§ 6 Ausblick und Zusammenfassung

Smarte Haushaltsgeräte sind bereits heute mit stark zunehmender Tendenz verbreitet. Von den technischen Möglichkeiten ausgehend, können diese zu einer weitgehenden Überwachung der Bürger eingesetzt werden. Wie gezeigt können die durch Smart Speaker sowie die mit ihnen verbundenen Sprachassistenten generierten Daten in bestimmten Fällen bereits unter der aktuellen Rechtsordnung zur Strafverfolgung eingesetzt werden. Um diese Technologien für die Strafverfolgung nützlich zu machen, ist folglich nicht zwangsläufig eine neue Ermächtigungsgrundlage erforderlich. Da es lediglich eine Frage der Zeit ist, bis die bereits im Juni 2019 entbrannte Diskussion um den staatlichen Zugriff auf Smart Speaker erneut in das Zentrum der politischen Diskussionen rücken wird, versucht diese Arbeit sodann zu berücksichtigende Streitpunkte bereits aufzugreifen und einer möglichen Lösung zuzuführen. Nach der hier vertretenen Auffassung muss bei Suche nach einem tauglichen Gesetzesvorbehalt zwar konstatiert werden, dass die Interaktion mit einem Smart Speaker nicht unter einen strafprozessualen Telekommunikationsbegriff wie er in § 100a StPO zu fordern ist, subsumiert werden kann und darüber hinaus auch § 100a Abs. 1 S. 3 StPO aufgrund der festgestellten Verfassungswidrigkeit nicht als Ermächtigungsgrundlage in Betracht kommt. Die Online-Durchsuchung nach § 100b StPO stellt hingegen unter rechtlichen Gesichtspunkten einen gangbaren Weg dar, auf Smart Speaker zuzugreifen. Einem solchen Vorgehen steht jedoch – jedenfalls im Falle „datenloser" Smart Speaker – die praktische Hürde gegenüber, dass mangels gespeicherter Datenbestände auf diesen Endgeräten kein abschöpfbareres Material vorhanden ist. Entgegen vereinzelten Literaturauffassungen, die sich bereits mit den rechtlichen Möglichkeiten rund um Smart Speaker beschäftigten, ist es zulässig das Endgerät derart zu manipulieren, dass es gem. § 100c StPO als Wanze der Strafverfolgungsbehörden genutzt werden kann. Jedenfalls bei Smart-Speakern auf denen selbst keine Datenbestände gespeichert sind, ist dabei keine Kollision mit dem IT-Grundrecht zu befürchten und § 100c StPO auch vor diesem Hintergrund als taugliche Ermächtigungsgrundlage nicht zu beanstanden. Anders kann sich dies dann darstellen, wenn ein Sprachassistent als Wanze fungieren soll, der unmittelbar in ein Smartphone integriert ist und auf welchem eine Vielzahl an anderweitigen privaten Datenbeständen gespeichert sind. Sodann wäre es umso

bedeutender, ob die Software zur Manipulation des Sprachassistenten derart konfiguriert ist, dass lediglich laufende Gespräche überwacht werden können; die ruhenden Daten jedoch unangetastet bleiben. Daneben stehen den Ermittlungsbehörden auch offenen Ermittlungsbefugnisse zur Verfügung, die es ihnen beispielsweise erlauben sich Kenntnis der Zugangsdaten zum Account des Betroffenen zu verschaffen, um dort gespeicherte Daten zu sichten, § 110 Abs. 3 StPO, und gegebenenfalls beschlagnahmen zu können, § 94 StPO. Neben der Durchsuchung des Accounts über den Zugang des Betroffenen, kommt auch eine Durchsuchung des Serveraccounts beim Dienstleistungsanbieter in Betracht, die sich jedenfalls bei einer Kooperationsbereitschaft des Dienstleistungsanbieters ebenfalls nach § 102 StPO richten kann. Gleichwohl vergegenwärtigt die in dieser Arbeit enthaltene Diskussion um mögliche Ermächtigungsgrundlagen einschließlich der hierzu bestehenden unterschiedlichen Auslegungsmöglichkeiten eine de lege lata nicht gänzlich zu negierende Rechtsunsicherheit. Ob eine (extensive) Auslegung strafprozessualer Normen vor dem Hintergrund des damit zusammenhängenden Strafprozesses als des Rechtsstaates schärfstes Schwert im Sinne der Rechtssicherheit erstrebenswert ist, erscheint zumindest fraglich. Insofern könnte es angezeigt sein, dass sich der Gesetzgeber umfassend mit den zukünftig durch Smart-Home-Technologien im Allgemeinen aufkommenden rechtlichen Herausforderungen für das Strafverfahren auseinandersetzt und sodann möglicherweise eine exakt hierauf abgestimmte einheitliche Ermächtigungsgrundlage kodifiziert. Dies vor allem vor dem Hintergrund, dass die hier gegenständlichen Smart Speaker nur einen Teil der sprach- oder gestengesteuerten Smart-Home-Technologien abbilden. Beispielswiese ist auch an via Gestensteuerung gesteuerte Geräte zu denken, anhand derer Aktivierung beispielsweise auf die Anwesenheit einer Person, zu einer bestimmten Uhrzeit, an einem bestimmten Ort geschlossen werden soll.

Neben der Frage nach den Zugriffsmöglichkeiten, dürfen die mit der Existenz von Smart Speakern und einem Zugriff auf hierüber generierte Daten wieder in den Fokus rückenden Streitpunkte im Rahmen der Verwertbarkeit nicht außer Acht gelassen werden. Allein der Umstand, dass in diesem Bereich viele Punkte seit Jahren in Rechtsprechung und Literatur umstritten sind, zeigt die Notwendigkeit einer fortlaufenden kritischen Würdigung, um die verwertbarkeitsfreundliche Haltung der Rechtsprechung nicht ohne Weiteres hinzunehmen. Abermals soll hier auf zwei zentrale Punkte des § 5 dieser Arbeit verdeutlichend hingewiesen werden: In einer zunehmend digitalisierten Welt, in der der Bürger mehr und mehr gläsern wirkt, erscheint es umso wichtiger, diesem eine Sphä-

re zuzugestehen, in der er ausschließlich für sich sein kann. Jedenfalls bei Selbstgesprächen muss das staatliche Strafverfolgungsinteresse dabei uneingeschränkt zurückstehen. Darüber hinaus kann eine Existenz in sozialen Bezügen nur dann möglich sein, wenn auch für qualifizierte Zwiegespräche mit einem beichtenden / reflektierenden Charakter eine strikte Zuordnung zum unverwertbaren Kernbereich erfolgt. Die Abwägungslösung ist zur Begründung eines unselbstständigen Beweisverwertungsverbotes trotz ihrer vermeintlichen Einzelfallgerechtigkeit kritisch zu sehen. In diese – überspitzt formuliert „Verwertbarkeitslösung" – sollten Schutzzweckgesichtspunkte einen erheblich größeren Einfluss erhalten, wenn schon von der Abwägungsdoktrin ein Abrücken nicht zu erwarten ist. Zu überdenken ist auch der Umgang mit durch Privatpersonen generierten Beweismitteln. Da gerade Dritte durch die fortschreitende Digitalisierung den Alltag der Bürger mehr und mehr prägen und möglicherweise gar informationstechnisch beherrschen, muss deren Verhalten auch im Hinblick auf die Verwertung solcher Informationen im Strafprozess klare, bestimmbare und rechtssichere Grenzen gegenüberstehen. Keine Lösung stellt es in diesem Zusammenhang dar, den Betroffenen auf seine alleinige Verantwortung in diesem Zusammenhang hinzuweisen und ihn gewissermaßen mittelbar aufzufordern sich der fortschreitenden Digitalisierung zu verwehren. Der Rekurs auf das durch das StGB als strafbar normierte Verhalten, kann eine deutliche Grenze darstellen anhand derer festzustellen ist, ob der durch den Privaten begangenen Rechtsverstoß derart gravierend ist, dass das in diesem Rechtsverstoß wurzelnde Unrecht nicht im hoheitlichen Verwertungsakt fortwirken darf. So sehr die effektive Strafverfolgung als gewichtiges Ziel zur Wahrung der Verfassung anzuerkennen ist, so sehr dürfen jedoch auch nicht die Rechte jedes Einzelnen (Straftäters) diesem scheinbar übergeordneten Ziel zum Opfer fallen. Es ist gerade dieser Spagat zwischen einer effektiven Strafverfolgung und der fraglichen Rechtfertigung des damit zusammenhängenden Eingriffs in die Grundrechte des Betroffenen, der die Rechtsprechung und Literatur auch in den kommenden Jahrzehnten permanent beschäftigen wird. Angesichts der stetig zunehmenden Möglichkeiten des Staates sich auch über vernetzte Geräte – wie Smart Speaker mitsamt den hiermit verknüpften Sprachassistenten – Informationen zu beschaffen, ist eine kritische Auseinandersetzung mit der Verwertbarkeit solcher Informationen von umso größerer Bedeutung. Diesen Spagat (zu) einseitig zugunsten der effektiven Strafverfolgung zu lösen, mag rechtspolitisch zuweilen sinnvoll erscheinen, kann jedoch nicht über die rechtsdogmatischen Unbehaglichkeiten eines solchen Vorgehens hinweghelfen.