www.stv-online.de

StV STRAFVERTEIDIGER

Justizvollzugsrecht/ Technische Aufzeichnungen und StPO

AUS DEM INHALT

Heft 10
Oktober 2018
Seiten 619 – 698
38. Jahrgang
Art.-Nr. 07764810
PVSt 20232

10

Carl Heymanns Verlag

Wenn das Haus mithört: Beweisverbote im digitalen Zeitalter

Prof. Dr. Sabine Gless, Basel[1]

Die eigenen vier Wände markieren traditionell den privaten Raum, in dem Menschen unbehelligt von der Wahrnehmung durch Aussenstehende eine höchstpersönliche Sphäre geniessen, die sie nach eigenen Vorstellungen gestalten. Diese Prämisse hat unser Denken über öffentliche und private Sphären über lange Zeit geprägt. Moderne Informationstechnologie bzw. der Einzug digitaler Assistenten in die private Lebensumgebung scheint die Idee einer unantastbaren Privatsphäre jedoch unaufhaltsam aufzulösen.[2] Das könnte auch bisher akzeptierte Grenzen strafrechtlicher Ermittlungen verändern.

A. Einleitung

Zwar schützten die eigenen vier Wände noch nie per se vor strafrechtlichen Ermittlungen: Wohnungen dürfen unter bestimmten Voraussetzungen durchsucht und in bestimmten Situationen abgehört werden. Aber vor einem staatlichen Ermittlungseingriff steht ein mehr oder weniger komplexes Verfahrensprozedere, das vor unangebrachten Übergriffen schützen sollte, und Beweisverbote sichern den Strafermittlungen grundsätzlich entzogene Bereiche. Stellen Personen diesen Schutz in gewissem Umfang zur Disposition, wenn sie in ihren Privathaushalt einen »elektronischen Butler« integrieren?

Digitale Sprachassistenten – wie bspw. »Alexa«, der Assistent von Amazon, oder »home« von google oder »Cortana« von Microsoft – sind eigentlich recht simple Systeme, die mit Mikrofon, Lautsprecher und Computerchip, immer mit dem Internet verbunden, darauf programmiert sind – aktiviert durch bestimmte Code-Worte – einfache Befehle auszuführen. Damit ein digitaler Assistent auf Befehl Musik abspielen, Licht dimmen, Witze erzählen oder Bestellungen abwickeln kann, braucht er ein Mikrofon, das immer »zuhört«. Er »streamt« ständig das gesprochene Wort und ist schon deshalb von Interesse für die Strafverfolgungsbehörden. Denn wer mithört, um Befehle auszuführen, kann möglicherweise auch reproduzieren und quasi als Zeuge in einem Verfahren »aussagen«. So kolportierte die deutsche Presse einen Rechtsstreit im amerikanischen Arkansas im November 2015, als mehrere Personen gemeinsam einen Abend mit Alkohol und Drogen verbracht hatten und am nächsten Morgen Einer tot im Whirlpool lag. Die ermittelnden Beamten vermuteten, dass das Amazon Echo in der Tatnacht aktiv war und Sprachaufzeichnungen oder Daten mit relevanten Informationen für die Sachverhaltsaufklärung auf Amazons Servern lagern könnten. Sie forderten Amazon zur Herausgabe der Daten oder eines Transkripts heraus.[3] Amazon verweigerte dies zunächst.[4] Als der Beschuldigte die Daten freigab und Amazon in einem eigenen Statement seine Rechtsposition dargelegt hatte, erhielten die Strafverfolgungsbehörden Zugang.[5] Seit Herbst 2016 ist Amazons Alexa bereits in Deutschland erhältlich. Auch andere Hersteller bieten jetzt digitale Assistenten in ihrem Verkaufssortiment an. Wie werden deutsche Strafermittler agieren, wenn das Haus mithören kann? Für eine erste Antwort auf diese Frage wird im Folgenden ein Szenario unserer digitalisierten Wohnzukunft und Schlaglichter auf den möglichen Zugriff von Strafverfolgungsbehörden auf dadurch generierte Daten gezeichnet. Das jüngste eingeführte Beweisverbot, § 100d StPO, dient anschliessend als Folie für eine kurze Diskussion der Beweisverbote im digitalen Zeitalter: Grund zur Hoffnung oder nur leere Versprechen?

B. Unsere digitale Zukunft: Die Wohnung hört und denkt mit

Unsere Lebenswelt wird in rasantem Tempo digitalisiert. Auch im privaten Heim werden einzelne Apparate schnell den Weg in Gesamtkonzepte finden. Die neueste Integration der digitalen Sprachassistenten in ein »KogniHome« deutet bereits den Weg an.[6]

I. »Digitale Sprachassistenten«

Digitale Sprachassistenten selbst sind letztlich recht einfach aufgebaut. Ihr Mikrofon ist dauerhaft eingeschaltet und filtert alle eingehenden Geräusche nach dem sog. Code- oder Aktivierungswort. Fällt dieses, wird der Befehl entgegengenommen, positiv oder negativ über den eingebauten Lautsprecher »beantwortet« und ausgeführt. Voraussetzung für dieses Zudienen ist eine Stand-by-Verbindung über das Internet mit der Cloud des Anbieters. Lokal verarbeiten die Geräte nur das Aktivierungswort. Die »Intelligenz« steckt in den Rechenzentren des jeweiligen Anbieters. Gemäss den Erklärungen von Amazon und den Nutzungsbedingungen für Alexa werden Umgebungsgeräusche erst nach Erkennen des Aktivierungsworts an die Firmenserver von Amazon übermittelt. Dort werden die Befehlseingaben zunächst als Sound-Datei abgespeichert und – für die Nutzer zugäng-

1 Schriftfassung des im Rahmen des 10. EU-Strafrechtstages am 16.09.2017 in Bonn gehaltenen Vortrages. *Verf.* dankt den Veranstaltern und allen Diskussionsteilnehmern sowie dem Schweizer Nationalfonds, dessen Unterstützung im Rahmen des NFP 75 Big Data <http://www.nfp75.ch/en/projects/module-2-societal-and-regulatory-challenges/project-gless> (abgerufen, wie alle nachfolgenden URLs, am 19.02.2018) die Vorarbeiten ermöglicht haben. *Verf.* ist Mitglied des Beirats dieser Zeitschrift.

2 Illustrativ das Zitat des Google-CEO *Eric Schmidt*: »If you have something that you don't want anyone to know, *maybe you shouldn't be doing it in the first place*«, siehe www.youtube.com/watch?v=A6e7wfDHzew.

3 Digitale Sprachassistenten können bisweilen bei Geräuschen aktiv werden, die fälschlicherweise als Aktivierungswort verstanden werden. So sendet das Gerät zufällige Geräuschkulissen an den Servercomputer. Aus solchen Aufzeichnungen erhofften sich die Behörden wohl Beweise aus der Tatnacht.

4 » [...] Amazon asks [...] the State in the first instance to make a heightened showing of relevance and need for any recordings. Specifically, the State must demonstrate: (1) a compelling need for the information sought, including that it is not available from other sources; and (2) a sufficient nexus between the information and the subject of the criminal investigation.«, so Amazons Argumentation, siehe Memorandum of Law in Support of Amazon's Motion to Quash Search Warrant, State of Arkansas v. James A. Bates, Case no. CR-2016-370-2, p. 2, https://news.vice.com/wp-content/uploads/2017/02/Azn-Brief-in-Support.pdf; »At the heart of that First Amendment protection is the right to browse and purchase expressive materials anonymously, without fear of government discovery« argumentierte Amazon, denn die Echo-Sprachaufnahmen können Informationen über den Gesundheitszustand oder politische Einstellungen einer Person beinhalten, siehe dazu http://fortune.com/2017/02/23/amazon-free-speech-alexa-murder.

5 Bis jetzt ist ungeklärt, ob Amazons Berufung auf das First Amendment einer gerichtlichen Analyse standhielte.

6 Siehe dazu mehr unter www.kogni-home.de, Universität Bielefeld.

lich – transkribiert abgelegt.[7] Für die Nutzer sind die Vorgänge allenfalls über ein Nutzerkonto nachvollziehbar. Weil nicht auszuschliessen ist, dass digitale Assistenten wirklich nur das aufnehmen, was unmittelbar nach einem Code-Wort gesprochen wird, und weil unklar ist, ob sie Umgebungsgeräusche sauber ausfiltern können oder wann genau die Aufnahme der gesprochenen Befehle beendet wird, sind sie mit Blick auf die Privatsphäre heikel und für Strafverfolgungsbehörden bei Ermittlungen interessant.

II. Zukunftsvision »KogniHome«: Wohnen im digitalen Zeitalter

Während »elektronische Butler« noch als Spielzeuge gelten mögen, arbeiten verschiedene Forschergruppen bereits an mithörenden und mitdenkenden Wohnungen. Darin soll eine Vielzahl von digitalen Assistenten das Verhalten der Bewohner umfassend erfassen, mithören, mitdenken und dadurch stets zu Diensten sein.[8] Ein elektronischer, vernetzter Spiegel empfiehlt das geeignete Outfit für den Tag; die moderne Eingangstür erkennt die Gesichter der Bewohner und öffnet die Tür; ein intelligenter Sessel spürt die Vitaldaten des Benutzers und bietet gegebenenfalls eine entspannende Massage an. Alle diese Assistenten dürften nicht nur miteinander, sondern auch mit den Strom- und Wasserwerken, Pflegediensten oder Lieferservices vernetzt sein. Solche Zukunftsvisionen eines »smarten Wohnens« müssten zumindest jene beunruhigen, die der Wohnung einen besonderen Status als grundrechtlich geschützten Rückzugsraum für Menschen ansehen. Die Wohnung gilt seit jeher als Ort der ganz persönlichen Lebensgestaltung – und auch als eine Grundvoraussetzung für ein Zusammenleben in einem freiheitlichen Staat.[9]

III. Digitalisierung unserer Lebenswelt – ein freiwilliger Schritt?

Heute wird solchen Bedenken oft beruhigend entgegengehalten, dass ja jeder selbst entscheiden könne, wieviel Freiheit er für die Bequemlichkeiten digitalisierter Helfer aufgeben wolle. Doch dieses Argument dürfte in einer zunehmend auf Informationstechnologie gestützten Lebenswelt bald an Überzeugungskraft verlieren. Für Digitalisierung gibt es vielfältige Gründe. Vor allem für Menschen mit Beeinträchtigungen, die – aufgrund des Lebensalters oder körperlicher Behinderungen – auf Hilfe angewiesen sind, öffnen Roboter das Versprechen eines selbständigeren Lebens. Für andere steigt mit der Vernetzung von Vorgängen in ihrer Arbeitswelt und Privatumgebung der Druck mitzumachen, um nicht abgehängt zu werden.[10]

Schon heute werden nicht nur jene, die sich aus individuellen Gründen für die Nutzung eines Sprachassistenten in ihrer Wohnung entscheiden, in ihrem privaten Verhalten digital erfasst.[11] Seit diesem Jahr sind Autos vorschriftsmässig mit dem sog. eCall-System ausgestattet: Eine in das Fahrzeug fest eingebaute SIM-Karte gewährleistet eine ständige Verbindung zu einer Notrufzentrale, um bei einem Unfall von gewissem Umfang automatisch Hilfe zu rufen. Damit dies funktioniert, aber eCall nicht bei einem leichten Auffahrunfall beim Parken die Rettungsstelle informiert, ist das System an verschiedene Sensoren und Sicherheitstechniken des Fahrzeugs gekoppelt. So lässt sich aber u.a. – aufgrund der charakteristischen Fahr- und Bremsweise – auch nachträglich feststellen, wer ein Fahrzeug zu einem bestimmten Zeitpunkt gefahren hat.[12] Schon seit der Einführung der elektronischen Gesundheitskarte im Oktober 2011 trägt praktisch jeder (gesetzlich) Krankenversicherte eine elektronische Gesundheitskarte mit sich, die bei neuen Medikamenten die gesamte Krankengeschichte automatisch und online prüft, um bspw. Gefahren im Zusammenhang von Wechselwirkungen mit anderen Medikamenten zu beseitigen.[13]

In der Zukunft dürften sich mehr Menschen zur Verbesserung ihrer gesundheitlichen Lage für eine sog. »smarte Prothese« entscheiden, die ihnen einen bewegungsfähigen Arm oder einen sehr leistungsfähigen Herzschrittmacher gibt, aber gleichzeitig nicht nur das Bewegungsprofil, sondern auch andere Körpertätigkeiten festhält.[14] Jedes einzelne Gerät und dessen Datenspuren können schliesslich in einem Strafverfahren gegen den Träger verwendet werden, wenn sich dieser zur Verweigerung der Aussage entscheidet, die Prothese aber gleichwohl ausgelesen wird.[15] Die Entscheidung für eine Digitalisierung von Alltagesvorgängen ist also in verschiedenen Fallkonstellationen nicht ganz freiwillig und dürfte oft das Resultat einer durch – mehr oder weniger starken äußeren Zwang – bestimmten Interessensabwägung sein.

C. Amtsaufklärung im digitalen Zeitalter

Weil es viele wichtige Individual- und Allgemeininteressen gibt, die für eine Digitalisierung bestimmter Vorgänge in der menschlichen Lebenswelt sprechen, erscheint es wahrscheinlich, dass das Verhalten der einzelnen Menschen bald in grösserem Umfang elektronisch auslesbar wird. Daran knüpfen sich viele Fragen: Wie sind diese durch Sensoren und Computersysteme generierten Informationen in einem Strafverfahren zu bewerten? Welche Grundkenntnisse in der Informatik müssen Staatsanwälte, Richter, Strafverteidi-

7 Aus den Alexa Nutzungsbedingungen vom 14.09.2016: »1.3 Sprachdienste. [...] Alexa leitet Audiodaten in die Cloud [...] und speichert Ihre Stimmeingaben [...] in der Cloud [...].«; »3.1 Informationen. Die Software stellt Amazon Informationen über die Verwendung von Alexa und Ihre Interaktionen [...] bereit (z.B. Gerätetyp, Sprachinformationen, Metadaten zum Inhalt, den Standort und Diagnosedaten). Durch Alexa übermittelte Informationen können auf Servern gespeichert werden, die sich außerhalb des Landes befinden, in dem Sie wohnen.«, siehe www.amazon.de/gp/help/customer/display.html?nodeId=201809740; Aus den Antworten auf häufig gestellte Fragen zu Alexa und Alexa-Geräten: »3. Kann ich überprüfen, was ich Alexa gefragt habe? Ja, Sie können Ihre Sprachinteraktionen mit Alexa überprüfen, indem Sie den Verlauf [...] aufrufen [und sich eine] an die Cloud gesendete Audiodatei anhören.«, offenbar sendet das Gerät auch nur nach Hören (oder Misshören) des Aktivierungsworts Daten an die Server von Amazon: »Amazon Echo und Echo Dot verwenden eine geräteinterne Stichworterkennung, um das Aktivierungswort zu erkennen. Wenn diese Geräte das Aktivierungswort erkennen, leiten sie Audiodaten in die Cloud, einschließlich eines Sekundenbruchteils vor Äußerung des Aktivierungswortes«, siehe www.amazon.de/gp/help/customer/display.html?nodeId=201602230.

8 *Ciminal/Herlitz* NZM 2016, 409 ff.

9 *Röhl*, Zur Unterscheidung von Öffentlichkeit und Privatheit v. 13.06.2010, www.rsozblog.de/zur-unterscheidung-von-offentlichkeit-und-privatheit.

10 *Schuldt*, Konnektivität: Die Vernetzung der Welt, siehe www.zukunftsinstitut.de/artikel/konnektivitaet-die-vernetzung-der-welt.

11 Der öffentliche Raum dürfte ohnehin immer engmaschiger mit Kameras überwacht werden, vgl. etwa zum Einsatz von Gesichtserkennung in Überwachungskameras am Berliner Bahnhof Südkreuz www.faz.net/aktuell/wirtschaft/agenda/der-tag-gesichtserkennung-am-berliner-bahnhof-suedkreuz-15131365.html.

12 Vgl. dazu etwa: http://www.autosec.org/pubs/fingerprint.pdf.

13 Siehe dazu weitere Informationen auf www.gkv-spitzenverband.de/krankenversicherung/telematik_und_datenaustausch/egk/egk.js.

14 Forscher entwickeln revolutionäre Handprothese, www.welt.de/gesundheit/article135213821/Forscher-entwickeln-revolutionaere Handprothese.html.

15 www.bbc.com/news/technology-40592520.

ger künftig besitzen, damit sie nicht gänzlich Computer-Sachverständigen ausgeliefert sind? Und welche Grenzen müssen für die Verwertung von Roboterwahrnehmungen gelten, um übergeordnete menschliche Interessen zu wahren?

Es stellt sich auch die Frage nach einem adäquaten Ansatz für Beweisverbote in einem digitalen Zeitalter. Denn selbst die hartgesottensten Strafverfolger dürften zustimmen, dass die Chance auf eine möglichst umfassende Wahrheitsermittlung beispielsweise nicht um den Preis der Aufgabe jeglicher Privatsphäre erkauft werden darf. Dabei ist klar, dass die eigenen vier Wände nicht an sich vor Ermittlungsmassnahmen schützen können. Es gibt *per se* auch keinen Grund, warum sich die Amtsermittlungspflicht nicht auf digitale Assistenten erstrecken sollte. Smartphone oder Auto generieren bekanntlich Daten, die als tatrelevante Informationen für ein Strafverfahren wichtig sein können.[16] Doch das deutsche Strafverfahrensrecht kennt kaum spezifische Regelung für eine Informationsgewinnung auf der Grundlage elektronischer Dateien und so stellt sich für die Strafverfolgungsbehörden immer wieder die Frage: Wie sind Beweise zu sichern, die durch moderne Informationstechnologie generiert werden?

I. Zugriff auf vorhandene Aufzeichnungen

Nach der Systematik der StPO liegt es nahe, auch bei einer Beweisgewinnung mit Hilfe digitaler Assistenten zwischen dem Zugriff auf bereits vorhandene Aufzeichnungen und einem möglichen Einsatz zur zeitgleichen Überwachung zu unterscheiden.

1. Digitale Assistenten als Zeugen?

Elektronische Geräte werden regelmässig dadurch zu Beweismitteln, dass Sachverständige sie auslesen. Weil digitale Assistenten auf menschlichen Zuruf antworten, lancierten Medien die Idee, digitale Sprachassistenten als Zeugen zu vernehmen: Wer – aktiviert durch ein Code-Wort – kommunizieren kann, könnte ja auch vor Gericht ein registriertes Geschehnis aus der Vergangenheit vortragen.[17] Eine solche Wiedergabe von automatisch Aufgezeichnetem entspräche aber nicht unserem Verständnis einer Zeugenaussage: Zeugen bekunden vielmehr eine eigene Wahrnehmung, die sie reflektieren können.[18] Zu einem kritischen Hinterfragen der eigenen Aufnahme sind digitale Assistenten nicht fähig. Die futuristisch anmutende Idee, Sprachassistenten als Zeugen zu vernehmen, deutet aber auf grundlegende Fragen hin, die sich stellen, wenn Roboterassistenten im strafprozessualen Beweisverfahren nicht mehr nur als Maschinen,[19] sondern als Personen angesehen werden, die über eigene Wahrnehmungen berichten können. Dann stellen sich natürlich weitere Fragen, etwa nach Zeugnisverweigerungsrechten eines Roboters, wenn er als unverzichtbarer Helfer das Leben eines behinderten Menschen ermöglicht.

2. Herausgabe von Daten und/oder Beschlagnahme beim Nutzer

Wollen Ermittlungsbehörden über digitale Sprachassistenten an Informationen kommen, würden sie wohl zunächst die betreffenden Nutzer bitten, ihnen zugängliche Daten zu überlassen. Ob sie so Datensätze erhalten, dürfte von vielen Umständen im Einzelfall abhängen. Anders als bei einer Computerbeschlagnahme stehen Nutzer normalerweise nicht in der Zwangslage, eine Beschlagnahme wichtiger IT-Infrastruktur durch die Herausgabe der Daten zu vermeiden. Denn von Interesse dürfte nicht der digitale Assistent sein, auf dem keine Daten gespeichert sind, sondern der Zugang zu den durch ihn generierten Daten, die regelmässig auf einem Nutzerkonto liegen. Die Beschlagnahme solcher Daten ist in analoger Anwendung von §§ 94 ff. StPO zulässig.[20] Bei einer Durchsuchung dürfen Ermittler nach herrschender Meinung bekanntlich auch auf »räumlich getrennte Speichermedien« zugreifen, soweit dies von dem Durchsuchungsort aus möglich ist.[21] Mit der zunehmenden Vernetzung[22] eröffnen sich hier theoretisch weitreichende Möglichkeiten immer weiterer Datensätze, auf die von einem Durchsuchungsort aus zugegriffen werden könnte.[23] In der Praxis ergeben sich aber verschiedene Probleme, unter anderem die Frage, inwieweit auf Daten zugegriffen werden darf, die im Ausland gespeichert sind.[24]

3. Herausgabe von Daten und/oder Beschlagnahme beim Anbieter

In verschiedenen Fallkonstellationen, etwa wenn sich Nutzer nicht kooperativ zeigen oder Daten bei ihnen nur teilweise vorhanden sind, dürften Ermittlungsbehörden die Anbieter zur Herausgabe relevanter Daten auffordern.[25] Zumeist dürften sie damit keinen Erfolg haben, schon weil es dem Image der Anbieter regelmässig nicht dienlich ist, wenn sie enger mit der Polizei als mit den eigenen Nutzern zusammenarbeiten.[26] Ein eindrückliches Beispiel dafür bietet die Auseinandersetzung zwischen Apple und dem US-amerikanischen FBI über eine sog. Entsperrung des iPhones der Attentäter von San Bernardino.[27] Auch beim Anbieter können Daten beschlagnahmt werden. Es gelten grundsätzlich die gleichen Regeln wie beim Nutzer und es dürften ähnliche Probleme aufkommen und darüber hinaus noch eigene Fragen, etwa die nach der Entschlüsselungspflicht von kryptographierten Daten, die bisher nicht anerkennt wird.[28]

4. Beschlagnahme illegal erlangter Daten bei einem Hacker?

Angesichts dieser Schwierigkeiten liegt es nicht so fern, den Weg zu wählen, den das US-amerikanische FBI in den vergangenen Jahren eingeschlagen hat, als es für die Entschlüs-

16 Zur Verwendung von Log-Daten und Fahrparametern aus dem E-Steuerungsgerät eines Mietwagens: LG Köln ZD 2017, 192; zur Verwertung von Aufnahmen fest installierter Kamerasysteme im Kraftfahrzeug *Niehaus* NZV 2016, 551.

17 Für ein Zukunftsszenario aus der Science-Fiction Literatur der 1950er-Jahre vgl. *Asimov*, The Naked Sun, 1957; zur aktuellen Rechtslage: *Momsen* FS Beulke, 2015, 871 ff.

18 Vgl. dazu *Pfeiffer*, StPO, 5. Aufl. 2005, Vor § 48 Rn. 1 ff.

19 So wie heute von – elektronisch aufgerüsteten – Unfallautos bekannt, vgl. etwa *Schlanstein* NZV 2016, 201 ff.

20 *Hilgendorf/Valerius*, Internet- und Computerstrafrecht, 2. Aufl. 2012, Rn. 774 ff. und 786 ff.

21 § 110 Abs. 3 StPO; vgl. zu Fragen der Einwilligung in die Durchsuchung eines Computers *Jahnel/Mader/Staudegger*, IT-Recht, 3. Aufl. 2012, S. 720 f.

22 *Gercke/Brunst*, Praxishandbuch Internetstrafrecht, 2010, Rn. 974.

23 *Beukelmann* NJW-Spezial 2017, 440; *Safferling/Rückert* JR 2017, 16.

24 SK-StPO/*Wolter/Jäger*, 5. Aufl. 2016, § 110 Rn. 9.

25 Vgl. dazu § 95 Abs. 1 StPO; *Pfeiffer* (Fn. 18), § 95 Rn. 1 ff.

26 Das hat sich in der Vergangenheit etwa bei Herausgabeverlangen von Daten aus Kraftfahrzeugen gezeigt, vgl. dazu *Schlanstein* NZV 2016, 201 (206).

27 Dazu bspw. *Revolidis*, The FBI vs. Apple: Twilight of Mobile Encryption and Privacy? ZD-Aktuell 2016, 05059.

28 Vgl. etwa *Gercke/Brunst* (Fn. 22), Rn. 979 sowie *Schlanstein* NZV 2016, 201 (206 ff.).

selung eines iPhones in der Hackerszene um Hilfe fragte.[29] Dass solche Wege praktisch beschritten werden, sagt aber natürlich noch nichts darüber, ob ein solches Vorgehen zu vor Gericht verwertbaren Erkenntnissen führt. Ob Behörden durch Private *illegal* erlangte Daten dann als Beweis verwerten können, ist bekanntlich nicht durch die StPO geregelt.[30]

II. Verwendung als Überwachungsgerät

Noch interessanter als der Zugriff auf vorhandene Aufzeichnungen könnte die Nutzung digitaler Assistenten als Überwachungsgerät sein.

1. Sprachassistenten als Mittel zum sog. Grossen Lauschangriff

Digitale Sprachassistenten als Abhörgeräte zu benutzen liegt nahe, da sie bereits mit aktivem Mikrophon in der Wohnung stehen. Zudem dürften Hersteller regelmässig »Hintertüren« für den Fall bereitstellen, dass sie ein Software-Update oder einen anderweitigen Zugriff für notwendig halten.[31] Allerdings fehlt eine Regelung dazu, ob Strafverfolgungsbehörden ein als Haushaltsassistent kreiertes Gerät ohne weiteres für eine akustische Wohnraumüberwachung nutzen dürften.[32] Und so bleibt unklar, welche strafverfahrensrechtliche Ermächtigungsgrundlage für diesen Eingriff einschlägig ist.[33]

2. Sprachassistenten und die sog. Quellen-TKÜ

Neue Formen einer Überwachung eröffnet die »Hauruck-Einführung«[34] der Quellen-TKÜ bzw. Online-Durchsuchung[35] im Rahmen einer Gesetzesänderung zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens.[36] Damit hat die grosse Koalition in der letzten Legislaturperiode innerhalb weniger Wochen einen Weg geschaffen, auf dem Strafverfolgungsbehörden künftig computertechnologisch gestützte Kommunikation verdächtigter Personen abfangen oder deren Computerspeicher unbemerkt – mit Hilfe von Spionagesoftware – durchsuchen und relevante Daten heimlich beschlagnahmen dürfen.[37] Strafrechtliche Ermittlungen über einen digitalen Assistenten könnten ein breites Spektrum von Massnahmen eröffnen: Über das zeitgleiche Lauschen am Mikrophon eines Sprachassistenten hinaus könnte man sich bei einer Weiterentwicklung und entsprechenden Vernetzung vorstellen, dass über den elektronischen Butler ein quasi verdeckt ermittelnder Bote losgeschickt wird, der – entsprechend vorprogrammiert – alle relevanten Informationen einsammelt.[38] Wie Strafverfolgungsbehörden mit den durch § 100b StPO eröffneten Optionen umgehen werden, ist noch offen. Der Anwendungsbereich der neuen Normen blieb bis ins Gesetzgebungsverfahren unklar.[39]

III. Zwischenergebnis

Darüber, wie Strafverfolgung im digitalisierten Zeitalter tatsächlich aussehen wird, lässt sich heute zum Teil nur spekulieren. Auch wenn Sprachassistenten und/oder andere Haushaltsgeräte mit Roboterfunktion in näherer Zukunft kaum automatisch die Polizei rufen dürften,[40] potentiell hilfreich ist eine dauernde Erfassung menschlichen Verhaltens durch die Sensoren ihrer digitalisierten Helfer für Strafverfolgungsbehörden sicherlich.[41] Unklar bleibt jedoch zum ersten, wie die generierte Information für die Sachverhaltsaufklärung im Strafverfahren fassbar wird.

Die Strafverfahrensordnung ist noch tief in der analogen Welt verankert. Das zeigt sich etwa daran, dass die Zuordnung der für eine Informationssammlung notwendigen Eingriffe – aufgrund der raschen Entwicklung computergestützter Technologie – zu den von der StPO zur Verfügung gestellten Ermittlungsmassnahmen schwer fällt.[42] Hier dürfte in der Zukunft § 100b StPO den Weg ebnen, wenn über digitale Sprachassistenten kommuniziert wird und eine Beschlagnahme von Daten an eine Telefonüberwachung grenzt, um dann in eine Online-Durchsuchung zu münden.[43] Diese Erweiterung deutet aber auch bereits die Kehrseite an: Zum zweiten stellt sich nämlich ganz grundsätzlich die Frage nach einer adäquaten Grenze neuer Möglichkeiten der Informationsbeschaffung in einer digitalisierten Lebensumgebung.

D. Grenzen der Amtsaufklärung im digitalen Zeitalter?

Die Frage, welche Grenzen für strafrechtliche Ermittlungen im digitalen Zeitalter gelten, ist noch offen.

I. Neue Falllinien

Die Multifunktionalität digitaler Assistenten, die einen Befehl – etwa zur Anwahl einer bestimmten Telefonnummer – entgegennehmen, speichern, den Telefonkontakt herstellen, während sie das Gesagte auf weitere Befehle »streamen«, erschwert schon die Entscheidung, welche strafverfahrensrechtliche Grundlage einschlägig für einen Zugriff auf möglicherweise für die Strafverfolgung relevante Daten ist. Die Zuordnung einer Ermittlungsmassnahme zu einer bestimmten Rechtsgrundlage ermächtigt Ermittlungsbehörden, gleichzeitig begrenzt es die Ermittlungen auf das rechtlich Zulässige.[44]

Die zunehmend schwieriger werdende Zuordnung von Ermittlungseingriffen zu den in der StPO vorgesehenen Zwangsmassnahmen ist aber nur ein Problem einer Amtsaufklärung im digitalen Zeitalter. Grundlegende Fragen ergeben sich auch dadurch, dass der Einzug digitaler Assistenten in den privaten Lebensraum anscheinend eine freiwillige Entscheidung von Individuen ist, sich einer permanenten

29 Hacker haben bereits Mikrophone digitaler Assistenten in »Wanzen« verwandelt, siehe www.spiegel.de/netzwelt/gadgets/amazon-echo-sicherheitsexperte-macht-lautsprecher-box-zur-wanze-a-1161194.html.

30 Vgl. BVerfGE 106, 28 (48 f.); BVerfG NJW 2010, 2937 (2938) = StV 2010, 666; BGHSt 56, 127 (134) = StV 2011, 336; *Rogall* JZ 2008, 818 (822 f., 825); *Gercke/Brunst* (Fn. 22), Rn. 750 m.w.N.; KK-StPO/*Senge*, 7. Aufl. 2013, Vor § 48 Rn. 52 m.w.N.

31 Zur Nutzung von Sicherheitslücken durch Sicherheitsbehörden: *Gercke/Brunst* (Fn. 22), Rn. 858.

32 Vgl. § 100c StPO.

33 Vgl. dazu auch *Safferling/Rückert* JR 2017, 9 (13).

34 Vgl. Zwischenruf von *Ströbele* in der Bundestagsdebatte vom 22.06.2017 (BT-Prot. 18/240, 24585, 24589 und 24594 D) sowie *Roggan* StV 2017, 821; *Singelnstein/Derin* NJW 2017, 2646.

35 Insgesamt zu Online-Zugriffen *Gercke/Brunst* (Fn. 22), Rn. 855 ff.

36 Gesetz v. 17.08.2017 – BGBl. I v. 23.08.2017, S. 3202.

37 *Safferling/Rückert* JR 2017, 9 (10 f.).

38 Vgl. auch *Safferling/Rückert* JR 2017, 9 (16).

39 Vgl. BT-Drs. 18/12785, S. 56; *Safferling/Rückert* JR 2017, 9 (11); *Stoklas/Wendorf* ZD-Aktuell 2017, 05725; *Beukelmann* NJW-Spezial 2017, 440.

40 Wie in der satirischen Verarbeitung durch NDR Extra 3 durchaus realistisch dargestellt, siehe http://daserste.ndr.de/extra3/sendungen/extra-3-Familie-Leben-mit-Sprachassistenten,extra13146.html.

41 Nicht nur für Ermittlungen, sondern auch zum sog. Profiling, vgl. *Singelnstein/Derin* NJW 2017, 2646 (2647).

42 Vgl. dazu *Gercke/Brunst* (Fn. 22), Rn. 639 ff.; *Hilgendorf/Valerius* (Fn. 20), Rn. 765.

43 Keine eigenmächtige Kombination von Ermittlungsbefugnissen durch Ermittlungsbehörden: *Gercke/Brunst* (Fn. 22), Rn. 869 m.w.N.; vgl. aber *Roggan* NJW 2015, 1995.

44 Mit Blick auf die neue Online-Durchsuchung *Singelnstein/Derin* NJW 2017, 2646 (2648).

Überwachung auszusetzen: Wer sich ein Mikrofon in die Wohnung stellt, welches das gesprochene Wort (jedenfalls teilweise) aufzeichnet, muss damit rechnen, dass andere bei Bedarf auf diese Dokumentation zugreifen oder gleich mithören.[45] Oder doch nicht? Die Strafprozessordnung bleibt hier eine Antwort schuldig. Die grundsätzliche Unterscheidung zwischen bewusst generierter Information, auf welche die Behörden grundsätzlich zugreifen dürfen, und der zeitgleichen Überwachung durch die Strafverfolgungsbehörden, die nur unter viel engeren Voraussetzungen zulässig ist, führt nicht weiter. Wie bereits angesprochen, verwischt die Technik die normativ gezogenen Grenzen, welche die StPO für den Zugriff auf bestehende Aufzeichnungen einerseits, und die Überwachung andererseits zieht. Aber diese Grenzen werden nicht obsolet, wenn sich jemand eines digitalen Assistenten bedient, der Gesprochenes »streamt«. Aus Sicht der Nutzer bleibt ihnen – wenn sie ohne Code-Wort sprechen – das flüchtige Gespräch oder die vertrauliche Kommunikation. Ohnehin verliert das Freiwilligkeitsargument an Überzeugungskraft, wenn Autos vorschriftsmässig mit dem neuen eCall-System ausgestattet und dadurch elektronisch auslesbar werden. Die Argumentation dürfte auch jenen gegenüber zu kurz greifen, die sich aufgrund ihrer gesundheitlichen Lage für eine »smarte Prothese« entscheiden (müssen) oder deren Arbeitgeber nur noch digitalisierte Strukturen zur Verfügung stellen.

II. Traditionelle Ansätze für Beweisverbote

Weil viele wichtige Individual- und Allgemeininteressen die Digitalisierung bestimmter Vorgänge in unserer Lebenswelt voraussichtlich vorantreiben wird, stellt sich mit Blick auf Strafverfahren dringlich die Frage: Welche Beweisverbote sollen im digitalen Zeitalter gelten? Denn (noch) ist das Strafverfahrensrecht vom Konsens geprägt, dass die Chance auf eine möglichst umfassende Wahrheitsermittlung nicht um jeden Preis, beispielsweise nicht um die Aufgabe jeglicher Privatsphäre, erkauft werden darf. Braucht es für eine Lebenswelt, in der Roboter beständig Informationen über Menschen generieren, neuer Ansätze oder genügen die aktuellen Verbote der Strafprozessordnung?

Wenn etwa deutsche Strafermittler nach einem mutmasslichen Tötungsdelikt einen aktiven digitalen Assistenten am Tatort finden und sich über das Nutzerkonto Zugang zu gespeicherten Dateien verschaffen würden, ist fraglich, ob die Beschlagnahme dieser Daten durch eine analoge Anwendung von § 97 StPO begrenzt wird.[46] Diese Norm schützt bekanntlich Mitteilungen zwischen Beschuldigten und Zeugnisverweigerungsberechtigten, allerdings nur, wenn die Daten »im Gewahrsam der zur Verweigerung des Zeugnisses Berechtigten« sind. Wenn Daten oder Dokumente nicht mehr bei dem Zeugnisverweigerungsberechtigten sind, dürfen die Strafverfolgungsbehörden zugreifen. Daten, die digitale Sprachassistenten generieren, sind zwar teilweise für den Nutzer über ein entsprechendes Alexa-Konto abrufbar, grundsätzlich aber beim Anbieter gespeichert. Schon deshalb dürfte der Schutz des § 97 StPO meist nicht greifen.

Will man die Schutzlücke schliessen, bedarf es neuer Lösungsansätze. Dabei ist die Zuflucht in neue gesetzliche Regelungen nicht der einzige, und vielleicht auch nicht der vielversprechendste Weg. Vielmehr könnte man zunächst in Erwägung ziehen, über die technische Ausgestaltung den gesetzlichen Schutz zu erhalten. Das wäre etwa zu erreichen, wenn die Kommunikation mit Zeugnisverweigerungsberechtigten ausschliesslich in deren Bereich gespeichert wird. Möglich ist aber auch eine Erweiterung des normativen Schutzbereichs von § 97 StPO. Es findet sich sogar *ein* Beispiel für eine gesetzliche Modifikation des Schutzbereiches: § 97 Abs. 2 S. 1 verbietet die Beschlagnahme einer elektronischen Gesundheitskarte mit Rücksicht auf die Vertraulichkeit der Krankengeschichte, obwohl sich die Chipkarte beim Patienten befindet. Denn diese Verschiebung ausserhalb der Sphäre des behandelnden Arztes erfolgte aus übergeordneten Gesichtspunkten. Hier hat der Gesetzgeber den traditionellen Ansatz einer normativen Beschränkung für eine bestimmte Fallkonstellation konsequent in das digitale Zeitalter weitergedacht.

III. Schutz des Kernbereichs privater Lebensgestaltung, § 100d StPO

Mit dem durch die Gesetzesänderung zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens[47] eingeführten Beweisverbot, § 100d StPO, hat der Gesetzgeber einen anderen Weg eingeschlagen: Wenn »tatsächliche Anhaltspunkte für die Annahme vor[liegen], dass durch eine Maßnahme nach den §§ 100a bis 100c *allein* Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden«, ist die Beweiserhebung von vorneherein unzulässig.[48]

1. Grund zur Hoffnung oder leeres Versprechen?

§ 100d definiert absolute Schranken – weitgehend unabhängig von den Modalitäten des Ermittlungseingriffes.[49] Das erscheint fortschrittlich. Denn es trägt dem Umstand Rechnung, dass eine schnell fortschreitende technologische Entwicklung strafverfahrensrechtliche Garantien für bestimmte Ermittlungseingriffe zunehmend leerlaufen lässt. Fraglich ist allerdings, wie das neue Beweisverbot durchgesetzt werden soll. Wie wird etwa bei einem automatisierten und vorprogrammierten Ermittlungseingriff (wie etwa der online-Durchsuchung) verhindert, dass nicht doch (*allein*) Erkenntnisse aus dem Kernbereich privater Lebensgestaltung (§ 100d Abs. 3 StPO) gewonnen werden? Wie müsste man dafür die Suchfunktion der Spähsoftware limitieren? Mit syntaktischen Kriterien etwa die Durchsuchung von bestimmten Text-, Bild- oder Videodateien von vorneherein ausschliessen? Oder mit zeitlicher Beschränkung, etwa keine nächtliche Kommunikation zu berücksichtigen, um damit den Kernbereich privater Lebensgestaltung zu schützen?

Die Schwierigkeiten, das versprochene Beweisverbot sinnvoll vorzuprogrammieren, provoziert die Frage nach dem Sinn oder Unsinn eines solchen Beweisverbotes: Gibt § 100d StPO Grund zur Hoffnung einer Neuorientierung von Beweisverboten im digitalen Zeitalter oder sind solche Rege-

45 Der öffentlichen Raum dürfte ohnehin immer engmaschiger mit Kameras überwacht werden, vgl. etwa zum Einsatz von Gesichtserkennung in Überwachungskameras am Berliner Bahnhof Südkreuz (o. Fn. 11).
46 BVerfG NJW 2002, 1410.
47 O. Fn. 36.
48 Hervorhebung durch *Verf.*; zur Problematik des einfachen Tatverdachts zwischen Tatsachenbegründung und kriminalistischen Erfahrungswerten *Gercke/Brunst* (Fn. 22), Rn. 716 und 794.
49 *Safferling/Rückert* JR 2017, 9 (14).

lungen letztlich nur leere Versprechen?[50] § 100d StPO fasst – unschwer zu erkennen – die Rechtsprechung des *BVerfG* zum Schutz der (digitalen) Privat- und Intimsphäre zusammen.[51] Mit weitsichtigen Urteilen verlangte das *Gericht*, dass gesetzliche Regelungen dafür Sorge tragen müssen, dass trotz zunehmender Möglichkeiten einer Überwachung, ein Kernbereich privater Lebensgestaltung bestehen bleibt.[52] Der Schutz gilt auch im Strafverfahren, insbesondere wenn bei Ermittlungen auf informationstechnische Systeme zugegriffen wird, namentlich auf elektronische Geräte in Wohnungen oder Kraftfahrzeugen, Steuerungsanlagen der Haustechnik etc., die »einen Einblick in wesentliche Teile der Lebensgestaltung einer Person« geben.[53] Informationen aus dem absolut geschützten Intimbereich sollen nicht ins Strafverfahren gelangen.[54] Diese an das Persönlichkeitsrecht anknüpfende Rechtsprechung war immer eine Gratwanderung, denn strafrechtliche Ermittlungen können und müssen in einen durch das Persönlichkeitsrecht grundsätzlich geschützten Bereich eindringen.[55] Dass dem Gesetzgeber mit der neuen gesetzlichen Regelung in § 100d StPO der Balanceakt gelungen ist, erscheint aus verschiedenen Gründen fraglich, insbesondere wegen Zweifeln an der praktischen Durchsetzbarkeit eines Beweisverbots, das sich im Zeitalter der Digitalisierung pauschal auf den Kernbereich privater Lebensgestaltung bezieht, ohne diesen theoretisch so neu zu fundieren, dass etwa eingesetzte Spähsoftware dementsprechend vorprogrammiert werden kann.

a) Praktische Durchsetzbarkeit

Die Durchsetzbarkeit von § 100d StPO in der Praxis ist schon deshalb unklar,[56] weil es bisher keine klare normative Bestimmung des Kernbereichs privater Lebensgestaltung gibt,[57] und damit auch keine Grundlage, aufgrund derer eine – letztlich wie ein verdeckter Ermittler agierende – Spähsoftware programmiert werden sollte, damit sie den geschützten Kernbereich vom Aussenbereich privater Lebensgestaltung abgrenzen kann. Ohne eine Definition des Bereichs, den eine algorithmisch programmierte Spähsoftware als Grenze beachten und den Fortgang einer Online-Durchsuchung stoppen muss, wird der »elektronische Ermittler« ungehindert und unbekümmert auch in den innersten Bereich privater Lebensgestaltung nach Informationen suchen.[58]

Es bleibt – anders als bei einer durch einen menschlichen Ermittler kontrollierten Informationssammlung – nur das nachträgliche Aussortieren. Damit ist aber gerade nicht erreicht, was der Gesetzgeber mit § 100d StPO erreichen wollte, dass es einen unantastbaren Bereich privater Lebensgestaltung gibt, der nicht zum Gegenstand einer Rechtsprechung wird, die nachträglich öffentlich festlegt, was noch und was *nicht* zum Kernbereich gehört.[59] Ein anschauliches Beispiel ist das Selbstgespräch. Hier herrschte bisher Einigkeit, dass Worte, die ein Mensch in einer »nicht öffentlichen Äußerungssituation« zu sich selbst spricht, unabhängig von ihrem Inhalt, nicht als Beweismittel in Frage kommen.[60] Es besteht Konsens über ein Recht, im Zwiegespräch mit sich selbst, Gedanken zu sortieren, selbst wenn die gesprochenen Worte mitgehört werden. Massgeblich sei, ob es sich unter Gesamtbewertung aller Umstände im Einzelfall um eine »eindimensionale Selbstkommunikation« handele, etwa bei einer unbewussten Äusserung, die letztlich nur darauf gerichtet ist, mit sich selbst ins Reine zu kommen.[61] Der Ort des Selbstgesprächs ist dabei nicht ausschlaggebend.[62] Es könnte sich um ein Krankenzimmer handeln[63] oder ein Kraftfahrzeug[64] oder die eigene Wohnung. Muss dies genauso gelten, wenn ein digitaler Assistent mithört?

Vor diesem Hintergrund erschliesst sich die praktische Bedeutung von § 100d Abs. 2 StPO, der die bereits bekannten Vorgaben für die akustische Raumüberwachung nun allgemein aufnimmt:

Für den Fall, dass Informationen aus dem Kernbereich privater Lebensgestaltung aufgenommen werden, müssen sie unverzüglich gelöscht werden. Das soll das rechtswidrige Eindringen in einen höchstpersönlichen Bereich aus strafprozessualer Sicht neutralisieren. Ob die strafverfahrensrechtliche Restitution so einfach funktioniert, soll hier dahingestellt bleiben.[65] Eine staatsfreie Privatsphäre ist bei einer automatisierten Durchsuchung von privaten Computersystemen jedenfalls nicht mehr gewährleistet: Es droht immer eine Blossstellung in einem höchstpersönlichen Bereich – unabhängig davon, ob am Ende für oder gegen eine Löschung entschieden wird. Daneben darf – auch in einer stabilen Demokratie – nicht vergessen werden, dass die Angst vor einer an Überwachung anschliessende Repression zu dem befürchteten chilling-Effekt der Selbstzensur in privater Diskussion bei marginalisierten Gruppen politisch Andersdenkender führen kann.[66]

b) Theoretisches Fundament für Beweisverbote im digitalen Zeitalter

Im Lichte der Diskussion um die praktische Durchsetzbarkeit erscheint eine unreflektierte Anknüpfung an die

50 Andere Monita bleiben hier ausgeblendet, etwa: dass § 100d Abs. 5 StPO nur Vertrauensverhältnisse nach § 53 StPO und nicht umfassend Zeugnisverweigerungsrechte schützt.

51 Vgl. BVerfG StV 2008, 169 Rn. 290–293; *Wehage*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von Informationsverarbeitungssystemen, 2013, 207; *Singelnstein/Derin* NJW 2017, 2646 (2647).

52 BVerfG StV 2008, 169 Rn. 169; vgl. auch BVerfGE 78, 77 (85); 84, 239 (279 f.); 92, 191 (197) = StV 1996, 143; 115, 320 (344 f.).

53 BVerfG StV 2008, 169 Rn. 173, 202 und 203.

54 BVerfGE 109, 279 = StV 2004, 169.

55 Vgl. BVerfGE 34, 238 (245); 80, 367 (376, 379 f.) = StV 1990, 1; 106, 28; vgl. auch BVerfGE 65, 1 (44, 54); 67, 100 (143).

56 Vgl. auch *Roggan* StV 2017, 821 (824 f.).

57 Dazu etwa: BVerfG StV 2008, 169 Rn. 169 und 290-299.

58 Vgl. SK-StPO/*Wolter* (Fn. 24), Vor § 151 Rn. 29. Ein im Pkw aufgezeichnetes Selbstgespräch eines sich unbeobachtet fühlenden Beschuldigten sei dem absolut geschützten Kernbereich zuzurechnen und damit unverwertbar, vgl. BeckOK-StPO/*Hegmann*, Stand: Ed. 28 24.08.2017, § 100f Rn. 21-26.

59 Vgl. BVerfGE, 27, 1 (6): Krankenakten, Dokumentation des Ehelebens in Ehescheidungsakten etc., vgl. Maunz-Dürig-GG/*di Fabio*, 81. Lfg. 2017, Art. 2 Rn. 158.

60 BGHSt 57, 71 = StV 2012, 269.

61 BGHSt 57, 71 = StV 2012, 269, im Anschluss an BGHSt 50, 206 = StV 2005, 591.

62 Dazu etwa *Jahn/Geck* JZ 2012, 561 ff.; *Momsen/Savic* KriPoZ 2017, 301 ff.

63 BGHSt 50, 206 = StV 2005, 591: Selbstgespräch sei – im Gegensatz zum Zwiegespräch – dadurch gekennzeichnet, dass Äußerungen nur für die eigenen Ohren bestimmt seien, anders als beim »Tagebuch«-Eintrag (BVerfGE 80, 367 = StV 1990, 1), bei dem durch das Festhalten der Gedanken auf Papier eine solche Abgeschlossenheit vom Aufzeichnenden gerade nicht gewollt sei.

64 BGHSt 57, 71 = StV 2012, 269 (im Anschluss an BGHSt 50, 206 = StV 2005, 591).

65 Zur Problematik der praktischen Durchsetzung von Verwertungsverboten etwa: *Pfeiffer* (Fn. 18), § 100d 1-7; *Wohlers/Blüsi* Recht 2015, 158 ff.

66 Vgl. etwa *Karig*, Befallen vom Überwachungsvirus vom 04.01.2015, www.deutschlandfunk.de/staatliche-ueberwachung-befallen-vom-ueberwachungsvirus.1184.de.html?dram:article_id=307639.

Drei Sphären-Theorie des *BVerfG* als theoretisches Fundament für Beweisverbote im digitalen Zeitalter zweifelhaft. § 100d StPO illustriert die Schwächen, wenn der Gesetzgeber eine Rechtsprechung des *BVerfG* zwar formal, nicht aber in ihrem dynamischen Geist eines mitwachsenden Beweisverbots umsetzt. Die Topoi des Drei-Sphären-Ansatzes, öffentlich-privat-intim,[67] müssen perspektivisch in den Urteilen des *BVerfG* fortgedacht werden, wie es sich vor allem im Urteil zur Online-Durchsuchung andeutet: Mit einer immer umfassenderen elektronischen Erfassung und einer Vernetzung der Daten verwischt die Unterscheidung zwischen öffentlich-privat-intim, weil mit der Weiterentwicklung der Datenauslesbarkeit aus öffentlichen Daten Intimes rekonstruiert werden kann.[68] Ein prominentes Beispiel dafür lieferte die Veröffentlichung anonymisierter Fahrten der Taxis in New York City in visualisierter Form,[69] mit Hilfe derer die mutmasslichen Besucher von Sex-Clubs ebenso identifiziert werden konnten wie vermutlich muslimische Taxifahrer.[70]

Im Lichte solcher Entwicklungen ist künftig zu bestimmen, welche Informationen als Erkenntnisse aus dem Kernbereich privater Lebensgestaltung verboten sind. Es wird sich eine Vielzahl grundlegender Fragen stellen. Die Verwertbarkeit eines Selbstgesprächs im Beisein eines Sprachassistenten betrifft insofern nur eine Detailfrage, die ein Schlaglicht auf das Problem eines Rechts auf ein Zwiegespräch mit sich selbst in einer zunehmend digital erfassten Welt wirft, in der man auf eine Flüchtigkeit des gesprochenen Wortes kaum mehr vertrauen darf, wenn dieses ständig durch einen Roboter »gestreamt« wird.[71]

IV. Technische Absicherung normativer Grenzen

Vorrangiges Problem der Beweisverbote im digitalen Zeitalter dürfte jedoch nicht die normative Fundierung, sondern die praktische Durchsetzung bleiben. § 100d StPO entfaltet nur Wirkung, wenn durch eine Vorprogrammierung der »elektronischen Ermittler« der Kernbereich privater Lebensgestaltung möglichst unangetastet bleibt. Die gesetzlichen Vorgaben müssen technisch so umgesetzt werden, dass Rechtsverletzungen von vorneherein vermieden werden. Bereits in den 90er-Jahren deutete sich eine technische Absicherung als Alternative zum normativen Gebot in der Diskussion über »privacy by design« an.[72] Dahinter stand die Idee, Produkte technisch so zu konstruieren, dass sie praktisch keine Daten ausserhalb des Gerätes generieren und so der Schutz der Privatsphäre bereits weitgehend mechanisch sichergestellt ist. Die Idee hat zwar Eingang in das EU-Recht gefunden,[73] praktisch konnte sie sich aber bisher nur wenig durchsetzen. Erst in jüngerer Zeit rückt dieser Ansatz – etwa in Zusammenhang mit Dataschutz Engineering – wieder stärker in den Fokus. In der juristischen Diskussion fordert man nun unter dem Schlagwort »legality by design«, dass normative Vorgaben umfassender algorithmisch verankert werden.[74]

Vor diesem Hintergrund erschliesst sich auch die Forderung nach einer Zertifizierung der von Strafverfolgungsbehörden eingesetzten Spähsoftware, die in Zusammenhang mit der Einführung der Online-Durchsuchung immer wieder vorgebracht wurde.[75] Denn eine Spähsoftware kann – anders als ein mithörender Mensch – nur dann rechtzeitig abschalten, wenn ihr die Achtung vor einem nicht antastbaren Kernbereich vorher einprogrammiert wurde. Insofern zeigt § 100d den digitalen Sprung. Programmierer brauchen klare Vorgaben, um Software im binären System vorzugeben, wann es »zu privat wird«. Technik ist hier entscheidend.

E. Fazit und Ausblick

Ein freiheitlicher Staat muss »Orte der Privatheit« nicht nur respektieren, sondern schützen – gerade im digitalen Zeitalter.[76] Ein blosses Beweisverbot zum Schutz des Kernbereichs privater Lebensgestaltung – ohne flankierende Massnahmen – genügt dafür nicht. § 100d StPO alleine würde nur scheinbar Privaträume schützen. Was lange als Substrat der Intimsphäre und »letztes Refugium zur Wahrung der Menschenwürde« galt,[77] um im Familienkreis Nöte zu teilen oder im Selbstgespräch mit sich ins Reine zu kommen, ist in Gefahr,[78] wenn rechtliche Regelungen nicht durch Technik abgesichert werden.

Wer angesichts dieses Befundes alleine auf die Selbstverantwortung des einzelnen verweist, verkennt die Dynamik der Digitalisierung: Die Unterscheidung zwischen einer freiwilligen Öffnung einer persönlichen Sphäre und einer Digitalisierung unter (staatlichem) Zwang mit Rücksicht auf übergeordnete Interessen ist fliessend und verschiebt sich mit technischem Fortschritt und gesellschaftlichen Bedürfnissen. Das zeigt sich bereits in vielen Bereichen, wie etwa im Strassenverkehr mit der Implementierung des eCall-Rettungssystems[79] oder in der Arbeitswelt, in der man sich zunehmend digitalisierter Strukturen bedienen muss, deren Modalitäten man nicht individuell bestimmen kann.[80] Es braucht nur wenig Phantasie um sich entsprechende Entwicklungen für Wohnungen und Häuser in naher Zukunft vorzustellen, in

67 BVerfGE 34, 238 (245); 80, 367 (376, 379 f.) = StV 1990, 1; 106, 28 (39, 44); Beschränkung des allgemeinen Persönlichkeitsrechts ist zum Schutz überwiegender Allgemeininteressen zulässig durch ein Gesetz oder auf Grundlage eines Gesetzes, das Voraussetzungen und Umfang der Beschränkung hinreichend klar umschreibt und dem Grundsatz der Verhältnismäßigkeit genügt, vgl. BVerfGE 65, 1 (44, 54); 67, 100 (143); 78, 77 (85); 84, 239 (279 f.); 92, 191 (197) = StV 1996, 143; 115, 320 (344 f.).

68 Vgl. etwa *Hilgendorf/Valerius* (Fn. 20), Rn. 766.

69 www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn.

70 www.theiii.org/index.php/997/using-nyc-taxi-data-to-identify-muslim-taxi-drivers.

71 BGHSt 57, 71 = StV 2012, 269.

72 Siehe dazu *Cavoukian*, Privacy by Design, The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices, abrufbar unter https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf; zu technischen Grenzen vgl. *Koops/Leenes* International Review of Law, Computers & Technology 2014, 159.

73 Art. 25 VO (EU) 2016/679 v. 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutz-Grundverordnung), ABl. L 119 v. 04.05.2016, 1.

74 *Hildebrandt*, Saved by Design? The Case of Legal Protection by Design, NanoEthics 2017, www.researchgate.net/publication/319295253_Saved_by_Design_The_Case_of_Legal_Protection_by_Design.

75 *Roggan* StV 2017, 821 (824 f.).

76 Vgl. dazu etwa das Minderheitsvotum der Richterinnen *Jäger* und *Hohmann-Dennhardt* zur Entscheidung des *BVerfG* betreffend die Zulässigkeit von Abhörmaßnahmen in Wohnräumen (BVerfGE 100, 382 [391]; *Rux* JZ 2007, 292); zur rechtlichen Problematik der (vielen, parallelen) deutschen Rechtsregelungen etwa: *Gercke/Brunst* (Fn. 22), Rn. 748 m.w.N.

77 BVerfGE 109, 279 (323) = StV 2004, 169.

78 Siehe dazu die Tagebuchentscheidung von 1989, BVerfGE 80, 367 (381) = StV 1990, 1; *Hohmann-Dennhardt* NJW 2006, 545.

79 Dazu etwa *Wohlers* BJM 2016, 113 (121); *Sander/Hollering* NStZ 2017, 193 (200); *Hilgendorf*, in: ders./Hötitzsch/Lutz (Hrsg.), Rechtliche Aspekte automatisierter Fahrzeuge, 2015, S. 15 (21).

80 Vgl. etwa aus der Perspektive von Strafverteidigern: *Jahn/Palm* AnwBl. 2011, 613 ff.

denen zur Aufrechterhaltung einer effizienten Stromversorgung nur noch sog. smart meter verwendet werden dürfen,[81] der Daten generiert, aus denen relativ einfach sehr persönliche Verbraucherprofile generiert werden können.

Unsere Rechtsordnung geht davon aus, dass es private Rückzugsräume für den einzelnen Menschen geben muss. Das gilt auch dann, wenn darin digitalisierte Systeme integriert sind. Die Vertraulichkeit solcher Systeme ist nicht nur Leitprinzip in der Rechtsprechung des *BVerfG*, sie ist strafrechtlich geschützt.[82] Das Vertrauen auf Privatsphäre verdient staatlichen Schutz, auch in der Ausgestaltung strafrechtlicher Ermittlungen. Die gesetzeskonforme Programmierung staatlicher Spähsoftware ist dabei nur ein Element, aber ein wichtiges. Spähsoftware funktioniert nur dann legal, wenn sie die Vorgaben des § 100d StPO achtet. Wird der Schutz eines nicht antastbaren Kernbereichs des Privaten nicht vor Einsatz einprogrammiert, so etabliert das Beweisverbot zwar eine begrüssenswerte Maxime, bleibt aber für die Praxis des Strafverfahrens nutzloses Wortgeklingel – ein leer laufender Kernbereichsschutz.[83]

81 *Ciminano/Herlitz* NZM 2016, 410 f.
82 Vgl. dazu etwa die strafrechtlichen Grenzen bspw. in § 202a StGB sowie *Gercke/Brunst* (Fn. 22), Rn. 867; *Rux* JZ 2007, 292.
83 Vgl. *Roggan* StV 2017, 821 (828 ff.); *Safferling/Rückert* JR 2017, 9 (22); *Singelnstein/Putzer* GA 2015, 564 ff.

Auf dem Weg zur technischen Dokumentation der Hauptverhandlung in Strafsachen

Richterin am BGH Dr. Louisa Bartel, Karlsruhe

Seit Jahrzehnten wird kontrovers darüber diskutiert, ob die tatrichterliche Hauptverhandlung in Strafsachen akustisch oder audiovisuell aufgezeichnet werden sollte, um die Wahrheitsfindung im Strafprozess zu verbessern und das Risiko von Fehlurteilen zu senken. Das reine Formalienprotokoll, das in erstinstanzlichen Verfahren vor den Landgerichten und den Oberlandesgerichten nichts über den Inhalt der Hauptverhandlung verrät, wird als unzeitgemäß kritisiert und als Hemmnis für eine wirksame Rechtskontrolle in der Revision identifiziert.[1] Von engagierten Strafverteidigern wird deshalb immer wieder die Forderung erhoben, die »Alleinherrschaft des Richters über die prozessuale Wahrheit«[2] zu beenden; die Deutungshoheit der Tatgerichte über den Hauptverhandlungsstoff sei durch eine fehlende Dokumentation des Hauptverhandlungsgeschehens unbegrenzt, sie bleibe unkontrolliert und führe dazu, dass relevanter Beweisstoff in den schriftlichen Urteilsgründen ausgeblendet oder übergangen, Aussageinhalte verfälscht oder sogar frei erfunden würden,[3] um das Urteil gegen eine effektive revisionsgerichtliche Kontrolle zu immunisieren. Die tatsächliche Dimension des Problems in der forensischen Praxis ist allerdings ungewiss.[4]

A. Einführung

Das plakative Bild, die Urteilsgründe hinterließen bei Strafverteidigern häufig den Eindruck, in einem »falschen Film«[5] gewesen zu sein, wird nur selten mit nachvollziehbaren Fakten belegt; es wäre aber geradezu erstaunlich, wenn die Sicht von Staatsanwaltschaft, Gericht und Verteidigung auf die Ergebnisse der Hauptverhandlung sich stets als übereinstimmend erwiesen. Vereinzelte Beispiele[6] belegen freilich, dass der Vorwurf eines allzu freien Umgangs mit dem Inbegriff der Hauptverhandlung, der geeignet ist, das Vertrauen in die Strafjustiz zu erschüttern, nicht nur theoretischer Natur ist.

An konkreten Gesetzesvorschlägen hat es in der Vergangenheit nicht gefehlt.[7] Im Jahr 2010 hat der Strafrechtsausschuss der Bundesrechtsanwaltskammer (Strauda) mit seinem »Entwurf eines Gesetzes zur Verbesserung der Wahrheitsfindung im Strafverfahren durch verstärkten Einsatz von Bild-Ton-Technik« einen konkreten Gesetzesvorschlag vorgelegt, der eine obligatorische Aufzeichnung der tatrichterlichen Hauptverhandlung in den erstinstanzlichen Verfahren vor den Landgerichten und Oberlandesgerichten vorschlägt; die Dokumentation sollte die Berichtigung des Hauptverhandlungsprotokolls in Zweifelsfällen ermöglichen und in der Revision uneingeschränkt als Mittel des revisionsgerichtlichen Freibeweisverfahrens[8] Verwendung finden können.

Demgegenüber wird die Idee einer technischen Dokumentation der Hauptverhandlung in der Richterschaft teils mit einer gewissen Skepsis, teils mit entschiedener Ablehnung betrachtet.[9] Insbesondere die Vorstellung, der Gesetzgeber könne die Verwendung einer technischen Dokumentation der erstinstanzlichen Hauptverhandlung künftig ohne jede Einschränkung als Mittel des revisionsgerichtlichen Freibeweisverfahrens zulassen mit der Folge, dass die Revisionsgerichte künftig verpflichtet sein könnten, zur Überprüfung des Revisionsvorbringens bei zulässig erhobener Verfahrensrüge ein vielstündiges Videoprotokoll zu betrachten und zu

1 *Mosbacher* StV 2018, 182.
2 *Malek* StV 2011, 559 (564).
3 Vgl. *Nestler* FS Lüderssen, 2002, S. 727 (731).
4 Nach einer Erhebung der AG Strafrecht des DAV aus dem Frühjahr 1989, an der 158 Mitglieder teilnahmen, gaben 72,1 % an, dass Zeugenaussagen »in vielen Fällen« falsch aufgenommen, missverstanden oder sonst unrichtig verarbeitet würden, 3,9 % gaben an, dass dies »für die Mehrzahl der Fälle« gelte, vgl. *Saldit* StraFo 1990, 54 (59).
5 Vgl. *Norouzi*, Vom Rekonstruktionsverbot zum Dokumentationsverbot. Schriftenreihe der Strafverteidigervereinigungen, 2011, S. 215; *E. Wilhelm* ZStW 117 (2005), 143 ff.
6 Vgl. das von *Norouzi* (Fn. 5) geschilderte Beispiel, das ein Urteil des *LG Mosbach* betrifft.
7 In einem Gesetzentwurf aus dem Jahr 1993 hatte der Strafrechtsausschuss des Deutschen AnwaltVereins eine Tonaufzeichnung gefordert; eine Änderung des Revisionsrechts wurde nicht angestrebt, vgl. AnwBl. 1993, 328 f.
8 Zur Überprüfung von Verfahrensrügen, nicht zur Überprüfung im Rahmen der Sachrüge.
9 Nach *Sandherr* (DRiZ 2017, 338 [341]) votierten 91 % der im Rahmen des »2. Strafkammertags 2017« an einer Online-Abstimmung Teilnehmenden gegen die Einführung einer Dokumentation der Hauptverhandlung.