SJZ

Schweizerische Juristen-Zeitung
Revue Suisse de Jurisprudence

Redaktion
Dr. Gaudenz G. Zindel, Rechtsanwalt
Dr. Meinrad Vetter, Oberrichter
Prof. Dr. Pascal Pichonnaz

Erscheint jeden Monat am 1. und 15.
Paraît le 1er et le 15 de chaque mois

12 15. Juni 2018, 114. Jahrgang

Schulthess §

Digitale Assistenten und strafprozessuale Beweisführung

«Hilfe, mein Haus belauscht mich!»

Prof. Dr. iur. Sabine Gless und Dario Stagno, MLaw, Universität Basel (Basel)*

Digitale Assistenten nehmen immer häufiger als intelligente Agenten in Wohnung, Arbeitsplatz, Fahrzeug und als smarte Prothesen im menschlichen Körper an unserem Privatleben teil. Die Autoren legen dar, wie vielfältig Nutzen und Gefahr bei Eingriffen in Aufzeichnungen digitaler Assistenten sind, namentlich bei der Sachverhaltsermittlung, zur Überwachung, als Beweismittel oder auch zur Verteidigung. In Bezug auf die gesetzliche Regelung von Beweiserhebungs- und Beweisverwertungsverboten hat die Schweiz eine Vorreiterrolle inne, doch konkrete Ansätze für eine inhaltliche Schranke zur Wahrung der Privatsphäre in Zeiten automatisierter Beweiserhebung fehlen. Bei der Suche nach einem adäquaten Schutz der Privatsphäre zeigen die Autoren, dass die Diskussion um «Privacy by Design» in Zusammenhang mit der neuen Datenschutzgesetzgebung in der EU die Entwicklung in der Schweiz massgeblich beeinflussen dürfte. ***Zi.***

Les assistants numériques participent de plus en plus à notre vie privée, en tant qu'agents intelligents dans les logements, les lieux de travail, les véhicules et en tant que prothèses intelligentes dans le corps humain. Les auteurs présentent les multiples avantages et les risques liés au recours à des enregistrements d'assistants numériques, en particulier pour la constatation de faits, pour la surveillance, à titre de moyen de preuve ou même pour se défendre. S'agissant de la réglementation relative aux interdictions de l'administration ou de l'exploitation de certains moyens de preuve, la Suisse joue un rôle pionnier; toutefois, à l'heure de l'administration automatique des preuves, il n'existe pas de mesures concrètes visant la protection de la sphère privée. En cherchant à établir une protection adéquate de la vie privée, les auteurs montrent que la discussion du «Privacy by Design», en lien avec la nouvelle législation sur la protection des données dans l'UE, pourrait influencer de manière décisive les conceptions en Suisse. ***P.P.***

I. Einleitung

Für Technologiebegeisterte begann das Jahr 2018 mit der CES-Messe in Las Vegas. Sie stand im Zeichen sog. «digitaler Assistenten», die versprechen, das Leben für Menschen in vielfältiger Hinsicht bequemer zu machen, etwa «elektronische Butler» wie bspw. Alexa oder Google Home, die auf Befehl das Licht dimmen, Musik abspielen oder einen Witz erzählen. Um funktionsfähig zu sein, müssen sie ständig zuhören. Sie sind mit Mikrofonen und Lautsprechern ausgestattet und filtern alle Umgebungsgeräusche nach ihrem Aktivierungswort, um allenfalls auf einen gesprochenen Befehl zu reagieren. Sie «streamen» alles Gehörte an die Server der Gerätebetreiber, zum Beispiel Amazon oder Google.[1] Welche Bedeutung hat es für strafrechtliche Ermittlungen, wenn Roboter zunehmend in unsere Lebensumgebung integriert werden? Wer Zugriff auf einen digitalen Assistenten hat, der laufend mithört, könnte theoretisch Gespräche rekonstruieren oder sogar zeitgleich mithören. Könnten Roboter vielleicht sogar zu Zeugen in einem Strafverfahren oder zu Überwachungsgeräten der Polizei oder gar verdeckten Ermittlern werden? Oder setzt das Recht hier Grenzen? Für eine Antwort auf diese Fragen bedarf es einer Vorstellung, wie digitale Assistenten künftig in unsere Lebensumgebung eingebettet sein könnten und wie Strafverfolgungsbehörden auf dadurch generierte Daten zugreifen könnten. Neben einer Analyse der *de lege lata* in der StPO normierten Rechtsgrundlagen und möglicher Beweisverbote stellt sich aus Sicht der Rechtswissenschaft die Grundsatzfrage nach der Verbindung zwischen Datenschutzrecht, Privatsphäre und strafrechtlicher Sachverhaltsaufklärung. Dabei darf man nicht vergessen: In der Rechtspraxis klafft oft eine beträchtliche Lücke zwischen den rechtlich vorgesehenen und den dann in der Ermitt-

* Dank gilt dem Schweizer Nationalfonds für seine Unterstützung im Rahmen des NFP 75 Big Data <http://www.nfp75.ch/en/projects/module-2-societal-and-regulatory-challenges/project-gless>.

1 Siehe <https://techcrunch.com/2017/05/08/amazon-to-control-70-percent-of-the-voice-controlled-speaker-market-this-year/> (12.3.2018).

lungsarbeit mit vertretbaren Kosten umsetzbaren Optionen. Die schöne neue Welt der Roboter hat ihren Preis.

II. Unsere Zukunft: Digitale Assistenten hören mit

Ein elektronischer Butler «streamt» das gesprochene Wort beständig: Kommunikation und Umgebungsgeräusche werden m.a.W. als Tondokument aufgezeichnet und, verschlüsselt, über eine Internetverbindung an den Gerätebetreiber (heute wohl meist in den USA) geleitet.[2] Dessen dürften sich die meisten Benutzer von digitalen Assistenten bewusst sein, denn die neuen elektronischen Helfer sind Gegenstand einer ausserordentlich hohen Medienpräsenz, die immer wieder die Funktionsweise und Privatsphärenbedenken vor Augen führt. Digitale Sprachassistenten, als Beispiel dient in dieser Abhandlung der sog. «Echo» von Amazon, sind letztlich recht einfach aufgebaut. Sie funktionieren aufgrund eines dauerhaft eingeschalteten Mikrofonsystems, das alle eingehenden Geräusche nach einem bestimmten Aktivierungswort filtert; beim Echo ist dieses standardmässig «Alexa». Fällt dieses, wird ein Befehl entgegengenommen und über den eingebauten Lautsprecher «beantwortet». Voraussetzung ist eine dauernde Verbindung über das Internet mit den Servern des Plattformbetreibers. Amazon verspricht, dass der «Echo» erst nach Herausfiltern des Aktivierungswortes eine Verbindung aufbaut und Gesprächsfetzen weiterleitet. Denn die eigentliche «Intelligenz» steckt regelmässig nicht im Assistenzsystem selbst, sondern in den Rechenzentren des Betreibers. Die Befehlseingaben werden auf Amazon-Servern – für die Nutzer bspw. über eine App auf dem Smartphone zugänglich – als Tondatei abgespeichert, aber auch transkribiert.[3] Letztlich lässt sich nicht garantieren, dass digitale Assistenten nur aufnehmen, was unmittelbar nach dem Aktivierungswort gesprochen wird. Es ist unklar, ob etwa Umgebungsgeräusche sauber herausgefiltert werden können oder wann genau die Aufnahme der gesprochenen Befehle tatsächlich beendet wird.[4]

Die Nutzer dürften das wissen und entscheiden sich gleichwohl für die Bequemlichkeit eines digitalen Helfers im Haushalt. Doch nicht alle setzen sich ganz freiwillig einer Beobachtung durch Roboter aus. In manchen Lebenssituationen besteht erheblicher Druck, eine Unterstützung durch *digital devices* anzunehmen, etwa für Menschen im fortgeschrittenen Lebensalter oder mit körperlichen Behinderungen, wenn ein Roboter ein selbständigeres Leben ermöglicht. Mit der Vernetzung von Vorgängen in Arbeitswelt und Privatumgebung dürfte sich künftig aber auch die breite Masse immer häufiger gezwungen sehen, digitale Assistenten in Arbeitsabläufe einzubeziehen, um nicht abgehängt zu werden.[5] Ein simples Beispiel für eine solche Entwicklung liefert die Autoindustrie: Seit diesem Jahr müssen in der EU verkaufte Neuwagen vorschriftsmässig mit dem sog. «eCall»-System ausgestattet sein, einem fest in das Fahrzeug eingebauten Notrufsystem, bestehend u.a. aus einer SIM-Karte mit ständiger Internetverbindung, um bei einem Unfall u.U. automatisch Hilfe zu rufen.[6] Damit dies auch nur dann passiert, wenn dringende Hilfe nötig ist, ist das System an verschiedene Sensoren des Fahrzeugs gekoppelt. Für die strafrechtliche Ermittlungsbehörde könnte der Umstand interessant sein, dass sich damit – bspw. aufgrund einer charakteristischen Fahrweise – nachträglich feststellen liesse, wer ein Fahrzeug zu einem bestimmten Zeitpunkt gefahren hat.[7]

Die Entscheidung für eine Digitalisierung der Lebensumgebung muss also nicht immer ganz frei gewählt, sondern

[2] Zur Verschlüsselung der Übertragung siehe bspw. <www.iot-tests.org/2017/06/careless-whisper-does-amazon-echo-send-data-in-silent-mode> (12.3.2018).

[3] Alexa-Nutzungsbedingungen vom 6.12.2017, <www.amazon.de/gp/help/customer/ display.html?nodeId=201809740> (12.3.2018); «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 an[...]-hören.»; «Echo [verwendet] 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 <https://www.amazon.de/gp/help/customer/display.html/ref=hp_left_v4_sib/258-9424951-1681848?ie=UTF8&nodeId=201602230> (12.3.2018).

[4] Spannend diesbezüglich sind aktuelle Bestrebungen von Amazon, wonach die Assistenten inskünftig dauernd zuhören könnten, um gezielt Werbemassnahmen zu ergreifen, vgl. <https://bazonline/wirtschaft/unternehmen-und-konjunktur/alexa-hör-zu/story/13489057> (10.5.2018)

[5] *Schuldt*, Konnektivität: Die Vernetzung der Welt, zukunftsInstitut, <www.zukunftsinstitut.de/artikel/konnektivitaet-die-vernetzung-der-welt/> (12.3.2018).

[6] EU-Verordnung 2015/758 vom 29. April 2015 über Anforderungen für die Typgenehmigung zur Einführung des auf dem 112-Notruf basierenden bordeigenen «eCall»-Systems in Fahrzeugen, ABl L 123, 19.5.2015, 77.

[7] Vgl. dazu etwa *Enev/Takakuwa/Koscher/Kohno*, Automobile Driver Fingerprinting, Proceedings on Privacy Enhancing Technologies, 1 (2016) 34–51, <http://www.autosec.org/pubs/fingerprint.pdf> (12.3.2018).

kann Resultat einer schwierigen Interessensabwägung sein, die durch – mehr oder weniger starken – äusseren Zwang bestimmt ist.

III. Sachverhaltsaufklärung mit Hilfe digitaler Assistenten

Weil es viele wichtige Individual- und Allgemeininteressen gibt, die für einen Einsatz von digitalen Assistenten zur Unterstützung von Menschen sprechen, dürfte menschliches Verhalten bald in grösserem Umfang elektronisch erfasst und dadurch anschliessend – jedenfalls theoretisch – auslesbar sein. Damit stellen sich viele neue Fragen, unter anderem: Dürften auch Strafverfolgungsbehörden auf die Informationen zugreifen, die digitale Assistenten sammeln und sie dann in einem Strafverfahren verwerten?

Dafür spricht die Pflicht zur Sachverhaltsaufklärung im Strafverfahren: Strafbehörden müssen alle zur Beurteilung der Tat und der beschuldigten Person bedeutsamen Tatsachen abklären (Art. 6 StPO). Das Beweisrecht ist entsprechend offen ausgestaltet. Mit Blick auf die technische Entwicklung verpflichtet Art. 139 Abs. 1 StPO deshalb zur Sachverhaltsaufklärung mit allen rechtlich zulässigen Beweisen nach dem aktuellen Stand der Wissenschaft.[8] Insofern könnte auch jede Information, die durch einen digitalen Assistenten generiert wird, zur Sachverhaltsaufklärung beitragen.

Es braucht wenig Fantasie, um sich vorzustellen, dass der vermehrte Einsatz digitaler Assistenten den Strafbehörden ein qualitativ neues Guckloch in das Privatleben einer tatverdächtigen Person eröffnen könnte, weil etwa Sprachassistenten den Zugriff auf bereits vorhandene Aufzeichnungen oder die Durchsuchung von Dateien oder sogar eine zeitgleiche geheime Überwachung ermöglichen.[9] In der Praxis stehen zwischen dem einen ungehinderten Blick bis in privateste Lebensbereiche natürlich noch faktische Hindernisse, wie die Kosten bestimmter Massnahmen oder die Datenspeicherung im Ausland.

A. Zugriff auf vorhandene Aufzeichnungen

Es stellt sich aber grundsätzlich die Frage: Können Strafermittler unbeschränkt Zugriff nehmen, wenn sie im Rahmen von Ermittlungen auf digitale Assistenten stossen, etwa neben einer Leiche einen aktivierten Amazon-Echo finden?[10] Dürfen sie versuchen, damit das vergangene Geschehen zu rekonstruieren?

1. Art. 162 StPO: Digitale Assistenten als Zeugen?

Weil digitale Assistenten mit ihren Benutzern sprachlich interagieren, könnte man auf die Idee kommen, sie als Zeugen zu vernehmen: Wer kommuniziert, kann auch vor Gericht registrierte Geschehnisse vortragen. Doch Roboter können nach unserem heutigen Verständnis nicht wirklich «bezeugen», also eigene Wahrnehmungen reflektiert wiedergeben.[11] Je menschenähnlicher Roboter allerdings künftig werden,[12] desto näher könnte der Gedanke rücken, dass sie bei der Sachverhaltsrekonstruktion mehr als auslesbare Maschinen sind.[13] Wenn sie je eine Art Zeugenstatus erhielten, stellte sich aber auch die Frage, ob ihnen ein Recht zu schweigen zukäme, angelehnt etwa an Zeugnisverweigerungsrechte von Strafverteidigern oder Familienmitgliedern.

2. Art. 157 StPO: Herausgabe von Daten durch Nutzer

Als einfachster Weg, um an die Daten eines digitalen Assistenten zu kommen, erscheint das Herausgabeverlangen an die beschuldigte Person. Diese könnte ihr zugängliche Daten freiwillig herausgeben und so mithelfen, ein Verfahren voranzubringen. Einen Anreiz hätte sie dazu allenfalls, wenn aufgezeichnete Daten sie nicht belasten, sondern entlasten würden, bspw. indem diese eine Anwesenheit an einem bestimmten Ort zum Tatzeitpunkt und damit ein Alibi dokumentierten. Eine allfällige Siegelung kann verlangt und eine spätere Verwendbarkeit muss geklärt werden.[14]

---

[8] BSK StPO-*Gless*, Art. 139 N 9; CR CPP-*Bénédict/Treccani*, Art. 139 N 2.

[9] Zur Audioüberwachung in der Wohnung vgl. die Rechtsprechung des Bundesgerichts in BGE 143 I 292; s.a. *Künzli/Müller/Tschentscher/Wyttenbach*, Die staatsrechtliche Rechtsprechung des Bundesgerichts in den Jahren 2016 und 2017, I.–IV., ZBJV *2017* 687 f.

[10] Vgl. bspw. <https://edition.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html> (12.3.2018).

[11] Vgl. dazu etwa BSK StPO-*Bähler*, Art. 162 N 7 sowie Art. 163 N 1.

[12] Vgl. dazu etwa <www.theguardian.com/world/2017/apr/04/chinese-man-marries-robot-built-himself> (12.3.2018).

[13] So wie heute von – elektronisch aufgerüsteten – Unfallautos bekannt, vgl. etwa *Schlanstein*, Nutzung von Fahrzeugdaten zur Optimierung der Verkehrsunfallaufnahme, NZV *2016* 201 ff.

[14] Zur Siegelung nach freiwilliger Herausgabe BGE 140 IV 28.

3. *Art. 265 StPO: Herausgabe von Daten durch Anbieter*

Die Option der Herausgabe steht Beschuldigten ohnehin nur offen, wenn sie auf Daten zugreifen können. Ist dies nicht der Fall, müssen Ermittlungsbehörden Anbieter digitaler Assistenten zur Herausgabe von Daten auffordern.[15] Verweigert ein Anbieter eine freiwillige Herausgabe – weil es dem Image regelmässig nicht dienlich sein dürfte, wenn man enger mit der Polizei als mit den eigenen Nutzern zusammenarbeitetet –,[16] kann gem. Art. 265 Abs. 3 StPO für den Fall der Nichtkooperation Strafe angedroht werden. Ein eindrückliches Beispiel für den komplexen Widerstreit von Interessen bot die Auseinandersetzung zwischen Apple und dem US-amerikanischen FBI über den Zugang zu iPhone-Daten der Attentäter von San Bernardino.[17] Ähnlich wollte in einem Mordfall, bei dem ein Amazon-Echo möglicherweise zum Tatzeitpunkt aktiv war und Geräusche aufgezeichnet hatte, Amazon keine Daten ohne Einverständnis des Verdächtigen herausgeben.[18]

4. *Art. 263 StPO: Beschlagnahme der Aufzeichnungen*

Werden Daten nicht freiwillig herausgegeben, steht eine (Beweis-)Beschlagnahme im Raum.[19]

Diese ist gemäss Art. 263 StPO auch bei Drittpersonen möglich, wenn diese voraussichtlich bspw. als Beweismittel gebraucht werden.[20] Grundsätzlich reicht den Strafbehörden eine forensische Kopie der Daten.[21] Der Beschlagnahme der Daten hat der Gesetzgeber aber gewisse Grenzen gesetzt, wenn ein anderes Interesse das Strafverfolgungsinteresse überwiegt, bspw. wenn Daten Informationen betreffen, die eine beschuldigte Person mit ihrem Strafverteidiger ausgetauscht hat.[22] Ob eine solche Einschränkung bei digitalen Assistenten in der Praxis tatsächlich wirksam befolgt werden könnte, erscheint zweifelhaft, wenn etwa unklar ist, welche Daten überhaupt registriert wurden.[23] Bei der Durchsuchung von Aufzeichnungen nach Art. 246 StPO handelt es sich um einen schwerwiegenden Eingriff in die Privatsphäre des Betroffenen, sodass dieser die Siegelung der Aufzeichnungen gem. Art. 248 StPO verlangen kann.[24]

In der Praxis ergeben sich weitere Schwierigkeiten: Zum einen befindet sich der Speicherort der Daten digitaler Assistenten meist ausserhalb der Schweiz,[25] zum anderen sind diese regelmässig verschlüsselt abgespeichert – und bisher erscheint unklar, wie weit die seit dem revidierten NDG bestehende Entschlüsselungspflicht von Schweizer Providern von Telekommunikationsdienstleistungen reicht.[26] Angesichts solcher Probleme liegt der Weg nahe, den das US-amerikanische FBI in dem erwähnten San-Bernardino-Fall eingeschlagen hat, als es sich Hilfe aus der Hackerszene holte. Den (teuren) Weg über eine Entsperrung des Passworts durch «private Anbieter» geht man mittlerweile auch in der Schweiz, bspw. in schweren Fällen organisierter Kriminalität.

B. Zugriff auf laufende Aufzeichnungen und zeitgleiche Überwachung

Nicht nur zur Rekonstruktion des in der Vergangenheit Gesprochenen, sondern vielleicht auch zur zeitgleichen Überwachung könnten digitale Assistenten benutzt werden. Es kann für Ermittlungsbehörden durchaus praktisch sein, dass Tatverdächtige zu Hause über das Internet vernetzte Mikrofone nutzen. Denn diese könnten «angezapft» werden, zumal die Hersteller in der Software regelmässig

15 Vgl. dazu BSK StPO-*Bommer/Goldschmid*, Art. 265 N 16 ff; CR CPP-*Lembo/Berthod*, Art. 265 N 4.

16 Das hat sich in der Vergangenheit etwa bei Herausgabeverlangen von Daten aus Kraftfahrzeugen gezeigt, vgl. dazu *Schlanstein* (Fn. 13) 206.

17 Dazu bspw. *Revolidis*, The FBI vs. Apple: Twilight of Mobile Encryption and Privacy?, ZD-Aktuell *2016*, 05059; <https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone> (12.3.2018).

18 Siehe <www.sueddeutsche.de/digital/digitales-leben-mitbewohner-mit-grossem-ohr-1.3314240> (12.3.2018).

19 Hier ist die gem. Art. 197 Abs. 2 StPO geforderte Zurückhaltung zu beachten, vgl. BSK StPO-*Weber*, Art. 197 N 14 ff.; Art. 265 Abs. 4 StPO.

20 BSK StPO-*Bommer/Goldschmid*, Art. 263 N 31; *Hilgendorf/Valerius*, Internet- und Computerstrafrecht, Ein Grundriss, 2. A., München 2012, Rn. 774 ff. und 786 ff.

21 Vgl. Art. 192 Abs. 2 StPO; Art. 247 Abs. 3 StPO; *Heimgartner*, Strafprozessuale Beschlagnahme, Wesen, Arten und Wirkungen – Unter Berücksichtigung der Beweismittel-, Einziehungs-, Rückgabe- und Ersatzforderungsbeschlagnahme, Zürich 2011, 90; BSK StPO-*Bürgisser*, Art. 192 N 8, wonach elektronische Datenaufzeichnungen Urkunden gleichgesetzt werden.

22 Vgl. Art. 264 Abs. 1 lit. a und b StPO.

23 BSK StPO-*Thormann/Brechbühl*, Art. 246 N 8.

24 BSK StPO-*Thormann/Brechbühl*, Art. 246 N 1, 8 f.; CR CPP-*Lembo/Berthod*, Art. 263 N 16 ff.

25 Vgl. Art. 31–34 CCC, betreffend im Ausland gespeicherter Computerdaten sowie Verkehrs- und Inhaltsdaten in Echtzeit; zum Territorialitätsprinzip *Graf*, Strafverfolgung 2.0: Direkter Zugriff der Strafbehörden auf im Ausland gespeicherte Daten?, Jusletter IT, 21.9.2017, Rz. 26 ff.

26 Vgl. dazu Art. 43 Abs. 2 NDG: «Von [den Providern] angebrachte Verschlüsselungen müssen sie entfernen»; *Arnold*, Daten aus dem Auto – Digitale Spuren im Strassenverkehr, Jusletter IT, 24.11.2016.

«Hintertüren» programmiert haben dürften, schon nur, um für notwendige Software-Updates Zugriff zu haben. Wäre es da nicht praktisch, auch die Ermittlungsbehörden nutzten diese Sicherheitsöffnungen, wenn die Voraussetzungen für geheime Überwachungsmassnahmen nach Art. 269 ff. StPO vorliegen?[27]

Fraglich ist aber schon im ersten Schritt, ob die strafprozessualen Grundlagen einen Eingriff in die Privatsphäre über ein Haushaltsgerät überhaupt vorsehen. Denn die StPO ist eher in der analogen Welt verhaftet und auf den Einsatz multifunktionaler digitaler Assistenten nicht wirklich vorbereitet.

1. *Art. 269 ff. StPO: Fernmeldeverkehrsüberwachung*

Das zeigt sich etwa bei der Frage, ob auf die durch digitale Assistenten generierten Daten im Wege einer Fernmeldeverkehrsüberwachung zugegriffen werden könnte. Als *Fernmeldeverkehr* gilt jede fernmeldetechnisch vermittelte Übertragung von Informationen an individuelle Empfänger.[28] Hier könnte man sich einerseits auf den Standpunkt stellen, dass elektronische Butler nicht der Telekommunikation mit anderen dienen, in der Schweiz können sie (noch) nicht einmal als Telefon benutzt werden.[29] Die an sie gerichteten Worte werden nur deshalb als elektrische Signale über Leitungen nach aussen vermittelt, damit sie Hilfsdienste verrichten.[30] Diese zweckorientierte Definition des Fernmeldeverkehrs schlösse eine Überwachung nach Art. 269 ff. StPO demnach derzeit aus. Dies könnte sich allerdings mit dem technologischen Fortschritt bald anders darstellen, wenn etwa eine Telefonfunktion in Assistenten integriert würde.[31]

2. *Art. 269ter StPO: Überwachung mit besonderen Informatikprogrammen*

Ein Rückgriff auf den – mit der Revision des BÜPF – neu geschaffenen Art. 269ter StPO erscheint auch nur auf den ersten Blick vielversprechend.[32] Auf dieser Grundlage können zum Zweck, den Inhalt einer Kommunikation und der Randdaten des Fernmeldeverkehrs in unverschlüsselter Form abzufangen und auszuleiten, sog. «besondere Informatikprogramme» in Datenverarbeitungssysteme eingeschleust werden.[33]

Der Begriff des Datenverarbeitungssystems ist zwar weit. Er soll alle technischen Einrichtungen erfassen, die nicht direkt lesbare und üblicherweise in kodierter Form vorhandene Informationen entgegennehmen, automatisiert bearbeiten und wieder abgeben.[34] Darunter fielen auch digitale Assistenten. Art. 269ter StPO zielt aber nur darauf, die Problematik der Verschlüsselung des *Fernmeldeverkehrs* zu umgehen. Nur die Telekommunikation dürfte folglich mit eingeschleuster GovWare überwacht werden.[35] Solange die Funktionen eines elektronischen Butlers nicht als Fernmeldeverkehr i.S.d. Art. 269 ff. StPO anzusehen sind, ergibt sich also auch aus Art. 269ter StPO keine Überwachungsgrundlage.

3. *Art. 280 StPO: Einsatz von Überwachungsgeräten*

Fraglich ist, ob Strafverfolgungsbehörden «Alexa und ihre Schwestern» auf der Grundlage von Art. 280 StPO als technische Überwachungsgeräte einsetzen dürften.[36] Was genau ein technisches Überwachungsgerät ist, erscheint noch ungeklärt.[37] Unstreitig zählen dazu die zu diesem

---

[27] *Pieth*, Schweizerisches Strafprozessrecht, 3. A., Basel 2016, 160 ff. m.w.H.

[28] Vgl. *v. Mangoldt/Klein/Starck*, Kommentar zum Grundgesetz, 6. A. München 2010, Art. 10 Rn. 39; die StPO beinhaltet keine Legaldefinition zum Begriff des Fernmeldeverkehrs. Gemeint ist der «Informationsaustausch auf Distanz über ein organisatorisches oder technisches Medium», bspw. über elektronische Netze, vgl. BSK-StPO-*Jean-Richard-dit-Bressel*, Art. 269 N 15; zur fernmeldetechnischen Übertragung von Informationen die Definitionen in Art. 3 lit. a und c FMG.

[29] Eine entsprechende Telefoniefunktion mit digitalen Assistenten existiert in den USA bereits und wird derzeit schrittweise auch in weiteren Ländern, zurzeit im Vereinigten Königreich, eingeführt, siehe <http://www.silicon.co.uk/networks/voip/google-free-phone-calls-via-home-speaker-229471?inf_by=5aa52c54671db8dd398b4c8f> (12.3.2018).

[30] Vgl. Art. 3 lit. b und c FMG.

[31] An der diesjährigen Entwicklerkonferenz Google I/0 hat der Technologiegigant eine neue Funktion seiner digitalen Assistenten vorgestellt, wonach der Assistent selbstständig Telefonanrufe tätigen kann, bspw. um Termine mit Dienstleistungsanbietern zu vereinbaren. Die Funktion namens «Google Duplex» erscheint dabei am Telefon wie ein Mensch – ein möglicher Ansatzpunkt für eine Fernmeldeüberwachung? Näheres zur Funktionsweise siehe <https://ai.googleblog.com/2018/05/duplex-ai-system-for-natural-conversation.html> (10.5.2018).

[32] Das revidierte BÜPF und entsprechende Anpassungen in der StPO sind am 1. März 2018 in Kraft getreten.

[33] BBl *2013* 2683, 2771 ff.; BBl *2013* 2789, 2807; *Teichmann*, Unzulässigkeit von Onlineuntersuchungen, Anwaltsrevue *2017*, 428 f.

[34] BSK StGB-*Weissenberger*, Art. 143bis N 8 ff.

[35] *Hansjakob*, Das neue BÜPF – Nötig oder Zwängerei?, ZStrR *2016* 438 f.

[36] BSK StPO-*Eugster/Katzenstein*, Art. 280 N 7 ff.

[37] *Ruckstuhl/Dittmann/Arnold*, Strafprozessrecht, 2011, 271; vgl. Botschaft zur Vereinheitlichung des Strafprozessrechts vom 21.12.2005, BBl *2006* 1085, 1251 f.; BSK StPO-*Eugster/Katzenstein*, Art. 280 N 16, 22.

Zweck hergestellten Kameras oder Mikrofone sowie Peilsender für eine Observation an nicht öffentlich oder nicht allgemein zugänglichen Orten.[38] Digitale Assistenten könnten u.E. unter diesen Begriff nur passen, nachdem die Behörden sie durch Spähsoftware entsprechend manipulieren. Fraglich ist, ob dies genügt, um sie zu einem strafprozessual anerkannten Überwachungsgerät zu machen. Denn dazu dürfte nicht nur die Funktionalität, sondern vor allem die Zuverlässigkeit der damit erfolgenden Beweiserlangung ausschlaggebend sein. Dies ist bei einem mit sog. «GovWare» modifizierten privaten Haushaltsgerät nicht ohne Weiteres der Fall.[39]

C. Zwischenergebnis

Der Zugriff von Strafermittlern auf die durch digitale Assistenten generierten Daten ist heute sowohl in rechtlicher als auch in praktischer Hinsicht weitgehend ungeklärt. Der generelle Auftrag zur Sachverhaltsaufklärung (Art. 139 StPO) spricht zwar grundsätzlich dafür, sich neuer Beweismöglichkeiten zu bedienen, aber diese müssen rechtlich zulässig sein, das heisst, Zwangsmassnahmen müssen gesetzlich geregelt sein und allfällige Beweisverbote beachtet werden.

IV. Beweisverbote im digitalen Zeitalter

Der strafprozessuale Auftrag, durch das Ermittlungsverfahren die Wahrheit zu finden, gilt nicht uneingeschränkt. Vielmehr wird dieser durch den Gesetzesvorbehalt begrenzt, wenn Grundrechte eingeschränkt werden (Art. 36 BV).[40] Dass es keine Wahrheitssuche um jeden Preis gibt, zeigen ferner die in Art. 140 und Art. 141 StPO etablierten Beweisverbote. Die eidgenössische StPO will eine klare und umfassende Regelung,[41] scheint aber noch stark in der analogen Welt verhaftet und nicht unbedingt vorbereitet auf das digitale Zeitalter.

A. Begrenzung der Beweiserhebung

Technologischer Fortschritt wirft immer wieder die Frage nach dem rechtlich Zulässigen im Strafverfahren auf.

1. *Gesetzliche Grundlage für den Zugriff auf digitale Assistenten*

Voraussetzung für die Zulässigkeit einer Zwangsmassnahme ist die Existenz einer gesetzlich normierten Rechtsgrundlage (Art. 197 Abs. 1 lit. a StPO).[42] Bei einem schwerwiegenden Eingriff in ein Grundrecht muss ein Gesetz im formellen Sinn den Eingriff hinreichend bestimmen. Für die Präzision der Regelung gelten hohe Anforderungen.[43] Fehlte eine Rechtsgrundlage ganz, wäre eine Beweiserhebung von vorneherein grundsätzlich unzulässig.[44] Existiert sie, muss jede Ermittlungshandlung weiter verhältnismässig sein (Art. 197 Abs. 1 lit. c StPO; Art. 36 Abs. 3 BV).

Der Zugriff auf digitale Assistenten und die durch sie generierten Daten tangiert das Grundrecht auf Schutz der Privatsphäre (Art. 13 BV) und insbesondere die Achtung des Privatlebens.[45] Als Rechtsgrundlage für eine Rekonstruktion von vergangenem Geschehen käme eine Beschlagnahme von Daten nach Art. 263 ff. StPO in Betracht.[46] Keine Rechtsgrundlage besteht aber für eine zeitgleiche Überwachung, solange digitale Assistenten weder als Geräte für den Fernmeldeverkehr (vgl. Art. 269 StPO oder Art. 269ter StPO) noch als Überwachungsgeräte (Art. 280 StPO) kategorisiert werden können. Allerdings könnte eine technische Weiterentwicklung digitaler Assistenten, etwa durch eine Telefonfunktion, oder eine Neu-Definition des «technischen Überwachungsgeräts» die Diskussion neu eröffnen.[47]

2. *Eingreifen von Beweiserhebungsverboten*

Man sollte sich deshalb bereits jetzt, im Vorfeld einer möglichen Nutzung von digitalen Assistenten als Mittel staatlicher Sachverhaltsaufklärung, fragen, ob nicht ohnehin Beweiserhebungsverbote eingreifen würden, wenn künftig

---

38 *Pieth* (Fn. 27) 168; BSK StPO-*Eugster/Katzenstein*, Art. 280 N 22 ff.

39 Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 27.2.2013, BBl *2013* 2683, 2701 f., 2771 ff.; BSK StPO-*Eugster/Katzenstein*, Art. 280 N 16; BSK StPO-*Jean-Richard-dit-Bressel*, Art. 269 N 2; *Teichmann*, Unzulässigkeit von Onlineuntersuchungen, Anwaltsrevue *2017*, 429; a.A. *Roos/Jeker*, Der «Grosse Lauschangriff», forumpoenale *2017* 412 f.; CR CPP-*Zufferey/Bacher*, Art. 280 N 5, 11 f.

40 Art. 36 BV und Art. 197 Abs. 1 lit. a StPO, vgl. a. *Pieth* (Fn. 27) 131; BSK StPO-*Weber*, Art. 197 N 1 f.

41 BSK StPO-*Gless*, Art. 139 N 2, Art. 140 N 2 f., Art. 141 N 2 ff.

42 *Pieth* (Fn. 27) 162; BSK-*Gless*, Art. 139 N 16; BSK-*Weber*, Art. 196 N 8, Art. 197 N 4 ff.

43 BSK BV-*Epiney*, Art. 36 N 33 ff.; BSK-*Weber*, Art. 197 N 4; BSK BV-*Diggelmann*, Art. 13 N 30; BSK BV-*Epiney*, Art. 36 N 35.

44 Zur Ausnahme: BSK BV-*Epiney*, Art. 36 N 40 ff.; CR CPP-*Viredaz/Johner*, Art. 197 N 4.

45 BSK BV-*Diggelmann*, Art. 13 N 26 f., 30.

46 BSK StPO-*Riedo/Fiolka*, Art. 6 N 67 ff.

47 BSK StPO-*Eugster/Katzenstein*, Art. 280 N 22.

Zugriff auf Inhalte von Familien- oder Selbstgesprächen in einer Privatwohnung genommen werden sollte.

Einschlägig erscheinen zunächst jene Beweiserhebungsverbote, die dem Schutz bestimmter Vertrauensverhältnisse dienen.[48] Sie verbieten etwa die zwangsweise Vernehmung bestimmter Personen als Zeugen, wie von Familienmitgliedern oder von Strafverteidigern (Art. 168–173 StPO), und sind für bestimmte Personengruppen auch noch durch Beschlagnahmeverbote und Abhörverbote flankiert, damit das Vernehmungsverbot nicht dadurch untergraben wird.[49] Eine solche Ausnahme von der grundsätzlichen Pflicht, einen strafrechtlich relevanten Sachverhalt aufzuklären, besteht nur in wenigen, gesetzlich genau definierten Situationen, etwa im Strafverteidiger-Mandanten-Verhältnis, [50] aber auch, wenn bei persönlichen Aufzeichnungen und Korrespondenz der beschuldigten Person ihr Interesse am Schutz ihrer Persönlichkeit das Strafverfolgungsinteresse überwiegt (Art. 264 Abs. 1 lit b StPO).[51] Wenn digitale Assistenten zunehmend in die menschliche Lebensumgebung integriert werden, fragt sich, ob diese Vorgabe ausreicht, um den intendierten Schutz einer höchstpersönlichen Sphäre zu erreichen oder ob es dafür weiterer, allenfalls auch technischer Vorkehrungen bedarf.

B. Beweisverwertungsverbote

Ein Schutz der Privatsphäre könnte auch durch Beweisverwertungsverbote erreicht werden. Selbst wenn Zugriff auf digitale Assistenten gewährt wird, beantwortet dies noch nicht die Frage der Zulässigkeit der Beweisverwertung.

1. *Art. 141 Abs. 1 StPO: Absolute Verwertungsverbote*

Absolut unverwertbar sind Beweise, deren Nutzung die StPO explizit untersagt.[52] Eine entsprechende Regelung findet sich mit Blick auf die geheime Überwachung in Art. 277 StPO. Dort ist festgehalten, dass Dokumente oder Datenträger sofort zu vernichten sind, wenn sie aus nicht durch eine vom Zwangsmassnahmengericht genehmigte Überwachung gewonnen wurden. Die aus diesen Quellen stammenden Informationen sind von einer Verwertung im Strafverfahren ausgeschlossen.[53]

Der neue Art. 269ter StPO über besondere Informatikprogramme zur Überwachung des Fernmeldeverkehrs enthält ebenfalls ein gesetzliches Verwertungsverbot. Abs. 3 hält fest, dass alle Erkenntnisse, die beim Einsatz besonderer Informatikprogramme erlangt werden und nicht durch die Grundvoraussetzungen des Einsatzes – bspw. das Vorliegen eines dringenden Tatverdachts oder eines entsprechenden Katalogdelikts (Art. 269ter Abs. 1 lit. b i.V.m. Art. 286 Abs. 2 StPO) – gedeckt sind, nicht verwertet werden dürfen und zu vernichten sind.[54] Das genannte Verwertungsverbot wirkt sich jedoch nur auf Verletzungen dieser Grundvoraussetzungen aus, nicht aber etwa in Fällen, in denen die anordnende Behörde bspw. eine zu ungenaue Überwachungsanordnung gestellt hat, bspw. die gewünschten Datentypen oder Räumlichkeiten gem. Art. 269ter Abs. 2 StPO nicht korrekt benannt hat. Wie ist in solchen Fällen vorzugehen, damit verhindert werden kann, dass der Einsatz von GovWare zu einer *fishing expedition* wird?[55]

2. *Art. 141 Abs. 2 StPO: Relative Verwertungsverbote*

Unverwertbar sind ferner Beweise, welche die Strafbehörden unter Verletzung von Gültigkeitsvorschriften erheben, ausser die Verwertung ist zur Aufklärung schwerer Straftaten unerlässlich.[56] Eine Norm gilt als Gültigkeitsvorschrift, wenn sie zentrale Verfahrensinteressen des Beschuldigten schützt. Die Vorschriften über die Durchsuchung von Aufzeichnungen (Art. 246 ff. StPO) könnten als Gültigkeitsvorschriften, welche zentral den Interessen von Beschuldigten dienen, eingestuft werden, wenn etwa deren Beachtung bei der Durchsuchung der durch digitale Assistenten generierten Daten und deren Beschlagnahme zwingend für eine Zuverlässigkeitsgewähr oder eben für den Schutz der Privatsphäre wäre.[57] Allerdings anerkennt die Rechtsprechung bekanntlich Verfahrensvorgaben nur selten als Gültigkeitsvorschriften, die

[48] BSK StPO-*Vest/Horber*, Vor Art. 168–176 N 1 ff.

[49] Vgl. BSK StPO-*Vest/Horber*, Vor Art. 168–176 N 2; BSK StPO-*Bommer/Goldschmid*, Art. 264 N 7 ff.

[50] BSK StPO-*Bommer/Goldschmid*, Art. 264 N 7, 21 ff.

[51] Vgl. Pra *2007* Nr. 113, 762 (Tagebuch); BGer, 19.12.2006, 1P_519/2006 (GPS); BV-SGK2-Vest, Art. 32 N 42; BSK StPO-*Gless*, Art. 141 N 10; *Vest/Eicker*, AJP *2005* 888 f.

[52] *Pieth* (Fn. 27) 192 f.; BSK StPO-*Gless*, Art.141 N 46 ff.; CR CPP-*Bénédict/Treccani*, Art. 141 N 3 ff.

[53] BSK-*Jean-Richard-dit-Bressel*, Art. 277 N 3 ff.; *Pieth* (Fn. 27) 167.

[54] Zum dringenden Tatverdacht *Pieth* (Fn. 27) 141; BSK StPO-*Jean-Richard-dit-Bressel*, Art. 269 N 34 ff.

[55] Vgl. bspw. zur Rechtsfolge der Beweisunverwertbarkeit bei zu ungenauen Angaben bei der Durchsuchung von Wohnräumen BSK StPO-*Gfeller*, Art. 241 N 10 m.H. auf BGer 6B_628/2013 vom 26.6.2014.

[56] *Pieth* (Fn. 27) 191 ff.; BSK StPO-*Gless*, Art. 141 N 63 ff.; CR CPP-*Bénédict/Treccani*, Art. 141 N 8 ff.

[57] BSK StPO-*Gless*, Art. 141 N 79; zum Siegelbruch und der Qualifikation als Gültigkeitsvorschrift i.S.v. Art. 141 Abs. 2 StPO *Graf*, Aspekte der strafprozessualen Siegelung, AJP *2017* 265 f.

dann mit gleicher Konsequenz, wie ausdrückliche Verwertungsverbote, strikt die Möglichkeiten der Beweisführung einschränken.

3. *Zwischenergebnis*

Das Fehlen expliziter Grenzen für eine strafprozessuale Beweiserhebung mithilfe digitaler Assistenten bis in den privatesten Lebensbereich erscheint stossend, wenn man sich vor Augen führt, dass die Einbettung von Robotern in unsere Lebensumgebung nicht immer eine freiwillige Entscheidung ist und eine umfassende Überwachung geeignet wäre, die Balance von Interessensabwägungen im Strafverfahren empfindlich zu stören, die im Hinblick auf das Zusammenspiel einer effizienten Strafverfolgung und eines genügenden Schutzes der Privatsphäre ohnehin bereits durch Datensammlungen, die nie vergessen, bedroht wird. Ob hier allgemeinere Notanker, wie die Berufung auf ein faires Verfahren oder auf die Wahrung der Menschenwürde helfen,[58] erscheint zweifelhaft.[59]

C. Lösungsansätze für einen adäquaten Schutz der Privatsphäre

Die Frage, wie in einem Zeitalter digitaler Assistenz ein adäquater Schutz der Privatsphäre gewährleistet werden könnte, stellt sich nicht nur in der Schweiz, sondern in allen Staaten, in denen Menschen Informationstechnologie und Robotik nutzen. Insofern könnte sich ein Blick über die Grenzen lohnen. Denn obwohl die Schweiz bei der gesetzlichen Regelung von Beweisverboten eine Vorreiterrolle hat,[60] fehlt bislang ein Ansatz für eine inhaltliche Schranke zur Wahrung der Privatsphäre in Zeiten automatisierter Beweiserhebung.

1. *Schutz des Kernbereichs privater Lebensgestaltung: § 100d D-StPO*

Bei einem Schutz der innersten Intimsphäre vor strafrechtlichen Ermittlungen scheint Deutschland nun vorangehen zu wollen. Durch die Gesetzesänderung zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens[61] gilt dort mit § 100d D-StPO ein neues Beweiserhebungsverbot für den Fall, dass tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch eine Überwachungsmassnahme «*allein* Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden»[62]. In diesen Fällen soll eine Beweiserhebung von vorneherein unzulässig sein.

Der deutsche Gesetzgeber geht hier also sehr viel weiter als Art. 264 Abs. 1 lit b StPO, der auf eine Interessensabwägung im Einzelfall abstellt.[63] § 100d D-StPO definiert einen absoluten Schutzbereich. Das hört sich fortschrittlich an. Fraglich ist allerdings, wie dieses Beweiserhebungsverbot durchgesetzt werden soll, wenn für die Beweissammlung vorprogrammierte Algorithmen zuständig sind. Nach der einschlägigen deutschen Regelung ist «soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden.»[64] Das bedeutet: Wenn deutsche Strafverfolgungsbehörden den Zugang über das Gerät für eine Wohnraumüberwachung und dann den Zugang zum digitalen Assistenten für eine Online-Durchsuchung nutzen, dann muss vor Durchführung der Ermittlungsmassnahme feststehen, dass sie vermeiden können, dass sie *allein* Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangen. Das dürfte schwierig sein, da schon unklar ist, wie die Grenze der «*allein* dem Kernbereich privater Lebensgestaltung» angehörenden Informationen allenfalls algorithmisch bestimmt werden sollte.

Auch die Übertragbarkeit der deutschen Lösung auf die Schweiz wirft viele Fragen auf, schon weil der schweizerische Datenschutzgesetzgeber traditionell von einer weiträumigen Ausnahme für Strafverfolgung ausgegangen ist.[65] Der kategorische Ausschluss jeglicher strafprozessualer Ermittlungsmethoden von einer datenschutzrechtlichen Bewertung wird jedoch seit längerem infrage gestellt und gerade der Zugriff auf Haushaltsgeräte durch sog. «GovWare» präsentiert einen Fall, in dem es einer Prüfung der Anforderungen an die Informationssicherheit und besonderer Datenbearbeitungsrisiken für die Rechte und

[58] Art. 3 Abs. 2 lit. c und d StPO; Art. 7, 29 BV.

[59] Zur engen Definition der Menschenwürde vgl. BSK BV-*Belser/Molinari*, Art. 7 N 6 sowie BGE 132 I 49 E. 5.1.

[60] Zur Vorreiterrolle der Schweiz bei der gesetzlichen Regelung von Beweisverboten, vgl. *Gless*, Gesetzliche Regelungen von Beweisverwertungsverboten – die Schweiz als Vorreiter?, in: Gropp/Hecker/Kreuzer/Ringelmann/Witteck/Wolfslast (Hrsg.), Strafrecht als ultima ratio. Giessener Gedächtnisschrift für Günter Heine, Tübingen 2016, 127 ff.

[61] Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, v. 17.8.2017, Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 58 vom 23.8.2017.

[62] Hervorhebung durch Verf.

[63] BSK StPO-*Bommer/Goldschmid*, Art. 264 N 7, 46 ff.

[64] § 100d Abs. 3, 1 D-StPO, abrufbar unter <https://www.gesetze-im-internet.de/stpo/__100d.html>.

[65] Illustrativ dafür: Botschaft zum Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1, BBl *1988* 432.

Freiheit der betroffenen Personen bedarf, die ganz getrennt von jenen Interessenskonflikten sind, die sich traditionell im Strafverfahren finden.[66]

2. *Legality by Design?*

Vor diesem Hintergrund erschliesst sich die Forderung nach einer datenschutzrechtlichen Prüfung von GovWare,[67] unabhängig von der – durch Ermittlungsbehörden und Zwangsmassnahmengerichte im Einzelfall zu beantwortenden – Frage, ob und wann Spähsoftware eingesetzt werden soll und darf.

Der Weg über die Technik ist in der sog. «privacy by design»-Strategie vorgegeben.

Bereits in den 90er-Jahren forderten Datenschützer einen solchen Weg:[68] Elektronische Geräte sollen so gebaut werden, dass bereits technisch sichergestellt ist, dass im Betrieb generierte Daten keines oder kaum mehr eines gesetzlichen Schutzes bedürfen, bspw. weil von Beginn an möglichst wenig Daten generiert werden und diese nicht auf längere Zeit aufbewahrt werden.

In den Mitgliedstaaten der EU wird dies nun durch Art. 25 DSGVO[69] vorgegeben. Unter Berücksichtigung des Stands der Technik, der Kosten der Umstände und Zwecke der Verarbeitung soll künftig durch das Treffen dafür geeigneter technischer sowie organisatorischer Massnahmen ein möglichst umfassender Datenschutz gewährleistet werden. Dafür sorgen sollen etwa Datenminimierung oder Pseudonymisierung generierter Informationen sowie ein «Privacy by default»-Ansatz. Die Hersteller der heute im Trend liegenden Elektronik kommen zu einem Grossteil aus den USA oder dem europäischen Import, sodass die Regelung der DSGVO bereits indirekt eine Wirkung auf den Schutz von Daten in der Schweiz haben dürfte.

Ein Pendant im Schweizer Recht könnte (nach dem Vorschlag des Bundesrates) mit Art. 6 E-DSG geschaffen werden.[70] Entsprechend des Vorschlags sollen bestimmte Voreinstellungen der Technik dem Datenschutz Rechnung tragen. Ähnlich der DSGVO soll das Ziel auch in der Schweiz durch entsprechende technische und organisatorische Massnahmen eingehalten werden. Dies unter Berücksichtigung des Stands der Technik, von Art/Umfang der Datenbearbeitung sowie den Risiken, welche die Bearbeitung für die Persönlichkeit und Grundrechte der betroffenen Personen mit sich bringen.[71]

V. Fazit

Bereits heute – und zukünftig wohl immer mehr – nehmen digitale Assistenten am Privatleben der Menschen teil. Wenn es hier künftig Grenzen für Strafermittlungen geben soll, dann müssen diese mit Blick auf die Besonderheiten der Einbettung von digitalen Assistenten in die menschliche Lebensumgebung definiert und gesetzlich fixiert werden. Anders als bei herkömmlichen Massnahmen wie Telefonüberwachung oder GPS-Tracking geht es hier um intelligente Agenten, die in Wohnung, Fahrzeuge, Arbeitsplatz integriert werden oder aber in Form von «smarten Prothesen»[72] sogar mit dem menschlichen Körper verschmelzen können. Roboter durchdringen damit die Räume, die nach unserem traditionellen Verständnis der Entwicklung eines Familienlebens, einer Intimsphäre oder einer freien Meinungsäusserung dienen.[73] Wer hier nur auf die Selbstverantwortung des Einzelnen verweist, verkennt die Dynamik der Digitalisierung: Die Unterscheidung zwischen der freiwilligen Öffnung einer persönlichen Sphäre und einer Aufgabe dieser Privatsphäre durch Digitalisierung unter (staatlichem) Zwang ist fliessend und verschiebt sich laufend sowohl mit dem technischen Fortschritt wie auch den Bedürfnissen der Gesellschaft. Die Diskussionen rund um «Privacy by Design» sowie um das neue Datenschutzrecht führen vor Augen, dass das Recht die Technik nur in bestimmten Grenzen regulieren, die technische Vorsorge die Einhaltung bestimmter normativer Grenzen aber effizient bewirken dürfte.

---

66 Ausf. dazu: *Rudin*, Überholte Ausnahmen beim Geltungsbereich, digma *2016* 122 ff. m.w.N.

67 Vgl. dazu etwa Bericht der Geschäftsprüfungskommission (des Kantonsrates des Kantons Zürich) vom 19. Mai 2016 über die Beschaffung und den Einsatz von Government-Software im Kanton Zürich (KR-Nr. 166/2016), 9 ff., Kurz-URL: <http://bit.ly/2cWlg46>; Tätigkeitsbericht 2015 des Datenschutzbeauftragten des Kantons Zürich, 10 f., Kurz-URL: <http://bit. ly/2cF1SMs>.

68 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> (12.3.2018).

69 Europäische Datenschutz-Grundverordnung, in Kraft ab dem 25.5.2018.

70 Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (Entwurf), BBl *2017* 7193, 7209.

71 Art. 6 Abs. 1 und 2 E-DSG.

72 Siehe etwa «Hirn an Roboter: Bitte bewegen!», <https://www.ethz.ch/de/news-und-veranstaltungen/eth-news/news/2016/09/hirn-an-roboter-bitte-bewegen.html> (17.9.2016).

73 BSK BV-*Diggelmann*, Art. 13 N 25.