeber wollte damit etwaigen Zweifeln an der Anwendbarkeit der Norm hinsichtlich moderner Formen der Nachrichtenübermittlung zuvorkommen.[438] Seit der Entstehung der Norm vermochten Modifizierungen und Anpassung derselben an dem ursprünglich gesetzgeberischen Ziel der Kenntniserlangung von Kommunikationsvorgängen im Ganovenmilieu nichts zu ändern. Für ein solches in der Gesetzesbegründung erwähntes Telefongespräch sind denklogisch zwei Personen erforderlich. Der Gesetzgeber wollte mit der der Schaffung der Norm den Strafverfolgungsbehörden die Möglichkeit geben, sich Kenntnis über ein nicht öffentliches Telefongespräch zwischen zwei Personen verschaffen zu können.

cc) Systematische Auslegung

In systematischer Hinsicht erscheint eine nähere Analyse zunächst schwierig, da der Telekommunikationsbegriff in der StPO im Übrigen nicht zum Vorschein kommt. Möglicherweise kann ein Blick auf § 99 StPO geworfen werden. Dieser erlaubt die Beschlagnahme von Telegrammen und Postsendungen als eine Form der Telekommunikation. Daraus lässt sich jedoch lediglich folgern, dass § 100a StPO nicht für jegliche Art von

435 *Günther* in: MüKo-StPO, § 100a StPO, Rn. 2.
436 BT-Drs, V/1880, S. 6.
437 *Hiéramente/Fenina*, StraFo 2015, 365, 369.
438 BT-Drs. 11/4316, S. 90.

Kommunikation einschlägig ist. Es verdeutlicht daher die Notwendigkeit eines strafprozessual anhand von § 100a StPO gebildeten Telekommunikationsbegriffes, liefert aber für dessen genauere Ausgestaltung keine zielführenden Anhaltspunkte. Zielführend erscheint ein Vergleich auf welche Art und Weise die Daten durch die §§ 100a ff. StPO gewonnen werden sollen. Während die Datengewinnung bei § 100a StPO durch den Zugriff auf einen Kommunikationsvorgang im Ganovenmilieu erfolgt, soll dies bei § 100b StPO vielmehr durch Infiltration eines informationstechnischen Systems erfolgen. Bei § 100c StPO wiederum erfolgt die Informationsgewinnung durch das Verwanzen der Wohnung des Betroffenen. Nach einem Vergleich dieser Normen wird daher ersichtlich, dass im Rahmen des § 100a StPO im Unterschied zu § 100b und c StPO mehrere Personen in den Vorgang auf welchen zugegriffen wird involviert sein müssen. § 100b StPO und 100c StPO erlauben hingegen auch den Zugriff auf einen unipersonal stattfindenden Vorgang in Form der Überwachung der Kommunikation einer Person mit ihren eigenen Daten[439] oder dem Abhören eines Selbstgesprächs im Rahmen des § 100c StPO.[440]

dd) Teleologische Auslegung

Schließlich ist die Norm auch nach ihrem Telos zu untersuchen. Dieser liegt darin, die Aufklärung von Straftaten durch heimliche Beweisgewinnung zu ermöglichen.[441] Diesem Zweck dienen jedoch letztlich sämtliche Normen der § 100a ff. StPO. Daher ist weiter zu beleuchten, welche Art von Erkenntnissen § 100a StPO im Unterschied zu anderen Ermittlungsbefugnissen hervorbringen soll. Hierzu wurde eine Unterscheidung zwischen Daten und Informationen vorgeschlagen.[442] Allerdings haben die § 100a ff. StPO im Ergebnis allesamt die Erlangung von Informationen und nicht lediglich bloßer Daten zum Ziel. Zielführender erscheint es daher im Zuge der Auslegung zu ermitteln, welche Erkenntnisse durch eine ausgewählte Zwangsmaßnahme hervorgebracht werden sollen. Die erhofften Erkenntnisse zielen auf getroffene Absprachen und Mitteilungen

439 *Sinn*, Stellungnahme zum Entwurf der BT-Drs. 18/11272, S. 5.

440 Vgl. BGHSt 50, 206. Neben dem möglichen Zugriff auf ein solches Selbstgespräch über § 100c StPO ist hinsichtlich dessen anschließender Verwertbarkeit anhand der Maßstäbe des Kernbereichsschutzes zu entscheiden.

441 *Gercke* Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren, S. 106.

442 *Demko*, NstZ 2004, 57, 61 mit Verweis auf *Weßlau*, ZStW 2001, 681, 689.

zur Planung, Durchführung oder (Nach-) Besprechung einer Straftat. Solche Absprachen können jedoch nur durch mehrere Personen erfolgen, da der schlichte Einzeltäter in der Regel mangels Mittäter oder Beteiligter mit niemanden über die Tat sprechen wird. Tut er dies doch, so würde er, selbst wenn er die Tat allein auszuführen gedenkt, deren Begehung wiederum mit einer anderen Person besprechen. Hierdurch läge wiederum eine Verständigung über die Planung der Tat und damit Kommunikation vor. Da gerade solche Erkenntnisse der Planung oder auch (Nach-)Besprechung einer Tat gewonnen werden sollen, kommt man ebenfalls zum Schluss, dass solche Erkenntnisse nur dann generiert werden können, wenn mehrere Personen an einem Telekommunikationsvorgang beteiligt sind.

Mit Blick auf das Bild, welches der Gesetzgeber bei der Schaffung der Norm vor Augen hatte (Telefongespräche abhören), muss zudem gefordert werden, dass der Vorgang der Telekommunikation dazu dienen muss, einer menschlichen Person eine Nachricht zu übermitteln.[443] Ganz außer Acht bleiben soll auch in diesem Zusammenhang die vielfach zitierte „Entwicklungsoffenheit des § 100a StPO“[444] nicht. Dabei ist jedoch strikt zwischen der Entwicklungsoffenheit auf Ebene des Art. 10 GG und des § 100a StPO zu trennen. Auf Ebene des § 100a StPO bedeutet diese Entwicklungsoffenheit, dass neben dem klassischen Telefongespräch auch Kommunikation mittels SMS, E-Mails, Chatnachrichten oder Internettelefonie überwacht werden darf.[445] Allerdings ändert auch ein solcher Wechsel des Kommunikationsmediums nichts daran, dass stets Telekommunikation im Sinne einer Nachrichtenübermittlung an eine andere Person im Zusammenhang mit etwaiger Ganovenkommunikation, wie es der Gesetzgeber bei der Kodifizierung des § 100a StPO vorgesehen hatte, im Vordergrund stehen muss. Offenbaren sich im Zuge der technischen Entwicklung wesensverschiedene Anwendungsmöglichkeiten zu dem angedachten Anwendungsfall, bei denen eben nicht mehr die klassische Ganovenkommunikation im Vordergrund steht, so können diese nicht von dem strafprozessualen Telekommunikationsbegriff aus § 100a StPO umfasst sein. Eine solche Ganovenkommunikation kann jedoch denklogisch nur zwi-

443 Ähnlich auch *Meinicke*, DSRITB 2013, 967, 971, wonach § 100a StPO originär für die Überwachung der Kommunikation zwischen zwei Individuen konzipiert sei.

444 *Bruns* in: KK-StPO, § 100a StPO, Rn. 4; *Hiéramente/Fenina*, StraFo 2015, 365, 370, m.w.N.

445 Zutreffend in diese Richtung auch *Hiéramente/Fenina*, StraFo 2015, 365, 370.

schen Mittätern oder Täter und Gehilfe von Statten gehen. Auch im Lichte einer teleologischen sind für Telekommunikation i.S.d. § 100a StPO daher zwei Menschen erforderlich.[446]

b) Telekommunikationswille

In der Vergangenheit ist es immer wieder vorgekommen, dass zum einen während des Abhörvorgangs beispielsweise auch auf Hintergrundgespräche, die eigentlich nicht Teil der unmittelbar überwachten Kommunikation darstellten und auf den ersten Blick daher eher unter § 100c StPO fallen mögen, zugegriffen wurde oder zum anderen mitgehört wurde, nachdem eine Verbindung nur versehentlich hergestellt oder nicht vollständig beendet wurde.[447] Ob solche Gespräche jedoch unter den Telekommunikationsbegriff fallen, entscheidend sich letztlich danach, ob für das Vorliegen von Telekommunikation ein Telekommunikationswille erforderlich ist.

Der Wortlaut des § 100a StPO enthält keine unmittelbaren Anhaltspunkte hinsichtlich der subjektiven Sichtweise des Betroffenen. Die Frage, ob man sich nur verständigen könne, wenn hierfür ein entsprechender Wille vorhanden ist, ließe sich mit dem Argument verneinen, dass Menschen vielfach kommunizieren, ohne sich hierüber bewusst zu sein, etwa durch Mimik oder Gestik. Die gesamte non-verbale Kommunikation über Körperhaltung und Ausdruck läuft daher beinahe täglich ohne ausdrücklichen Kommunikationswillen ab. Dabei ist allerdings zu beachten, dass es sich im Rahmen des § 100a StPO lediglich um verbale Kommunikation handelt. Eine solche ist unter normalen Umständen nicht ohne den Willen zur Kommunikation möglich. Selbst bei einem Selbstgespräch – das im Regelfall aufgrund des fehlenden Kommunikationspartners – nicht unter § 100a StPO fällt, handelt der Sprechende in dem Bewusstsein nun eben mit sich selbst zu kommunizieren. Ausgehend vom Wortsinn der Kommunikation müsste man daher das Vorliegen eines Kommunikationswillens als erforderlich erachten. Systematische und historische Auslegung helfen an dieser Stelle ebenfalls nicht weiter. Vergegenwärtigt man sich erneut Sinn und Zweck einer heimlichen Aufklärung von Straftaten könnte man auf einen Telekommunikationswillen verzichten. Schließlich soll Ziel einzig und allein das Erlangen belastbarer Informationen durch den Zugriff auf Telekommunikationsmedien sein.

---

446 So auch *Eidam*, NJW 2016, 3511, 3512.
447 Vgl. BGH, NJW 2003, 2034, 2035.

Auch die Rechtsprechung hatte sich in der Vergangenheit häufiger mit der Frage nach dem Vorliegen eines Kommunikationswillen sowie mit den möglichen Anforderungen an diesen zu beschäftigen. Das BVerfG urteilte, dass der Betroffene zumindest über ein potenzielles Bewusstsein verfügen müsse, in jenem Moment nach außen zu kommunizieren.[448] Auch der BGH urteilte zur Verwertbarkeit eines sog. Raumgesprächs in die gleiche Richtung. Während der Zugriff auf ein Raumgespräch eigentlich den klassischen Anwendungsfall des § 100c StPO wiedergibt, soll unter gewissen Voraussetzungen, auf das während eines solchen Raumgesprächs Gesprochene auch über § 100a StPO zugegriffen werden können. Voraussetzung hierfür ist gerade nicht, dass sich der konkrete Vorgang mit aktuellem Willen oder Wissen der betroffenen Person vollzieht.[449] Nach den Ausführungen der Richter am Bundesgerichtshof ist jedoch erforderlich, dass „*nach willentlicher Herstellung einer Telekommunikationsverbindung durch die Zielperson […] aus deren Sicht versehentlich [Informationen] übertragen werden*"[450]. Entscheidend soll also sein, dass der Betroffene die Verbindung selbst hergestellt oder die versehentliche Aufrechterhaltung durch ihn verursacht wurde. Dabei genügt es bereits, wenn der Betroffene das Telekommunikationsmedium in Betrieb setzt oder in betriebsbereitem Zustand hält.[451] Dem folgend würde dann wohl bereits in einem Fall, in dem der Betroffene sein Mobiltelefon ohne Tastatursperren in der Tasche trägt und durch die Gehbewegung unbemerkt und ungewollt eine Verbindung hergestellt wird, die notwendigen Voraussetzungen für einen Telekommunikationswillen erreicht sein.[452]

Es wird deutlich, dass die Anforderungen an einen vorhandenen Telekommunikationswillen äußerst gering sind. Diese geringen Anforderungen zugrunde liegend erscheint es bereits überaus fraglich überhaupt noch von einem wirklichen Willen zur Telekommunikation zu sprechen. Vielmehr entsprechen die entwickelten Maßstäbe eher einer Einordnung in Risikosphären. So wie das Telekommunikationsmedium in Betrieb genommen wurde, ist es der Nutzer, der für sämtliche „Selbstständigkeiten" seines Gerätes verantwortlich ist. Er trägt das Risiko, dass auf eine sodann auch ohne sein Wissen aufgebaute oder nicht beendete Verbindung von

448 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13 -, Rn. 20 = teilweise in NJW 2016, 3508 ff.
449 BGH, NJW 2003, 2034, 2035.
450 BGH, NJW 2003, 2034, 2035.
451 BGH, NJW 2003, 2034, 2035.
452 *Gercke*, JZ 2004, 347, 348.

Seiten des Staates zugegriffen werden kann. Das Kriterium der Veranlassung stellt einen sachgerechten Mittelweg zwischen dem Erfordernis eines vollständig notwendigen Kommunikationswillens und dem kompletten Verzicht hierauf dar. Das Erfordernis eines Telekommunikationswillen, dem sich der Betroffene vollumfänglich bewusst ist, würde zu erheblichen Beweisschwierigkeiten führen. Die Strafverfolgungsbehörden müssten den entsprechenden Willen prozessrechtlich nachweisen, was vielfach nicht gelingen würde. Auf der anderen Seite würde ein gänzlicher Verzicht auf ein solches Kriterium die Freiheit des Einzelnen zu sehr einengen und die Ermächtigungsgrundlage des § 100a StPO zu sehr in die Nähe des § 100c StPO rücken lassen. Sofern dem Nutzer eine willensgesteuerte Veranlassung zugeschrieben werden kann, wurde das Abhören der Gespräche nicht gezielt durch die Strafverfolgungsbehörden forciert, sondern erst durch möglicherweise fahrlässiges Handeln der Betroffenen, die den ursprünglichen Telekommunikationsvorgang in Gang setzen, ermöglicht. Diese haben den Vorgang durch Ihr Handeln veranlasst und damit den Strafverfolgungsbehörden erst die Möglichkeit gegeben Erkenntnisse zu sammeln.[453] Daher ist zu konstatieren, dass sofern die übrigen Voraussetzungen für Telekommunikation vorliegen, es sich bereits dann um Telekommunikation i.S.d. § 100a StPO handeln kann, wenn diese jedenfalls menschlich veranlasst oder in Gang gesetzt wurde.

c) Zwischenergebnis

Unter Berücksichtigung dessen ist Kommunikation i.S.d. § 100a StPO jeder menschlich veranlasste Vorgang, der nach seinem objektiven Verständnis unmittelbar dazu dient oder dienen sollte, eine Mitteilung an eine nicht mit dem Veranlasser des Vorgangs identische menschliche Person zu übermitteln. Dass die Nachricht an einen menschlichen Empfänger gerichtet werden muss, stellt sicher, dass die Antwort des Empfängers individuell und nicht aufgrund einer mathematischen oder technischen Formel zu Stande gekommen ist. Solch eine „berechnete" Antwort wäre mit dem Verständnis der Kommunikation in § 100a StPO nicht vereinbar, da ein für Kommunikation immanentes Erfordernis fehlen würde. Die zu erwartende Antwort darf gerade nicht technisch und objektiv vorhersehbar sein. Damit aus Kommunikation schließlich Telekommunikation im Sinne des § 100a StPO wird muss der beschriebene Vorgang der Mitteilungsüber-

453 A.A. *Fezer*, NstZ 2003, 625, 628.

mittlung durch ein technisches Mittel geschehen, das nach seinem objektivem Verständnis für die Nachrichtenübermittlung in die Ferne geschaffen wurde.[454] Zusammenfassend ist der Begriff der Telekommunikation im Rahmen des § 100a StPO nicht synonym zum Telekommunikationsbegriff des Art. 10 GG auszulegen, sondern es ist vielmehr ein eigener personell-individueller Telekommunikationsbegriff heranzuziehen.

d) Nutzung eines Sprachassistenten in der Form eines Smart Speakers im Sinne des personell-individuellen Telekommunikationsbegriffs

Es bleibt zu klären, inwiefern bei der Nutzung eines Smart Speakers unter Zugrundelegung des personell-individuellen Telekommunikationsbegriffs von Telekommunikation gesprochen werden kann. Sofern direkt auf die Hardware des Smart Speakers zugegriffen werden soll und hierauf gespeicherte Informationen erlangt werden sollen, fehlt es an einem erforderlichen Übermittlungsvorgang. Es würde keine Telekommunikation vorliegen. Da sich der personell-individuelle Telekommunikationsbegriff nicht an der Legaldefinition des § 3 Nr. 22 TKG orientiert, wäre es für ein Übersenden bereits ausreichend, wenn dieses zwar noch nicht stattfand, jedoch im nächsten Moment ohne weiteres zutun des Nutzers erfolgen würde. Auch im Stadium der Übermittlung der Audiodatei zum Sprachassistenten liegt nach diesem Begriffsverständnis aber aus mehreren Gründen keine Telekommunikation vor. Zum einen fehlt es bereits an dem Erfordernis zweier menschlicher Personen. Hinzu kommt, dass die Antwort des Sprachassistenten aufgrund bestimmter Algorithmen berechnet wurde, ihr mithin die notwendige Individualität abhandenkommt. Daher fehlt es an der erforderlichen Verständigung in Form einer individuell aufeinander eingehenden Konversation. Zum anderen ist zu beachten, dass ein Sprachassistent grundsätzlich ein Mittel zur Informationsgewinnung, nicht jedoch zur Informationsübertragung darstellt. Dieser Funktion ist sich auch der Nutzer eines Sprachassistenten bewusst. Würde auf diesen dennoch unter Heranziehung des § 100a StPO zugegriffen, so würde dessen eigentliche Funktion umfunktioniert. Für Zugriffe auf solche Arten

454 Tele entstammt dem griechischen tēle und wird im deutschen Sprachgebrauch mit fern/weit assoziiert, vgl. https://de.wiktionary.org/wiki/tele-#:~:text=%5B1%5D%20vorangestelltes%20Wortbildungselement%20in%20Fremdw%C3%B6rtern,tele)%20%E2%86%92%20grc%20%E2%80%9Efern%E2%80%9C (zuletzt abgerufen am 31.10.2021).

von digitalen technischen Geräten ist § 100a StPO nach dessen Sinn und Zweck nicht geschaffen. Bei dem Zugriff auf einen Sprachassistenten steht gerade nicht die Verständigung zwischen zwei Personen aus dem Ganovenmilieu im Vordergrund, sondern eine Kenntniserlangung hinsichtlich der durch den Betroffenen durchgeführten Informationsabfragen. Auch sofern sich die Daten bereits auf den Servern des Dienstleisters befinden, ergibt sich kein anderes Bild. Es fehlt an den grundlegenden Voraussetzungen, um von Telekommunikation im Sinne des § 100a StPO sprechen zu können. Somit bleibt festzuhalten, dass § 100a StPO keine taugliche Ermächtigungsgrundlage zum Zugriff auf die durch Sprachassistenten erlangte Informationen bietet.

4) Verschlüsselung der Daten

Ein weiteres Problem, dem sich ein Zugriff nach § 100a Abs. 1 S. 1 StPO gegenübersieht, liegt darin begründet, dass die Daten während des Übertragungsweges von Hardware zum Server verschlüsselt übertragen werden.[455] Um diesem technischen Fortschritt Rechnung zu tragen, wurden die Vorschriften in Form von § 100a Abs. 1 S. 2, 3 StPO geschaffen.[456] Neben der Frage, inwiefern unter Zuhilfenahme dieser neugeschaffenen Normen auf Sprachassistenten zugegriffen werden könnte, sehen sich diese Normen auch verfassungsrechtlichen Bedenken gegenüber. Auf jene Problemfelder soll im Folgenden näher eingegangen werden.

II) § 100a Abs. 1 S. 2 StPO n.F.

1) Allgemeines

Bezüglich unverschlüsselter Daten hat der Dienstleistungsanbieter nach §§ 100a Abs. 4 StPO, 110 Abs. 1 TKG die erforderlichen technischen Vorkehrungen zu treffen, um den Behörden eine Kopie der zu überwachenden Telekommunikationsinhalte zur Verfügung stellen können, sodass die Erlangung solcher Daten – die Einschlägigkeit des § 100a StPO vorausge-

455 vgl. https://support.apple.com/de-de/HT202303 (zuletzt abgerufen am 31.10.2021).

456 BT-Drs. 18/12785, S. 48; *Bruns* in: KK-StPO, § 100a StPO, Rn. 42.

setzt – keine größeren Probleme bereiten würde.[457] Nachdem jedoch inzwischen ein Großteil der über das Internet laufende Kommunikation verschlüsselt erfolgt[458], werden den Ermittlungsbehörden nach erfolgter Aufzeichnung durch den Dienstleistungsanbieter oft nur verschlüsselte Daten geliefert. Die Daten werden lediglich in kryptierter Form aufgezeichnet, ohne dass dem Dienstleistungsanbieter oder den Strafverfolgungsbehörden ein Zugriff auf die unverschlüsselten Kommunikationsinhalte möglich ist. Deren Entschlüsselung wiederum würde die Behörden vor technisch nicht zu überwindende Hürden stellen oder sich jedenfalls langwierig und kostenintensiv gestalten.[459] Ganz im Gegenteil ist es sogar ein gesetzgeberisches Anliegen zum Schutze vertraulicher Daten vor Zugriffen Dritter eine Weiterentwicklung und Verbesserung der Verschlüsselungstechnologien herbeizuführen.[460] Die Stärkung des Datenschutzes ohne eine gleichzeitige gesetzgeberische Reaktion hinsichtlich der staatlichen Ermittlungsbefugnisse, würde jedoch die Ermächtigung des § 100a Abs. 1 S. 1 StPO zu einem stumpfen Schwert verkommen lassen. Um auch weiterhin eine effektive Strafverfolgung zu gewährleisten, muss somit eine Überwachung direkt an der Quelle, und noch vor erfolgter Verschlüsselung möglich sein. Bei der Nutzung eines Sprachassistenten würden dann durch das Mikrofon aufgezeichnete Audiosignale noch vor der verschlüsselten Übermittlung an den Server abgegriffen.

2) Verfassungsmäßigkeit des § 100a Abs. 1 S. 2 StPO n.F.

Zur technischen Umsetzung dieses Vorhabens ist die Installation einer Software zur Ausleitung der Kommunikation vor deren Verschlüsselung notwendig.[461] Hierfür eröffnen sich den Ermittlungsbehörden grundsätz-

457 *Bruns* in: KK-StPO, § 100a StPO, Rn. 37.

458 „*Viele Apple-Dienste verwenden eine Ende-zu-Ende-Verschlüsselung, was bedeutet, dass nur du auf deine Daten zugreifen kannst, und zwar nur auf vertrauenswürdigen Geräten, auf denen du mit deiner Apple-ID angemeldet bist.In einigen Fällen können deine iCloud-Daten auf den Servern von Drittanbietern – wie Amazon Web Services oder Google Cloud Platform – gespeichert werden, aber diese Partner haben nicht die Schlüssel, um deine auf ihren Servern gespeicherten Daten zu entschlüsseln*“, vgl. https://support.apple.com/de-de/HT202303 (zuletzt abgerufen am 31.10.2021).

459 BT-Drs. 18/12785, S. 48.

460 BT-Drs. 18/12785, S. 48.

461 *Bruns* in: KK-StPO, § 100a StPO, Rn. 42; *Bär* in: BeckOK-PolR Bayern, Art. 42 PAG, Rn. 93.

lich zwei verschiedene Wege. Da § 100a Abs. 1 StPO keine Erlaubnis zum Betreten einer Wohnung beinhält, bleibt letztlich nur die Infiltration des Systems über das Internet. Hierüber kann zum einen unter Ausnutzung bestehender Sicherheitslücken des Systems ein Trojanisches Pferd aufgespielt werden.[462] Andernfalls ist eine Infiltrationsmethode zu wählen, die eine aktive Aktion des Betroffenen erfordern. Beispielweise kann mittels eines per E-Mail verschickten Anhangs, welcher den Empfänger zum Öffnen animiert, der Trojaner installiert werden.[463]

Hinsichtlich des grundrechtlichen Schutzes der Betroffen solcher infiltrierter technischer Systeme hob das Bundesverfassungsgericht in seiner Entscheidung zur Online-Durchsuchung aus dem Jahr 2008 hervor, dass das allgemeine Persönlichkeitsrecht auch ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sog. IT-Grundrecht) enthält.[464] Dies war erforderlich, da das Gericht den bisherigen Grundrechtsschutz zum Schutz informationstechnische Systeme, „*die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten*“[465] nicht für genügend erachtete. Art. 13 GG biete weder Schutz vor Zugriffen gegen die Infiltration eines informationstechnischen Systems noch vor einer Datenerhebung aus den Datenspeichern, selbst wenn sich dieses System in der eigenen Wohnung befinde.[466] Anders als das Grundrecht auf informationelle Selbstbestimmung, das vor der einzelnen Datenerhebung als solcher schützt[467], soll das IT-Grundrecht den Einzelnen vor einem Zugriff auf die Gesamtheit der in informationstechnischen Systemen umfangreich vorhandenen persönlichen Daten bewahren.[468] Auch das aus dem allgemeinen Persönlichkeitsrecht abgeleitete Recht auf informationelle Selbstbestimmung, das zwar Gefährdungen für die Persönlichkeitsentfaltung verhindern soll, kann im Falle der Infiltration eines informationstechnischen Systems diesen Schutz möglicherweise nicht immer bieten. Beim Zugriff auf ein komplettes System stehen dem Zugreifenden äußerst große und aussagekräftige Datenbe-

462 *Popp*, ZD 2012, 51, 52; *Skistims/Roßnagel*, ZD 2012, 3, 3 f.
463 *Hansen/Pfitzmann*, DRiZ 2007, 225, 227.
464 BVerfGE 120, 274 ff.
465 BVerfGE 120, 274, 314.
466 BVerfGE 120, 274, 310.
467 *Gersdorf* in: BeckOK-InfoMedienR, Art. 2 GG, Rn. 17 f.
468 BVerfGE 120, 274, 313.

stände zur Verfügung. Das Gewicht eines solchen Zugriffs für die eigene Persönlichkeit gehe weit über das einzelner Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, hinaus.[469] Ein solcher Eingriff in die Integrität eines informationstechnischen Systems, stellt daher im Gegensatz zur klassischen Telefonüberwachung beim Telekommunikationsanbieter ein qualitatives Mehr dar, weshalb ein solcher Eingriff naturgemäß schwerer wiege.[470][471] Mit der Infiltration eines informationstechnischen Systems zum Zweck der Quellentelekommunikationsüberwachung sei bereits der Grundstein gelegt, um das System insgesamt zu durchleuchten. Hierdurch komme es zu einer Gefährdungssituation, die weit über die hinausgehe, die mit einer bloßen Überwachung der laufenden Telekommunikation einhergehen würde.[472] Den damit einhergehenden spezifischen Gefährdungen der Persönlichkeit des Einzelnen mitsamt der Möglichkeit der Strafverfolgungsbehörden ein komplettes Persönlichkeitsprofil zu erstellen, könne das Fernmeldegeheimnis allein nicht oder nicht hinreichend begegnen.[473] Ein tatsächlicher Eingriff in ein informationstechnisches System im Sinne einer Eröffnung des Schutzbereichs des IT-Grundrechts ist jedoch nur dann anzunehmen, wenn durch die Infiltration des Systems eine Datenfülle gewonnen werden könnte, die einen tiefen Einblick in die persönlichen Lebensverhältnisse des Einzelnen gewährt.[474] Hiervon ist nur dann auszugehen, wenn das Zielsystem komplett durchleuchtet werden soll und auch bereits gespeicherte Daten gescannt werden. Sofern die Ermittlungsbehörden lediglich auf „laufende", aber aufgrund fortschreitender Technik verschlüsselte Kommunikation zugreifen, darf das informationstechnische System daher derart infiltriert werden, dass zwar eine Ausleitung laufender Kommunikation möglich ist,

469 BVerfGE 120, 274, 313.
470 *Stadler*, MMR 2012, 18, 19; *Popp*, ZD 2012, 51, 53.
471 Aufgrund dieses Umstands und weil die §§ 100a, b StPO a.F. keine Einschränkung dahingehend enthielten, dass lediglich laufende Telekommunikation aufgezeichnet werden dürfe, konnten diese Normen vor Schaffung des § 100a Abs. 1 S. 2 StPO aufgrund eines Verstoßes gegen den Wesentlichkeitsvorbehalt, der den Gesetzgeber verpflichtet, für eingriffsintensive Maßnahme eine gesetzliche Grundlage zu schaffen, keinesfalls als Befugnisnorm für eine Quellentelekommunikationsüberwachung herangezogen werden. Somit war es nur folgerichtig, dass mit § 100a Abs. 1 S. 2 StPO hierzu eine neue Befugnis geschaffen wurde. A.A. LG Landshut, Beschluss vom 20.1.2011 – 4 Qs 346/10; *Bär*, MMR 2011, 691, 692 f.
472 BVerfGE 120, 274, 308.
473 BVerfGE 120, 274, 309.
474 BVerfGE 120, 274, 313 ff.

jedoch nicht auf gespeicherte Inhalte zugegriffen und diese durchleuchtet werden können. Sodann liegt kein Eingriff in das IT-Grundrecht vor, sondern lediglich ein solcher in das Telekommunikationsgeheimnis des Art. 10 GG.[475] Das Telekommunikationsgeheimnis sieht sich in einem solchen Fall lediglich den Gefährdungen gegenüber, für die das Grundrecht ursprünglich geschaffen wurde: Den Schutz laufender Telekommunikation.

Problematisch bleibt, dass die Eingriffsintensität der Quellen-TKÜ über die des herkömmlichen Anwendungsfalls des § 100a Abs. 1 S. 1 StPO hinausgeht. Es kommt zu einem Zugriff auf die Telekommunikation bereits auf dem Gerät des Betroffenen, also schon unmittelbar vor einem eigentlich erforderlichen dynamischen Übermittlungsvorgang. Dies lässt leichte Parallelen zur Online-Durchsuchung erkennen. Der entscheidende Unterschied zu einer Parallelität mit der Online-Durchsuchung liegt allerdings darin, dass auch § 100a Abs. 1 S. 2 StPO lediglich den Zugriff auf „laufende" Kommunikation erlaubt. Die Infiltration des Systems darf technisch lediglich zulassen, die zum aktuellen Zeitpunkt ausgehende Kommunikation vor deren Verschlüsselung auszuleiten. Hingegen darf nicht auch auf gespeicherte Daten oder sonstige auf dem System gespeicherte Kommunikation zugegriffen werden.[476] Auch nach der Implementierung solcher gesetzlichen Schranken, die verbieten auf ruhende Kommunikation zuzugreifen, bestehen Bedenken, dass diese nicht garantieren können, dass tatsächlich lediglich auf „laufende" Telekommunikation zugegriffen wird.[477] Hierzu hat das BVerfG hinsichtlich dem präventiv angelegten Pendant zur Quellentelekommunikation in Form des § 20l Abs. 2 BKAG a.F. entschieden, dass „*ob oder wie sich durch technische Maßnahmen sicherstellen lässt, dass ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet wird, […] die Anwendung der Norm, nicht aber ihre Gültigkeit [betrifft].*

475 BVerfGE 141, 220, Rn. 228; *Buermeyer*, StV 2013, 470, 473.

476 BT-Drs. 17/12541, S. 78; hinsichtlich der technischen Möglichkeit dieser Begrenzung siehe *Fox,* Stellungnahme, S. 8. Danach kann der Leistungsumfang einer installierten Durchsuchungssoftware erheblich variieren und auf verschiedene Funktionen, wie beispielsweise auf das Abfangen von gesendeten und empfangenen elektronischen Nachrichten, mithin dem Anwendungsfall der Quellentelekommunikation, begrenzt und ausgeweitet werden.

477 Diese technischen Zweifel beziehen sich darauf, dass bei der Scannung eines Systems keine Selektion zwischen gespeicherten Daten und gespeicherten übertragenen Daten, die sodann einer ehemals laufenden Telekommunikation zuzuordnen wären, möglich ist, da die auf dem Rechner bereits gespeicherten Daten keine eindeutigen und verlässlichen Kennzeichnungen verschiedener Dateninhalte enthalten, vgl. *Freiling*, Stellungnahme, S. 6.

[…] Das Gesetz lässt jedenfalls keinen Zweifel, dass eine Quellen-Telekommunikationsüberwachung nur bei einer technisch sichergestellten Begrenzung der Überwachung auf die laufende Telekommunikation erlaubt ist".[478] Allein der Umstand, dass infolge eines Missbrauchs oder ähnlichem bei der durchgeführten Infiltration die Gefahr eines vollständigen Durchleuchtens besteht, stellt daher eine bloße Frage der Gesetzesanwendung dar und lässt die Gültigkeit der Norm unberührt. Diesen Anforderungen kommt § 100a Abs. 5 Nr. 1a StPO nach, der inhaltsgleich zum alten § 20l Abs. 2 BKAG a.F. formuliert ist.

Die Schaffung des § 100a Abs. 1 S. 2 StPO entbindet jedoch nicht von einer exakten Prüfung, ob es sich bei dem Verhalten, auf welches zugegriffen werden soll, um Telekommunikation im Sinne des § 100a StPO handelt. Denn die Gesetzesänderung diente ausschließlich dazu, mit den technischen Entwicklungen der Informationstechnik Schritt zu halten und – ohne auf gespeicherte Daten des informationstechnischen Systems zuzugreifen – eine Telekommunikationsüberwachung auch dort durchführen zu können, wo diese auf Basis der alten Überwachungstechnik ansonsten nicht mehr realisierbar gewesen wäre.[479] Insofern kann auf die verschiedenen Interpretationsmöglichkeiten zum Telekommunikationsbegriff verwiesen werden. Mithin liegt bei einer vorzuziehenden strafprozessualen Ausgestaltung des Telekommunikationsbegriffes auch hier keine Telekommunikation vor. Fraglich ist jedoch, zu welchem Ergebnis in dieser Fallgestaltung, die vor allen Dingen von der Rechtsprechung favorisierte technikorientiere Auffassung gelangen würde. Schließlich erfolgt der eigentliche Zugriff vor der Verschlüsselung und damit vor dem Aussenden dieser Daten.[480] Bei strikter Zugrundelegung der Legaldefinition aus § 3 Nr. 22 TKG erscheint es daher zunächst schwierig, im Zugriff vor der verschlüsselten Übertragung bereits ein Aussenden, Übermitteln oder Empfangen von Signalen zu erblicken. Vielmehr ähnelt der Zugriff im Rahmen der Quellen-Telekommunikationsüberwachung einem Zugriff im zeitlichen Stadium, zu dem sich die Daten noch auf dem Gerät vor Ort befinden. Für einen Zugriff vor der Übertragung wurde allerdings bereits dargelegt, dass mangels eines dynamischen Übermittlungsvorgangs ein Zugriff direkt auf das Gehäuse sowohl nach der rein technischen als auch nach der technikorientierten Auffassung ausscheiden müsse. Allerdings würde eine solche restriktive Auslegung den Sinn und Zweck des neu

478 BVerfGE 141, 220, Rn. 234.
479 GesBegr. BT-Drs. 18/12785, S. 50.
480 *Becker/Meinicke*, StV 2011, 50, 51.

geschaffenen § 100a Abs. 1 S. 2 StPO vereiteln. Ziel der Quellen-TKÜ ist schließlich gerade die Überwachung von Telekommunikation direkt an der Quelle, noch bevor diese vor der Übertragung verschlüsselt werden kann.[481] Die Rechtsprechung hat sich seit Einführung des § 100a Abs. 1 S. 2 StPO hierzu noch nicht geäußert, es ist jedoch anzunehmen, dass sie dieses dogmatische „Problemchen" unter Berufung auf Sinn und Zweck der Gesetzesänderung löst. Gleichwohl würde sich bei Zugrundelegung des vorzuziehenden personell-individuellen Telekommunikationsbegriffes diese Frage freilich schon gar nicht stellen. Da der Zugriff unmittelbar vor Verschlüsselung der Daten erfolgt und diese sich im nächsten Moment im Übermittlungsvorgang befinden, würde dieser Umstand das Vorliegen von Telekommunikation nicht hindern. Im Gesamten entspricht § 100a Abs. 1 S. 2 StPO daher den verfassungsrechtlichen Vorgaben.

3) Informationstechnisches System

a) Allgemeines

Obwohl sich das Bundesverfassungsgericht in der Entscheidung zur Online-Durchsuchung ausgiebig zum IT-Grundrecht äußerte, hielt sich das Gericht mit Ausführungen zum Begriff des informationstechnischen Systems zurück. Überblicksartig wurde darauf verwiesen, dass die Informationstechnik einen beträchtlichen Teil im Leben der Bevölkerung einnehme und sich in einer Vielzahl der Gegenstände befinden, die die Bürger täglich umgeben.[482] Diese oberflächliche Beschreibung ist dahingehend zu präzisieren, dass ein informationstechnisches System selbst im Rahmen des Datenverarbeitungsprozesses neben den gespeicherten Daten des Nutzers weitere Daten erzeugen muss, die gleichfalls hinsichtlich seines Verhaltens ausgewertet werden können.[483] In der Literatur wird die Rechtsprechung des Bundesverfassungsgericht teilweise derart verstanden, dass nur solche Systeme, die einen äußerst großen und aussagekräftigen Datenbestand aufweisen und somit Rückschlüsse auf wesentliche Teile der Lebensgestaltung ermöglichen, als informationstechnische Systeme zu verstehen seien.[484] Dieser Schluss geht jedoch fehl. Das Bundesverfassungsgericht

481 BT-Drs. 17/12541, S. 78.
482 BVerfGE 120, 274, 304.
483 *Hauck* in: LR-StPO, § 100a StPO, Rn. 101.
484 *Hauck* in: LR-StPO, § 100a StPO, Rn. 102.

hat diese Formel lediglich zur Abgrenzung des allgemeinen Persönlichkeitsrechts in Form des Rechts auf informationelle Selbstgestaltung und des IT-Grundrechts verwendet. Ein informationstechnisches System kann jedoch sowohl in dem einen als auch in dem anderen Fall vorliegen und betroffen sein. Im von der „Gegenauffassung" zitierten Urteil formuliert das BVerfG an der entsprechenden Stelle sogar ausdrücklich, dass „*nicht jedes informationstechnische System […] des besonderen Schutzes durch eine eigenständliche pesönlichkeitsrechtliche Gewährleistung [bedarf]*".[485] Dadurch wird deutlich, dass auch ein informationstechnisches System betroffen sein kann, ohne dass der Schutzbereich des IT-Grundrechts eröffnet ist. Eine Infiltration eines informationstechnischen Systems wird erst dann einen Eingriff in das strengeren Rechtfertigungsanforderungen unterworfene IT-Grundrecht darstellen[486], wenn dadurch eine Vielzahl persönlichkeitsrelevanter Daten über die eigene Lebensgestaltung gewonnen würden. Dies wird regelmäßig erst bei einem Zugriff auf eine komplette, auf einem informationstechnischen System ruhende Datensammlung der Fall sein.

b) Doppelnatur

Auch der Begriff des informationstechnischen Systems offenbart – ähnlich zum Begriff der Telekommunikation aus § 100a StPO – eine Doppelnatur. Auf der einen Seite stellt das informationstechnische System das Schutzgut des IT-Grundrechts dar, was aus einer verfassungsrechtlichen Perspektive betrachtet wiederum ein weites Begriffsverständnis für angezeigt erscheinen lässt. Auf der anderen Seite handelt es sich um das Zugriffsobjekt einer strafprozessualen Ermittlungsmethode, was wiederum ein eher enges Verständnis erforderlich macht.[487]

485 BVerfGE 120, 274, 313.

486 Vgl. *Hoffmann-Riem*, JZ 2008, 1009, 1015, wonach durch die Schaffung des IT-Grundrechts der Schutzumfang der informationellen Selbstbestimmung nicht auf weitere Schutzdimensionen ausgedehnt wird, sondern dieser nötige und weitergehende Schutz in der grundrechtlichen Konkretisierung des IT-Grundrechts über strengere Anforderungen verwirklicht wird.

487 *Hauck* in: LR-StPO, § 100a StPO, Rn. 103 f.

aa) Begriffsverständnis im Sinne des § 100a Abs. 1 S. 2, 3 StPO

Teilt man den Begriff des informationstechnischen Systems in die beiden begrifflichen Einzelteile, so muss es sich bei einem System um eine Einheit technischer Anlagen handeln, die einer gemeinsamen Funktion dienen. Unter Informationstechnik ist die elektronische Informations- und Datenverarbeitung zu verstehen, womit sowohl Vorgänge der Kommunikation als auch solche der Datenverarbeitung umfasst sind.[488] Im Zuge einer systematischen und im Lichte des § 100a StPO erfolgten Auslegung wird vorgeschlagen, den Begriff des informationstechnischen Systems § 100a Abs. 1 S. 2 und 3 StPO ebenfalls kommunikationsbezogen auszulegen. Das informationstechnische System müsste daher konkret zu Kommunikationszwecken herangezogen werden.[489] Dieser Versuch einer Einengung des Begriffs wirkt in gewisser Weise gekünstelt und ist in Anbetracht dessen, dass § 100a Abs. 1 S. 2 StPO ohnehin nur für die Aufzeichnung von Kommunikationsvorgängen herangezogen werden darf auch inhaltsleer. Aufgrund dieser Voraussetzung wird ein informationstechnisches System ohnehin nur Ziel etwaiger Ermittlungsmaßnahmen sein, wenn sich hiervon Kommunikationsinhalte erhofft werden. Zwangsläufig weist das System sodann einen Telekommunikationsbezug auf, sodass diese zusätzliche Beschränkung auf Ebene des informationstechnischen Systems nicht erforderlich ist. Der Begriff ist vielmehr im Einklang mit seinem Wortlaut rein technisch zu verstehen. Das Endgerät zur Nutzung eines Sprachassistenten stellt daher aufgrund der verbauten Hard- und Software mitsamt der Technik zur Übertragung an die Serverzentren und der damit einhergehenden Datenverarbeitung in Form der Übermittlung ein informationstechnisches System dar.

bb) Server des Dienstleistungsanbieters als informationstechnisches System

Sofern sich die Daten nicht auf der lokalen Hardware befinden, sondern ein Zugriff auf die Server des Dienstleistungsanbieter erforderlich ist, ist fraglich, ob es sich auch bei diesem Server um ein informationstechnisches System handelt. Auf den ersten Blick scheint dies zuzutreffen, schließlich handelt es sich bei einem Server um ein hochkomplexes System, auf

488 Vgl. zum Ganzen *Hauck* in: LR-StPO, § 100a StPO, Rn. 105.
489 *Hauck* in: LR-StPO, § 100a StPO, Rn. 107.

welchem zudem die eigentliche Datenverarbeitung stattfindet. Dennoch könnte in Anbetracht der geplanten Infiltration eines Servers an eine Reduktion des Begriffs „informationstechnisches System" zu denken sein.[490] Für eine solche Erforderlichkeit streite, dass die kryptografischen Schlüssel zur Entschlüsselung stets nur den kommunizierenden Parteien bekannt sein dürften und die Dienstleistungsanbieter nicht dazu gezwungen werden dürften, den Schlüsselaustausch einer sich aufbauenden Verschlüsselung zu beeinträchtigen, wodurch sie selbst die bei der Nutzung ihres Systems garantierte Verschlüsselung der Nachrichtenübermittlung umgehen würden.[491] Dass die Unternehmen so ihre eigene geheimen Verschlüsselungen entschlüsselbar machen würden, stehe im Widerspruch zu den Eckpunkten deutscher Kryptopolitik.[492] Diese Kritik vermag jedoch nicht zu überzeugen. Ob die Strafverfolgungsbehörden die Daten vor der Verschlüsselung am Gerät des Betroffenen oder nach erfolgter Übertragung und Entschlüsselung aus den Servern ableiten ist sowohl hinsichtlich der Eingriffsintensität als auch hinsichtlich praktischer Folgen für den betroffenen Bürger ohne Unterschied. Es obliegt dem Staat hinsichtlich der gewonnenen Schlüssel mit der notwendigen Vorsicht zu agieren, sodass die Server des infiltrierten Dienstleistungsanbieters nicht durch unbefugte Dritte ebenfalls ausgelesen werden können. Das Bestehen einer solchen praktischen Gefahr kann jedoch nichts an der Möglichkeit ändern, auch auf Cloud-Server als informationstechnisches System zugreifen zu können. Entsprechend hat auch das BVerfG die Cloud als informationstechnisches System i.S.d. des § 20k Abs. 1 BKAG a.F. anerkannt.[493]

4) Ergebnis

Zwar sind sowohl das Endgerät als auch der Sprachassistent als informationstechnisches System im Sinne des § 100a Abs. 1 S. 2 StPO einzuordnen und damit grundsätzlich einer Quellen-Telekommunikationsüberwachung zur Umgehung einer Datenverschlüsselung zugänglich. Um unter Wahrung des Gesetzesvorbehalts im Rahmen der Quellen-Telekommunikationsüberwachung Daten abzufangen, müssten jedoch auch die übrigen

490 *Hauck* in: LR-StPO, § 100a StPO, Rn. 114; *Chaos Computerclub*, Stellungnahme, S. 18 f.
491 *Chaos Computerclub*, Stellungnahme, S. 18.
492 *Chaos Computerclub*, Stellungnahme, S. 18.
493 BVerfGE 141, 220, Rn. 209.

Voraussetzungen der Ermächtigungsgrundlage erfüllt sein. Zur rechtmäßigen Anordnung der Maßnahme müsste daher stets Telekommunikation im Sinne des § 100a StPO vorliegen. Nach zutreffendem strafprozessualem Begriffsverständnis ist dies bei der Nutzung eines Sprachassistenten jedoch nicht der Fall, sodass auch § 100a Abs. 1 S. 2 StPO als Ermächtigungsgrundlage ausscheidet.

III) § 100a Abs. 1 S. 3 StPO n.F.

1) Allgemeines

Eine im Kontext des § 100a StPO nicht zu erwartende Vorschrift wurde durch das am 24.08.2017 in Kraft getretene Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens in Form des § 100a Abs. 1 S. 3 StPO eingefügt.[494] Damit können nun auch auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können. Neben dem naheliegenden Fall des Zugriffs auf die Hardware des Endgeräts des betroffenen Nutzers, stellt sich zudem die Frage, ob über § 100a Abs. 1 S. 3 StPO auch die Daten nach erfolgter Entschlüsselung und Speicherung auf dem Server des Dienstleistungsanbieters abgegriffen werden könnten. Für ein solches Vorgehen gegen den Dienstleistungsanbieter müsste dieser als Betroffener angesehen werden. Betroffener in § 100a Abs. 1 S. 3 StPO könnte grundsätzlich auf zwei verschiedene Arten zu verstehen sein. Zum einen könnte mit Betroffener der Beschuldigte gemeint sein, gegen den Erkenntnisse gesammelt werden sollen und der daher vom Ergebnis der Erkenntnissammlung „betroffen" ist. Zum anderen könnte der Betroffene auch sein, in wessen Rechte die Zwangsmaßnahme eingreift. Für diesen Fall könnte Betroffener eines Eingriffs sowohl der Absender und Empfänger als auch der Dienstleistungsanbieter sein. Eine Antwort auf diese Frage gibt das Gesetz letztlich selbst: § 100a Abs. 3 StPO bestimmt, dass sich eine Maßnahme gegen den Beschuldigten sowie unter bestimmten Voraussetzungen auch gegen einen Nichtbeschuldigten richten könne. Von dem Nichtbeschuldigten müsste zu erwarten sein, dass er für den Beschuldigten bestimmte oder

494 Vgl. BGBl. 2017 I 3202.

von ihm herrührende Mitteilungen entgegennimmt oder weitergibt oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt. Für die Nutzung eines Sprachassistenten von Bedeutung ist dabei die letzte Alternative der Nutzung eines informationstechnischen Systems. Insofern könnte der Nutzer indem er an den Sprachassistent Befehle erteilt diesen als informationstechnisches System nutzen, welches der Dienstleistungsanbieter zur Verfügung stellt. In diesem Fall könnten die Strafverfolgungsbehörden auf die dort gespeicherten Informationen nach deren Entschlüsselung zugreifen. Sowohl in diesem Fall als auch beim Zugriff auf die Hardware vor Ort wäre jedoch weitere Voraussetzung, dass diese Kommunikation auch während des laufenden Übertragungsvorgangs aufgezeichnet werden dürfte. Unter Zugrundelegung des vorzuziehenden personell-individuellen Telekommunikationsbegriffs wäre dies jedoch wie gesehen nicht möglich, sodass sich an dieser Stelle, weitere Ausführungen erübrigen.

2) Verfassungsmäßigkeit der Vorschrift

Sofern die Rechtsprechung jedoch einem technikorientierten Kommunikationsverständnis zugeneigt ist und daher die Nutzung eines Sprachassistenten unter § 100a Abs. 1 StPO fassen müsste, würde ein Zugriff nach § 100a Abs. 1 S. 3 StPO in Betracht kommen. Gegen diese neu gefasste Vorschrift und damit auch gegen den sich auf § 100a Abs. 1 S. 3 StPO stützenden Zugriff müssen jedoch erhebliche verfassungsrechtliche Bedenken erhoben werden.

a) Keine Begrenzung auf laufende Telekommunikation

Im Unterschied zu § 100a Abs. 1 S. 1 StPO, der den Zugriff auf unverschlüsselte bzw. im Falle des § 100a Abs. 1 S. 2 StPO auf verschlüsselte Kommunikation erlaubt, rechtfertigt § 100a Abs. 1 S. 3 StPO einen weitergehenden Zugriff auch auf bereits vergangene und damit abgeschlossene Kommunikationsinhalte, deren Übertragungsvorgang bereits vollständig abgeschlossen ist und die auf einem hierzu benutzten informationstechnischen System gespeichert sind.[495] Insofern ist jedoch zu beachten, dass nach der Auffassung des BGH auch § 100a Abs. 1 S. 1 StPO einen Zugriff

495 *Bruns* in: KK-StPO, § 100a StPO, Rn. 44.

auf bereits ruhende Kommunikationsinhalte außerhalb eines Kommunikationsvorgangs rechtfertige, sofern diese nicht im alleinigen Herrschaftsbereich des Betroffenen gespeichert sind.[496] Im Übrigen stehen § 94 StPO und § 100a StPO in keinem Exklusivitätsverhältnis, sodass es unschädlich sei, dass das BVerfG in seiner IMAP-Entscheidung[497] entschied, dass beim Provider gespeicherte E-Mails auch mit der offenen Maßnahme des § 94 StPO beschlagnahmt werden können.[498] Ein Zugriff auf ruhende Kommunikationsdaten über § 100a StPO sei daher unter der genannten Voraussetzung auch wegen der im Vergleich zur Beschlagnahme deutlich strengeren Anforderungen im Wege eines Erst-Recht-Schlusses zulässig.[499] Die fehlende Begrenzung hinsichtlich laufender Kommunikation dürfte aus Sicht des BGH im Rahmen des § 100a Abs. 1 S. 3 StPO daher unschädlich sein. Gleichwohl ist kritisch zu sehen, dass § 100a Abs. 1 S. 3 StPO der Verwässerung des in der StPO tradierten Regelungskonzept Vorschub leistet. Von den Grundsätzen dieses Regelungskonzeptes ausgehend sollte § 100a Abs. 1 S. 1 und S. 2 StPO eine Eingriffsermächtigung für die heimliche Überwachung laufender Kommunikation darstellen. Diesen Ausgangsgedanken des historischen Gesetzgebers weichte der BGH bereits in der o.g. Entscheidung auf. Dagegen sollte die heimliche Durchsuchung ruhender – sich außerhalb eines Kommunikationsvorgangs – befindlicher Daten unter den Regelungsgehalt des § 100b StPO mitsamt dessen strengeren Voraussetzungen fallen.

---

496 BGH, NJW 2021, 1252, 1554; BGH, NJW 2009, 1828.

497 BVerfGE 124, 43 ff.

498 BGH, NJW 2021, 1252, 1554. Insofern wies auch bereits das BVerfG auf die bestehenden verschiedenen Möglichkeiten eines Zugriffs auf solche Daten nach § 94 StPO oder § 100a StPO hin, ohne dies jedoch abschließend zu bewerten, vgl. BVerfGE 124, 43, 60.

499 BGH, NJW 2021, 1252, 1554: kritisch zu dieser Begründung vgl. *Grözinger*, NStZ 2021, 358 f.; *Hiéramente* WiJ 2021, 19, 21 f. Der durch den BGH vorgenommene Erst-Recht-Schluss, komme vor dem Hintergrund des gänzlich unterschiedlichen Regelungsgehalts des § 94 StPO (Beschlagnahme) und des § 100a StPO (Überwachung) nicht in Betracht. Im Übrigen ist lediglich aufgrund des insofern zustimmungswürdigen Umstandes, dass die §§ 94 StPO und 100a StPO in keinem Exklusivitätsverhältnis stehen noch nicht gesagt, dass eine Ermittlungsmaßnahme nach § 100a Abs. 1 S. 1 StPO auch solche E-Mails umfasst, die zum Zeitpunkt des Zugriffs bereits versandt oder empfangen wurden, aber noch beim Provider gespeichert sind. Die Beantwortung dieser Frage richtet sich einzig nach den konkreten tatbestandlichen Voraussetzungen der Ermächtigungsgrundlage, vgl. zutreffend *Trüg*, JZ 2021, 560, 564. Vgl. hierzu auch oben Fn. 401.

b) Verstoß gegen die Maßstäbe des IT-Grundrechts

Wenig überraschend rückt die Vorschrift durch den Zugriff auf Vergangenes besonders in den Dunstkreis der Online-Durchsuchung nach § 100b StPO. Aus technischer Sicht kann diese Form der Quellentelekommunikationsüberwachung bereits nicht mehr von einer Online-Durchsuchung unterschieden werden. In dem einen wie dem andern Fall erfolgt eine Infiltration des Zielsystems zur Scannung sämtlicher gespeicherter Inhalte und damit ein Eingriff in die Integrität und Vertraulichkeit informationstechnischer Systeme. Trotz dieser Gleichheit mit § 100b StPO dürfen die Daten bei Heranziehung des § 100a Abs. 1 S. 3 StPO unter den niedrigeren Voraussetzungen des § 100a StPO ausgelesen werden.[500] Möglicherweise steht der neu eingefügte § 100a Abs. 1 S. 3 StPO diesbezüglich in einem Widerspruch zur Rechtsprechung des Bundesverfassungsgerichts hinsichtlich des IT-Grundrechts. Wie gesehen soll nicht die Infiltration eines jeden IT-Systems vom Schutzbereich des Grundrechts umfasst sein, sondern nur solche, die eine Datenfülle aufweisen, die einen tiefen Einblick in die persönlichen Lebensverhältnisse des Einzelnen gewährt.[501] Ferner müssen die Daten einen Persönlichkeitsbezug aufweisen und in der Vertraulichkeit auf Geheimhaltung preisgegeben worden sein.[502] Eine solche erhebliche Datenmenge wie für die Einschlägigkeit des IT-Grundrechts erforderlich, wird nur dann betroffen sein, wenn gerade auch auf Daten zugegriffen wird, die über einen längeren Zeitraum gespeichert und somit für die Zukunft konserviert wurden. Auch auf solche konservierten Daten soll über § 100a Abs. 1 S. 3 StPO zugegriffen werden. Aufgrund der umfangreichen betroffenen Datenmengen, die nicht nur den aktuellen Kommunikationsinhalt wiedergeben, sondern auch sämtliche in der Vergangenheit liegende Kommunikationsinhalte offenbaren, darf der Zugriff hierauf nur nach Maßgabe des strengeren § 100b StPO erfolgen. Dies gilt jedoch nur, sofern die Daten im alleinigen Herrschaftsbereich des Betroffenen gespeichert sind. So führt das BVerfG in seiner Entscheidung zur Online-Durchsuchung aus, dass ein Eingriff dann nicht mehr an Art. 10 GG zu messen ist, wenn die Daten nach Abschluss eines Kommunikationsvorgangs im alleinigen Herrschaftsbereich[503] eines Kommunikati-

500 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 9.
501 BVerfGE 120, 274, 314.
502 *Luch*, MMR 2011, 75, 75.
503 Um einen solchen alleinigen Herrschaftsbereich handelt es sich nicht im Falle eines E-Mail-Postfachs, auf das der Nutzer nur über eine Internetverbindung

onsteilnehmers verbleiben und dieser geeignete Schutzmaßnahen gegen einen Zugriff treffen kann.[504] Sofern jedoch die in der Folge einer Infiltration bewirkten spezifischen Gefährdungen der Persönlichkeit durch ein Zugriff auf einen kompletten Datenspeicher durch Art. 10 Abs. 1 GG nicht hinreichend begegnet werden können und daher ein Schutz durch das neu geformte IT-Grundrecht von Nöten ist[505], kann der Eingriff in dieses Grundrecht, welches gerade den erhöhten Gefährdungen Rechnung tragen soll, konsequenterweise nicht auch unter den gleichen Voraussetzungen des § 100a StPO erfolgen, die bereits für einen Eingriff in Art. 10 GG maßgeblich sind. Ansonsten würde eben jene höhere Gefährdung für persönlichkeitsrelevantere Informationen faktisch überhaupt nicht zum Ausdruck kommen. Es ist nicht zu erklären, weshalb Inhalte, die zwar während des Übermittlungsvorgangs gem. § 100a Abs. 1 S. StPO hätten abgegriffen werden können, sodann aber auf einem informationstechnischen System gespeichert bleiben, das dem *alleinigen* Macht- und Herrschaftsbereich des Betroffenen unterfällt, gleichwohl nach § 100a Abs. 1 S. 3 StPO abgreifbar sein sollen. Obwohl diese Daten nach § 100a Abs. 1 S. 3 StPO nicht während eines unsicheren Übertragungsweges oder auf einen fremdbeherrschten Speicherplatz abgegriffen werden und sie daher bei einer entsprechenden Persönlichkeitsrelevanz dem IT-Grundrecht unterfallen, kann der Eingriff unverständlicherweise nach den milderen Voraussetzungen des § 100a StPO erfolgen.

c) Verhältnismäßigkeit hinsichtlich des Straftatenkatalog

Dass § 100a StPO im Vergleich zu § 100b StPO eine deutlich niedrige Eingriffsschwelle besitzt, zeigt sich an diversen Punkten. So wird bereits bei einem Vergleich der jeweils in Absatz 2 aufgeführten Katalogtaten deutlich, dass für § 100a StPO im Verhältnis zu § 100b StPO bereits vermeintliche Bagatelldelikte genügen, um eine Anordnung nach § 100a StPO zu erteilen. So genügt für eine Anordnung nach § 100a StPO beispielsweise bereits der Anfangsverdacht hinsichtlich einer Bestechlichkeit und

zugreifen kann. Dieses unterfällt weiterhin dem Schutzbereich des Art. 10 GG, vgl. BVerfGE 124, 43, 54 f.; BGH NJW 2021, 1252, 1254. Anders ist dies dann, wenn die E-Mails ausschließlich auf dem Endgerät des Betroffenen gespeichert sind.

504 BVerfGE 120, 274, 307 f.

505 BVerfGE 120, 274, 309.

Bestechung von Mandatsträgern nach § 108e StGB oder Delikte aus der Abgabenordnung nach § 100a Abs. 2 Nr. 2 StPO. Die Möglichkeit bereits beim Vorliegen solcher Delikte von vergleichsweise untergeordneter Bedeutung in das IT-Grundrecht eingreifen zu können, widerspricht der Rechtsprechung des Bundesverfassungsgerichts, wonach Eingriffe in das IT-Grundrecht nur der Verfolgung von Straftaten dienen dürfen, die ein überragend wichtiges Rechtsgut schützen.[506] Hierzu zählen Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berühren.[507] Diesen Maßstäben genügt der Katalog des § 100a StPO freilich nicht, der bereits das bloße Vermögen, das Vertrauen in die staatliche Verwaltung oder die Integrität des Sports als schützenswertes Rechtsgut beinhaltet. Dass die in § 100a StPO und § 100b StPO aufgezählten Straftaten von unterschiedlichem Gewicht sind, zeigt sich zudem darin, dass § 100b Abs. 1 StPO von „besonders schweren" Straftaten spricht, während in § 100a Abs. 1 StPO lediglich von „schweren" Straftaten die Rede ist.

d) Erhöhte Eingriffsintensität

Dass auch dieser Unterschied im Zuge der Gesetzgebung durchaus bemerkt wurde, zeigt der Versuch, den neu gefassten § 100a Abs. 1 S. 3 StPO durch die Darstellung des Zugriffs nach Satz 3 als „funktionales Äquivalent"[508] zur herkömmlichen Telekommunikationsüberwachung zu rechtfertigen. Als funktionales Äquivalent soll die neue Befugnis deshalb zu verstehen sein, da durch diverse Schutzvorrichtungen sichergestellt werden soll, dass lediglich Telekommunikation vernommen wird, die als laufende Telekommunikation auch über § 100a Abs. 1 S. 1, 2 StPO hätte erhoben werden können.[509] An eben diesen Schutzvorrichtungen äußerten Sachverständige bereits vor einigen Jahren erhebliche Bedenken. Es sei technisch überhaupt nicht möglich auszuschließen, dass bei der Infiltration eines kompletten Systems tatsächlich nur entsprechende Kommunikationsdaten erhoben würden.[510] Selbst wenn man von der Wirksamkeit

506 BVerfGE 120, 274, 326.
507 BVerfGE 120, 274, 328.
508 Ausschuss-Drucksache 18(6)334, S. 20.
509 Ausschuss-Drucksache 18(6)334, S. 21.
510 BVerfGE 120, 274, 309.

dieser Einschränkungen ausginge, müsste unter Heranziehung der Rechtsprechung des Bundesverfassungsgerichts die Äquivalenz zwischen § 100a Abs. 1 S. 1, 2 StPO und § 100a Abs. 1 S. 3 StPO verneint werden. Als Frage der Gesetzesanwendung, nicht aber der Gesetzesgültigkeit[511], ist § 100a Abs. 1 S. 3 StPO möglicherweise auf schlicht funktionaler Ebene und unter einer ergebnisorientierten Betrachtungsweise ein entsprechendes Äquivalent zu § 100a Abs. 1 S. 1, 2 StPO, jedoch keinesfalls hinsichtlich der damit einhergehenden Eingriffsintensität.[512] Durch die Infiltration des gesamten Systems um dieses auch komplett zu durchleuchten, wird die Eingriffsintensität der einfachen Telekommunikationsüberwachung und auch der Quellentelekommunikationsüberwachung um ein Vielfaches überstiegen. Dies gründet neben dem Eindringen des Staates in den von der Außenwelt abgeschiedenen Hoheitsbereich auf einem weiteren informationstechnischen Argument. Die praktische Umsetzung der gesetzgeberisch angedachten Einschränkungen, dass lediglich Daten über Kommunikationsinhalte, die in zeitlicher Hinsicht nach der richterlichen Anordnung stattfanden, erfasst werden sollen, intensiviert den staatlichen Eingriff weiter. Um diese Prüfung überhaupt durchführen zu können, ist es erforderlich, dass der eingesetzte Trojaner zunächst alle gespeicherten Inhalte ausliest und auswertet, um sodann zu entscheiden, ob es sich um Telekommunikationsinhalte handelt, die auch in zeitlicher Hinsicht unter Beachtung des § 100a Abs. 5 Nr. 2 StPO durch § 100a Abs. 1 S. 3 StPO erhoben hätten werden dürfen.[513] Bereits dieser Schritt stellt allerdings eine dem Staat zurechenbare Kenntnisnahme und mithin eine durch den Staat erfolgte Online-Durchsuchung dar. Da es jedoch auch bei anderen Überwachungsmaßnahmen durchaus der Fall sei, zunächst den Gesamtbestand an Kommunikation zu überprüfen, bevor in einem weiteren Schritt nicht verwertbare Inhalte (z.B. wegen des Kernbereichsschutzes) ausgesondert werden, soll es sich bei der bloßen Analyse der Meta-Daten mittels der eingesetzten Software um keine Online-Durchsuchung handeln.[514] Allerdings

511 BVerfGE 141, 220, Rn. 234.

512 Siehe auch *Grözinger*, Die Überwachung von Cloud-Storage, S. 300.

513 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 17. Im Vergleich zum Fall des § 100a Abs. 1 S. 3 StPO ist der entscheidende Unterschied, dass der eingesetzte Trojaner im Rahmen des § 100a Abs. 1 S. 2 StPO gerade diesen Zwischenschritt nicht erbringen muss. Dort müssen keine ruhenden Daten danach untersucht werden, ob es sich bei Ihnen um Kommunikation handelt auf die zugegriffen werden könnte, sondern lediglich alle aktuell ausgehenden Daten vor deren Verschlüsselung ausgeleitet werden.

514 *Kraus*, Stellungnahme, S. 8.

liegt bereits durch die für eine Maßnahme nach § 100a Abs. 1 S. 3 StPO erforderliche Infiltration und kompletten Scannung des Systems und der damit einhergehenden Gefährdungssituation für die gesamten Daten des Betroffenen eine Online-Durchsuchung vor. Dass dabei der konkrete Inhalt der kontrollierten Daten noch nicht unmittelbar durch menschliche Personen erfasst wird, ist an dieser Stelle nicht von Bedeutung. Erfasst werden schließlich die Metadaten, die in Anbetracht ihrer Menge, die sich wiederum dadurch ergibt, dass durch § 100a Abs. 1 S. 3 StPO auf den gesamten Datenbestand zugegriffen werden muss, ebenso Rückschlüsse auf die Persönlichkeit des Betroffenen zulassen können und somit ebenfalls vom IT-Grundrecht erfasst sind. Zudem verkennt der Vergleich mit dem Kernbereichsschutz und der dabei erforderlichen Überprüfung des Gesamtdatenbestands, dass es hier auf einer früheren Stufe – vor Fragen der tatsächlichen Beweiserhebung- oder Beweisverwertbarkeit – um die Frage nach einer überhaupt tauglichen Eingriffsbefugnis hierzu geht. In diesem Kontext sind Argumente aus dem Bereich des Kernbereichsschutzes nicht dienlich. Der Vergleich hinkt daher und ist nicht zielführend. Vielmehr soll durch ein Vorgehen nach § 100a Abs. 1 S. 3 StPO lediglich mittels einer Online-Durchsuchung durch die Hintertür ausfindig gemacht werden, auf welche Daten sodann unter dem Schein der Gesetzeskonformität durch § 100a Abs. 1 S. 3 StPO zugegriffen werden kann.

Hinzu kommt, dass die gesetzgeberische Argumentation, dass es sich bei § 100a Abs. 1 S. 3 StPO um ein bloßes funktionales Äquivalent handle[515], auch aus einem weiteren Punkt fehlgeht. Wenn es der Gesetzgeber aufgrund der Ähnlichkeit sowie der hypothetisch bestandenen Möglichkeit auf diese Informationen sowieso hätte zugreifen zu können, auch bei früherer Kommunikation „*verfassungsrechtlich nicht [für] geboten [erachtet], die wegen der besonderen Sensibilität informationstechnischer Systeme [...] aufgestellten höheren Anforderungen des Bundesverfassungsgerichts [für Eingriffe in das IT-Grundrecht] anzuwenden*“[516], verkennt dies die Systematik des § 100a StPO. Bereits die in § 100a Abs. 1 S. 2 StPO eingefügte Quellentelekommunikationsüberwachung stellt eine Ausnahme dazu dar, dass der Einsatz eines Trojaners zur Infiltration eines Systems eigentlich nur unter den Voraussetzungen des § 100b StPO möglich ist.[517] Das Vorgehen der Bundesregierung erweckt jedoch den Anschein, als wolle sie eine bestehende Ausnahme im selbem Atemzug um eine weitere Ausnahme erweitern.

515 Ausschuss-Drucksache 18(6)334, S. 20.
516 Ausschuss-Drucksache 18(6)334, S. 20.
517 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 16.

Dabei können Ausnahmen ihrem Sinn nach „*gerade nicht analog angewendet werden, sondern sind restriktiv auszulegen*".[518]

e) Zwischenergebnis

Bei der Infiltration eines informationstechnischen Systems, auf welchem der Betroffene Kommunikationsdaten- und Inhalte gespeichert hat, die in seiner alleinigen Herrschaftssphäre stehen, ist, aufgrund des Zugriffs auf den kompletten Datenbestand, ein Eingriff in das neu geschaffene IT-Grundrecht anzunehmen. Ein solcher Eingriff kann nicht unter Heranziehung des § 100a Abs. 1 S. 3 StPO legitimiert werden. § 100a StPO kann beim Vorliegen seiner Voraussetzungen von vornherein lediglich Eingriffe in das Fernmeldegeheimnis aus Art. 10 GG und das aus dem allgemeinen Persönlichkeitsrecht entspringende Recht auf informationelle Selbstbestimmung legitimieren. Aus den dargelegten Gründen ist § 100a Abs. 1 S. 3 StPO, der diese verfassungsrechtliche Differenzierung mitsamt der Systematik der §§ 100a ff. StPO, missachtet, verfassungswidrig.

IV) Überwachung eines Sprachassistenten als Minusmaßnahme zu § 100a StPO

Vereinzelt wird in der Literatur die Frage aufgeworfen, ob eine Maßnahme, die nicht unter eine entsprechende Ermächtigungsgrundlage subsumiert werden kann, als sog. Minusmaßnahme dennoch zulässig sei.[519] Voraussetzung hierfür wäre, dass die Überwachung eines Sprachassistenten als eine im Vergleich zum klassischen Fall der Telekommunikationsüberwachung mildere Maßnahme klassifiziert werden kann. Würde man dies beispielsweise für die Überwachung des Surfverhaltens im Internet andenken, so wäre zu konstatieren, dass die Überwachung des Surfverhaltens keineswegs eine mildere, sondern vielmehr eine einschneidendere Maßnahme als die herkömmliche Telekommunikationsüberwachung darstellt.[520] Durch

518 Stellungnahme des Deutschen Anwaltvereins zu dem Gesetzentwurf der Bundesregierung – Drs.18/11272, S. 11; abrufbar unter: https://anwaltverein.de/de/newsroom/sn-44-17-einfuehrung-der-online-durchsuchung-und-quellen-tkue?file=files/anwaltverein.de/downloads/newsroom/stellungnahmen/2017/DAV-SN_44-17_%C3%84nderungsantrag.pdf (zuletzt abgerufen am 31.10.2021).

519 *Braun*, jurisPR-ITR 18/2013 Anm. 5; *Albrecht*, jurisPR-ITR 14/2013 Anm. 4.

520 *Hiéramente*, StraFo 2013, 96, 101.

die Überwachung des Surfverhaltens würden Informationen von solcher Qualität zusammengetragen, die es ermöglichten, umfassende Persönlichkeitsprofile zu erstellen. Durch die Auswertung des Surfverhaltens ließen sich umfassende Rückschlüsse auf die Persönlichkeit hinsichtlich sozialer Aktivitäten, sexueller Vorlieben, dem Gesundheitszustand und ähnlichem zusammentragen, die oftmals in dieser Detailgenauigkeit nicht einmal engsten Freunden und Familienangehörigen bekannt sein dürften.[521] Die Überwachung der Netzaktivitäten über einen längeren Zeitraum kann zur Erhebung einer Masse an personenbezogenen Daten führen, die ausgewertet eine Eingriffstiefe in die Persönlichkeitsrechte der Betroffenen vergleichbar mit einer Online-Durchsuchung erreichen können.[522] Die Überwachung der Netzaktivitäten stellt damit eine die Grundrechte des Betroffenen erheblich einschränkende Maßnahme dar. Aufgrund der dargestellten Ähnlichkeit dieses Falles zur Nutzung eines Sprachassistenten sind die Wertungen übertragbar. Selbst wenn ein Großteil der persönlichkeitsrelevanten Informationsverschaffung noch nicht über einen Sprachassistenten abgewickelt werden sollte, sondern noch über den klassischen Weg mit Tastatur und Computer erfolgt, können Sprachassistenten dennoch für die exakt gleichen Aufgaben herangezogen werden.

V) § 100b StPO

Nach § 100b Abs. 1 StPO darf auch ohne Wissen des Betroffenen mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und daraus Daten erhoben werden, wenn der Verdacht besteht, dass der Betroffene Täter einer in Absatz 2 genannten besonders schweren Straftat sein könnte, diese 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. Durch eine Infiltration der im Gehäuse verbauten Software oder des Sprachassistenten in Form des Severs des Dienstleistungsanbieters, könnte ein Zugriff auf gespeicherte Daten unter den Voraussetzungen des § 100b StPO möglich sein. Im Unterschied zu § 100a StPO steht hier nicht die Erfassung etwaiger Kommunikationsvorgänge, sondern eine vollumfängliche Ausforschung des infiltrierten informationstechnischen Systems im Vordergrund. Eine erforderliche Ermäch-

521 *Hiéramente*, StraFo 2013, 96, 100 f.
522 BVerfGE 120, 274, 324 f.

tigung hierzu fand sich in der Strafprozessordnung gleichwohl über viele Jahre nicht. Erst im Jahr 2017 kam es im Zuge der Reform zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, zur Schaffung der heutigen Eingriffsbefugnis. Diese erlaubt, dass ohne Wissen des Betroffenen in ein von diesem benutzten informationstechnischen System eingegriffen wird und Daten erhoben werden. Vor Kodifizierung dieser Norm war den Ermittlungsbehörden nur der offene Zugriff auf „ruhende" Daten im Rahmen der Durchsuchungs- und Beschlagnahmevorschriften, §§ 94 ff., 102 ff. StPO möglich.[523] § 100b StPO ergänzt die Ermittlungsmaßnahmen um eine Möglichkeit des verdeckten Zugriffs. Obgleich des Unterschiedes zwischen offener und verdeckter Durchsuchung, wurde die verdeckte Online-Durchsuchung mit dem Argument, dass dem Ermittlungsverfahren kein Offenheitsgrundsatz zu Grunde läge, unter Heranziehung des § 102 StPO ehemals selbst durch den BGH akzeptiert.[524] Mit Beschluss vom 25.11.2006 stellte ein Ermittlungsrichter jedoch fest, dass die verdeckte Online-Durchsuchung mangels laufender Kommunikation nicht auf § 100a StPO, mangels eines offenen Zugriffs nicht auf § 102 StPO und aufgrund der hohen Eingriffsintensität auch nicht auf die Ermittlungsgeneralklausel gestützt werden kann.[525] Diese Sichtweise fand in der Folge Zustimmung, sodass eine verdeckte Online-Durchsuchung lange Zeit als unzulässig betrachtet wurde.[526]

Entscheidendes Abgrenzungsmerkmal der Online-Durchsuchung zur Telekommunikationsüberwachung ist daher grundsätzlich die Bewegung der Daten und die damit korrelierende Frage, ob sich diese hierdurch in der „freien Umlaufbahn" (mit der Konsequenz eines geringeren Schutzes) befinden oder im Hoheitsgebiet der Privatsphäre des Einzelnen ruhen und daher besonders geschützt sind.

1) Infiltration des Endgeräts

a) Möglichkeiten der Infiltration

Die hierfür notwendige Infiltration des betroffenen Systems ist auf verschiedenen Wegen durchführbar. Es ließen sich die Systeme bereits bei

523 *Brodowski*, JR 2009, 402, 411.
524 Vgl. BGH, StV 2007, 60, 61; *Hofmann*, NStZ 2005, 121, 123.
525 BGHSt 51, 211, 218.
526 *Cornelius*, JZ 2007, 798, 799; *Valerius*, JR 2007, 275, 277.

der Fertigung mit entsprechenden Funktionen oder Sicherheitslücken ausstatten. Es bestünde dann jedoch die Gefahr, dass solche Sicherheitslücken nicht nur durch die Strafverfolgungsbehörden, sondern auch durch Unbefugte Dritte ausgenutzt würden. Auch die Gesetzesbegründung legt nahe, dass die Systeme nachträglich mit einem entsprechenden Programm infiltriert werden sollen.[527] Die nachträgliche Infiltration lässt sich in zwei verschiedene Möglichkeiten unterscheiden. Möglich ist zum einen ein physischer Zugriff auf das System, wozu die Wohnung betreten und die benötigte Software auf dem zu durchsuchenden System installiert wird.[528] In diesem Fall müsste § 100b StPO allerdings zum Betreten der Wohnung ermächtigen und damit einen Eingriff in Art. 13 GG rechtfertigen. Ausgehend von den Gesetzesmaterialien wird Art. 13 GG nicht als durch § 100b StPO einschränkbares Grundrecht genannt.[529] Daher wird zurecht angenommen, dass die Anordnung nach § 100b StPO nicht die Befugnis umfasst, die Wohnung des Betroffenen zum Zwecke der Infiltration des informationstechnischen Systems heimlich zu betreten.[530] Darüber hinaus ist eine Konstruktion dieser Befugnis über eine Annex-Kompetenz weder rechtlich zulässig noch erforderlich. Bei dem Betreten der Wohnung würde es sich um einen eigenständigen Grundrechtseingriff handeln, nicht jedoch um eine bloße Begleitmaßnahme der Online-Durchsuchung. Ferner stehen den Strafverfolgungsbehörden im Rahmen des § 100b StPO Möglichkeiten der Infiltration zur Verfügung, die Art. 13 GG nicht aufgrund des Zutritts zur Wohnung des Grundrechtsberechtigten tangieren.[531] Als ein solches Mittel ist hier ein Fernzugriff durch den Einsatz eines Staatstrojaner denkbar. Das Aufspielen eines solchen Trojaners könnte durch das Ausnutzen von unbemerkten Sicherheitslücken (sog. Zero-Day-Exploits) oder durch eine täuschende Manipulation des Nutzers, beispielsweise durch sog. Phishing, erfolgen, indem einem Nutzer infizier-

527 BT-Drs. 18/12785, S. 53.

528 *Soiné*, NStZ 2018, 497, 501; *Derin/Golla*, NJW 2019, 1111, 1112.

529 Vgl. *Soiné*, NStZ 2018, 497, Fn. 64.

530 ; *Soiné*, NVwZ 2012, 1585,1588 f., *ders*., NStZ 2018, 497, 501; *Derin/Golla*, NJW 2019, 1111,1112; *Singelnstein/Derin*, NJW 2017, 2646, 2647; *Graf* in: BeckOK-StPO, § 100a StPO, Rn. 117 auch hinsichtlich § 100a Abs. 1 S. 2 StPO; a.A. *Bruns* in: KK-StPO, § 100b StPO, Rn. 4, der eine Annexkompetenz bejaht, wenn keine anderen erfolgsversprechenden Möglichkeiten bestehen.

531 *Soiné*, NStZ 2018, 497, 500, der ferner davon ausgeht, dass von dem Verbot der heimlichen Wohnungsbetretung dann ausnahmsweise abgewichen werden könne, wenn außer einer Maßnahme nach § 100 b StPO zusätzlich eine Überwachung nach § 100c StPO besteht.

te Dateien übermittelt werden durch deren Öffnen sich das System selbst infiltriert.[532]

b) Infiltration des Endgeräts zur Online-Durchsuchung

Bei dem vom Betroffenen genutzten Endgerät handelt es sich zwar um ein informationstechnisches Gerät des Betroffenen im Sinne des § 100b StPO[533], jedoch sind in der Praxis auf der Software des Endgeräts in der Regel keine ruhenden Kommunikationsdaten gespeichert. Da eine solche Speicherung einen absoluten Ausnahmezustand darstellt, ist die Infiltration nach § 100b StPO zu direkten Informationsgewinnung von untergeordneter Bedeutung.

c) Infiltration des Endgeräts zur Online-Live-Überwachung

Von der Online-Durchsuchung kann begrifflich die Online-Überwachung, aber auch die Online-Live-Überwachung unterschieden werden. Während eine Online-Durchsuchung einen einmaligen punktuellen Zugriff auf die Daten eines informationstechnischen Systems umfasst, meint die Online-Überwachung eine Überwachung über einen bestimmten längeren Zeitraum.[534] Dabei besteht in Form der Online-Live-Überwachung für die Ermittlungsbehörden die Möglichkeit über das infiltrierte Endgerät ablaufende Aktivitäten in Echtzeit zu überwachen und so Kenntnis von gegenwärtig ablaufenden Vorgängen zu erhalten.[535] Noch zu klären ist, ob zur Ermöglichung einer solchen Live-Überwachung technische Funktionen des Endgeräts durch die Strafverfolgungsbehörden aktiviert werden dürfen, um den Verdächtigen mithilfe dieser Funktionen ausspähen zu können. Anerkannt ist dagegen die Möglichkeit, den Betroffenen durch kriminalistische List zur Nutzung und daher Aktivierung der Sensorik beispielsweise des Mikrofons des Sprachassistenten zu animieren.[536] Sodann können die Strafverfolgungsbehörden auf die durch das Endgerät aufge-

532 *Derin/Golla*, NJW 2019, 1111, 1112; *Soiné*, NStZ 2018, 497, 501 f.; *Blechschmitt*, StraFo 2017, 361, 362.
533 A.A.: *Graf* in: BeckOK-StPO, § 100b StPO, Rn. 11.
534 *Hornick*, StraFo 2008, 281, 282.
535 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 8.
536 *Soiné*, NStZ 2018, 497, 502.

zeichneten Audioaufzeichnungen zugreifen, indem sie die während des folgenden Übertragungsvorgangs übermittelten Daten ausleiten.

2) Zugriff auf Mikrofon und Kamera

Einer näheren Betrachtung zuzuführen, ist jedoch die Frage, ob die im Endgerät verbauten Komponenten über § 100b StPO auch zur mittelbaren Informationsgewinnung genutzt werden dürften. Es stellt sich daher die Frage, ob im Rahmen des § 100b Abs. 1 StPO auf Kamera oder Mikrofon des Endgeräts eines Sprachassistenten bzw. des Smart Speakers fremdgesteuert zugegriffen werden dürfte.[537] Aus technischer Sicht ist es ohne weiteres möglich, mittels der aufgespielten Überwachungssoftware auch eine vollumfängliche Raumüberwachung, beispielsweise durch eine Aktivierung des Mikrofons, der Kamera oder weiterer sensorischer Systeme des betroffenen Geräts, zu ermöglichen.[538] Wenngleich nach Angaben des Bundesinnenministeriums solche Maßnahmen zum jetzigen Stand nicht geplant sind,[539] fragt sich ob diese denn rechtlich überhaupt zulässig wären.

a) Wortlaut

Ausweislich des Wortlauts darf in ein informationstechnisches System eingegriffen werden, um daraus Daten erheben zu können. Unter Bezugnahme auf die Weite des Wortlauts, wird argumentiert, dass dieser einer Aktivierung der sensorischen Systeme des überwachten Geräts nicht entgegenstünde.[540] Sofern mittels dieser Instrumente Daten aus der Umgebung aufgefangen werden, würden diese schließlich im weitesten Sinne aus dem infiltrierten System gewonnen und an die Ermittlungsbehörden weitergeleitet.[541] Der Passus „dürfen Daten daraus erhoben werden“ ist jedoch

537 Erstmals zu dieser noch ungeklärten Frage *Rüscher*, NStZ 2018, 687, 690; mit bloßem Hinweis auf diese Fragestellung *Eschelbach* in: SSW-StPO, § 100b StPO, Rn. 4.
538 *Fox*, Stellungnahme, S. 8.
539 Fragenkatalog der SPD-Bundestagsfraktion, S. 13, vgl. https://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt abgerufen am 31.10.2021).
540 *Eschelbach* in: SSW-StPO, § 100b StPO, Rn. 4; *Weber;* jM 2021, 252, 255.
541 *Eschelbach* in: SSW-StPO, § 100b StPO, Rn. 4.

vielmehr so zu verstehen, dass über § 100b StPO lediglich Daten erhoben werden dürfen, die zum Zeitpunkt der Infiltration oder in deren Verlauf durch eine Handlung des Nutzers selbst auf diesem System gespeichert wurden.[542] Davon nicht umfasst ist, dass diese Daten nach der Infiltration in einem weiteren Schritt noch gewonnen werden müssen. Insofern ist mit dem Wortlaut der Norm also zu differenzieren, ob unmittelbar auf gespeicherte Daten zugegriffen werden kann oder ob dieser Zugriff nur mittelbar erfolgen könnte, da die Daten erst noch neu zu generieren wären.[543] Zweiteres wäre schließlich bei Sprachassistenten der Fall, da deren Kamera oder Mikrofon erst extern aktiviert werden müsste, um sodann mögliche Daten erheben zu können. Diese Form der mittelbaren Beweisgewinnung kann mit dem Wortlaut des § 100b Abs. 1 StPO nicht in Einklang gebracht werden. Dieser gestattet lediglich die direkte Erhebung der Daten aus dem System, nicht jedoch dessen manipulative Nutzung und Erhebung durch das System selbst.[544]

b) Historie

Sofern versucht wird die Norm aus einem historischen Blickwinkel zu betrachten, wird dies aufgrund ihrer erst kurzen Existenz keine Aufschlüsse liefern. Jedoch könnte mit Blick auf die Gesetzesbegründung anzunehmen sein, dass die Verwendung sensorischer Systeme vom Umfang der Norm umfasst sein soll. Ausweislich derer soll neben dem Zugriff auf gespeicherte Daten, auch ein Zugriff auf das gesamte Nutzerverhalten möglich sein.[545] Mit dem Verweis auf das gesamte Nutzungsverhalten war jedoch nicht die Aktivierung etwaiger Systeme durch die Strafverfolgungsbehörden, sondern eine sog. Live-Überwachung der Nutzung des Beschuldigten derart gemeint, dass die Behörden dem Nutzer „heimlich über die Schulter blicken" und so seine aktuellen Vorgänge verfolgen können.[546]

542 so auch Rüscher, NStZ 2018, 687, 691; *Roggan*, StV 2017,821, 826; *Großmann*, JA 2019, 241, 244; *Gercke* in: HK-StPO, § 100b StPO, Rn. 11; *Soiné*, NStZ 2018, 497, 502; *Brodowski* in: BeckOK-ITR, X, § 100b StPO, Rn. 5.

543 *Kruse/Grzesiek*, KritV 2017, 331, 345.

544 *Singelnstein/Derin,* NJW 2017, 2646, 2647; vom Gegenteil ausgehend wohl *Huber*, NVwZ 2007, 880, 883.

545 BT-Drs. 18/12785, S. 54.

546 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 5.

c) Systematik

In Anbetracht dessen, dass es sich bei der neu geschaffenen Befugnis um eine der eingriffsintensivsten Ermittlungsbefugnisse der StPO handeln soll und deren Voraussetzung an die der akustischen Wohnraumüberwachung aus § 100c StPO angelehnt seien,[547] könnte anzunehmen sein, dass sodann auch eine (akustische) Wohnraumüberwachung auf Grundlage des § 100b StPO möglich sein müsse. Verglichen mit den übrigen Ermittlungsbefugnissen findet im Gegensatz zu § 100a StPO und § 100c StPO, bei § 100b StPO nicht lediglich eine Überwachung der aktuellen Kommunikation, sondern vielmehr sämtlicher vergangener und laufender Daten auf dem betroffenen System statt. Wenn jedenfalls eine akustische Wohnraumüberwachung unter den Voraussetzungen des § 100c StPO angeordnet werden darf, dann müsse eine solche auch durch Einschaltung des Mikrofons unter den Voraussetzungen des § 100b StPO zulässig sein, auf dessen Straftatenkatlog § 100c StPO indes explizit verweist. Teilweise wird sogar behauptet, die neu geschaffene Online-Durchsuchung legitimiere sämtliche Eingriffe, die bisher auf Grundlage des § 100c StPO möglich waren.[548] Dem kann jedoch nicht gefolgt werden. Ungeachtet dessen, dass § 100c StPO dann praktisch ohne eigenständige Funktion wäre, sind § 100b StPO und § 100c StPO hinsichtlich ihrer Anordnungsvoraussetzungen gerade nicht gleich. Im Unterschied zu § 100b StPO ist für eine Anordnung nach § 100c Abs. 1 Nr. 3 StPO weiter erforderlich, dass auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen des Beschuldigten erfasst werden, die für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten von Bedeutung sind. Gemessen an den Eingriffsvoraussetzungen handelt es sich bei § 100b StPO mithin auch keineswegs um die schwerwiegendsten strafprozessuale Ermächtigungsgrundlage. Vielmehr bleibt es dabei, dass § 100c StPO die ultima ratio der heimlichen Ermittlungsmaßnahmen darstellt.[549] Hinzu kommt ein gewichtiger Unterschied zwischen § 100b und § 100c StPO. Während die Datenfülle, auf die unter den Voraussetzungen des § 100b StPO zugegriffen werden kann, sicherlich immens ist, gilt es bei einer Wohnraumüberwachung einen weiteren Aspekt zu bedenken. Gespräche in den eigenen vier Wänden finden tatsächlich vollkommen abgeschnitten von der Außenwelt statt. Eine Verbindung zur

547 *Singelnstein/Derin*, NJW 2017, 2646, 2647.
548 *Beukelmann*, NJW Spezial 2017, 440.
549 *Großmann*, GA 2018, 439, 442.

Außenwelt besteht nicht einmal – wie im Falle der Nutzung eines informationstechnischen Systems – durch die Inanspruchnahme etwaiger technischer Geräte. Während bei der Nutzung eines technischen Geräts permanent Spuren hinterlassen werden, ist es hinsichtlich eines Gesprächs in der eigenen Wohnung die „Flüchtigkeit des gesprochenen Wortes“[550], die im Zuge einer Wohnraumüberwachung mittels eines externen Eingriffs konserviert wird. Das Abhören und Speichern solcher Nachrichten ist im Kanon der Eingriffsbefugnisse der §§ 100a ff. StPO explizit der Wohnraumüberwachung nach § 100c StPO zugewiesen. Im Übrigen hätte der Gesetzgeber, sofern er sich für eine akustische oder visuelle Wohnraumüberwachung mit Hilfe der infiltrierten Geräte aussprechen wollte, dies durch einen Verweis auf § 100c StPO deutlich machen können.[551] Ein solcher Verweis ist ebenso nicht erfolgt, sodass eine Wohnraumüberwachung auch unter systematischen Gesichtspunkten nicht auf § 100b StPO gestützt werden darf.

Gegen eine aktive Aktivierung von Kamera und Mikrofon durch die Strafverfolgungsbehörden spricht ferner ein Vergleich mit den bereits seit längerer Zeit in diversen Landes- und Bundesgesetzten normierten Befugnissen zur Online-Durchsuchung mit präventiver Ausrichtung. Bereits hinsichtlich dieser polizeirechtlichen-präventiven Norm entwickelte das Bundesverfassungsgericht enge Zulässigkeitsvoraussetzungen[552]. Wenn bereits für präventive Maßnahmen, durch deren Hilfe der sich aus einer Gefahr entwickelnde Schaden noch verhindert werden könnte solch strenge Anforderungen gelten, dann muss dies erst recht für repressive Maßnahmen gelten, die „lediglich“ die Sanktionierung einer bereits eingetretenen Straftat ermöglichen sollen. Mit diesem engen Verständnis lässt sich dann aber nicht vereinbaren, den Wortlaut der Norm in seiner denkbar weitesten Form zu lesen. Eine historisch vergleichende Betrachtung legt daher ein enges Verständnis des Wortlauts nahe, was eine Aktivierung sensorischer Systeme des informationstechnischen Systems ausschließt.

550 BGHSt 57, 71, 75 ff.
551 *Rüscher*, NStZ 2018, 687, 691.
552 Sowohl in § 20k BKAG a.F. als auch in § 5 Abs. 2 Nr. 11 VSG NRW wurde die Online-Durchsuchung aufgrund ihrer Unbestimmtheit bzw. einer zu weiten Begriffsfassung durch das BVerfG für verfassungswidrig erklärt, vgl. BVerfGE 120, 274, 302 ff.; BVerfGE 141, 220, 304 ff.

d) Telos

§ 100b StPO soll der heimlichen Ausspähung eines technischen Systems dienen und dabei den Zugriff auf gespeicherte Daten ermöglichen. Auf diesem Wege sollen Informationen zur Aufklärung einer Katalogtat des § 100b Abs. 2 StPO heimlich ausgelesen werden. Ziel der Ermächtigungsgrundlage ist daher das Ausspähen eines informationstechnischen Systems, nicht aber eines Wohnraums. Dieses Ergebnis bestätigt auch Gesetzesbegründung, in der sich im Zusammenhang mit der Infiltration eines informationstechnischen Systems ausführlich mit möglichen Eingriffen in das IT-Grundrecht auseinandergesetzt wird, nicht aber mit einem möglichen Eingriff in Art. 13 GG.[553] Ein Eingriff in den Schutzbereich der Unverletzlichkeit der Wohnung liegt jedoch nahe, wenn dieser akustisch oder gar visuell überwacht wird. Der Gesetzgeber selbst spricht von der Beeinträchtigung des Art. 13 GG jedoch stets nur im Zusammenhang mit einem Vorgehen nach § 100c StPO.[554] Es sollte daher gerade nicht Sinn und Zweck des § 100b StPO sein, in die Privatsphäre der Wohnung einzudringen.

e) Zwischenergebnis

Es bleibt festzuhalten, dass die Aktivierung von Mikrofon oder Kamera infiltrierter Systeme nicht von § 100b StPO gedeckt ist. Die Nutzung dieser Instrumente wird dadurch jedoch nicht gänzlich ausgeschlossen. Ausgeschlossen ist lediglich die Aktivierung der Systeme seitens der Strafverfolgungsbehörden. Sofern jedoch das System infiltriert wurde und sich der Nutzer zur Verwendung der Kamera oder des Mikrofons entscheidet, können bei einer Live-Überwachung die dabei offenbarten Information über § 100b StPO abgegriffen werden.[555] Wird folglich ein infiltriertes Gerät vor Ort durch den Nutzer aktiviert und zeichnet das Mikrofon sodann ein Gespräch des Nutzers zur Weiterleitung an den Sprachassistenten auf, kann diese Kommunikation über § 100b StPO abgefangen werden. Offen bleibt damit die Frage nach der Verwertbarkeit eines auf diese Weise erlangten Beweises, worauf im weiteren Verlauf gesondert eingegangen werden soll.

553 BT-Drs. 18/12785, S. 48.
554 BT-Drs. 18/12785, S. 48.
555 *Brodowski* in: BeckOK-ITR, X, § 100c StPO, Rn. 7.

3) Infiltration der Server des Dienstleistungsanbieters

Daneben ist ebenso an eine Infiltration der Server des Dienstleistungsanbieters zu denken. § 100b StPO stellt eine allumfassende Eingriffsbefugnis dar,[556] die sich nicht darin erschöpft lediglich auf informationstechnische Systeme des Verdächtigen zuzugreifen. Unter den Voraussetzungen des § 100b Abs. 3 StPO kann auf die Cloud-Server des Dienstleistungsanbieter als „andere Person" zugegriffen werden, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass der Beschuldigte deren informationstechnisches System nutzt. Bei einer derartigen Maßnahme ist zudem zu beachten, dass nicht lediglich der Dienstleistungsanbieter als unbeteiligte Person betroffen ist, sondern mittelbar auch sämtliche weitere Personen, deren Daten aufgrund der Nutzung einer Dienstleistung des Anbieters ihre Daten auf dem infiltrierten Server speichern. § 100b Abs. 3 S. 2 StPO legitimiert lediglich den Zugriff auf das informationstechnische System einer anderen Person (des Dienstleistungsanbieters), wenn auf Grundlage bestimmter Tatsachen davon auszugehen ist, dass der Beschuldigte informationstechnische Systeme der anderen Person benutzt und der alleinige Zugriff auf sein eigenes informationstechnisches System nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsorts eines Mitbeschuldigten führen wird. Hinsichtlich der Frage, wie es sich auswirkt, dass auf diesem Server persönlichkeitsrelevante Daten von Millionen anderer Unbeteiligter Nutzer gespeichert sind, erlaubt § 100b Abs. 3 S. 3 StPO die Maßnahme auch dann auszuführen, wenn andere Personen unvermeidbar betroffen sind. Aus dem Einschub „unvermeidbar" ergeben sich hohe Anforderungen an die Verhältnismäßigkeit eines solchen Vorgehens. Praktisch wird diese Anforderung jedoch zu Recht als inhaltsleer bezeichnet. Vielfach werden vor der Anordnung Anhaltspunkten für eine sachgerechte Beurteilung fehlen. Die Verhältnismäßigkeitsprüfung wird sodann lediglich auf vagen Prognosen beruhen.[557] Dass die Drittbetroffenheit im konkreten Fall der Infiltration des Servers einen Dienstleistungsanbieters mit Kunden im dreistelligen Millionenbereich weltweit jedoch evident ist, dürfte keine vage Prognose darstellen. Insofern sind in diesen Fällen an die Verhältnismäßigkeitsprüfung – wenngleich der Gesetzgeber den Zugriff trotz Drittbetroffenheit grundsätzlich zulässt – tatsächlich hohe Anforderungen, vergleichbar mit denen der ultima ratio Klausel in § 100c Abs. 1 Nr. 4 StPO, zu stellen. Zudem ist im Falle der angedachten Sys-

556 *Grözinger*, StV 2019, 406, 411.
557 *Hauck* in: LR-StPO, § 100c StPO, Rn. 117.

teminfiltration beim unverdächtigen Dienstleistungsanbieter § 100b Abs. 1 Nr. 3 StPO besondere Bedeutung beizumessen. Die von den Ermittlungsbeamten erhofften Informationen werden beim Dienstleistungsanbieter in aller Regel auch mittels einer offenen Ermittlungsmaßnahme im Rahmen einer Durchsuchung und einer möglichen Beschlagnahme gesichert werden können.[558] Notwendig wäre eine heimliche Überwachung vielmehr dann, wenn ein Bekanntwerden der Überwachung den Ermittlungserfolg gefährden würde. Allerdings ist bei einem Dienstleistungsanbieter regelmäßig nicht zu befürchten, dass dieser Aufzeichnungen der Kunden zur Vereitelung eines Zugriffs löschen würden. Vielmehr haben die Dienstleistungsanbieter in der Praxis Kontaktstellen für behördliche Anfragen eingerichtet, die sodann mit den Behörden kooperieren.[559]

4) Verfassungswidrigkeit des § 100b StPO

a) Fehlende ultima-ratio Ausgestaltung

Auch die neu geschaffene Online-Durchsuchung sieht sich verfassungsrechtlichen Bedenken ausgesetzt. Diese gründen vor allem auf einem Vergleich mit § 100c StPO und dessen strengeren Voraussetzungen, wenngleich § 100b StPO für den schwerwiegenderen Grundrechtseingriff empfunden wird.[560] Es wird kritisiert, dass die Online-Durchsuchung im Unterschied zur akustischen Wohnraumüberwachung – nicht als ultima ratio ausgestaltet ist.[561] Während § 100b Abs. 1 Nr. 3 StPO fordert, dass ein Vorgehen auf andere Weise lediglich „wesentlich" erschwert sein müsse, muss ein Vorgehen auf andere Weise für eine Anordnung nach § 100c Abs. 1 Nr. 4 StPO „unverhältnismäßig" erschwert sein. Das Bestehen dieses Unterschieds wäre verfassungsrechtlich aber jedenfalls dann nicht zu beanstanden, wenn – entgegen teilweiser Stimmen in der Literatur – auch

558 Vgl. § 4, A., IX), 1).
559 *Gercke* in: Borges/Meents Cloud-Computing, § 20, Rn. 38.
560 *Singelnstein/Derin*, NJW 2017, 2646, 2647.
561 *Park*, Durchsuchung und Beschlagnahme, § 4, Rn. 838; vgl. die anhängige Verfassungsbeschwerde (AZ: 2 BvR 897/18, 2 BvR 1797/18, 2 BvR 1838/18, 2 BvR 1850/18, 2 BvR 2061/18) gegen die Regelungen der Strafprozessordnung zur Online-Durchsuchung und Quellen-Telekommunikationsüberwachung beim Bundesverfassungsgericht, abrufbar unter: https://www.fdpbt.de/sites/default/files/2021-07/20210714_VfB_Pressefassung_0.pdf (zuletzt abgerufen am 31.10.2021).

nach Schaffung des § 100b StPO, weiter § 100c StPO den schwerwiegendsten Grundrechtseingriff darstellen würde. Hinsichtlich der Online-Durchsuchung ist zuzugeben, dass der Zugriff auf Vergangenes eine erhebliche Eingriffsintensität mit sich bringt. Dass solche Eingriffe die durch § 100c StPO legitimierten Eingriffe in die Unverletzlichkeit der Wohnung übersteigen, kann allerdings nicht ohne einhergehende Begründung behauptet werden.[562] *Buermeyer* begründet den schwerwiegenderen Eingriff durch § 100b StPO damit, dass durch eine akustische Wohnraumüberwachung zu erlangende Erkenntnisse auch im Wege einer Online-Durchsuchung generiert werden können, wenn das Mikrofon des Systems heimlich aktiviert wird.[563] Daraus folge, dass Online-Durchsuchung gegenüber dem Großen Lauschangriff „*ein – erhebliches – Plus, kein Aliud oder gar Minus*" darstelle.[564] Dieses Argument kann aber bereits deshalb nicht durschlagen, da wie gezeigt, der aktive Einsatz eines Mikrofons oder der Kamera unzulässig ist. Um die Eingriffsintensität eines Eingriffs nach § 100c StPO bestimmen zu können, sind ferner auch die bereits beschriebenen Charakteristika eines Gesprächs in der eigenen Wohnung zu beachten. Solche Gespräche werden im Vertrauen auf absolute Abgeschiedenheit und Isolation von etwaigen Dritten geführt. Es ist mittlerweile bekannt, dass die Nutzung eines informationstechnischen Geräts stets mit gewissen Risiken einhergeht und rückverfolgbare Spuren hinterlassen werden. Auch verfassungsrechtlich ist die eigene Wohnung seit jeher als Rückzugsort besonders privilegiert. Zum einen konkretisiert Art. 13 GG in seiner einfachgesetzlichen Ausgestaltung die Menschenwürdegarantie. Zum anderen beinhaltet Art. 13 GG neben diesem engen Bezug zur Menschenwürde das verfassungsrechtliche Gebot unbedingter Achtung einer Privatsphäre des Bürgers, die diesem eine höchstpersönliche Entfaltung ermöglicht.[565] Die in der eigenen Wohnung ablaufenden Gespräche sind alleine aufgrund dieses Umstands von vorherein mit dem Stempel der Privat- und Vertraulichkeit versehen. Für die Nutzung eines informationstechnischen Systems wiederum kann dies nicht in der gleichen allgemeingültigen Weise dargelegt werden. Dies zeigt bereits der Umstand, dass das Bundesverfassungsgericht nicht bei jeder Infiltration eines informationstechnischen Systems auch die Eröffnung des IT-Grundrechts für erforderlich hält. Bei Zugrundelegung dessen ist die pauschale Einordung, es handle sich bei der neu geschaffenen Online-

562 So jedoch *Singelnstein/Derin,* NJW 2017, 2646, 2647.
563 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 15.
564 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 15.
565 BVerfGE 109, 279, 313.

Durchsuchung um den schwerwiegendsten Eingriff der Strafprozessordnung, daher nicht haltbar.[566] Eine unterschiedliche Ausgestaltung des ultima ratio Gedankens ist daher verfassungsrechtlich nicht zu beanstanden und führt nicht zu einer Verfassungswidrigkeit der Vorschrift.

b) Unzureichende Ausgestaltung des Kernbereichsschutzes

Hinsichtlich der Ausgestaltung des Kernbereichsschutzes in § 100d Abs. 1 bis 3 StPO wird kritisiert, dass es dort an einem Beweiserhebungsverbot fehle, wie es § 100d Abs. 4 S. 2 StPO für den Fall des § 100c StPO normiere.[567] Danach ist das Abhören und Aufzeichnen unverzüglich zu unterbrechen, wenn sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Allerdings gestaltet sich die Online-Durchsuchung insofern wesensverschieden zur Wohnraumüberwachung. Wenn im Rahmen einer Wohnraumüberwachung Gespräche mitgehört werden, die dem Kernbereichsschutz unterfallen, können in diesem Moment faktisch keine weiteren Beweise erhoben werden. Die sofortige Unterbrechung der Abhörmaßnahme stellt daher die logische Konsequenz dar. Im Rahmen einer Online-Durchsuchung können jedoch unmittelbar andere Bereiche des infiltrierten Systems durchleuchtet werden, die nicht dem Kernbereichsschutz unterfallen. Ein sofortiger Abbruch der Durchsuchung bei Auffinden kernbereichsrelevanter Daten ist daher grundsätzlich nicht erforderlich. Daher genügt es, wenn sich der Kernbereichsschutz hier erst auf Beweisverwertungsebene und nicht bereits auf der Beweiserhebungsebene beachtet wird. Die Anforderungen an den Kernbereichsschutz sind auf der Erhebungsebene im Rahmen einer Online-Durchsuchung ein Stück weit zurückgenommen. Der Schutz vor Kernbereichsverletzungen zielt bei der Online-Durchsuchung nicht vordergründig darauf, das Festhalten eines nur flüchtigen, höchstvertraulichen Moments zu verhindern.[568] Stattdessen soll vermieden werden, dass aus einem Gesamtdatenbestand (von ohnehin digital vorliegenden Informationen) höchstvertrauliche Informationen ausgelesen werden, die jedoch in ihrer Gesamtheit regelmäßig nicht an die Vertraulichkeit des Verhaltens oder der Kommu-

566 Im Ergebnis auch Sinn, Stellungnahme zum Entwurf der BT-Drs. 18/11272, S. 12.
567 vgl. *Grözinger*, Die Überwachung von Cloud-Storage S. 309 ff.
568 BVerfGE 141, 220, Rn. 218 f.

nikation in einer Wohnung heranreichen.[569] Anders gestaltet sich dies jedoch im Falle einer Live-Überwachung. Die Situation einer Live-Überwachung ist identisch zu der einer Wohnraumüberwachung: Dem Betroffenen wird bei der Nutzung des informationstechnischen Systems in Echtzeit „über die Schulter geschaut"[570]. Sobald der Kernbereich betroffen ist, muss der Staat seine Live-Überwachung daher auch hier abbrechen. Da bezüglich der Live-Überwachung eine dem § 100d Abs. 4 S. 2 StPO entsprechende Regelung fehlt, hält *Grözinger* den Kernbereichsschutz des § 100d Abs. 4 S. 2 StPO für ungenügend.[571] Dem ist, sofern eine Live-Überwachung im Raum steht, zuzustimmen. Ob dies jedoch zur Verfassungswidrigkeit des § 100d StPO und damit auch zu einer Verfassungswidrigkeit des mit dem Kernbereichsschutz synallagmatisch verknüpften § 100b StPO führen muss, ist zweifelhaft. Es erscheint möglich, § 100d Abs. 3 StPO einer verfassungskonformen Auslegung zu unterziehen. Um dem verfassungsrechtlichen Interesse an einer Normerhaltung nachzukommen und zu verhindern, dass sich die gesetzgeberischen Kapazitäten in einer Fülle an Normkorrekturen erschöpfen, ist die verfassungskonforme Auslegung heute allgemein anerkannt.[572] Ihre Grenze findet sie jedoch dort, wo zum Wortlaut der Norm und zum gesetzgeberischen Willen ein ersichtlicher Widerspruch bestehen würde.[573] § 100d Abs. 3 S. 2 StPO enthält die Maßgabe, erlangte Informationen über den Kernbereich unverzüglich zu löschen. Solange es sich bei dem Zugriff nicht um eine Live-Überwachung handelt, stellt dies keinen Streitpunkt dar. Hinsichtlich der in Echtzeit durchgeführten Wohnraumüberwachung hat jedoch auch der Gesetzgeber erkannt und in § 100d Abs. 4 S. 2 StPO normiert, dass der Kernbereichsschutz hier besonders gefährdet erscheint. Bei Schaffung des § 100d Abs. 3 S. 2 StPO hatte der Gesetzgeber die Möglichkeit einer Online-Live-Durchsuchung in Form einer Online-Live-Überwachung und die offensichtliche Parallele zur Wohnraumüberwachung schlicht nicht vor Augen. Die Normierung des Gesamten § 100d StPO zeigt jedoch, dass der Kernbereichsschutz dem Gesetzgeber ein bedeutendes Anliegen war. Die hier vorgeschlagene Unterbrechung der Online-Überwachung in Echtzeit engt den Wortlaut des § 100d Abs. 3 S. 2 StPO auch nicht contra legem ein, sondern

569 BVerfGE 141, 220, Rn. 218 f.
570 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 5.
571 *Grözinger*, Die Überwachung von Cloud-Storage, S. 312.
572 *Voßkuhle*, AöR 2000, 177, 183; *Lüdemann*, Jus 2004, 27, 29; FS-Larenz/*Göldner*, 199, 200.
573 BVerfGE 110, 226, 267.

erweitert diesen im Sinne eines einheitlichen Schutzes des höchstpersönlichen Kernbereichs. § 100d Abs. 3 S. 3 StPO ist einer verfassungskonformen Auslegung zugänglich, die im Falle der live ablaufenden Online-Überwachung auch angezeigt erscheint. Eine Verfassungswidrigkeit der Vorschrift des § 100d Abs. 3 S. 2 StPO und damit auch des § 100b StPO ist nicht anzunehmen.

c) Zu weiter Anlasstatenkatalog

In der Entscheidung zum BKA-Gesetz wurden Eingriffe in das IT-Grundrecht nur zum Schutz überragend wichtiger Verfassungsgüter wie Leib, Leben, Freiheit der Person oder solcher Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berühren, erlaubt.[574] Da der Straftatenkatalog des § 100b StPO als Anlasstaten jedoch auch solche Taten enthält, die keines der soeben genannten Rechtsgüter schützen (beispielsweise Geld- und Wertzeichenfälschung, § 100b Abs. 2 Nr. 1c StPO, der Hehlerei, § 100b Abs. 2 Nr. 1k StPO, der Geldwäsche, § 100b Abs. 2 Nr. 1 StPO oder der Bestechlichkeit und Bestechung, § 100b Abs. 2 Nr. 1m StPO), soll § 100b StPO verfassungswidrig sein.[575] Dabei wird jedoch verkannt, dass ebenso ein informationstechnisches System im Sinne des § 100b StPO betroffen sein könne, ohne den Eingriff am Maßstab des IT-Grundrechts messen zu müssen.[576] Wenn der Eingriff jedoch nur am Maßstab des Rechts auf informationelle Selbstbestimmung zu messen ist, können konsequenterweise auch Delikte, die keine überragend wichtigen Verfassungsgüter schützen, Anlass zu einer Online-Durchsuchung geben. Entscheidend ist also vielmehr, ob die gewonnenen Daten im konkreten Einzelfall einen derart tiefen Einblick in die persönliche Lebensgestaltung ermöglichen, dass ein Schutz durch das IT-Grundrecht erforderlich ist.[577] Dies wird bei einem privat genutzten informationstechnischen System anzunehmen sein, sodass in verfassungskonformer Auslegung des § 100b StPO eine Anordnung zur Online-Durchsuchung nur dann erfolgen darf, wenn der Tatverdacht hinsichtlich eines Delikts besteht, das dem Schutz eines der genannten wichtigen Rechtsgüter dient. Ebenso gut ist aber vorstell-

574 BVerfGE 120, 274, 326 f.
575 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 13.
576 BVerfGE 120, 274, 313.
577 BVerfGE 120, 274, 314.

bar, dass beispielsweise informationstechnische Systeme eines Unternehmens zur Nachverfolgung diverser Finanzströme infiltriert werden sollen. Im Zuge dessen wäre aber nicht zu erwarten ist, dass dadurch Inhalte offenbart werden, die das Erstellen eines umfassenden Persönlichkeitsprofils eines Menschen erlauben. In diesem Fall ist sodann auch nicht das IT-Grundrecht einschlägig, sondern lediglich das Recht auf informationelle Selbstbestimmung. Die Anordnung einer Online-Durchsuchung kann sodann in verfassungskonformer Weise auch aufgrund eines der „mindergewichtigen" Delikte aus dem Straftatenkatalog des § 100b StPO erfolgen. Somit ist § 100b StPO nicht aufgrund des normierten Straftatenkatalogs verfassungswidrig. Die Norm muss im Zuge ihrer Anwendung lediglich auch diesbezüglich im hier ausgeführten Umfang verfassungskonform angewandt werden.

d) Fehlerhafter Schutz von Berufsgeheimnisträgern

Zuletzt soll die Einschränkung in § 100d Abs. 5 S. 2 StPO, wonach sich der Schutz gegenüber Berufsgeheimnisträgern offenbarten Informationen aus § 100d Abs. 5 S. 1 StPO nicht auf deren Berufshelfer erstreckt, die Verfassungswidrigkeit der Vorschrift zum Kernbereichsschutz begründen.[578] § 100d Abs. 5 S. 1 StPO würde daher in solchen Fällen bedeutungslos, wenn auf den absolut geschützten Inhalt über einen Umweg rechtmäßig zugegriffen werden könnte. Gerade in der Praxis lässt sich organisatorisch kaum verhindern, dass bestimmte Kommunikation nicht höchstpersönlich mit dem Berufsgeheimnisträger, sondern auch mit dessen Berufshelfern, wie dem Sekretariat oder einer Arztgehilfin, erfolgt.[579] Jedoch gilt es zu beachten, dass § 100d Abs. 5 S. 2 StPO bezüglich gewonnener aber unter § 53a StPO fallender Erkenntnisse lediglich hinsichtlich der Frage der Verwertbarkeit eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes vorsieht. Eine Abwägung auf der Ebene der Beweiserhe-

578 Vgl. Stellungnahme des Deutschen Anwaltvereins zu dem Gesetzentwurf der Bundesregierung – Drs.18/11272, S. 11; abrufbar unter: https://anwaltverein.de/de/newsroom/sn-44-17-einfuehrung-der-online-durchsuchung-und-quellen-tkue?file=files/anwaltverein.de/downloads/newsroom/stellungnahmen/2017/DAV-SN_44-17_%C3%84nderungsantrag.pdf (zuletzt abgerufen am 31.10.2021), S. 21; kritisch auch *Grözinger*, Die Überwachung von Cloud-Storage, S. 315; Az. der anhängigen Verfassungsbeschwerden: 2 BvR 897/18, 2 BvR 1797/18, 2 BvR 1838/18, 2 BvR 1850/18, 2 BvR 2061/18.

579 *Basar/Hiéramente*, HRRS 2018, 336, 338.

bung ist gerade nicht vorgesehen. Insofern gewährleistet bereits § 100d Abs. 2 StPO die Unantastbarkeit des Kernbereichs privater Lebensgestaltung uneingeschränkt und losgelöst von jedweder Abwägung.[580] Zudem sind die gegenüber Berufshelfern getätigten Äußerungen auch auf der späteren Ebene der Beweisverwertung nicht uneingeschränkt, sondern nur unter Heranziehung eines Verhältnismäßigkeitskorrektivs verwertbar.

Aus der Rechtsprechung des Bundesverfassungsgerichts zu § 100c StPO ist zu folgern, dass Inhalte, die einem Gespräch mit einem Berufsgeheimnisträger entstammen, bereits auf Beweiserhebungsebene in der Regel einen höhere Schutzwürdigkeit aufweisen als solche mit bloßen Berufshelfern.[581] Dies ist auch angemessen, schließlich ist es nicht erforderlich, dass der Betroffene mit einem Berufshelfer in der gleichen Offenheit kommuniziert wie mit dem Berufsgeheimnisträger. Im Rahmen der ersten Kontaktaufnahme mit einer auf Strafrecht spezialisierten Kanzlei müssen beispielsweise gegenüber dem Sekretariat keine vertraulichen Details genannt werden, vielmehr wird der Hinweis auf ein laufendes Ermittlungsverfahren mit Angabe der entsprechenden vorgeworfenen Delikte genügen, um zu prüfen, ob ein persönlicher Termin zur Besprechung mit dem Rechtsanwalt in Frage kommt. Die Informationen über ein laufendes Ermittlungsverfahren stellt für die Strafverfolgungsbehörden jedoch keinen Mehrwert dar, sondern ist bereits bekannt.

Hinsichtlich einer Online-Durchsuchung ist die Differenzierung zwischen Berufgeheimnisträger und Berufshelfer zudem auch von untergeordneter Bedeutung. Denn es ist festzuhalten, dass das informationstechnische System in Form des Servers einer Kanzlei oder einer Praxis als Ganzes dem § 100d Abs. 5 S. 1 StPO unterfällt. Eine Differenzierung zwischen den informationstechnischen Systemen, die schwerpunktmäßig durch den Berufgeheimnisträger und solchen, die schwerpunktmäßig durch dessen Berufshelfer bedient werden, erscheint nicht rechtssicher durchführbar. Vielmehr stellt der Berufgeheimnisträger das komplette informationstechnische System zu Verfügung, weshalb es auch im Wege einer Gesamtbetrachtung einheitlich diesem zuzurechnen ist. § 100d Abs. 5 S. 2 StPO erlangt hinsichtlich der Online-Durchsuchung daher nur dann Bedeutung, wenn auf das private informationstechnische System der Berufshelfer zugegriffen werden soll. Dass ein Berufshelfer auf einem solchen in der Regel

580 BVerfG, Beschluss vom 11. Mai 2007 – 2 BvR 543/06 -, Rn. 51 = teilweise in NJW 2007, 2753 ff.

581 BVerfG, Beschluss vom 15. Oktober 2009 – 2 BvR 2438/08 -, Rn. 12 = teilweise in NJW 2010, 287; BVerfGE 109, 279, 328.

keine Kanzleiinterna speichern sollte, ist daher ratsam. In einem solchen Fall müsste im Zuge einer Verhältnismäßigkeitsprüfung die Verwertbarkeit dieser Informationen geprüft werden. Von Bedeutung dabei könnte sein, ob der Rechtsanwalt den Informationen durch die Auslagerung eine geringe Vertraulichkeit beigemessen hat, was für eine Verwertbarkeit sprechen könnte. Auf der andern Seite könnte aber die Verwertung sogar den Schutzzweck des § 100d Abs. 5 S. 1 StPO umgehen, wenn dem Berufsgeheimnisträger die durch Art. 12 GG garantierte freie Wahl seiner Art der Berufsausübung (Arbeitsprozesse auf private informationstechnische Systeme seiner Angestellten auszuweiten) faktisch untersagt würde. Eine endgültige Abwägung kann stets nur im konkreten Fall vorgenommen werden.

e) Zwischenergebnis

Es erscheint daher gut vertretbar, wenn das BVerfG die bereits anhängige Verfassungsbeschwerde[582] hinsichtlich § 100b StPO zu Recht als unbegründet zurückweisen wird. § 100b StPO ist jedenfalls im Wege einer verfassungskonformen Auslegung verfassungsrechtlich nicht zu beanstanden.

5) Ergebnis

Hinsichtlich § 100b StPO ist zu konstatieren, dass Smart Speaker zwar hierunter zu subsumieren sind, der Erkenntnisgewinn in der Praxis jedoch begrenzt ist. Jedenfalls so lange eine Speicherung der Daten nicht auf der Hardware des infiltrierten Endgeräts erfolgt, können durch eine Infiltration dieses Gerätes keine ruhenden Daten abgegriffen werden. Hierfür wäre die Infiltration des Servers des Dienstleistungsanbieters erforderlich. Interessant bleibt einzig die Möglichkeit der Live-Überwachung im Rahmen des § 100b StPO. Insofern können Mikrofon und Kamera smarter Assistenten zwar nicht durch die Strafverfolgungsbehörden aktiviert werden, doch ist während einer aktiven Nutzung des Sprachassistenten das Mithören seitens der Strafverfolgungsbehörden möglich. Insofern stellen sich aber weitere Probleme im Rahmen der Verwertbarkeit der durch solch eine Live-Überwachung erlangten Informationen.

582 AZ: 2 BvR 897/18, 2 BvR 1797/18, 2 BvR 1838/18, 2 BvR 1850/18, 2 BvR 2061/18.

VI) § 100c StPO

Eine weitere Möglichkeit Smart Speaker für die Strafverfolgung zu gewinnen, könnte die Durchführung einer Wohnraumüberwachung gem. § 100c StPO darstellen.[583] § 100c Abs. 1 StPO erhält die Befugnis, das von Personen „in einer Wohnung nichtöffentlich gesprochene Wort mit technischen Mitteln" abzuhören und aufzuzeichnen. Entsprechend gestattet die Vorschrift nach einhelliger Ansicht lediglich die akustische Überwachung und Aufzeichnung des nichtöffentlichen gesprochenen Wortes in Wohnungen.[584] Nicht ausdrücklich geregelt ist, ob die Wohnung zum Anbringen der für eine Überwachung erforderlichen Technik heimlich betreten werden darf. Insoweit ist aber, da der Inhalt der Norm ansonsten schlicht nicht umsetzbar wäre, von einer Annexkompetenz auszugehen.[585] In eben dieser Verwanzung eines Wohnraums liegt allerdings ein nicht zu unterschätzendes praktisches Problem. Die Strafverfolgungsbehörden dürfen, während sie die Räume, in welchen sich der Beschuldigte mutmaßlich aufhält, präparieren, nicht entdeckt werden, da ansonsten die Heimlichkeit und damit der Erfolg der Maßnahme in Gefahr gerät. Vielmehr bestünde dann die Gefahr, dass der Betroffene den Umstand, dass seine Wohnung verwanzt ist für sich ausnutzt und den Strafverfolgungsbehörden, die von einer heimlichen Überwachung ausgehen, gezielt falsche Informationen zukommen lässt. Da für das Verwanzen einer Wohnung mitsamt dem Anbringen der notwendigen Technik zuweilen mehrere Stunden einzuplanen sind, stellt dies ein erhebliches Risiko dar. Der Betroffene darf nicht vor dem Ende der Verwanzung in seine Wohnung zurückkehren.[586] Hinzu kommt die Gefahr, dass verbaute Wanzen durch die Betroffenen entdeckt werden und sodann die Verbindung getrennt wird. Neben der aufzuwendenden Zeit wurden auch wegen der für eine Wohnraumüberwachung anfallenden Kosten kritisiert, dass „Aufwand und Ertrag in keinem Verhältnis zueinander stünden"[587]. In den vergangenen Jahren sank

583 Als theoretische Idee jedoch im Rahmen des § 100b StPO bereits bei *Kruse/Grzesiek*, KritV 2017, 331, 335.

584 *Günther* in: MüKo-StPO, § 100c StPO, Rn. 3; *Bruns* in: KK-StPO, § 100c StPO, Rn. 4.

585 *Bruns* in: KK-StPO, § 100c StPO, Rn. 4; *Hegmann* in: BeckOK-StPO, § 100c StPO, Rn. 3.

586 *Meyer-Wieck*, Der große Lauschangriff, S. 136.

587 *Wolter* in: SK-StPO, § 100c StPO, Rn. 10a; *Hauck* in: LR-StPO, § 100c StPO, Rn. 5.

die Zahl angeordneter Wohnraumüberwachungen unter anderem daher auf durchschnittlich sieben Anordnungen pro Jahr.[588]

Diese Probleme könnten vermieden werden, wenn sich die Strafverfolgungsbehörden die Mikrofone eines Gegenstandes, den der Betroffene selbst in seine Wohnräume verbringt, als Wanze zu Nutzen machen dürften. Insofern könnte das Mikrofon des Endgerätes genutzt werden, um Gespräche aus der Wohnung mitzuhören und aufzuzeichnen.

1) Smart Speaker als technisches Mittel im Sinne des § 100c StPO

Hierzu müsste es sich bei dem Endgerät, welches als Wanze dienen soll, um ein technisches Mittel im Sinne des § 100c StPO handeln. Hierunter werden die klassischen Abhöreinrichtungen wie batteriebetriebene Minisender (sog. Wanzen), modernere GSM-Abhörgeräte oder Richtmikrofone gefasst. Die Akkulaufzeit solcher Wanzen beträgt jedoch in der Regel zwischen fünf Stunden bis maximal vier Tagen. GSM-Abhörgeräte verfügen zwar über deutlich größere Laufleistung, sind aufgrund ihrer Größe jedoch auch schwerer zu verstecken.[589] Neben dem Installationsaufwand könnten auch solche praktischen Probleme durch Nutzung der Mikrofone des Endgeräts eines Sprachassistenten umgangen werden.

a) Wortlaut

Nach dem Wortlaut lässt sich der Geltungsbereich der Vorschrift nicht exakt eingrenzen. Schließlich handelt es sich bereits immer dann um ein Mittel, wenn die Nutzung einer Sache der Erreichung eines bestimmten Zieles dienlich ist.[590] Das technische Endgerät würde zur Wohnraumüberwachung eingesetzt und es ermöglichen das in der Wohnung Gesprochene wahrzunehmen und aufzuzeichnen. Der Wortlaut der Norm lässt keine Zweifel aufkommen, dass es sich dann bei einem solchen Endgerät um ein technisches Mittel im Sinne des § 100c StPO handelt.

---

588 *Wolter* in: SK-StPO, § 100e StPO, Rn. 6.
589 *Hauck* in: LR-StPO, § 100c StPO, Rn. 85.
590 Duden, Bedeutung des Wortes „Mittel“, abrufbar unter: https://www.duden.de/rechtschreibung/Mittel_Arznei_Geld_Behelf (zuletzt abgerufen am 31.10.2021).

b) Historie

Gemessen an einer historischen Betrachtung des § 100c StPO könnte zu fordern sein, dass es sich bei technischen Mittel im Sinne des § 100c StPO um solche der Strafverfolgungsbehörden handeln müsse, da andernfalls die diesen zustehende Annexkompetenz, die Wohnung des Beschuldigten für Installationszwecke zu betreten, obsolet wäre.[591] Eine solche Annexkompetenz würde es schließlich nur dann benötigen, wenn im Eigentum des Staates stehende technische Geräte in die Wohnung verbracht und dort angeschlossen werden müssen. Naheliegender ist mit Blick auf die angezeigte Annexkompetenz, jedoch der Schluss, dass mit diesem Zugeständnis keineswegs die Annahme einhergehen sollte, dass die Strafverfolgungsbehörden eigene Mittel einzusetzen haben. Vielmehr sollte allein für den Fall, dass ein solches Anbringen in der Wohnung notwendig würde das hierzu erforderliche Betreten miterfasst sein. Dass der Gesetzgeber mit dem Zuerkennen dieser Annexkompetenz zum Ausdruck bringen wollte, dass die Strafverfolgungsbehörden eigene technischer Mittel einzusetzen haben, ist den Gesetzesbegründungen nicht zu entnehmen. Im Hinblick auf die zeitliche Entstehung der Norm kann dies auch nicht weiter verwundern.[592] In den zurückliegenden Jahrzehnten war schlicht noch nicht denkbar, dass eines Tages auch nicht der Strafverfolgungsbehörde gehörende technische Mittel zu einer Wohnraumüberwachung genutzt werden könnten.

c) Systematik

Gegen die Heranziehung des Endgeräts des Betroffenen soll ferner eine systematische Auslegung unter verfassungsrechtlichen Gesichtspunkten sprechen. Die Pflicht zur Nutzung staatlicher Mittel für eine Maßnahme gem. § 100c StPO wird laut *Rüscher* im Rahmen einer systematischen Betrachtung deutlich. Bei Betrachtung der Ermittlungsmaßnahmen in den §§ 94 bis 111q StPO wird der Begriff des technischen Mittels in diversen Normen genannt (§§ 100a, 100b, 100c, 100f, 100h, 100i StPO). Dabei handle es sich allerdings stets um eigene Mittel der Straf-

591 *Rüscher*, NStZ 2018, 687, 690; *Brodowski* in: BeckOK-ITR, X, § 100c StPO, Rn. 6.

592 Die Regelung des § 100c StPO trat durch das Gesetzes zur Verbesserung der Bekämpfung der Organisierten Kriminalität vom 04.05.1998 in Kraft, vgl. BT-Drs. 13/8651, S. 10.

verfolgungsbehörden. Dies würde vor allem anhand der §§ 100a Abs. 1 S. 2, 100b Abs. 1 StPO deutlich, da dort mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen werde.[593] Daher sei das informationstechnische System dem Betroffenen zuzuordnen, während das technische Mittel der Strafverfolgungsbehörde zugeordnet sein müsse.[594] Bereits diese Maßstabsbildung erscheint jedoch angesichts des weiten Wortlauts nicht überzeugend.[595] Selbst wenn man jedoch diesen Maßstab zugrunde legen würde, so wäre die aufgespielte Software zur Aktivierung des Mikrofons als das staatliche Mittel zu sehen. Dagegen kann nicht vorgebracht werden, dass es alleine durch das technische Mittel der Software nicht möglich wäre, das in einer Wohnung gesprochene Wort aufzuzeichnen, sondern das entscheidende technische Mittel das informationstechnische Systems des Betroffenen sei, welches für das Aufzeichnen der Gespräche unabdingbar ist.[596] Denn im Unterschied zu § 100b StPO fordert der Wortlaut des § 100c StPO gerade kein dem Betroffenen zuzuordnendes informationstechnisches System, sondern setzt lediglich das Abhören mittels eines technischen Mittels voraus.

Hinzu kommt, dass auch ein Vergleich mit § 100i StPO kein anderes Ergebnis nahe legt. Gem. § 100i Abs. 1 Nr. 2 StPO darf durch technische Mittel der Standort eines Mobilfunkendgerätes ermittelt werden. Das technische Mittel stellt hierbei der sog. IMSI-Catcher dar, durch den eine virtuelle Funkzelle aufgebaut wird, in die sich das Mobiltelefon des Betroffenen irrtümlich einwählt.[597] Obiger Argumentation folgend, müsste aber konstatiert werden, dass das entscheidende Mittel zur Standortbestimmung das Mobiltelefon des Betroffenen darstellt. Ohne dieses wäre eine Standortbestimmung nicht möglich. Dadurch wird deutlich, dass es gerade nicht ausgeschlossen ist, dass die Strafverfolgungsbehörden durch ein eigenes technisches Mittels wiederum ein technisches Mittel des Betroffenen im Sinne der Strafverfolgung „manipulieren". Die aufgespielte Software auf das Endgerät des Betroffenen kann daher mit dem IMSI-Catcher, der Smart Speaker im Eigentum des Betroffenen mit dessen Mobiltelefon im Rahmen des § 100i StPO verglichen werden. Aus dem Kanon der Eingriffs-

593 *Rüscher*, NStZ 2018, 687, 690.
594 *Rüscher*, NStZ 2018, 687, 690; *Weber*, jM 2021, 252, 256; *Brodowski* in: BeckOK-ITR, X, § 100c StPO, Rn. 7; ablehnend *Anders*, ZJS 2020, 70, 77.
595 zutreffend auch *Anders*, ZIS 2020, 70, 77.
596 *Rüscher*, NStZ 2018, 687, 690.
597 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 14.

befugnisse ergibt sich daher nicht zwangsläufig, dass das entscheidende technische Mittel dem Staat zuzuordnen sein muss.

d) Telos

Sinn und Zweck der 1998 geschaffenen Wohnraumüberwachung war es, den bis dahin von heimlichen staatlichen Ermittlungen ausgenommen Wohnraum abhören zu können.[598] Der Gesetzgeber hatte im Rahmen der Ausgestaltung der Norm jedoch darauf verzichtet, konkrete Mittel zu benennen, um den Strafverfolgungsbehörden zu ermöglichen, entsprechend der technologischen Entwicklung auf diejenige Technik zurückgreifen zu können, die für die konkrete Maßnahme am geeignetsten erscheint.[599] Von dieser Entwicklung umfasst ist aber nicht nur die technische Fortentwicklung von Richtmikrofonen bis hin zur Möglichkeit über eine Laserabtastung Schallwellen an Fenstern abzufangen und in gesprochene Worte rückzuübersetzen,[600] sondern auch solche technische Geräte für Abhörmaßnahmen zu nutzen, die Betroffene freiwillig in ihrer Wohnung verwahren. Sinn und Zweck der Vorschrift ist einzig aus der Ferne einen Zugriff auf in diesem Moment gesprochene Worte zu ermöglichen. Aus teleologischen Gesichtspunkten spricht daher nichts gegen die Annahme, das Endgerät des Betroffenen mittels einer Software zur staatlichen Wanze umzuwandeln. Das eine solche Möglichkeit der Strafverfolgungsbehörden existiert, erkannte das BVerfG bereits im Jahr 2008 als es formulierte, dass mittels der Infiltration eines informationstechnischen Systems zur Nutzung der an das System angeschlossenen Peripheriegeräte (bspw. ein Mikrofon), bestimmte Vorgänge innerhalb der Wohnung überwacht werden könnten.[601]

2) Kollision mit IT-Grundrecht

Das Aufspielen einer Software zur permanenten akustischen Überwachung soll einen Eingriff in das aus Art. 2 Abs. 1 GG i.V.m. Art 1 Abs. 1 GG abgeleitete Grundrecht der Integrität informationstechnischer Systeme be-

598 BGBl. I 845; *Günther* in: MüKo-StPO, § 100c StPO, Rn. 1.
599 *Günther* in: MüKo-StPO, § 100c StPO, Rn. 50.
600 *Hauck* in: LR-StPO, § 100c StPO, Rn. 85.
601 BVerfGE 120, 274, 310.

gründen. Die damit verbundene Eingriffsintensität ginge jedoch über das hinaus, was der Gesetzgeber bei Erlass des § 100c StPO intendierte, da der Gesetzgeber sich über einen solchen Grundrechtseingriff in das IT-Grundrecht bei Erlass des § 100c StPO nicht bewusst war.[602]

Bewusst musste sich der Gesetzgeber jedoch sein, dass mit jeder Abhörmaßnahme jedenfalls ein Eingriff in das aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG entspringende Recht auf informationelle Selbstbestimmung einhergeht.[603] Denn das Recht auf informationelle Selbstbestimmung schützt vor jeder Form der Erhebung, schlichter Kenntnisnahme oder auch Speicherung von persönlichen Informationen.[604] Damit kann aus diesem Recht auch das Recht Herr über das eigene gesprochene Wort zu bleiben, also frei darüber bestimmen zu können, welchen Personen Zugang zum eigenen gesprochenen Wort gewährt werden soll, abgeleitet werden. Jenes im Privaten gesprochene Wort wollen sich die Strafverfolgungsbehörden im Rahmen des § 100c StPO jedoch zu eigen machen. Mit dem Abhören des gesprochenen Wortes über das Endgerät geht daher zwar ein Eingriff in das Recht auf informationelle Selbstbestimmung, nicht jedoch ein Eingriff in das Grundrecht der Integrität informationstechnischer Systeme einher. Dieses Grundrecht soll seinen Inhaber vor einem unberechtigten Zugriff auf die auf einem informationstechnischen System gespeicherten Daten schützen. Sofern die Strafverfolgungsbehörden allerdings das Endgerät bildlich gesprochen zur Wanze umfunktionieren, soll gerade kein Zugriff auf gespeicherte Datenbestände erfolgen, sondern das aktuell gesprochene Wort unter den strengen Voraussetzungen des § 100c StPO abgehört werden. Letztlich handelt es sich dabei um das Ergebnis mitsamt der gleichen Eingriffsintensität, das auch durch das Anbringen von Wanzen oder anderen Abhörinstrumenten in der Wohnung des Beschuldigten eintreten würde. Ein zusätzlicher Schutz durch das IT-Grundrecht erscheint daher für die hier zugrunde liegende Sachverhaltskonstellation weder erforderlich, noch liegen die Voraussetzungen für die Eröffnung dessen Schutzbereiches vor. Als problematisch erweist sich jedoch, dass auch wenn durch das Aufspielen der Überwachungssoftware zum kontrollierten Einsatz des Mikrofons der Schutzbereich des IT-Grundrecht nicht eröffnet ist, ein Zugriff auf ein informationstechnisches System im Sinne der Strafprozessordnung vorliegen könnte. Ein solcher Zugriff

602 *Rüscher*, NStZ 2018, 687, 690; *Marx*, DVBl 2020, 488, 492 bzgl. § 46 Abs. 1 BkAG.
603 BVerfGE 109, 279, 365.
604 *Di Fabio* in: Maunz/Dürig-GG, Art. 2 Abs. 1 GG, Rn. 176.

auf ein informationstechnisches System sollte nach dem Willen des Gesetzgebers nur unter den Voraussetzungen des § 100b StPO erfolgen.[605] In der Literatur wird daher vereinzelt vermutet, dass der Zugriff auf ein informationstechnisches System zur Softwareinstallation zwecks der Durchführung eines Lauschangriff mittels eines Smart Home Endgeräts eher bei § 100b StPO zu verorten sein dürfte.[606]

3) Stellungnahme

Der Wortlaut und auch eine historische Betrachtung lassen nicht daran zweifeln, „Smart Home" Endgeräte als Ohr der Strafverfolgungsbehörden im Rahmen des § 100c StPO nutzen zu können. Den Zweck einer solchen heimlichen Aufzeichnung betrachtend, erscheint es ebenfalls möglich dies auf dem Wege zu erreichen, ein technisches Gerät des Betroffenen als Abhörquelle zu nutzen. Lediglich die systematische Sichtweise erhebt gegen die Umwandlung des Endgeräts zur Wanze Bedenken. Der zum Abhören erforderliche Zwischenschritt bedarf das Aufspielen einer Software und daher jedenfalls ein Zugriff auf die Software des informationstechnischen Systems des Endgeräts. Es bleibt zu fragen, ob der Zugriff auf ein solches System nur unter Heranziehung des § 100b StPO möglich ist. Dies mag auf den ersten Blick nahe liegen, nennt doch lediglich der Wortlaut des § 100b StPO die Befugnis zum Eingriff in ein informationstechnisches System. Jedoch greift eine solche Betrachtung zu kurz. § 100b StPO regelt den Eingriff in ein informationstechnisches System, um aus diesem Daten zu erheben. Im Rahmen des Lauschangriffs unter Nutzung des sich in der Wohnung befindlichen Smart Speakers sollen aus dem informationstechnischen System jedoch gerade keine Daten erhoben werden, sondern vielmehr in der Wohnung ablaufende Vorgänge überwacht werden. Sämtliche auf dem System gespeicherten Informationen über den Nutzer bleiben unberührt. Obwohl zur Zielerreichung auf ein informationstechnisches System zugegriffen wird, ist aufgrund der vollkommen unterschiedlichen Zielrichtung einer Wohnraumüberwachung im Vergleich zu einer Online-Durchsuchung kein systematischer Konflikt zwischen den Befugnisnormen des § 100b StPO und § 100c StPO auszuma-

605 BS-Drs. 19/11478 als Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Benjamin Strasser, Stephan Thomae, Manuel Höferlin, weiterer Abgeordneter und der Fraktion der FDP, S. 3.

606 *Blechschmitt*, MMR 2018, 361, 365.

chen. Während bei der Online-Durchsuchung das informationstechnische System selbst nach Informationen durchsucht wird, soll bei der Wohnraumüberwachung lediglich das informationstechnische System als Wanze dienen. Diese Sichtweise steht daher auch in keinem Widerspruch zu der einhelligen Auffassung, dass § 100c StPO selbstredend keine Befugnis für eine Online-Durchsuchung enthält.[607] Denn zu einer solchen Online-Durchsuchung kommt es im hier genannten Fall gerade nicht. Ferner ist festzuhalten, dass die hohe Eingriffsintensität eines Vorgehens nach § 100b StPO nicht bereits durch die bloße technische Infiltration eines informationstechnischen Systems begründet wird. Denn allein dadurch wäre es nicht möglich persönlichkeitsrelevante Daten über den Betroffenen zu erhalten. Vielmehr bedarf es hierfür eines zweiten Schrittes, die durch die Infiltration geschaffene Möglichkeit, das System nach Informationen zu durchsuchen, sodann auch aktiv auszunutzen. Da es bei der Infiltration des Smart Speakers zur Nutzung des Mikrofons nicht zu diesem zweiten Schritt einer aktiven Durchsuchung kommt, liegt auch kein Eingriff in das IT-Grundrecht vor. Dieses schützt nicht bereits die Unantastbarkeit technischer Systeme an sich, sondern kommt erst im Zusammenspiel mit der Gefahr einer aus diesem System erfolgten Informationsgewinnung zum Tragen.[608] Insofern führt auch das BVerfG aus, dass das IT-Grundrecht beim Zugriff auf informationstechnische Systeme anzuwenden sei, wenn dieses System Daten des Betroffenen in einem derartigen Umfang enthält, dass durch den Zugriff auf das System ein Einblick in wesentliche Teile der Lebensgestaltung einer Person gegeben wäre oder ein aussagekräftiges Bild der Persönlichkeit daraus abzuleiten wäre.[609] Das Gericht hält das IT-Grundrecht folglich nur dann für das einschlägige Grundrecht, wenn das informationstechnische System die entsprechende Datenvielfalt in sich enthält. Im Rahmen der Wohnraumüberwachung stellt allerdings keineswegs der Zugriff auf die in dem als Wanze genutzten System möglicherweise enthaltenen Daten das Ziel der Strafverfolgungsbehörden dar. Vielmehr sollen mittels des informationstechnischen Systems neue – von dem informationstechnischen System als solchem unabhängige – Gespräche in der Wohnung abgehört werden. Die entsprechenden Daten sind folglich

607 *Eschelbach* in: SSW-StPO, § 100c StPO, Rn. 5.

608 A.A. *Hoffmann-Riem*, JZ 2008, S. 1009, 1019, der den Schutz des IT-Grundrechts auf sämtliche infolge einer Infiltration gewonnen Informationen erstreckt; *Meinicke*, DSRITB 2018, 835, 851, der einen Eingriff in das IT-Grundrecht bei jedweder Infiltration eines informationstechnischen Systems für angezeigt erachtet; *Marx*, DVBl 2020, 488, 492.

609 BVerfGE 120, 274, 314.

nicht im infiltrierten Gerät enthalten, sondern werden erst durch dessen Nutzung als Wanze erschaffen.

Ferner kommt dem IT-Grundrecht nach der Rechtsprechung des BVerfG nur dann Bedeutung zu, wenn durch einen Zugriff auf ein informationstechnisches System auch Daten erhoben werden, die wiederum nicht durch die übrigen Grundrechte vor einem Zugriff geschützt sind.[610] Nur in diesem Fall bleibt eine Schutzlücke, die durch das allgemeine Persönlichkeitsrecht in seiner im IT-Grundrecht erlangten Ausprägung zu schließen ist.[611] Das Bundesverfassungsgericht ist demnach der Ansicht, dass nur, sofern kein Schutz durch die Grundrechte der Art. 10 GG, Art. 13 GG oder durch das Recht auf informationelle Selbstbestimmung gewährleistet werden kann, die Infiltration eines informationstechnischen Systems auch eine Beeinträchtigung darstellt, die den Schutz durch das IT-Grundrechts bedarf.[612] Dies bedeutet aber gleichfalls, dass es das Bundesverfassungsgericht für möglich erachtet, dass durchaus ein informationstechnisches System infiltriert werden kann und dennoch ein ausreichender Schutz durch die genannten Grundrechte besteht. Mithin, dass nicht jede Infiltration eines solchen Systems den Schutz des neu geschaffenen IT-Grundrechts bedarf. Insofern ist zudem zu beachten, dass das BVerfG in seiner Entscheidung zur Online-Durchsuchung einen Schutz durch das IT-Grundrecht nur deshalb für notwendig erachtete, da die lediglich auf dem heimischen Rechner ruhenden Daten nicht in den Schutzbereich des Art. 10 GG fielen und ansonsten eine Schutzlücke bestanden hätte.[613] Hätte daher in der gleichen Situation ein Schutz durch andere Grundrechte bestanden, so hätte das Gericht trotz der vorhanden Infiltration des Systems kein Schutz durch das IT-Grundrecht für notwendig erachtet.

Bei der Infiltration eines Endgeräts zur Nutzung des Mikrofons schützen jedoch unter Umständen bereits das Grundrecht aus Art. 13 GG sowie in jedem Falle das aus dem Recht der informationellen Selbstbestimmung abgeleitete Recht am eigenen gesprochenen Wort den Betroffenen hinreichend.[614] Im Urteil zur Online-Durchsuchung stellte auch das Bundesverfassungsgericht fest, dass es unter anderem dem Schutzbereich des Art. 13 GG unterfiele, wenn mittels der Infiltration eines sich einer Woh-

610 BVerfGE 120, 274, 308.
611 BVerfGE 120, 274, 308.
612 BVerfGE 120, 274, 302; *Gercke* in: HK-StPO, § 100b StPO, Rn. 2.
613 BVerfGE 120, 274, 307 f.; vgl. auch *Gähler*, HRRS 2016, 340, 345.
614 Vgl. bzgl. der Legitimation mittels § 100c StPO einen Eingriff in diese Grundrechte zu rechtfertigen, *Gercke* in: HK-StPO, § 100c StPO, Rn. 1.

nung befindlichen informationstechnischen Systems, bestimmte Vorgänge innerhalb einer Wohnung mittels der an dem System angeschlossenen Mikrofone überwacht werden sollen.[615] Zwar würde Art. 13 GG keinen Schutz gegen die infolge der Infiltration mögliche Datenerhebung aus dem System bieten,[616] doch ist dies im hiesigen Kontext aus zwei Gründen nicht von Bedeutung. Zum einen soll es wie dargelegt zu einer solchen Datenerhebung aus dem System gar nicht kommen. Zum anderen sind auf dem infiltrierten Endgerät in Form eines Smart Speakers im Unterschied zu einem Personalcomputer auch keine Datenbestände gespeichert, sodass eine solche Erhebung bereits aus praktischen Gesichtspunkten ausscheidet und eine Kollision mit dem IT-Grundrecht nicht zu befürchten ist.[617] Somit handelt es sich bei der Manipulation eines Smart Speakers nicht um einen Zugriff in ein informationstechnisches System, durch den auf dem System vorhandene Daten ganz oder teilweise ausgespäht werden sollen oder können. Es besteht mithin auch nicht die Gefahr, durch eine Datenerhebung *aus* dem informationstechnischen System „*einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten*“[618]. Im Übrigen erscheint es widersprüchlich, das insofern mildere Vorgehen eines ferngesteuerten Softwarezugriffs zu versagen, jedoch zu erlauben, die Wohnung des Betroffenen durch mehrere Beamte zu betreten und sodann im Smart Speaker eine zusätzliche Hardwarekomponente oder eine Wanze zu verbauen. Ferner ist zu beachten, dass die Anordnung der Wohnraumüberwachung hohen Hürden unterliegt, sodass nicht die Gefahr besteht, dass jeder Nutzer eines Smart Speakers infolge der einfacheren Möglichkeit der Strafverfolgungsbehörden eine Wohnraumüberwachung ohne aufwendige Verkabelung der Wohnung durchführen zu können, vorschnell Betroffener einer solchen Maßnahme zu werden droht. Nach alledem ist der Zugriff auf Smart Speaker zur Durchführung eines Lauschangriffs unter den Voraussetzungen des § 100c StPO zuzulassen.[619] Durch § 100c StPO nicht gedeckt bleibt der Zugriff auf das Endgerät, um dessen Kamera für eine visuelle

615 BVerfGE 120, 274, 310.
616 BVerfGE 120, 274, 311.
617 Anders könnte dies zu beurteilen sein, wenn ein Sprachassistent in einem Smartphone integriert ist, auf welchem selbst wiederum persönlichkeitsrelevante Daten gespeichert sind.
618 BVerfGE 120, 274, 314.
619 Offenlassend *Gless*, StV 2018, 671, 674; *Anders,* ZIS 2020, 70, 76; ablehnend *Rüscher*, NStZ 2018, 687, 690; *Meinicke*, DSRITB 2018, 835, 851; *Weber,* jM 2021, 252, 256; *Brodowski* in: BeckOK-ITR, X, § 100c StPO, Rn. 6 f.

Überwachung zu nutzen. Art. 13 Abs. 3 GG sowie § 100c StPO umfassen nach ihrem ausdrücklichen Wortlaut lediglich die akustische nicht aber die visuelle Wohnraumüberwachung.

4) Verpflichtung der Hersteller zur Mitwirkung

Darüber hinaus stellt sich die Frage, ob die Strafverfolgungsbehörden die Hersteller smarter Endgeräte verpflichten können, in ihre Geräte „Hintertüren" (sog. backdoors) einzubauen, um das Mikrofon ohne gesonderten Hack der Behörden zu aktivieren.[620] Bereits der ehemalige Bundesinnenminister de Maizière, forderte Hintertüren in IT-Systemen, damit Lausch- und Überwachungsbefugnisse nicht durch technische Sicherungen erschwert werden.[621] Hierzu müssten die Systeme bereits bei ihrer Anfertigung mit entsprechenden Funktionen oder Sicherheitslücken ausgestattet werden.[622] Damit ginge jedoch einher, dass solche bewusst geschaffenen Sicherheitslücken auch von Dritten unberechtigten Personen genutzt werden könnten. Die Anbieter zu verpflichten, die bestehende Sicherungen gezielt auszulassen ist daher mit den seit 20 Jahren geltenden Krypto-Eckpunkten der Bundesregierung nicht zu vereinbaren.[623] Kryptografische Backdoors würden eine enorme Gefahr gegenüber der organisierten Kriminalität, Akteure der Wirtschaftsspionage oder ausländische Geheimdiensten begründen.[624] Eine entsprechende Ermächtigungsgrundlage zum Einbau solcher Hintertüren kann damit nicht verfassungskonform sein.[625] Zwar stellt das Nachverfolgen konkreter Verdachtslagen ein legitimes staatliches Sicherheitsinteressen dar, sodass auch unterschiedlich geartete Zugriffe auf technologische Endgeräte möglich sein müssen. Auch wenn durch die Existenz von Kryptografie dieser Zugriff unweigerlich wesentlich erschwert wird, kann die Schwächung dieser Errungenschaft der Kryptopolitik aus den späten 90er Jahren jedoch keine verfassungsrechtlich verhältnismäßige Gangart zur Erreichung einer einfacheren Strafverfolgung sein.[626] Die generelle Absenkung des Sicherheitsstandards un-

620 *Krempl*, c´t 2019, Heft 14, 36.
621 Vgl. *Schaar*, MMR 2018, 125, 126; *Blechschmitt*, MMR 2018, 361, 365 m.w.N.
622 *Derin/Golla*, NJW 2019, 1111, 1112.
623 MMR 1999, XVII, XVIII; *Krempl*, c´t 2019, Heft 14, 36; vgl. auch § 4, B.), V), 1) a).
624 *Hornung*, MMR 2015, 145, 146.
625 *Hornung*, MMR 2015, 145, 146; *Meinicke*, DSRITB 2012, 773, 776.
626 *Hornung*, MMR 2015, 145, 146.

terschiedlicher Technologien würde ein Einfallstor für Kriminelle unterschiedlichster Richtungen darstellen und kann mit dem einfacheren und weniger komplizierten Zugriff auf entsprechende Systeme nicht aufgewogen werden. Gerade angesichts der großen Menge an dadurch weniger geschützten unbeteiligten IT-Systemen und den im Vergleich hierzu verschwindend geringen Zugriffen der Strafverfolgungsbehörden auf solche Systeme kann ein angemessener Interessensausgleich nicht hergestellt werden.

VII) Kombination aus § 100b und § 100c StPO

Sofern die Durchführung des Lauschangriffs unter Heranziehung des § 100c StPO abgelehnt wird, wird angedacht diesen durch ein Zusammenspiel der §§ 100b, 100c StPO zu legitimieren. Nur auf diesem Wege könnte unter Heranziehung des § 100b StPO in ein informationstechnisches System eingegriffen werden, um unter Heranziehung des § 100c StPO gleichfalls in Art. 13 GG einzugreifen.[627] Zwar sprechen keine Gründe gegen den gleichzeitigen Einsatz mehrerer heimlicher Ermittlungsmethoden, sofern diese dem Grundsatz der Verhältnismäßigkeit entsprechen und daher nicht zu einer Rundumüberwachung mitsamt einer umfassenden Erstellung eines Persönlichkeitsprofils führen.[628] Dennoch wurde der durch *Rüscher* vorgebrachte Gedanke durch diesen sogleich wieder verworfen. In der Kombination der §§ 100b, 100c StPO würde kein gleichzeitiger Einsatz der Ermittlungsbefugnisse im Sinne einer parallel ablaufenden Online-Durchsuchung und einer zeitgleich ablaufenden Wohnraumüberwachung stattfinden, sondern es würde eine einheitliche Überwachungsmethode aus zwei getrennt voneinander zu betrachtenden Ermittlungsbefugnissen als „neuartiges Ermittlungsmittel" geschaffen.[629] Unabhängig davon, dass es eines solchen Konstrukts, aufgrund der bestehenden Zugriffsmöglichkeit nach § 100c StPO, nicht bedarf, würde aufgrund der Frage welche Eingriffsvoraussetzungen einem solchen Zusammenspiel aus bestehenden Ermächtigungsgrundlagen zu Grunde zu legen wären, eine gewisse Rechtsunsicherheit entstehen, die weder erforderlich ist und die es im Übrigen auch generell zu vermeiden gilt.

---

627 *Rüscher*, NStZ 2018, 687, 692.
628 BVerfGE 112, 304, 319.
629 *Rüscher*, NStZ 2018, 687, 692.

VIII) § 100f StPO

Neben der Möglichkeit im Rahmen des „großen Lauschangriffs" auf Smart Speaker in Wohnungen zuzugreifen, bleibt die Frage, ob daneben auch außerhalb von Wohnungen – beispielsweise auf die in Smartphones verbauten Sprachassistenten – zugegriffen werden kann. Dies wäre vor allen Dingen von großem Interesse, wenn die Verdächtigen während eines Spaziergangs oder – gerade bei Delikten des Wirtschaftsstrafrechts – im Büro abgehört werden sollen. Seinem Wortlaut nach erlaubt § 100f StPO das Abhören oder Aufzeichnen des außerhalb von Wohnungen gesprochenen nichtöffentlichen Wortes mit technischen Mitteln. Als Eingriffsvoraussetzung erfordert er zudem lediglich das Vorliegen einer Katalogtat nach § 100a Abs. 2 StPO anstelle wie § 100c StPO das Vorliegen einer in § 100b Abs. 2 StPO genannten Tat. Im Unterschied zu § 100c Abs. 1 Nr. 4 StPO ist darüber hinaus lediglich gefordert, dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise mindestens wesentlich erschwert aber nicht unverhältnismäßig erschwert wäre. Im Übrigen sind die Eingriffsvoraussetzungen bis auf § 100c Abs. 1 Nr. 3 StPO gleich. Die im Gesamten milderen Eingriffsvoraussetzungen bei § 100f StPO legen daher bereits aufgrund eines Erst-Recht-Schlusses nahe, dass die Strafverfolgungsbehörden, wenn schon die Überwachung gar in der besonders schützenswerten Wohnung des Betroffenen erlaubt ist, erst Recht außerhalb der Wohnung von diesem geführte Konversationen abhören können. Hinsichtlich der Voraussetzung, dass dieser Zugriff mittels eines technischen Mittels erfolgen muss, kann im Vergleich zu § 100c StPO nichts anderes gelten.[630]

IX) §§ 102 ff., 110 Abs. 3 StPO

Die dargestellten heimlichen Überwachungsmöglichkeiten werden ergänzt durch die der offenen Ermittlungsbefugnisse. Zentraler Bestandteil hiervon sind die Durchsuchungsvorschriften der §§ 102 ff. StPO. Ziel einer solchen Durchsuchung ist entweder die Ergreifung des Verdächtigen (Ergreifungsdurchsuchung) oder das Auffinden von Beweismitteln (Ermittlungsdurchsuchung). Die §§ 102, 103 StPO ermächtigen jedoch zum einen lediglich zu einer groben Sichtung durch Inaugenscheinnahme.[631] Zum

630 Vgl. oben A. VI).
631 *Süptitz/Utz/Eymann*, DuD 2013, 307, 308.

anderen enthalten sie auch keine Reglung auf elektronisch archivierte Datenbestände zuzugreifen, die sich nicht in den Räumlichkeiten des Durchsuchungsobjekts befinden, da sie dezentral in einer Cloud gespeichert sind.[632] Die detailliertere Durchsicht von aufgefundenen Papieren oder ganzen Aktenordnern wird in § 110 StPO gesondert geregelt ist. Bezüglich elektronisch gespeicherter Daten von besonderer Relevanz ist dabei § 110 Abs. 3 StPO, der auch die Durchsicht extern abgelegter elektronischer Daten erlaubt, sofern auf diese von einem Speichermedium in den durchsuchten Räumlichkeiten zugegriffen werden kann.[633] Dadurch wird eine inhaltliche Prüfung dieser Daten ermöglicht, um zu entscheiden, ob diese aufgrund ihrer Bedeutung für das weitere Strafverfahren durch richterliche Beschlagnahme zu sichern sind. Zeitlich betrachtet stellen die Durchsuchungsvorschriften daher eine Vorstufe zur Beschlagnahme nach den §§ 94 ff. StPO dar.[634] Ziel einer Durchsicht, die im Idealfall bereits während der laufenden Durchsuchungsmaßnahme durch Techniker des LKA abgeschlossen ist, ist es, im Rahmen der Ermittlungsdurchsuchung zu bestimmen, welche Unterlagen für die Verfahrenszwecke tatsächlich relevant sind und damit förmlich beschlagnahmt werden müssen, um so eine übermäßige Datenerhebung von für das Verfahren irrelevanter Daten zu vermeiden.[635] Hierfür können die IT-Spezialisten des LKA auf den Einsatz spezieller Software zurückgreifen, die eine Durchsuchung anhand von Suchbegriffen ermöglicht.[636] Letztlich stellt § 110 StPO daher eine Norm dar, die die von der Beschlagnahme ausgehende Eingriffsintensität verringern soll.[637] Dies bringt jedoch mit sich, dass die Auswertung extern, also in Echtzeit beim Beschuldigten vor Ort und vor allem zeitlich an die Dauer der Durchsuchung geknüpft ist. Endet die Durchsuchung, so endet auch die Befugnis aus § 110 Abs. 3 StPO beim Beschuldigten vor Ort.

1) Physische Hardware

Finden die Ermittlungsbehörden vor Ort einen Datenträger auf, so können sie diesen entweder mitnehmen (vorläufige Sicherstellung) oder eine

632 *Graßie/Hiéramente*, CB 2019, 191, 192.
633 *Gercke* in: HK-StPO, § 110 StPO, Rn. 18; *Graßie/Hiéramente*, CB 2019, 191, 192; Angerer DRiZ 2019, 428, 431.
634 *Blechschmitt*, MMR 2018, 361, 363.
635 BT-Dr 16/5846, S. 63; *Graßie/Hiéramente*, CB 2019, 191, 192.
636 *Graßie/Hiéramente*, CB 2019, 191, 192.
637 BVerfGE 113, 29, 58; BVerfGE 124, 43, 72; *Beulke/Meininghaus*, StV 2007, 63, 64.

Datenkopie vor Ort fertigen.[638] Handelt es sich bei dem Gegenstand um einen mobilen Datenträger wird regelmäßig eine forensische Duplikation der Daten angefertigt. Diese Duplikation wird sodann als Arbeitsversion zum permanenten Zugriff der Ermittlungsbehörden abgespeichert und zum anderen als reine Sicherungskopie, die zum Ausschluss einer Veränderung der Metadaten unangetastet beim IT-Referenten verbleibt.[639] Da die Hardware so unter Umständen gar nicht mitgenommen werden muss, trägt dieses Vorgehen dem Verhältnismäßigkeitsgrundsatz in besonderer Weise Rechnung.[640]

2) Digitale Serverdaten

Anders stellt sich dies bei der Sicherstellung von Beweismitteln in Netzwerken dar. Es ist hier bereits aus Kapazitätsgründen regelmäßig unmöglich, das gesamte Netzwerk oder den gesamten Server vorläufig sicherzustellen. Die Unverhältnismäßigkeit eines solchen Vorgehens wäre ferner evident, wenn man sich vergegenwärtigt, dass es sich bei einem solchen Server in der Regel um den eines Dritten (häufig eines Unternehmens in Form des Dienstleistungsanbieters) handelt. Auf diesem sind neben den Daten des Betroffenen die Daten von im Zweifel Millionen anderer Personen gespeichert, die zweifelsohne unangetastet bleiben müssen.[641]

a) Entwicklung des § 110 Abs. 3 StPO

Bei § 110 Abs. 3 StPO handelt es sich um eine vergleichsweise junge Norm mit deren Kodifizierung der Gesetzgeber darauf reagierte, dass die herkömmlichen Befugnisnormen aus einer Zeit stammen, in der elektronisch gespeicherte Daten eine Seltenheit darstellten. War über lange Zeit die Aktenablage das vorherrschende Mittel zur Archivierung von Daten, werden diese heute vermehrt digital gespeichert. Als Reaktion hierauf sollten die auf physische Gegenstände in Papierform anwendbaren Vorschriften über die Gewinnung von Beweismitteln auf sämtliche Medien ausgeweitet werden, die menschliche Gedankenerklärungen und sonstige Informationen

638 *Bell*, Beschlagnahme und Akteneinsicht, S. 11 ff.
639 *Bär* in: Handbuch des Wirtschafts- und Steuerstrafrechts, Kapitel 28, Rn. 59.
640 *Greven* in: KK-StPO, § 94 StPO, Rn. 13; *Basar/Hiéramente*, NStZ 2018, 681, 682.
641 *Basar/Hiéramente*, NStZ 2018, 681, 682.

verkörpern oder speichern.[642] Im Zeitalter der fortschreitenden Digitalisierung sind es vor allem verschiedene Modelle des Cloud-Computing, auf deren neuartige Strukturen der Gesetzgeber reagieren musste. Auch im Rahmen der Sichtung der durch Sprachassistenten aufgezeichneten Daten tritt diese Problematik hervor. Die Datensichtung gelingt durch einen bloßen unmittelbaren Zugriff auf den als Durchsuchungsobjekt vorhandenen physischen Gegenstand nicht mehr. Vielmehr benötigen die Strafverfolgungsbehörden die Möglichkeit auch die auf einem virtuellen Speicher in Form eines Servers gespeicherten Unterlagen zu durchsuchen. Auf jenes Problem der dezentralen Datenspeicherung hat der Gesetzgeber mit der Erweiterung des § 110 StPO um Absatz 3 reagiert, indem die Durchsichtsmöglichkeiten auf verbundene Speichermedien erstreckt wurden.[643] § 110 Abs. 3 StPO ermächtigt mithin die Ermittlungsbehörden, sich Zugang zum Online-Account des Betroffenen zu verschaffen, um bereits während der Durchsuchung ausloten zu können, inwiefern eine förmliche Beschlagnahme überhaupt erforderlich ist.[644]

b) Voraussetzungen

aa) Allgemeines

§ 110 Abs. 3 StPO fordert für einen Online-Zugriff, die Gefahr des drohenden Datenverlusts. Die Gefahr darf nicht bloß behauptet werden, vielmehr müssen konkrete Anhaltspunkte vorliegen.[645] Mit entscheidend ist in diesem Zusammenhang, ob der Nutzer in der Lage ist, einen irreversiblen Datenverlust beim Dienstleistungsanbieter herbeizuführen. Es wird hinsichtlich Sprachassistenzsysteme zur Bejahung konkreter Anhaltspunkte für eine solche Gefahr jedoch bereits ausreichend sein, dass der Betroffene die Möglichkeit hat, gespeicherte Cloud-Inhalte zu löschen.[646] Sowie ein Tatverdächtigter von dem geplanten Zugriff auf seine Daten beim Dienstleistungsanbieter erfahren würde, würde er seinen zeitlichen Vorsprung

642 *Obenhaus*, NJW 2010, 651, 651.
643 Vgl. BS-Drs. 19/11478 als Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Benjamin Strasser, Stephan Thomae, Manuel Höferlin, weiterer Abgeordneter und der Fraktion der FDP, S. 3; *Bär*, ZIS 2011, 53, 54.
644 *Wolter* in: SK-StPO, § 110 StPO, Rn. 6; *Graßie/Hiéramente*, CB 2019, 191, 192.
645 *Park*, Durchsuchung und Beschlagnahme, Rn. 823.
646 Vgl. https://www.amazon.de/gp/help/customer/display.html?nodeId=201602230 (zuletzt abgerufen am 31.10.2021).

nutzen, um mögliche ihn belastenden Aufzeichnungen über seinen Account zu löschen. Um § 110 Abs. 3 StPO nicht seines Sinnes zu berauben, darf keine konkrete Zugriffsmöglichkeit im Zeitpunkt der Durchsuchung auf die gesondert gespeicherten Daten gefordert werden. Eine abstrakte Zugriffsmöglichkeit muss in diesen Fällen genügen.[647] In Extremfällen käme man ansonsten zu dem verwunderlichen Ergebnis, dass sich der Betroffene durch einen defekten Computer oder einer im Moment der Durchsuchung nicht vorhandenen Internetverbindung der Durchsicht entziehen könnte.[648] Erforderlich ist lediglich, dass ein Zugriff auf die räumlich getrennten Speichermedien mit den lokalen informationstechnischen Systemen möglich ist.[649] Insofern ist bei Sprachassistenten zu beachten, dass im Unterschied zu Fällen des herkömmlichen Cloud-Storage (bspw. Dropbox), in denen direkt über das informationstechnische Endgerät in Form einer Desktopanwendung die Durchsicht der gespeicherten Daten erfolgen kann, dies beim Sprachassistenten nicht unmittelbar über das informationstechnische Endgerät möglich ist. Vielmehr ist mittels der Zugangsdaten über einen Computer eine Anmeldung bei dem beim Dienstleistungsanbieter hinterlegten Account erforderlich, um auf das räumliche getrennte Speichermedium in Form des Servers zugreifen zu können. Dies hindert die Anwendung der Vorschrift auf Sprachassistenten jedoch mitnichten.[650] Denn es muss lediglich mittels eines von der Durchsuchung betroffenen Systems auf die Cloudserver zugegriffen werden können.[651] Für die Praxis ist daher entscheidend, dass im Durchsuchungsbeschluss die räumlich getrennten Speichermedien, auf die sich die Durchsicht beziehen kann, wenigstens gegenständlich beschrieben werden.[652]

---

647 *Brodowski/Eisenmenger,* ZD 2014, 119, 122; *Park*, Durchsuchung und Beschlagnahme, Rn. 825.

648 *Brodowski/Eisenmenger,* ZD 2014, 119, 122.

649 *Gercke* in: HK-StPO, § 110 StPO, Rn. 18.

650 Vgl. den Verweis auf „digitale Assistenten wie „Alexa" (Amazon), „Siri" (Apple), „Cortana" und „Hello" (Microsoft und Google)" *Bruns* in: KK-StPO, § 110 StPO, Rn. 8.

651 *Wicker*, MMR 2013, 765, 767.

652 *Herrmann/Soiné,* NJW 2011, 2922, 2925; *Knierim*, StV 2009, 206, 211; vertiefend vgl. *Hiéramente*, wistra 2016, 432, 433; zu den Anforderungen vgl. aktuell BGH, Beschluss vom 09.02.2021 – StB 9/20, StB 10/20; a.A.: *Ladiges* in: Radtke/Hohmann, § 110 StPO, Rn. 16.

bb) Möglichkeiten der Sichtung

Die Sichtung ist für die Ermittlungsbeamten auf verschiedenen Wegen durchführbar. Über seinen Wortlaut hinaus, der eine Wegnahme des durchsuchten Gegenstandes oder Datenträgers nicht vorsieht, ist § 110 StPO im Hinblick der Gewährleistung einer effektiven und gründlichen Durchsicht weit zu verstehen, sodass auch eine Mitnahme des Datenträgers möglich ist (vorläufige Sicherstellung).[653] In diesem Fall haben die Ermittlungsbeamten schließlich gem. § 98 Abs. 2 S. 1 StPO innerhalb von drei Tagen die richterliche Bestätigung der vorläufigen Sicherstellung zu beantragen. Die Durchsicht hat sodann unter Beachtung des Verhältnismäßigkeitsgrundsatzes und der konkreten Umstände des Einzelfalles zügig zu erfolgen, muss aber – auch in der gerichtlichen Bestätigung – nicht ausdrücklich befristet werden.[654]

Bezüglich eines Smart Speaker ist an dieser Stelle jedoch problematisch, dass die Mitnahme des vermeintlichen Datenträgers in Form des Endgeräts keinen Mehrwert darstellen würde, da hierauf keine gespeicherten Inhalte zu finden sind.[655] Zur Sichtung der aufgezeichneten Daten sind lediglich die Zugangsdaten zum Account des Betroffenen entscheidend. Um dem Betroffenen die Möglichkeit zu nehmen, sich nach der erfolgten Durchsuchung selbst in seinem Account einzuloggen und entsprechende Aufnahmen zu löschen, stellt sich die Frage, ob die Strafverfolgungsbehörden auch ermächtigt sind, die Zugangsdaten temporär zu ändern oder wenigstens eine virtuelle Versiegelung anzubringen. Ob dies im Sinne einer effektiven Strafverfolgung möglich ist, dürfte letztlich eine Frage der Verhältnismäßigkeit, insbesondere eine solche der Erforderlichkeit, darstellen. Hinsichtlich milderer Mittel ist vor allem an eine Sicherungskopie zu denken, vgl. § 110 Abs. 3 S. 2 StPO. Dadurch wird der zum Zeitpunkt der Durchsuchung vorhandene Datenbestand eingefroren und ein Beweismittelverlust ist nicht zu befürchten. Insbesondere wird durch ein derartiges Vorgehen auch vermieden, dass die Strafverfolgungsbehörden im Rahmen der Sichtung zu späteren Zeitpunkten mehrere Male immer wieder unmit-

653 BGH, NStZ 2003, 670, 671; *Köhler* in: Meyer-Goßner/Schmitt, § 110 StPO, Rn. 2; *Hegmann* in: BeckOK-StPO, § 110 StPO, Rn. 8; *Bruns* in: KK-StPO, § 110 StPO, Rn. 9.

654 BGH, Beschluss. v. 20.–5.2021 – StB 21/21; BGH, NStZ 2003. 671, 671.

655 Zur Frage, ob ein Datenträger bzw. die Hardware, auf der unmittelbar potenzielles Beweismaterial gespeichert ist zur Durchsicht auf Grundlage des § 110 StPO ohne Beschlagnahme mitgenommen werden darf, vgl. *Liebig*, Der Zugriff auf Computerinhaltsdaten, S. 35 ff.

telbar auf den Server zugreifen und dabei womöglich auch neue, nach der durchgeführten Durchsuchung, aufgezeichnete Nachrichten einsehen. Ein solches Vorgehen wäre nicht durch die Befugnisnorm des § 110 StPO gedeckt, da diese lediglich den einmaligen, punktuellen Zugriff auf ein Speichermedium erlaubt.[656] Nach Erstellen der Sicherungskopie darf daher keine Verbindung mehr zum Server aufgebaut werden. Ansonsten würden die Grenzen zur Online-Durchsuchung verwischt, da jeder weitere Zugriff auf räumlich getrennte Speichermedien keine bloße Durchsicht, sondern eine Überwachung darstellen würde.[657] Dieses Vorgehen ist für den Betroffenen bedeutend milder als die mit einer Beschlagnahme einhergehende Entziehung der Nutzungsmöglichkeiten des entsprechenden Gegenstandes oder im Falle elektronischer Daten einer anzudenken Zugangssperre, sodass dadurch dem Verhältnismäßigkeitsgrundsatz in besonderer Weise genügt wird.[658] Die Beachtung des Verhältnismäßigkeitsgrundsatzes einer Sichtung nach § 110 Abs. 3 StPO weiter unterstreichend, kann zudem bereits in der Durchsuchungsanordnung nach § 105 StPO der Zeitraum aus welchem Aufzeichnungen Gegenstand einer Sicherungskopie sein sollen zeitlich begrenzt werden. Erhoffen sich die Ermittler Erkenntnisse zu einer konkreten Mordnacht so wird es in der Regel ausreichend sein, die Aufzeichnungen weniger Tage vor und nach dem Tattag zu sichten. Unabhängig von der technisch bedingten Sinnlosigkeit das Endgerät des Sprachassistenten als physische Hardware sicherzustellen, scheidet wie dargelegt auch die (vorläufige) Sicherstellung des kompletten Servers aus Verhältnismäßigkeitsgesichtspunkten aus. Stattdessen muss die Sichtung mittels eines unmittelbaren Zugriffs auf die konkreten Daten des Betroffenen vorgenommen werden (sog. Live-Forensik[659], während das betroffenen System noch „online" ist, daher noch läuft). Problematisch dabei ist, dass mit einem solchen unmittelbaren Zugriff stets Veränderungen im System einhergehen, wodurch die sog. Metadaten verwischt werden können.[660] Im Übrigen kann auch die sog. Live-Forensik das Problem nicht lösen, dass keine ausreichende Vorsortierung der zu sichernden Daten möglich ist.

656 *Köhler* in: Meyer-Goßner/Schmitt, § 110 StPO, Rn. 6; *Zerbes / El-Ghazi*, NStZ 2015, 425, 432.

657 *Brodowski/Eisenmenger,* ZD 2014, 119, 125.

658 BT-Drs. 16/5846, S. 63.

659 Vgl. *Heinson*, IT-Forensik, S. 37; BSI Leitfaden „IT – Forensik", 2011, S. 13, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 31.10.2021).

660 *Basar/Hiéramente*, NStZ 2018, 681, 682.

Aufgrund der zeitlichen und ressourcentechnischen Umstände bei einer Durchsuchung, ist oftmals lediglich die Sicherung ganzer Verzeichnisse umsetzbar, was regelmäßig eine breitflächige Sicherung verfahrensirrelevanter Daten bedeutet.[661] Gleichwohl darf auf eine sorgfältige Durchsicht zum Ziel der Aussonderung nicht beweisrelevanter Daten nicht mit dem Argument verzichtet werden, dass der auf einem Datenträger gespeicherte Datenbestand ein einziges Beweismittel sei.[662] Beweismittel ist stets der konkrete Inhalt sowie die Metadaten der Dateien, nicht jedoch der gesamte Datenträger hinsichtlich der sich darauf befindlichen Dateien.[663] Allein der Umstand, dass potentiell beweisrelevante Daten auf einem Server gespeichert sind, legitimiert ferner nicht dazu, den gesamten Datenbestand des Serverlaufwerks zu kopieren.[664]

cc) Möglichkeiten zur Passworterlangung

Um den Accountzugriff zu ermöglichen, ergibt sich aus § 110 Abs. 3 StPO jedoch keine Verpflichtung für den von der Durchsuchung Betroffenen, den Ermittlungsbehörden den Zugriff auf einen solchen Account durch die Herausgabe möglicher Passwörter zu ermöglichen.[665] Unter Zugrundelegung des nemo-tenetur Grundsatzes muss der Beschuldigte sich an seiner eigenen Überführung nicht aktiv beteiligen.[666] Der nemo-tenetur-Grundsatz ist als Ausdruck der uneingeschränkten rechtsstaatlichen Achtung der Menschenwürde in Art. 20 Abs. 3 GG verankert und verbietet es den Beschuldigten zu zwingen, aktiv an seiner Überführung mitzuwirken.[667] Ob und inwieweit der Beschuldigte im Strafverfahren mitwirkt, muss er – nicht zuletzt aufgrund seiner verfassungsrechtlichen Stellung als Verfahrensbeteiligter und nicht bloßes Objekt des Verfahrens – selbstbestimmt entscheiden können.[668] Ebenso hat daher ein zwangsweises Hinwirken

661 *Basar/Hiéramente*, NStZ 2018, 681, 683.
662 BVerfGE 113, 29, 61.
663 *Szesny*, WiJ 2012, 228, 231.
664 *Szesny*, WiJ 2012, 228, 231.
665 *Obenhaus*, NJW 2010, 651, 652 f.
666 *Neuhaus*, StV 2020, 489, 490; *Rottmeier/Eckel*, NStZ 2020, 193, 199.
667 BVerfG, NJW 2013, 1058, 1061; *Momsen*, DRiZ 2018, 140, 141.
668 BVerfG, NJW 2013, 1058, 1061; ebenso zählt der Grundsatz der Selbstbelastungsfreiheit zum Kern des von Art. 6 EMRK garantierten Rechts auf ein faires Strafverfahren schützt den Beschuldigten gegen unzulässige Zwangs- und Druckausübung seitens der Strafverfolgungsbehörden, vgl. EGMR, StV 2003,

auf die Preisgabe der Daten gem. § 136a Abs. 1 StPO zu unterbleiben.[669] Sofern die Zugangsdaten nicht freiwillig herausgegeben werden, kommen für die Strafverfolgungsbehörden verschiedene Möglichkeiten in Betracht.

(1) Technische Entschlüsselung

Naheliegend ist der Versuch einer technischen Entschlüsselung. Bereits in der Gesetzesbegründung heißt es hierzu, dass sich die Strafverfolgungsbehörden zwar nicht mittels eines heimlichen staatlichen Hackerangriffes Zugang zum gesicherten Server verschaffen dürfen, die Durchsuchung und damit auch die Möglichkeit der Datensichtung jedoch zwangsweise durchsetzbar bleiben muss.[670] Dies bedeutet, dass nachdem der Betroffene die Herausgabe der Zugangsdaten verweigert hat, es den Ermittlungsbeamten gestattet ist, mittels einer Software das vom Betroffenen benutzte technische System nach den hier zwischengespeicherten Passwörtern zu durchleuchten.[671] Eine Möglichkeit stellt in diesem Kontext die die „Brute-Force"-Methode dar, mittels derer durch das Ausprobieren aller möglichen Passwortkombinationen die Zugangsdaten errechnet werden können.[672] Um die für diese Berechnungsprozesse notwendige Rechnerleistung zu minimieren und die Entschlüsselung zu beschleunigen, können alle auf dem Computer gespeicherten Worte indiziert werden und die Entschlüsselungsversuche im Rahmen der Brute-Force-Methode auf die in diesem

257, 259; zu den verfassungsrechtlichen Grundlagen des Nemo-tenetur Grundsatzes vgl. *Böse*, GA 2002, 98 ff.

669 *Bäumerich*, NJW 2017, 2718, 2720; *Gercke*, MMR 2008, 291, 298; *Gerhards*, Recht auf Verschlüsselung, S. 294 f.

670 BT-Dr 16/5846, S. 64.

671 *Zerbes/El-Ghazi*, NStZ 2015, 425, 432; *Peters*, NZWiSt 2017, 465, 467.

672 *Hegmann* in: BeckOK-StPO, § 110 StPO, Rn. 18. Dabei ist jedoch zu berücksichtigen, dass für ein solches Vorgehen große Rechnerleistungen erforderlich sind. Bereits ein handelsüblicher Computer bräuchte beispielsweise für das Herausfinden eines komplexen achtstelligen Passworts mit Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen ca. 83 Tage. Besteht das Passwort hingegen lediglich aus Kleinbuchstaben, nimmt der entsprechende Prozess nur noch 35 Minuten in Anspruch. Trotz dieser unter Umständen erheblichen Zeitspanne ist zu berücksichtigen, dass den Strafverfolgungsbehörden in der Regel hochleistungsfähige Computer zur Verfügung stehen, das korrekte Passwort nicht erst als letzte denkbare Alternative herausgefunden wird und die Betroffenen nicht immer ein komplexes Passwort verwenden werden, vgl. *Grözinger*, Die Überwachung von Cloud-Storage, nach BSI, IT-Grundschutz, S. 50.

Index enthaltenen Wörter beschränkt werden bzw. um entsprechende Mutationen (z. B. mit Zahlen oder Sonderzeichen, Groß-, Kleinschreibung) ergänzt werden.[673] Nach anderer Auffassung soll dies angesichts des Umstandes, dass damit ein gravierender, verdeckter (Begleit-)Eingriff in die Integrität des externen informationstechnischen Systems einhergehe, nicht erlaubt sein.[674] Es bliebe allenfalls die Möglichkeit dass die Ermittler die Zugangsdaten selbst – als zwischengestaltete menschliche Aktion – eingeben, nachdem diese beispielsweise in den Unterlagen des Betroffenen während einer Durchsuchung aufgefunden wurden.[675] Nur auf diese Weise könnten die Zugangshindernisse des Servers auf dem dafür vorgesehen Wege und damit rechtmäßig aufgehoben werden. Dafür, dass jedoch darüber hinausgehend auch der Einsatz entsprechender technischer Mittel zur Kenntniserlangung der Zugangsdaten als „Annexkompetenz" von § 110 Abs. 3 StPO umfasst sein muss, spricht, dass auch im Rahmen der Durchsuchung nach § 102 StPO gefundene Behältnis aufgebrochen werden dürfen.[676] Ob ein physisches oder virtuelles Zugangshindernis durchbrochen wird, kann dabei keinen Unterschied machen.

(2) Bestandsdatenabfrage gem. § 100j StPO

Zudem käme in Betracht die Zugangsdaten im Rahmen einer Nutzungs- und Bestandsdatenabfrage gem. § 100j StPO beim Dienstleistungsanbieter zu erfragen.[677] Die im Zuge der Änderung des Telekommunikationsgesetzes zum 01.07.2013 in Kraft getretene Vorschrift,[678] ermöglicht es von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des TKG erhobenen Daten zu verlangen. Gem. § 113 Abs. 1 S. 2 TKG[679] gilt

673 *Willer/Hoppen*, CR 2007, 610, 615.
674 *Brodowski/Eisenmenger,* ZD 2014, 119, 123.
675 *Brodowski/Eisenmenger,* ZD 2014, 119, 123.
676 *Obenhaus*, NJW 2010, 651, 653; *Köhler* in: Meyer-Goßner/Schmitt, § 110 StPO, Rn. 6.
677 *Krause*, Kriminalistik 2014, 213, 214.
678 *Bruns* in: KK-StPO, § 100j StPO, Rn. 1.
679 Nach BVerfG, NJW 2020, 2699, Rn. 134 ff., ist § 113 TKG überdies verfassungswidrig, da die auf alleiniger Grundlage des § 113 TKG erfolgte Bestandsdatenabfrage nicht den Grundsätzen der Verhältnismäßigkeit genügt. Der Norm fehlt es an normierten Eingriffsschwellen, die sicherstellen, dass Auskünfte nur bei einem auf tatsächliche Anhaltspunkte gestützten Anlass eingeholt werden

dies theoretisch auch für die hier gefragten Zugangssicherungscodes.[680] In Anbetracht dessen, dass die Server des Sprachassistenten räumlich getrennte Speichermedien des Endgeräts darstellen, scheint die Vorschrift wie geschaffen für die hiesige Situation. Dies zeigen auch die Gesetzgebungsmaterialien, nach denen die Vorschrift auf Vorgänge des Cloud Computing Anwendung finden soll.[681] Dem gesetzgeberische Willen nach sollte durch die Neuregelung des § 100j StPO am Beispiel des Cloud-Computing durch die Herausgabe der Zugangsdaten ein Zugang zu extern abgespeicherten Daten ermöglicht werden.[682] Dabei ist zu beachten, dass Voraussetzung für eine Abfrage, die einen Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, darstellt, das Vorliegen der gesetzlichen Voraussetzungen für die beabsichtige Form der Nutzung der Zugangsdaten notwendig ist, § 100j Abs. 1 S. 2 StPO.[683] Soll heimliche laufende Telekommunikation überwacht werden, müssen die Voraussetzungen des § 100a StPO vorliegen, sollen archivierte Daten öffentlich durchsucht oder beschlagnahmt werden, müssen regelmäßig die Voraussetzung einer Durchsuchung gem. §§ 102 ff. StPO oder einer Beschlagnahme nach §§ 94 ff. StPO vorliegen.[684] Bezogen auf Cloud-Computing in Form der Nutzung eines Smart Speakers muss § 100a StPO als Rechtsgrundlage jedoch ausscheiden, da dessen Nutzung keine Telekommunikation im Rahmen des § 100a StPO darstellt. Bleiben noch mögliche offenen Ermittlungsbefugnisse. Gegen eine Heranziehung der §§ 94 ff. StPO wird vorgebracht, dass die Passwort Herausgabe und die anschließende Durchsuchung der Cloud nur heimlich erfolgen könne, da der Betroffene ansonsten, sobald er von der Maßnahme Kenntnis erlangt, sein Passwort ändern und belastende Inhalte löschen würde.[685] Dem ist insofern zuzustimmen, dass bei Durchführung der Bestandsdatenauskunft eine Verzögerung zwischen Anfrage und Durchsuchung eintritt, in welcher der Beschuldigte womöglich belastende Aufzeichnungen löschen könnte. Allerdings ist

können. Hinsichtlich der Strafverfolgung ist diesbezüglich wenigstens das Vorliegen eines Anfangsverdachts erforderlich.

680 *Schnabel*, CR 2012, 253, 255.

681 BR-Drs. 664/1/12, S. 13 f.

682 *Graf* in: BeckOK-StPO, § 100j StPO, Rn. 23; *Bär*, MMR 2013, 700, 702; *Bruns* in: KK-StPO, § 100j StPO, Rn. 7; *Dalby*, CR 2013, 361, 363.

683 BT-Drs. 17/12034, S. 13; *Burhoff*, StRR 2015, 8, 9; im Unterschied zu § 113 TKG normiert § 100j Abs. 1 S. 2 StPO damit gesetzliche Eingriffsschwellen.

684 *Keller* in: HH-Ko/MedienR, Abschnitt 90, Rn. 24; *Hauck*, StV 2014, 360, 362.

685 *Dalby*, CR 2013, 361, 368.

nicht vorgeschrieben, dass der Betroffene unmittelbar von der Bestandsdatenabfrage zu informieren ist. Vielmehr ist gem. § 100j Abs. 4 S. 2 StPO die Benachrichtigung erst dann vorzunehmen, wenn hierdurch der Zweck der Auskunft nicht mehr vereitelt würde. Daher ist es gesetzeskonform, eine zunächst heimliche Bestandsdatenabfrage durchzuführen, um sodann in Kenntnis der Passwörter den Beschuldigten aufzusuchen und über dessen technische Geräte eine offene Durchsuchung seiner Cloud durchzuführen. Durch eine heimliche Bestandsdatenauskunft verliert die sich anschließende Durchsuchung nicht ihren Charakter als offene Ermittlungsbefugnis, sofern jedenfalls sie selbst offen durchgeführt wird. Somit bleibt § 94 StPO als Rechtsgrundlage für das Zugreifen auf Cloud-Inhalte im Zusammenspiel mit § 100j Abs. 1 S. 2 StPO erhalten.

Problematisch ist jedoch, ob der Cloud-Anbieter überhaupt als Verpflichteter des § 100j StPO angesehen werden kann.[686] Voraussetzung wäre, dass dieser eine Telekommunikationsdienstleistung erbringt oder an einer solchen mitwirkt. Da bereits § 100j StPO auf das Telekommunikationsgesetz verweist und die Bestandsdatenabfrage mit den dortigen Vorschriften kohäriert, müsste der Cloud-Anbieter daher eine Telekommunikationsdienstleistung im Sinne des Telekommunikationsgesetzes erbringen.[687] Dies sind gem. § 3 Nr. 24 TGK in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über TK-Netze bestehen. Hinsichtlich der Übertragung der Audioaufzeichnungen in die Cloud handelt es sich dabei zweifelsohne um einen solchen Datentransportvorgang im Sinne des TKG. Allerdings wird dieser Übertragungsvorgang gerade nicht vom Cloud-Anbieter, sondern dem Access-Provider, der das Internet bereitstellt, erbracht.[688] Der Cloud-Dienstleister stellt lediglich die Schnittstellen bereit, um die Inhalte nach der Übertragung in die Cloud als Rechenzentrum zu verbringen. Der Transport, mithin die Übertragung der Inhalte als solche, erfolgt dabei vorgelagert durch den von ihm genutzten Transportdienstleister (den Access-Provider), der unabhängig von dem Cloud Dienstleister fungiert.[689] Nur der Access-Provider erbringt daher eine Leistung, die in der Übertragung von Signalen besteht. Dieser Übermittlungsvorgang durch den Access-Provider erfolgt vollständig losgelöst von der Leistungserbringung

686 vgl. auch *Wicker*, MMR 2014, 298, 300.
687 *Wicker*, MMR 2014, 298, 300; *Boos/Kroschwald/Wicker*, ZD 2013, 205, 206.
688 *Wicker*, MMR 2014, 298, 300; *Boos/Kroschwald/Wicker*, ZD 2013, 205, 206.
689 *Kremer/Völkel*, CR 2015, 501, 503.

zwischen Cloud Service und Nutzer.[690] Anbieter von Clouddienstleistungen sind daher nicht mit Telekommunikationsdienstleistern gleichzusetzen.[691] Da Anbieter von Clouddienstleistungen mithin keine Anbieter von Telekommunikationsdienstleistungen sind, sind sie auch nicht Adressat eines Auskunftsverlangens nach § 100j StPO.[692] Um auf § 100j StPO zurückzukommen, kann diese Norm daher nur eine Auskunftsanfrage bei dem Access-Provider (bspw. Deutsche Telekom, 1&1, Freenet oder Vodafone) als Telekommunikationsanbieter legitimieren, die zwar rechtlich zulässig, in der Praxis jedoch nicht zielführend sein wird. Der Telekommunikationsdienstleister kann lediglich Auskunft über Bestandsdaten im Sinne der § 95 und 111 TKG geben, worunter Rufnummern, der Name und die Anschrift des Anschlussinhabers oder das Datum des Vertragsbeginns fallen. Nicht hierunter fallen jedoch Bestandsdaten des Cloud-Nutzers beim Cloud-Anbieter. Diese durch den Cloud-Anbieter erhobenen Bestandsdaten werden stattdessen durch § 14 TMG erfasst, wonach der Telemedienanbieter (daher Apple, Amazon oder Google) personenbezogene Daten eines Nutzers "*erheben und verwenden [darf], soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind*". Diese Bestandsdaten und vor allem die Nutzungsdaten in Form der Merkmale zur Identifikation des Nutzers nach § 15 Abs. 1 Nr. 1 TMG, worunter auch die Zugangsdaten fallen[693], liegen wiederum dem von § 100j StPO erfassten Access-Provider nicht vor, da sie nur vom Cloud-Anbieter als Telemedienanbieter erhoben werden können.[694] Somit hat der Telekommunikationsdienstleister, der die entsprechende Dienst-

690 *Boos/Kroschwald/Wicker*, ZD 2013, 205, 206.

691 *Eschelbach* in: SSW-StPO, § 100j StPO, Rn. 10; *Grünwald/Döpkens*, MMR 2011, 287, 288.

692 *Gercke* in: HK-StPO, § 100j StPO, Rn. 6; *Greco* in: SK-StPO, § 100j StPO, Rn. 11; *Hauck* in: LR-StPO, § 100j StPO, Rn. 15a; *Wicker*, MMR 2014, 298, 300; *Boos/Kroschwald/Wicker*, ZD 2013, 205, 206; *Bedner*, Cloud Computing, S. 115; *Bunzel*, Der strafprozessuale Zugriff auf IT-Systeme, S. 367 f.; *Zimmermann*, JA 2014, 321, 326; *Schuster/Reichl*, CR 2010, 38, 43; a.A., jedoch ohne eingehende Begründung und mit bloßem Verweis auf die Gesetzgebungsmaterialien: *Köhler* in: Meyer-Goßner/Schmitt, § 100j StPO, Rn. 3; *Bär*, MMR 2013, 700, 702; *Bruns* in: KK-StPO, § 100j StPO, Rn. 7; *Dalby*, CR 2013, 361, 363.

693 *Schreibauer* in: Auernhammer-DSGVO/BDSG, § 15 TMG, Rn. 7; *Zscherpe* in: Taeger/Gabel-BDSG, § 15 TMG, Rn. 17.

694 *Wicker*, MMR 2014, 298, 300 f.; *dies*., Cloud-Computing und staatlicher Strafanspruch, S. 389.

leistung nicht selbst erbringt, keine Kenntnis der Zugangsdaten und kann diese folglich auch nicht herausgeben.[695][696]

(3) Auskunftsverlangen gem. §§ 15 Abs. 5 S. 4 TMG i.V.m. § 14 Abs. 2 TMG

Da es sich bei den Cloud-Anbietern zwar um Anbieter von Informations- und Kommunikationsdiensten handelt, diese aber gleichzeitig keine Telekommunikationsdienstleister darstellen, sind diese aufgrund der Negativformulierung in § 1 TMG als Telemediendienstanbieter anzusehen.[697] Telemediendienste leisten mehr als die bloße Signalübertragung über ein Telekommunikationsnetz.[698] Insbesondere Clouddienste mit Software-as-a-Service, Function-as-a-Service oder auch Plattform-as-a-Service Anwendungen, sind aufgrund ihrer Bereitstellung der genutzten Software als Telemedienanbieter einzuordnen. Schließlich wird dabei nicht die Signalübertragung übernommen, sondern wie auch im Falle von Sprachassistenten das komplette Management von entfernten Infrastrukturen und Ressourcen.[699] Eine Ausnahme könnte allenfalls dann anzudenken sein, wenn der Cloud-Anbieter zugleich Leistungen eines Access-Providers erbringt (d.h. das zur Verfügung stellen eines eigenen selbst betriebenen Zugangsdienstes) und seinen Nutzern so ein kompletten Netzwerk-as-a-Service Dienst zur Verfügung stellt.[700] Jedoch sind bei der Nutzung eines Smart Speakers der geläufigen Marken Amazon oder Google der Internetzugang einerseits und die Cloud Computing-Dienste anderseits technisch unabhängige Leistungen und werden von separaten Anbietern erbracht. Während der Internetzugang durch den Accesprovider bzw. Telekommunikationsdienstleister erbracht wird, erfolgt die Verarbeitung der Sprachbefehle in der Cloud durch Amazon oder Google als Telemediendienstanbieter. Daher könn-

695 *Hartmann* in: HK-GS, § 100j StPO, Rn. 11; *Wicker*, MMR 2014, 298, 302.
696 Zur Einschlägigkeit des § 100j StPO bzgl. eines E-Mail-Providers, vgl. *Redeker* in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 12, Rn. 217 ff.
697 So *Hauck* in: LR-StPO, § 100j StPO, Rn. 15a; *Greco* in: SK-StPO, § 100j StPO, Rn. 11; *Nolte* in: Borges/Meents Cloud-Computing, § 11 Rn. 24 f. m.w.N. zur Ansicht, ob das TMG auf Cloud-Dienste generell keine Anwendung finden soll.
698 *Martini* in: BeckOK-InfoMedienR, § 1 TMG, Rn. 11; vgl. auch OLG München, MMR 2019, 532, Rn. 61.
699 *Bedner*, Cloud Computing, S. 116; *Müller*, Cloud Computing, S. 221; *Boos/Kroschwald/Wicker*, ZD 2013, 205; vgl. auch BT-Drs. 16/3078, S. 13.
700 *Kremer/Völkel*, CR 2015, 501, 505; *Müller*, Cloud Computing, S. 197.

ten die Strafverfolgungsbehörden ihr Auskunftsverlangen auf §§ 15 Abs. 5 S. 4 TMG i.V.m. § 14 Abs. 2 TMG stützen. § 14 Abs. 2 TMG besagt, dass *„auf Anordnung der zuständigen Stellen […] der Diensteanbieter im Einzelfall Auskunft über Bestandsdaten erteilen [darf], soweit dies für Zwecke der Strafverfolgung […] erforderlich ist"*. Gem. § 15 Abs. 5 S. 4 TMG ist diese Vorschrift auf die Auskunftserteilung hinsichtlich Nutzungsdaten ebenfalls anzuwenden. Die §§ 15 Abs. 5 S. 4 TMG i.V.m. § 14 Abs. 2 TMG enthalten allerdings keine Befugnis der öffentlichen Stellen zum Auskunftsverlangen, sondern bestimmen lediglich den Umfang und Zweck der Übermittlungsbefugnis des Dienstanbieters.[701] Dies folgt unmittelbar aus der Formulierung des § 14 Abs. 2 TMG, der von „darf" und nicht wie § 100j StPO davon spricht, dass die Behörden berechtigt sind, eine Sache zu verlangen. Eine solche Befugnisnorm wie § 100j StPO, die auf entsprechende Vorschriften des TMG verweist, findet sich nicht. Auch nach dem Willen des Gesetzgebers stellt § 14 Abs. 2 TMG keine Ermächtigungsvorschrift da, sondern soll lediglich sicherstellen, dass der Telemedienanbieter an ihn herangetragene Auskunftsansprüche nicht aus datenschutzrechtlichen Gründen zurückweist.[702] Stattdessen liegt die datenschutzrechtliche Verantwortung hinsichtlich der Zulässigkeit der Datenübermittlung bei der anordnenden öffentlichen Stelle.[703] Es ist daher erforderlich, dass das Auskunftsverlangen auf eine entsprechende spezialgesetzliche Erhebungsbefugnis auf Seiten der Sicherheitsbehörden gestützt wird.[704] Als solche Befugnis wird teilweise § 95 Abs. 1 StPO[705] oder auch § 161 StPO[706] bemüht.

Für die Anwendbarkeit des § 14 Abs. 2 TMG auf Cloud-Anbieter kann schließlich offenbleiben, ob der Gesetzgeber Cloud-Dienstleistungsanbieter fälschlicherweise als Telekommunikationsdienstleister einordnete oder die durch die Existenz des TMG erforderliche Differenzierung zwischen Telekommunikationsdienstleitern und Telemediendienstleistern verkannte. Zwar ging der Gesetzgeber ausweislich der Gesetzgebungsmaterialien davon aus mit der Kodifizierung des § 100j StPO explizit Fälle des Cloud-Computing zu regeln, doch ändert dies nichts an der Unanwendbarkeit der §§ 95, 111, 113 Abs. 1 S. 2 TKG auf den Cloud-Dienstleister. Ein Auskunftsanspruch könnte sich lediglich nach § 15 Abs. 5 S. 4 TMG i.V.m.

701 *Karg*, DuD 2015, 85, 87.
702 *Zscherpe* in: Taeger/Gabel-BDSG, § 14 TMG, Rn. 42.
703 BS-Drs. 16/3078, S. 16.
704 *Zscherpe* in: Taeger/Gabel-BDSG, § 14 TMG, Rn. 42; *Karg*, DuD 2015, 85, 87; *Hoeren*, NJW 2007, 801, 805.
705 *Kipker/Voskamp*, ZD 2013, 119, 120 f.
706 *Wicker*, Cloud-Computing und staatlicher Strafanspruch, S. 406 f.

§ 14 Abs. 2 TMG und den spezialgesetzlichen strafprozessualen Vorschriften richten. Gegen eine Heranziehung der Generalklausel des § 161 StPO spricht entschieden, dass aufgrund der gewichtigen Bedeutung der Nutzungsdaten in Form der Zugangssicherungscodes der mit deren Erhebung verbundenen Eingriff in Art. 10 GG durch die Generalklausel nicht zu rechtfertigen ist.[707] Es blieben somit wiederum die §§ 94 ff. StPO deren praktische Anwendung allerdings ebenfalls an einer technisch bedingten Grenze scheitern. Aus Gründen der Datensicherheit speichert ein Großteil der Dienstleistungsanbieter die Passwörter nicht im Klartext, sondern verschlüsselt.[708] Sodann besitzt der Telemedienanbieter selbst nur einen sog. Hashwert[709], hat aber keine Kenntnis des Passwortes.[710] Da der Telemedienanbieter das Passwort daher nicht im Sinne des Telemediengesetzes im Klartext erhoben hat, kann er dieses auch nicht an die Strafverfolgungsbehörden herausgeben.[711]

(4) Zwischenergebnis

Zur Passworterlangung scheidet daher ein Vorgehen gegen den Cloud-Anbieter nach § 100j StPO i.V.m. §§ 95, 111, 113 Abs. 1 S. 2 TKG aus, da dieser nicht Verpflichteter des Anspruchs ist. Ein Auskunftsverlangen nach § 15 Abs. 5 S. 4 TMG i.V.m. § 14 Abs. 2 TMG i.V.m. §§ 94 ff. StPO scheitert in der Regel daran, dass der Cloud-Dienstleistungsanbieter das Passwort faktisch mangels Kenntnis nicht herausgeben kann. Es kommt daher nur der Einsatz eines Keyloggers oder anderweitiger Cracking-Tools in Betracht.[712] Insbesondere ist diese Vorgehensweise mangels Einschlägigkeit des § 100j StPO zur Bestandsdatenauskunft beim Cloud-Anbieter,

707 *Karg*, DuD 2015, 85, 88; *Bunzel*, Der strafprozessuale Zugriff auf IT-Systeme, S. 370.

708 BVerfG, NJW 2020, 2699, 2700.

709 Hashwert bezeichnet im Bereich der Computertechnik eine Verschlüsselung, die mittels eines Algorithmus errechnet wird und einem bestimmten Datensatz zugeordnet ist. Der ursprüngliche Inhalt der Datei kann damit nicht rekonstruiert werden, vgl. *Grützner/Jakob*, Compliance von A-Z, Hashwert(-funktion).

710 Vgl. BR-Drs. 664/1/12, S. 14.

711 *Wicker*, Cloud-Computing und staatlicher Strafanspruch, S. 406; *Grözinger*, Die Überwachung von Cloud-Storage, S. 247.

712 In technischer Hinsicht ermöglicht das Keylogging die Protokollierung aller Tastenanschläge, wodurch die verwendeten Passwörter nachvollzogen werden können, vgl. *Skistims/Roßnagel*, ZD 2012, 3, 5; *Fox*, DuD 2007, 827, 830; *Bunzel*, Der strafprozessuale Zugriff auf IT-Systeme, S. 69.

nicht durch die vermeintlich abschließende Regelung in § 100j StPO ausgeschlossen.[713]

3) § 110 Abs. 3 StPO im Verhältnis zum Dienstleistungsanbieter

Im Zusammenhang mit einem Vorgehen nach § 110 Abs. 3 StPO wird vereinzelt als problematisch erachtet, dass es sich dabei zwar gegenüber dem Betroffenen um eine offene Maßnahme handelt, der Dienstleistungsanbieter und Betreiber der Cloud im Stadium der Datensichtung jedoch keine Kenntnis der auf dem eigenen Server ablaufenden staatlichen Sichtung hat. Ihm gegenüber handelt es sich um einen heimlichen Eingriff.[714] Da den Strafverfolgungsbehörden durch ihre Ermittlungen jedoch nur die Zugangsdaten zum Account des tatverdächtigen Betroffenen, mithin nur zu dessen gespeicherten Aufzeichnungen bekannt werden, werden keine dem Dienstleistungsanbieter von weiteren Nutzern anvertraute Daten eingesehen. Daher wahrt es den Rechtsschutz des Anbieters, dass dieser nach § 110 Abs. 3 S. 2 Hs. 2 StPO durch die entsprechende Anwendung von § 98 Abs. 2 StPO bei einem Zugriff auf seine Daten eine richterliche Bestätigung der Beschlagnahme beantragen kann.[715] Im Zuge dieser binnen drei Tagen einzuholenden gerichtlichen Entscheidung, muss sodann auch dem Dienstleistungsanbieter nach § 33 Abs. 3 StPO rechtliches Gehör gewährt werden.[716] Im Übrigen schützt die Offenheit einer Maßnahme nur den unmittelbar durch sie Betroffenen, nicht jedoch inhaltlich Unbetroffene wie den Dienstleistungsanbieter.[717]

713 *Graf* in: BeckOK-StPO, § 100j StPO, Rn. 20, der davon ausgeht, dass die Möglichkeiten strafprozessualer Zugriffe auf Zugangsdaten durch die Neufassung des § 100j StPO nunmehr abschließend geregelt sind eine Umgehung der hierdurch festgeschriebenen Vorgehensweise und der damit einhergehenden Anforderungen rechtswidrig sein wird; ebenso *Burhoff*, StRR 2015, 8, 9.

714 *Gercke* in: HK-StPO, § 110 StPO, Rn. 34; *Singelnstein*, NStZ 2012, 593, 598.

715 *Bär*, ZIS 2011, 53, 54.

716 A.A.: *Puschke/Singelnstein*, NJW 2008, 113, 115.

717 *Wicker*, Cloud-Computing und staatlicher Strafanspruch, S. 375.

X) § 94 ff. StPO

1) Durchsuchung und Beschlagnahme beim Verdächtigen

Erfolgt sodann eine Durchsuchung beim Verdächtigen, im Zuge derer auch die genutzte Cloud durchsucht werden soll, stellt sich die Frage auf, welche Rechtsgrundlage diese Durchsuchung der Cloud zu stützen ist. Richtet sich die Durchsuchung der Cloud nach § 102 StPO könnte sie bei dem, der als Täter oder Teilnehmer einer Straftat verdächtig ist, bereits dann vorgenommen werden, wenn lediglich zu vermuten ist, dass die Durchsuchung zum Auffinden von Beweismitteln führen wird. Würde sich die Durchsuchung der Cloud dagegen nach § 103 StPO richten, wäre für deren Durchsuchung erforderlich, dass Tatsachen die Annahme begründen, die gesuchte Spur oder Sache befinde sich in den zu durchsuchenden Räumen, mithin in der Cloud. In diesem letztgenannten Fall wären die Anordnungsvoraussetzungen bedeutend strenger. Eine Durchsuchungsanordnung nach § 102 StPO sieht sich dabei vor allem dem Problem gegenüber, dass die zu durchsuchende Sache als dem Beschuldigten gehörend anzusehen sein müsste. Daher könnte anzunehmen sein, dass der Cloud-Speicher eine dem Beschuldigten gehörende Sache darstellen müsste. Dabei kommt es nicht auf die genaue Eigentumszuordnung an, vielmehr ist bereits der Besitz an einer solchen Sache ausreichend, um sie als dem Beschuldigten gehörend anzusehen.[718] Für einen Besitz ist in diesem Zusammenhang lediglich erforderlich, dass der Verdächtige wenigstens Mitgewahrsam in Form einer faktischen Zugriffsmöglichkeit auf die Daten besitzt.[719] Der Anwendbarkeit des § 102 StPO würde daher lediglich der Alleingewahrsam des Cloud-Anbieters entgegenstehen. Der Gewahrsam beschreibt ein tatsächliches Herrschaftsverhältnis über die Sache, das von einem Herrschaftswillen und der tatsächlichen Verfügungsgewalt getragen wird.[720] Zwar hat der Cloud-Nutzer keinen Zugriff auf den Cloud-Server als solchen und damit folgerichtig bereits unstreitig nicht einmal Mitgewahrsam an diesem. Angesichts dessen, dass aber nicht die Art des durchsuchten Mediums, sondern sein Inhalt (d.h. die Eignung der aufzufindenden Daten als Beweismittel) entscheidend für die Anordnung

718 BGH, StV 2007, 60, 61.
719 *Tsambikakis* in: LR-StPO, § 102 StPO, Rn. 40; *Wohlers/Jäger* in: SK-StPO, § 102 StPO, Rn. 15a; *Köhler* in: Meyer-Goßner/Schmitt, § 102 StPO, Rn. 10a.
720 *Kindhäuser* in: NK-StGB, § 242 StGB, Rn. 29 f.

der Durchsuchung ist,[721] muss entscheidender Bezugspunkt im Rahmen des § 102 StPO nicht der Gewahrsam des Betroffenen an dem Server als Datenträger, sondern an den hierauf abgespeicherten Inhaltsdaten sein.

Dies bestätigt auch ein Vergleich mit der Situation der E-Mail-Beschlagnahme. Auch dabei ist bezüglich der Gewahrsamszuordnung entscheidend, dass der Verdächtige faktische Zugriffmöglichkeiten auf die Nachrichten einschließlich der Datenanhänge hat. Es wird bei der Durchsuchung und Beschlagnahme im Falle von E-Mails daher nicht auf den Server als Sache abgestellt, sondern gefragt, ob der Nutzer eine Verfügungsmöglichkeit über die E-Mails – oder über die gespeicherten Daten in der Cloud – innehat.[722] Ebenso können für die Gewahrsamseinordnung in der Cloud die Grundsätze zu Durchsuchungen bei gemieteten Räumen herangezogen werden. Bei einer Durchsuchung in einem Hotelzimmer genügt ebenfalls eine Anordnung nach § 102 StPO, da aufgrund der vertraglich geregelten Nutzungsüberlassung eine Verfügungsbefugnis – und daher Gewahrsam – des Hotelzimmerbewohners besteht.[723] Bei Daten in der Cloud ist es deshalb sachgerecht, auf die Verfügungsgewalt hinsichtlich der gespeicherten Daten selbst und nicht hinsichtlich des Datenträgers – vergleichbar mit dem Hotelzimmer, in dem der Gast seine persönlichen Dinge ablegt – abzustellen.[724] Auch wenn der Cloud-Nutzer also keinen Gewahrsam an dem Datenträger als Sache hat, so hat er die erforderliche Verfügungsgewalt an dem in der Cloud gespeicherten Datenbestand. Ein solcher Mitgewahrsam kommt den Sprachassistenznutzern unter anderem entscheidend durch die vorhandene Löschungsmöglichkeit der aufgezeichneten Audio-Dateien zu. Es ist dem Kunden des Dienstleistungsanbieter jederzeit möglich durch ein Login die Tür zum persönlichen Cloud-Speicher zu öffnen und Aufzeichnungen zu löschen. Dieser Mitgewahrsam in Form des faktischen Zugriffs auf die Sache und ihren Inhalt ist ausreichend, um die Durchsuchung der Cloud des Betroffenen auf § 102 StPO stützen zu können.

721 BGH, StV 2007, 60, 61.
722 *Wicker*, DSRITB 2013, 981, 989.
723 *Wicker*, DSRITB 2013, 981, 989.
724 *Wicker*, DSRITB 2013, 981, 989.

a) Ermächtigungsgrundlage zur Beschlagnahme

Entscheidend ist schließlich die Frage auf, welcher strafprozessualen Grundlage die im Rahmen der Durchsuchung aufgefundenen beweisrelevanten Daten beschlagnahmt werden dürfen. Während für den ähnlich gelagerten Fall der E-Mailbeschlagnahme als mögliche Ermächtigungsgrundlagen sowohl § 100a StPO, als auch § 94 StPO sowie § 99 StPO in Betracht kommen[725], muss § 100a StPO in Bezug auf die auf Servern des Sprachassistenten gespeicherten Audioaufzeichnungen konsequenterweise erneut von vorn herein ausscheiden.[726] Wenn schon während des Übermittlungsvorganges keine Telekommunikation vorliegt, so kann diese erst recht nicht vorliegen, wenn die Daten nicht mehr in Bewegung sind, sondern auf dem Server ruhen.

aa) § 99 StPO

In seiner richtungsweisenden Entscheidung zur E-Mail Beschlagnahme hielt der BGH eine Postbeschlagnahme nach § 99 StPO für möglich: Die Beschlagnahme von auf dem Server des E-Mail Providers gespeicherten Nachrichten ist mit der Beschlagnahme anderer Mitteilungen, die sich zumindest vorübergehend bei einem Post- oder Telekommunikationsdiensteleister befinden, vergleichbar.[727] Auch ohne spezifische gesetzliche Regelung sei die E-Mail-Beschlagnahme daher unter den Voraussetzungen des § 99 StPO zulässig. Es ist aber zu bezweifeln, ob dies auch für den Fall der Beschlagnahme von gespeicherten Cloud-Aufzeichnungen gelten kann. Schließlich stützte der BGH die Anwendbarkeit des § 99 StPO entscheidend auf die Vergleichbarkeit der E-Mail-Kommunikation mit der postalischen Briefkommunikation, bei welcher sich der zu beschlagnahmende Brief zur Überbringung an die Zielperson im Gewahrsam des Postdienstleisters befinden müssen. Auf den der Nutzung eines Sprachassistenten zugrunde liegenden Sachverhalt ist dieser Vergleich jedoch nur eingeschränkt anwendbar. Zum einen handelt es sich bei den hier aufge-

725 Vgl. *Szebrowski*, MMR 2009, V, m.w.N.

726 A.A. hinsichtlich der Einschlägigkeit des § 100a StPO BGH, NJW 2021, 1252, 1554; im Ergebnis zustimmend *Abraham*, HRRS 2021, 356, 364 f.; kritisch vgl. *Grözinger*, NStZ 2021, 358 f.; *Hiéramente* WiJ 2021, 19, 21 f.; vgl. dazu im Übrigen oben Fn. 401.

727 BGH, NJW 2009, 1828, 1828.

zeichneten Daten bereits um keine an den Verdächtigen gerichtete Kommunikation. Zum anderen wurde der Inhalt der Audioaufzeichnungen auch gerade nicht zum Zwecke der Übermittlung in den Gewahrsam des Dienstleistungsanbieters gegeben. Der Inhalt der Aufzeichnungen wird von diesem vielmehr zur Verbesserung seines eigenen Angebots gespeichert. Hinsichtlich § 99 StPO muss ferner entscheidend sein, dass es sich bei den beschlagnahmten Gegenständen, um von diesen Unternehmen beförderte Sendungen handelt. Wenngleich der BGH unter den Sendungsbegriff in entsprechender Anwendung auch nicht-körperliche Nachrichten fasste, ist für eine solche Sendung stets typisch, dass die versendete Nachricht zur Kenntnisnahme an einen Menschen versandt wird[728] und anschließend an einer anderen Stelle inhaltsgleich in Empfang genommen wird. Bei der Nutzung eines Sprachassistenten wird anders als im Falle des E-Mail-Verkehrs die übermittelten Nachrichten nicht als solche an einer anderen Stelle abgeliefert, sondern lediglich die in der Nachricht enthaltene Anweisung ausgeführt. Vor allem geht es dabei nicht um die Übermittlung, um der Übermittlung willen, sondern es steht die Übermittlung zur Befehlsausführung im Vordergrund. Die im Rahmen der Nutzung eines Sprachassistenten aufgezeichneten Audiodaten können daher nicht als Sendung im Sinne von § 99 StPO erfasst werden. § 99 StPO stellt daher keine taugliche Ermächtigungsgrundlage dar.

bb) § 94 StPO

In Betracht kommt darüber hinaus die allgemeine Beschlagnahmevorschrift, § 94 StPO. Diese ist weiter gefasst als die Vorschrift der Postbeschlagnahme. Jedoch sind Daten keine körperlichen Gegenstände und so grundsätzlich kein taugliches Beschlagnahmeobjekt sein.[729] Da die zu beschlagnahmenden Informationen vorerst nicht in körperlichen Gegenständen manifestiert sind, würde grundsätzlich nur die Beschlagnahme der entsprechenden Hardware in Betracht kommen. Die Beschlagnahme einer kompletten EDV-Anlage dürfte jedoch in vielen Fällen, gerade sofern in Wirtschaftsstrafsachen dadurch ganze Unternehmen zum Erliegen kommen würden, unverhältnismäßig sein. Gleiches gilt für die Beschlagnahme

728 Vgl. *Menges* in: LR-StPO, § 99 StPO, Rn. 25.

729 *Wohlers* in: SK-StPO, § 94 StPO, Rn. 26; *Gercke* in: HK-StPO, § 94 Rn. 18; *Lemcke*, Die Sicherstellung, S. 19 ff.; *Bär*, MMR 1998, 577, 579; *Kemper*, NStZ 2005, 538, 541.

eines kompletten Servers, auf dem darüber hinaus auch eine Vielzahl an Informationen Dritter gespeichert sind. Durch die Beschlagnahme der EDV-Anlage oder des Servers würde zudem ein Eingriff in Art. 14 GG und vielfach auch in Art. 12 GG des Betroffenen erfolgen.[730] Daher wird in der Praxis die Anfertigung von Kopien der gangbare Weg zur Umsetzung der Beschlagnahme darstellen.[731]

Mangels hierfür vorhandener Ermächtigungsgrundlage und eines daraus folgenden Verstoßes gegen den Vorbehalt des Gesetzes könnte dies kritisch gesehen werden.[732] Da das Duplizieren der Aufzeichnungen oder Daten letztlich eine Maßnahme darstellt, die im Vergleich zu einer Beschlagnahme des Nutzerkontos oder gar des kompletten Servers die Eingriffsintensität verringert, muss das Ergebnis eines Erst-Recht-Schluss sein, dass nicht zuletzt die Verhältnismäßigkeit das Anfertigen bloßer Kopie der Daten in der Praxis – sofern ebenfalls unter verhältnismäßigem Aufwand möglich – gebietet.[733] Zum Umgang mit dieser Situation haben sich daher zwei Lösungsmöglichkeiten entwickelt. Entgegen dem vermeintlichen Wortlaut („Gegenstände") soll es auf die Körperlichkeit im Zusammenhang mit elektronischen Daten nicht ankommen. Denn für den historischen Gesetzgeber war im Zeitpunkt der Normschaffung nicht ersichtlich, dass elektronische Daten als nichtkörperliche Informationen für die Beweisführung im Strafverfahren noch bedeutsam werden könnten.[734] Im weiteren Verlauf zeigte jedoch die Ergänzung der Strafprozessordnung um die §§ 98a ff. StPO, dass der Gesetzgeber sodann auch von der Beschlagnahmefähigkeit von Datenbeständen ausgegangen ist.[735] § 94 StPO erfasst somit sämtliche Gegenstände, denen ein Beweiswert zukommen kann und die für die Untersuchung von Bedeutung sein könnten.[736] Ebenso wie das Anfertigen von Kopien im Falle der Beschlagnahme von körperlichen

730 *Menges* in: LR-StPO, § 94 StPO, Rn. 28 m.w.N.
731 *Süptitz/Utz/Eymann*, DuD 2013, 307, 309; *Menges* in: LR-StPO, § 94 StPO, Rn. 14; *Kassebohm* in: Auer-Reinsdorff/Conrad IT-R-HdB, § 43, Rn. 434; *Basar/Hiéramente*, NStZ 2018, 681, 682.
732 Vgl. zur Problematik *Bell*, Beschlagnahme und Akteneinsicht, S. 99 ff.
733 *Köhler* in: Meyer-Goßner/Schmitt, § 94 StPO, Rn. 16b; *Kemper*, NStZ 2005, 538, 540.
734 BVerfGE 113, 29, 50.
735 BVerfGE 113, 29, 50.
736 Vgl. BGH, StV 2007, 60, 61; *Menges* in: LR-StPO, § 94 StPO, Rn. 11; *Gerhold* in: BeckOK-StPO, § 94 StPO, Rn. 3; *Köhler* in: Meyer-Goßner/Schmitt, § 94 StPO, Rn. 16b.

Unterlagen seit langem anerkannt ist[737], kann auch das Anfertigen von Kopien digitaler Daten ohne Weiteres auf § 94 StPO gestützt werden. Dieses Ergebnis stützt eine Literaturauffassung zudem darauf, dass in der Datenkopie ein Minus zur Beschlagnahme des Servers liegt, sodass eine Datenkopie nach § 94 StPO zulässig ist, obwohl unkörperliche Daten für sich nicht § 94 StPO unterliegen.[738]

Bereits hinsichtlich der Beschlagnahme von E-Mails wurde das Vorgehen nach § 94 StPO aufgrund eines Eingriffs in Art. 10 GG, der durch § 94 StPO nicht zu rechtfertigen sei, scharf kritisiert.[739] Im Zusammenhang mit der verfassungsrechtlichen Einordnung einer E-Mail wird gemeinhin zwischen dem Weg der E-Mail vom Absender bis zum Ankommen im Speicher des Serverbetreibers (Phase 1), der dortigen Speicherung vor der Kenntnisnahme (Phase 2), dem anschließenden Abruf durch den Empfänger (Phase 3) und der abschließende Speicherung der E-Mail im Online-Postfach des Providers (Phase 4) unterschieden.[740] Während die erste und dritte Phase nahezu einhellig dem Schutzbereich des Fernmeldegeheimnisses zugeordnet werden, ist die Zuordnung in den Phasen 2 und 4 deutlich umstrittener.[741] Korrekt ist jedoch, dass der Schutzbereich aus Art. 10 GG trotz der ruhenden Kommunikation (aufgrund der Speicherung der Nachrichten auf dem Server des Providers) auch in Phase 2 und 4 eröffnet ist.[742] Zwar kann der Nutzer durch Zugangssicherungen wie Passwörter versuchen, die auf dem Server gespeicherten Nachrichten vor einem Zugriff Dritter zu schützen. Er hat jedoch keine technische Möglichkeit, die Weitergabe der Nachrichten durch den Dienstleistungsanbieter – der gerade nicht Kommunikationsteilnehmer ist – zu verhindern. Dieser fortbestehende technisch bedingte Mangel an Beherrschbarkeit ist ausschlaggebend für den besonderen Schutz, der auch ruhenden Daten in den Phasen 2 und 4 durch das Fernmeldegeheimnis zuteilwer-

737 *Ciolek-Krepold*, Durchsuchung und Beschlagnahme in Wirtschaftsstrafsachen, Rn. 358; *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, S. 275.

738 *Wohlers* in: SK-StPO, § 94 StPO, Rn. 26; *Gercke* in: HK-StPO, § 94 Rn. 18, 22; *Schäfer* wistra 1989, 8, 12; *Weber/Meckbach*, NStZ 2006, 492, 493.

739 *Beulke/Swoboda*, Strafprozessrecht, Rn. 392.

740 *Krüger*, MMR 2009 680, 681.

741 *Krüger*, MMR 2009 680, 681.

742 BVerfGE 124, 43, 55.; *Grözinger*, GA 2019, 441, 446; *Neuhöfer*, JR 2015, 21, 23; *Kleine-Vossbeck*, Electronic Mail, S. 142 f.; anders ist dies in den Fällen, in denen nach Abschluss eines Kommunikationsvorgangs gespeicherte Inhalte der zuvor durchgeführten Kommunikation im Herrschaftsbereich *eines* Kommunikationsteilnehmers ruhen, vgl. BVerfGE 124, 43, 54 f.; *Wenzel*, NZWiSt 2016, 85, 88.

den muss.[743] Aus der Eröffnung des Schutzbereiches wird sodann gefolgert, dass jedenfalls in Phase 2 ein Zugriff nur unter den strengeren Eingriffsvoraussetzungen des § 100a StPO möglich sei. Andernfalls würde der Schutz während dieses Stadiums aufgrund der technisch notwendigen Zwischenspeicherung auf dem Server des Providers abgeschwächt, da bereits unter den geringeren Eingriffsvoraussetzungen des § 94 StPO ein Zugriff erfolgen könnte.[744] Das BVerfG hält dem entgegen, dass sich weder aus der Systematik oder dem Telos der 94 ff. StPO noch den Gesetzesmaterialien Anhaltspunkte entnehmen lassen, dass ein Eingriff in Art. 10 GG nur aufgrund von § 99, § 100a und § 100g StPO zulässig ist.[745] Die Differenzierung in verschiedene zeitliche Stadien zugrunde legend, kommen im Falle eines staatlichen Zugriffs nach der Kenntnisnahme durch den Empfänger und dem Verbleiben der Nachricht auf dem Provider-Server (Phase 4) jedoch selbst die Kritiker der höchstrichterlichen Rechtsprechung zu dem Schluss, dass aufgrund der bewussten Entscheidung des Nutzers die Daten auf einem fremden Server zu speichern, ein Zugriff über § 94 StPO – trotz der durch das Bundesverfassungsgericht festgestellten Betroffenheit des Art. 10 GG, die unabhängig von einer Zwischen- oder Endspeicherung gegeben ist[746] – nicht zu beanstanden ist.[747]

Es ist jedoch bereits fraglich, ob die Diskussion hinsichtlich der Zugriffsmöglichkeiten in Phase 2 bei der Nutzung eines Sprachassistenten überhaupt zum Tragen kommt. Schließlich befinden sich die Daten zu keiner Zeit zum Abruf bereit auf dem Server des Dienstleistungsanbieters, sondern werden durch den Nutzer (im Sinne der E-Mail-Rechtsprechung des BGH daher durch den Absender) in die Cloud transportiert. Die Situation ähnelt daher weniger dem Stadium „Ruhen auf dem Serverprovider vor Abruf durch den Empfänger", sondern vielmehr dem Stadium „Verbleiben der Nachricht auf Server nach Kenntniserlangung (Phase 4)".[748] Schließlich besteht für die Benutzer des Sprachassistenten – jedenfalls in der Theorie – die Möglichkeit, Aufzeichnungen aus der

743 BVerfGE 124, 43, 55, vgl. zur Schutzbereichseröffnung auch § 4, B), I), 2), c); a.A.: *Krüger*, MMR 2009 680, 682; *Brunst*, CR 2009, 591, 592.

744 *Beulke/Swoboda*, Strafprozessrecht, Rn. 392; *Neuhöfer*, JR 2015, 21, 24; FS-Hamm/*Spatscheck*, 733,

747; *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 305; *Meinicke*, DSRITB 2012, 773, 784 f.

745 BVerfGE 124, 43, 58 f.

746 BVerfGE 124, 43, 55.

747 *Beulke/Swoboda*, Strafprozessrecht, Rn. 392.

748 Vgl. *Schelzke*, HRRS 2013, 86, 89.

Cloud zu löschen.[749] Dadurch würde den Nutzern zu einem gewissen Grad die Herrschaft über ihre Daten zurückübertragen. Verwaltet der Nutzer seine Daten anschließend nicht aktiv (indem er beispielsweise solche löscht), handelt es sich um eine bewusste Entscheidung des Nutzers seine Aufzeichnungen unter anderem zur Verbesserung des genutzten Systems in der Cloud zu belassen. Dies ist vergleichbar mit der Aufbewahrung einer Akte mit diversen Unterlagen, bei der sich der Betroffene ebenfalls bewusst dazu entscheidet, die darin verkörperten Inhalte nicht zu vernichten. Deren Beschlagnahme erfolgt klassischerweise auf Grundlage des § 94 StPO. Insofern ist es nur folgerichtig auch die auf einer Cloud gespeicherten Daten über § 94 StPO zu beschlagnahmen.[750]

2) Durchsuchung und Beschlagnahme beim Dienstleistungsanbieter

Verlief die Durchsuchung beim Verdächtigen nach § 102 StPO nicht erfolgreich, sodass die Beamten auch keine Daten nach § 110 Abs. 3 StPO sichten konnten, da es beispielsweise nicht gelang die Passwörter zum Accountlogin ausfindig zu machen, wird die Möglichkeit der Durchsuchung und der Beschlagnahme beim Dienstleistungsanbieter relevant. In diesen Fällen müssen die zielführenden Maßnahmen gegenüber demjenigen ergriffen werden, der die Daten in unmittelbarem Gewahrsam hat. Als Gewahrsamsinhaber kennzeichnet sich derjenige, der unmittelbaren Zugriff auf das externe Speichermedium hat,[751] mithin jedenfalls der Dienstleistungsanbieter und Inhaber der Serversysteme. Gem. § 103 StPO ist die Durchsuchung auch bei „anderen Personen" möglich. Als andere Person im Sinne des § 103 StPO werden alle Personen erfasst, die im Zusammenhang mit der Durchsuchung zugrunde liegenden Strafverfahren nicht als Beschuldigte gelten.[752] Auf den betroffenen Serversystemen sind darüber hinaus weitere Daten von einer Vielzahl gänzlich unbeteiligter Personen gespeichert. Daher gewinnt im Zusammenhang mit der Durchsuchung beim Dienstleistungsanbieter auch § 108 StPO an Bedeutung. § 108 StPO erlaubt den Strafverfolgungsbehörden, Aufzeichnungen die im Rahmen

749 Vgl. https://www.amazon.de/gp/help/customer/display.html?nodeId=201602230 (abgerufen am 31.10.2021).
750 Vgl. im Ergebnis *Dalby*, CR 2013, 361, 368; *Gless*, StV 2018, 671, 673; *Anders*, ZIS 2020, 70, 75; a.A.: *Neuhöfer*, JR 2015, 21, 25 f.
751 *Obenhaus*, NJW 2010, 651, 653.
752 *Köhler* in: Meyer-Goßner/Schmitt, § 103 StPO, Rn. 1.

der Durchsuchung entdeckt werden und auf eine andere, durch die mit der Anordnung der Durchsuchung nicht in Verbindung stehende Straftat hindeuten, zu beschlagnahmen. Diese „Gefahr" für sämtliche durch eine Serverdurchsuchung beim Dienstleistungsanbieter mittelbar betroffenen Kunden, wird durch die heutige Technik größtenteils entschärft, da eine saubere Trennung der Daten der einzelnen Nutzer auf dem durchsuchten Server gewährleistet ist. Sämtliche Daten können dem betreffenden Nutzer zugeordnet werden, sodass die Behörden bei einer Durchsuchung nur den dem Beschuldigten zugeordneten Datensatz durchsuchen. Eine wirkliche Suche, bei der auch den Dienstleistungsanbieter selbst oder dessen weitere Kunden belastendes Material gefunden werden könnte, findet folglich gar nicht statt. Daher ist die Gefahr hinsichtlich eines Zufallsfundes nach § 108 StPO sehr gering.[753] Aufgrund dieser technischen Separationsmöglichkeit und dem Ausschluss der Gefahr für Dritte stellt sich jedoch erneut die Frage, ob es sich sodann überhaupt um eine Durchsuchung gem. § 103 StPO oder nicht vielmehr um eine solche beim Verdächtigen, die auch nach § 102 StPO durchgeführt werden kann, handelt.

Dabei sind zwei Situationen zu unterscheiden. Zum einen könnte der Dienstleistungsanbieter seiner Verpflichtung aus § 95 StPO folgend den entsprechenden Datensatz freiwillig herausgeben. In dieser Situation vergleicht *Bell* die Durchsuchung beim Dienstleistungsanbieters mit der Durchsuchung eines Bankschließfaches, da die Beamten dort wie auch bei der Durchsuchung der Cloud lediglich die Sachen bzw. Daten des Verdächtigen, nicht jedoch auch fremde Räume wie die des Dienstleistungsanbieters, durchsuchen.[754] Dem ist zuzustimmen, denn die Suche nach beweisrelevanten Daten findet auch bei der Durchsuchung eines Cloudnetzwerkes erst innerhalb des dem Verdächtigen zugeordneten Datensatzes und nicht innerhalb der kompletten Cloud statt.[755] Weigert sich der Dienstleistungsanbieter jedoch die Daten des Beschuldigten Cloud-Nutzers herauszugeben, ist eine umfassende Durchsuchung auf dessen Cloud-Servern notwendig. Da sodann der komplette Datenträger des Dienstleistungsanbieters durchsucht wird, muss sich diese Durchsuchung auch deshalb nach dem strengeren § 103 StPO richten.[756]

---

753 *Bell*, Strafverfolgung und die Cloud, S. 131.

754 *Bell*, Strafverfolgung und die Cloud, S. 131; Wicker, Cloud-Computing und staatlicher Strafanspruch, S. 349 f.

755 *Wicker*, Cloud-Computing und staatlicher Strafanspruch, S. 348.

756 *Wicker*, Cloud-Computing und staatlicher Strafanspruch, S. 350, dies. DSRITB 2013, 981, 991.

Teilweise wird dagegen eingewandt, dass unter Heranziehung des § 103 Abs. 2 StPO auch eine solche Durchsuchung beim Dienstleistungsanbieter nach den Voraussetzungen des § 102 StPO ablaufen könne.[757] Nach § 103 Abs. 2 StPO gelten die strengeren Beschränkungen des § 103 Abs. 1 StPO nicht für Räume, deren Inhaber zwar ein Dritter ist, in denen sich jedoch der Beschuldigte im Zusammenhang mit der Verfolgung aufgehalten hat. Bezogen auf eine Cloud sei es erforderlich, den Gehalt des § 103 Abs. 2 StPO, der von der körperlichen Anwesenheit des Verdächtigen ausgeht, so anzuwenden, dass der verdächtige Cloud-Nutzer sich bei der Nutzung des Speicherdienstes dort aufgehalten hat, wenngleich er dort nicht körperlich anwesend war. Hierfür spreche der Technikfortschritt, der es erfordere, nicht auf die faktische körperliche Anwesenheit des Verdächtigen abzustellen, sondern auch einen virtuellen Zugang genügen zu lassen.[758] Diese Sichtweise würde jedoch den eigentlichen Inhalt des § 103 Abs. 2 StPO überstrapazieren. Dieser lässt eine Anordnung nach §§ 102, 103 Abs. 2 StPO unter den Voraussetzungen des § 102 StPO nur zu, wenn der Beschuldigte in den durchsuchten Räumen ergriffen wird oder sich dort während seiner Verfolgung aufgehalten hat. Insofern fordert § 103 Abs. 2 StPO ein Aufhalten in einem solchen Raum während seiner Flucht und nicht zu einem beliebigen in der Vergangenheit liegenden Zeitpunkt.[759] Wenn jede Cloudnutzung als Aufenthalt im Sinne des § 103 Abs. 2 StPO eingeordnet wird, wird damit die weitere Voraussetzung, dass sich der Betroffene während dieses Aufenthalts zusätzlich auf der Flucht befunden haben muss, übergangen. Es müsste daher für eine Durchsuchung beim Dienstleistungsanbieter gem. §§ 102, 103 Abs. 2 StPO feststehen, dass der Betroffene sich während der Speicherung der Audioaufzeichnungen bereits auf der Flucht befand.

Hinsichtlich des praktischen Ablaufs einer Beschlagnahme beim Dienstleistungsanbieter wird befürchtet, dass die hierfür zuständigen Kontaktstellen des Unternehmers den Behörden freiwillig über die gesetzliche Verpflichtung hinausgehende Unterstützungsleistungen anbieten und so der Schutz des Verdächtigen, dem in gewisser Weise sämtliche Ermittlungsbefugnisse mittelbar dienen, untergraben wird.[760] Diese für den Verdächtigen missliche Situation ist jedoch aus strafprozessualer Sicht jedenfalls auf

757 *Wicker*, DSRITB 2013, 981, 992 f.
758 *Wicker*, DSRITB 2013, 981, 993.
759 *Hegmann* in: BeckOK-StPO, § 103 StPO, Rn. 19; *Hauschild* in: MüKo-StPO, § 103 StPO, Rn. 14.
760 *Gercke* in: Borges/Meents Cloud-Computing, § 20, Rn. 38.

Ebene des bloßen Zugriffs auf etwaige Daten nicht zu beanstanden. Zwischen dem betroffenen Nutzer und dem Dienstleistungsanbieter besteht kein besonderes Vertrauensverhältnis auf Grund dessen zu befürchten wäre, dass sich dieser mit der Preisgabe etwaiger Informationen zurückhalten würde. Die Ermittlungsbehörden sind jedoch als an Recht und Gesetz gebundenen Teile der Exekutive angehalten, den Zeitraum, aus welchem Unterlagen benötigt werden, möglichst genau einzugrenzen, sodass die Dienstleistungsanbieter nicht aus vermeintlichem Selbstschutz sämtliche gespeicherte Daten über den betroffenen Nutzer offenlegen.[761]

3) Ergebnis

Bestehen Anhaltspunkte, dass ein Sprachassistent belastende Aufzeichnungen aufgezeichnet haben könnte und diese in der Cloud des Dienstleistungsanbieters gespeichert sind, besteht zunächst die Möglichkeit im Rahmen einer Durchsuchung beim Verdächtigen, § 102 StPO, sich in dessen Account einzuloggen und eine Sichtung der dort aufgezeichneten Audio-Dateien vorzunehmen, § 110 Abs. 3 StPO. Sodann kann zur genaueren Überprüfung eine Sicherungskopie erstellt werden, um die entsprechenden Aufzeichnungen in den Räumen der Strafverfolgungsbehörden auszuwerten. Ergeben sich keine beweisrelevanten Informationen sind die Sicherungskopien unverzüglich zu löschen und der Betroffene zu benachrichtigen, andernfalls sind die Unterlagen durch richterlichen Beschluss zu beschlagnahmen.[762] Ein mehrmaliges Einloggen in den Account des Betroffenen zu einer fortlaufenden Sichtung der dort gespeicherten Aufzeichnungen ist nicht von der Befugnisnorm umfasst. Dem Betroffen wird dennoch zu raten sein, sein Passwort zu ändern. Zudem können die Strafverfolgungsbehörden auch eine offene Durchsuchung des Serveraccounts beim Dienstleistungsanbieter vornehmen, die sich ebenfalls nach § 102 StPO richtet. Werden im Rahmen einer Durchsuchung belastende Aufzeichnungen entdeckt, können auch solche digital in einer Cloud gespeicherte Daten gem. § 94 StPO, beschlagnahmt werden. Dies kann wiederum sowohl beim Verdächtigen, sofern das Passwort zum Zugang in die Cloud ausfindig gemacht werden kann, als auch beim Dienstleistungsanbieter vor Ort geschehen. Im zweiten Fall wird es jedoch regelmäßig als Minusmaßnahme genügen, eine Kopie der Datenbestände zu fertigen, um

761 *Wicker*, Cloud-Computing und staatlicher Strafanspruch, S. 374.
762 *Wohlers/Jäger* in: SK-StPO, § 110 StPO, Rn. 27.

nicht komplette Server durch eine staatliche Beschlagnahme zum Erliegen zu bringen.

XI) Ermittlungsgeneralklausel, § 161 StPO

Bei einer entsprechend geringeren Grundrechtsrelevanz kommt als Ermächtigungsgrundlage auch die Ermittlungsgeneralklausel des § 161 Abs. 1 StPO in Betracht. Diese ermächtigt die Ermittlungsbehörden zum Zugriff auf alle öffentlich zugänglichen Informationen.[763] Bezüglich elektronischer Beweismittel ist im Zusammenhang mit der Generalklausel oft von einer Beweisbeschaffung durch eine „virtuelle Streife"[764] zu lesen. Dabei werden frei zugängliche Informationen wie Chatrooms oder Websites durch die Ermittlungsbehörden auf strafbare Handlungen überprüft.[765] Der freie Zugang für jedermann hat zur Folge, dass grundsätzlich kein Eingriff in die Grundrechte des Betroffenen vorliegt.[766] Dies liegt darin begründet, dass, infolge des freien Zugangs kein Vertrauen in die Identität und Diskretion der Kommunikationspartner bestehen kann. Dem Internetnutzer muss insofern bekannt sein, dass er die Angaben seines Gesprächspartners nicht überprüfen kann und sodann die sich hieraus ergebenden Kommunikationsbeziehungen nicht schutzwürdig sein können.[767] Der Nutzer geht vielmehr bewusst das Risiko ein, dass es sich bei seiner Gesprächsperson auch um staatliche Ermittlungsbeamte handeln könnte oder diese einen Chatverlauf in öffentlichen Foren mitlesen können.

Die Position des BVerfG ist an dieser Stelle jedoch nicht unumstritten. So werden Bedenken laut, dass nur auf Grundlage einer leichter vorzunehmenden Täuschung im Internetverkehr und der deswegen fehlenden Schutzwürdigkeit keine Generalerlaubnis für die Ermittlungsbehörden zur Ermittlung in offenen Bereichen des World Wide Web erfolgen dürfe.[768] Dabei wird sich eines Umkehrschlusses bedient, dass der digital Handelnde gerade aufgrund der geringeren Möglichkeiten die Identität des Kommunikationspartner im Internet zu ermitteln eine stärkere Absicherung

763 *Brunst* in: Gercke/Brunst, Internetstrafrecht, Rn. 782.
764 Vgl. dazu *Eisenmenger*, Die Grundrechtsrelevanz virtueller Streifenfahrten, S. 21 ff.
765 *Bär* in: Handbuch des Wirtschafts- und Steuerstrafrechts, Kapitel 28, Rn. 121.
766 BVerfGE 120, 274, 344 f.; *Hornick*, StraFo 2008, 281, 285.
767 BVerfGE 120, 274, 345.
768 *Eifert*, NVwZ 2008, 521, 522.

bedarf, als er dies in der nicht digitalen Welt bedürfte.[769] Diese Sichtweise verkennt jedoch, dass es gerade die Verantwortung des Einzelnen ist, wem er sich offenbart. Es ist nicht der Staat, der für eine stärke Absicherung des Einzelnen in Diskussionsforen oder Chatrooms Sorge tragen muss, sondern der verfassungsrechtlich gewollte mündige Bürger, der für sich selbst und die von ihm preisgegebenen Informationen in diesem Zusammenhang die uneingeschränkte Verantwortung trägt. Schließlich könnten die betroffenen Personen auch keinen Schutz ersuchen, wenn sie online nicht mit Beamten der Strafverfolgungsbehörden, sondern mit einem privaten Dritten kommunizieren und schließlich dieser sein erlangtes Wissen den Strafverfolgungsbehörden zur Verfügung stellt.[770]

Die Grenze eines Handelns auf Grundlage der Generalklausel wird aber dort zu ziehen sein, wo Informationen gezielt zusammengetragen, gespeichert und ausgewertet werden sollen.[771] Hier greift aufgrund einer Gefährdungslage für die Grundrechte des Einzelnen wieder der Gesetzesvorbehalt. Sofern beispielsweise der Zugang zu Foren, Chats oder ähnlichen nur nach einer Anmeldung mit echten Daten und einer Prüfung durch den Anbieter möglich ist, wäre der Staat beispielsweise darauf zu verweisen, verdeckte Ermittler unter einer Legende zu lassen – dies freilich nur bei Vorliegen der Voraussetzungen der speziellen Ermächtigungsgrundlage des § 110a StPO.[772] Auf die Generalklausel kann eine polizeiliche Streifenfahrt durch das Internet daher nur dann gestützt werden, wenn dabei Informationen gewonnen werden, die der Betroffene für die Öffentlichkeit frei zugänglich gemacht hat. Es dürfen daher keine Barrieren zu überwinden sein, um an die Informationen zu gelangen. Die Informationsbeschaffung müsste für jedermann auf gleiche Art ohne weitere Zwischenschritte möglich sein. Beispiele hierfür sind Beiträge in frei zugänglichen Foren. Bei der Nutzung eines Sprachassistenten begibt sich der Betroffene jedoch nicht in einen frei zugänglichen Bereich. Sofern dieser zur Informationsbeschaffung genutzt wird, erfolgt dieser Vorgang lediglich zwischen den Nutzer und den Severn des Dienstleistungsanbietern. Einen Dritten ist der Zugriff hierauf nicht ohne weiteres möglich. Zum Zugriff auf Sprachassistenten eignet sich die Ermittlungsgeneralklausel daher nicht.

769 *Brunst* in: Gercke/Brunst, Internetstrafrecht, Rn. 788.
770 So zur Hörfalle *Beulke/Swoboda*, Strafprozessrecht, Rn. 738, 742.
771 BVerfGE 120, 274, 345.
772 vgl. *Kudlich*, GA 2011, 193, 199.

XII) Übergeordnete Problematik: Serverstandort

Ein weiteres Problem in der praktischen Anwendung der Ermittlungsbefugnisse, die unmittelbar auf den Server des Dienstleistungsanbieters zugreifen, liegt darin begründet, dass die großen Anbieter von Cloud-Severn wie Apple, Google, oder Amazon mit ihrem Sitz nicht in Deutschland, sondern im Ausland angesiedelt sind. Daher stellt sich die Frage, inwiefern deutsches Strafprozessrecht zu Anwendung kommen kann. Ein Zugriff deutscher Behörden auf Server, die sich im Ausland befinden, würde ein Eingriff in fremde Souveränitätsrechte darstellen und setzt daher grundsätzlich ein Rechtshilfeersuchen an den betreffenden ausländischen Staat voraus.[773] Auch Ausnahmen von diesem Grundsatz, wie sie Art. 32 lit.a der Cybercrime Konvention normiert, werden in einem solchen Fall in der Regel nicht einschlägig sein. Weder sind die auf den Servern gespeicherten Daten öffentlich zugängliche Computerdaten, Art. 32 lit.a Cybercrime-Konvention, noch wird von einer freiwilligen Zustimmung der befugten Person zur Weitergabe der Daten an inländische Strafverfolgungsbehörden (Art. 32 lit. b Cybercrime-Konvention) ausgegangen werden können. Die inländischen Strafverfolgungsbehörden sind zur Durchführung eines Zugriffs sodann auf ein förmliches Rechtshilfeersuchen angewiesen. Sofern der Speicherort jedoch nicht feststellbar ist (was angesichts des Umstandes das international tätige Cloudanbieter die Rahmendaten der Datenspeicherung nicht immer offen legen werden nicht selten der Fall sein wird[774]) wird vertreten, dass in diesen Fällen auch ein Speicherort im Inland nicht ausgeschlossen werden kann.[775] Hierfür spreche, dass international agierende Anbieter für ihre Dienste in der Regel auch Host-Server in Deutschland benutzen. So wirbt beispielsweise Microsoft seit den Datenzugriffen US-amerikanischer Nachrichtendienste[776] damit, die Nutzerdaten unter Einhaltung des deutschen Datenschutzrechts in Deutschland zu speichern.[777] Da somit nicht jeder Zugriff auf Server eines ausländischen Unternehmens zwangsläufig zu einem tatsächlichen Zugriff auf im Ausland gespeicherte Daten führt, sollen entsprechende Maßnahmen nur

773 *Zerbes/El-Ghazi*, NStZ 2015, 425, 430; *Brunst*, DuD 2011, 618, 620 f.
774 *Bruns* in: KK-StPO, § 110 StPO, Rn. 8a; *Krause*, Kriminalistik 2014, 213, 215.
775 *Krause*, Kriminalistik 2014, 213, 215; *Soiné* NStZ 2018, 497, 500; *Angerer*, DRiZ 2019, 428, 431; *Köhler* in: Meyer-Goßner/Schmitt, § 110 StPO, Rn. 7b; *Wicker*, MMR 2013, 765, 768.
776 *Voigt*, MMR 2014, 158, 160.
777 Vgl. https://www.microsoft.com/de-de/cloud/deutsche-rechenzentren (zuletzt abgerufen am 31.10.2021).

unzulässig sein, wenn ein ausschließlich ausländischer Speicherort sicher feststeht.[778] Jedenfalls bei einer Maßnahme nach § 110 Abs. 3 StPO ist zudem zu beachten, dass sofern der Zugriff auf den Serveraccount über den Computer des Betroffenen erfolgt, es sich dabei um eine Ermittlungshandlung im Inland handelt, für die ohnehin kein Rechtshilfeersuchen zu stellen wäre.[779]

XII) Ergebnis

Der stetig wachsende Markt smarter Assistenten, bringt auch neue Ermittlungsmöglichkeiten für die Strafverfolgungsbehörden mit sich. Umsetzbar sind diese neuen Möglichkeiten nur unter strenger Beachtung des Gesetzesvorbehalts. Als möglicher Vorbehalt kann dabei jedenfalls § 100a StPO nicht dienen. Ein Zugriff auf Übermittlungsvorgänge zwischen Endgerät und Sprachassistent nach § 100a Abs. 1 S. 1, 2 StPO scheidet mangels des Vorliegens von Telekommunikation im Sinne des § 100a StPO ebenso aus, wie ein Zugriff auf ruhende, gespeicherte Telekommunikationsdaten nach § 100a Abs. 1 S. 3 StPO aufgrund der Verfassungswidrigkeit dieser Vorschrift. Auch die klassische Online-Durchsuchung nach § 100b StPO ist hinsichtlich des beim Betroffenen platzierten Endgeräts rechtlich zwar möglich, im Hinblick auf fehlende gespeicherte Datenbestände auf diesen Endgeräten in der Praxis jedoch nicht zielführend. Zielführender erscheint die ebenfalls unter § 100b StPO mögliche Live-Überwachung. Zwar dürfen sensorische Systeme des Smart Speakers dabei nicht bewusst aktiviert werden, allerdings ist es möglich, in Echtzeit ablaufende Geschehen in der Wohnung mitzuhören, sofern der Betroffene den Smart Speaker aktiviert. Umfangreichere Befugnisse bringt die Wohnraumüberwachung, die es erlaubt das Endgerät derart zu manipulieren, dass es als Wanze der Strafverfolgungsbehörden fungiert. Dann ist eine durchgehende akustische Wohnraumüberwachung des Betroffenen möglich, die nicht an die Aktivierung des Smart Speakers durch den Nutzer geknüpft ist. Auch wenn auf den Endgeräten ohnehin keine ruhenden Daten gespeichert sind, ist dafür Sorge zu tragen, dass die Software zur Manipulation des Sprachassistenten in Form des Smart Speakers derart konfiguriert ist, dass lediglich laufenden Kommunikationsvorgänge überwacht werden können.

---

778 *Bruns* in: KK-StPO, § 110 StPO, Rn. 8a.

779 *Wicker*, MMR 2013, 765, 769; *Köhler* in: Meyer-Goßner/Schmitt, § 110 StPO, Rn. 7b.

Hinsichtlich der offenen Ermittlungsbefugnissen ist zunächst auf eine Durchsuchung beim Verdächtigen, § 102 StPO zu verweisen. Im Rahmen derer sind die Strafverfolgungsbehörden ermächtigt mittels eines Keyloggers sich in Kenntnis der Zugangsdaten zum Account des Betroffenen zu bringen, um dort gespeicherte Daten sichten zu können, § 110 Abs. 3 StPO. Eine Bestandsdatenauskunft nach § 100j StPO ist zur Erlangung der Zugangsdaten aufgrund der Personenverschiedenheit von Access-Provider und Cloud-Anbieter nicht zielführend. Daneben kommt ebenso eine Durchsuchung des Serveraccounts beim Dienstleistungsanbieter nach § 102 StPO in Betracht. Eine Beschlagnahme im Rahmen der Durchsuchung aufgefundener beweisrelevanter Daten ist gem. § 94 StPO sowohl beim Verdächtigen als auch beim Dienstleistungsanbieter möglich. Es bestehen damit durchaus Möglichkeiten für die Strafverfolgungsbehörden unter Einhaltung des Gesetzesvorbehalts in bestimmten Situationen rechtmäßiger Weise auf Smart Speaker zu Ermittlungszwecken zuzugreifen.