Die Sicherstellung und Auswertung des Smartphones – Kriminalpolitischer Anpassungsbedarf?

von Polizeirat Stephan Ludewig[*]

Abstract
Zu Beginn der 1980er Jahre war es erstmals möglich ein Mobiltelefon auf dem freien Markt zu erwerben.[1] Durch technische Innovationen entwickelte sich das Mobiltelefon im Verlauf der folgenden Jahrzehnte zu dem zentralen Kommunikations- und Computergerät im Leben moderner Menschen und stellt für viele Nutzer heute den wichtigste Datenspeicher dar.[2] Im Rahmen ihrer Sicherstellung und Auswertung steht die Digitale Forensik vor einigen rechtlichen und technischen Herausforderungen. Der Beitrag beschäftigt sich mit einem möglichen rechtlichen Anpassungsbedarf der Ermächtigungsgrundlagen zur Erlangung elektronischer Beweismittel.

At the beginning of the 1980s it was possible for the first time to purchase a mobile phone on the open market. Through technical innovations, the mobile phone developed over the following decades into the central communication and computer device in the lives of modern people and today represents the most important data storage device for many users. Digital forensics faces a number of legal and technical challenges as part of its seizures and evaluation. The article deals with a possible legal need to adapt the bases of authorization for obtaining electronic evidence.

I. Einleitung

Nach einer Studie des Branchenverbandes *Bitkom* besaßen im Jahr 2018 acht von zehn Deutschen ein Smartphone, was einer Gesamtzahl von ca. 57 Millionen Nutzern entspricht.[3] Auf ihm lassen sich E-Mails, Adressen, Telefonnummern speichern und es enthält darüber hinaus den Terminkalender, sämtliche, zum Teil sehr intime, Kommunikationsdaten und Bilder sowie ggf. eine Historie besuchter Orte. Schon durch die Verknüpfung von wenigen dieser Informationen lässt sich ein detailliertes Nutzungs- und ggf. Persönlichkeitsprofil seines Besitzers erstellen.[4] Dies konnte jüngst im Mordprozess an der Freiburger Studentin *Maria L.*[5] beobachtet werden. Im Ermittlungsverfahren wurde das Smartphone des Angeklagten Hussein K., ein iPhone 6S, von den Ermittlern zunächst mit Hilfe eines externen Dienstleisters entsperrt und die Daten anschließend aus dem Gerät extrahiert. Insbesondere in den tiefen Dateistrukturen des Gerätes konnten umfassende Daten, wie der Gerätestandort zu bestimmten Zeitpunkten, die Standorte registrierter WLAN sowie die Daten aus einer sog. Fitness App, extrahiert werden. Aus dem Datenbestand ergab sich eine Indizienkette, die es ermöglichte, dass Tatgeschehen umfassend zu rekonstruieren.[6]

Elektronische Beweismittel erlangen nicht zuletzt Aufgrund der ubiquitären Verfügbarkeit[7] von Datenverarbeitungssystemen (DV-Systemen) für Strafverfolgungsbehörden immer größere Bedeutung. Gleichzeitig stellt dieser Bedeutungszuwachs die Strafverfolgungsbehörden und die Strafgerichte vor neue Herausforderungen und wirft sowohl mit Blick auf rechtliche Vorgaben als auch in technischer Hinsicht eine Vielzahl von Fragen auf.[8] Insbesondere im Bereich der Digitalen Forensik ist aufgrund des schnellen Fortschritts im Bereich der IT, z. T. fraglich auf welcher gesetzlichen Grundlage die Gewinnung dieser Beweismittel erfolgen kann, ob die gültigen gesetzlichen Bestimmungen auch den Bereich der Digitalen Forensik abdecken oder ob sich ggf. Anpassungsbedarf ergibt.[9] Die aktuellen Diskussionen bzgl. der Sicherstellung und Auswertung von Smartphones reichen dabei von der Auffassung, Mobiltelefone auch zum Beweis einer vergleichsweise niedrigschwelligen Verkehrsordnungswidrigkeit auslesen zu dürfen[10] bis hin zur Verortung derartiger Maßnahmen in der Nähe der „Online Durchsuchung“ und dem sich daraus ergebenden Anpassungsbedarf bestehender Vorschriften.[11]

---

* Der *Verfasser* ist derzeit in der Polizeidirektion Thüringen eingesetzt.

1 Das erste Mobiltelefon konnte im Jahr 1983 für den Preis von 3.995 USD auf dem freien Markt erworben werden wobei der Funktionsumfang des Gerätes nur in der Möglichkeit bestand Ortsunabhängige Gespräche zu führen. Vgl. https://praxistipps.chip.de/seit-wann-gibt-es-handys-entwicklung-im-zeitverlauf_101085 (zuletzt abgerufen am 26.7.2019).

2 Vgl. *Lane/Miluzzo/Lu/Peebles/Choudhury/Campbell,* in: IEEE Commun. Mag. 2010, 140.

3 Vgl. *Bitkom,* Smartphone-Markt wächst um 3 Prozent auf 34 Milliarden Euro, abrufbar unter: https://www.bitkom.org/Presse/Presseinformation/Smartphone-Markt-waechst-um-3-Prozent-auf-34-Milliarden-Euro (zuletzt abgerufen am 29.7.2019).

4 Vgl. *Spehr,* Jeder Schritt zählt , abrufbar unter: https://www.faz.net/aktuell/technik-motor/digital/datenschutz-und-privatsphaere-jeder-schritt-zaehlt-14494871.html?printPagedArticle=true#pageIndex_0 (zuletzt abgerufen am 29.7.2019).

5 *LG Freiburg*, Urt. v. 22.3.2018 – 6 KLs 101 Js 37818/16 – Ak 4/17 jug.

6 Vgl. *Buchheim,* Mordfall Maria L., abrufbar unter: http://www.badische-zeitung.de/freiburg/cybercrime-firma-hackte-fuer-die-polizei-hussein-k-s-handy--147897230.html (zuletzt abgerufen am 29.7.2019).

7 Vgl. BVerfGE 120, 274 (305).

8 Vgl. *Warken,* NZWiSt 2017, 289.

9 Vgl. *Czerner,* in: Labudde/Spranger, Forensik in der digitalen Welt, S. 265.

10 *Ternig/Lellmann,* NZV 2016, 454.

11 *Momsen,* DRiZ, 2018, 140; *Peters,* NZWiSt 2017, 465; *Wenzel,* NZWiSt 2016, 85.

II. Funktionsumfang moderner Smartphones

Smartphones sind technische Einheiten, die über Netzwerke mit anderen Einheiten verbunden sind und untereinander über einen stetigen Datenaustausch kommunizieren. Dabei werden permanent Daten erzeugt, gespeichert oder gesendet, was zu einer nie dagewesenen Masse an Daten führt, welche in der Gesamtschau noch nie so aussagekräftig waren.[12] Trotz einer Vielzahl weiterer Funktionen sind Smartphones in erster Linie Telekommunikationsgeräte. Mit ihnen lassen sich mobile Telefonate führen oder Kurzmitteilungen versenden. Die Daten hierzu werden, je nach Nutzerverhalten und Gerätekonfiguration, kurzfristig oder dauerhaft im Smartphone gespeichert.[13] Obwohl nicht speziell dafür entwickelt, können Smartphones als anspruchsvolle Sensoren fungieren. Eingebaute Kameras dienen als Video- und Bildsensoren. Das Mikrofon dient, wenn nicht für Telefonate verwendet, als akustischer Sensor. Die integrierten GPS-Empfänger erzeugen metergenaue Standortinformationen. Andere Sensoren wie Gyroskope, Beschleunigungs- und Näherungssensoren können gemeinsam verwendet werden, um Kontextinformationen zu ermitteln[14]. Externe Sensoren können über Bluetooth oder drahtgebundene Verbindungen, einfach mit dem Telefon verbunden werden.[15] Die Vielzahl der Sensoren ermöglicht u. a. die Verfolgung von Echtzeitaktivitäten oder die Überwachung von Vitalfunktionen.[16]

Die hohe Verfügbarkeit von Smartphones und die Möglichkeit der Vernetzung mit Alltagsgeräten macht das Smartphone auch zur Steuerungszentrale für Wearables. Vier von zehn Befragten gaben im Rahmen einer *Bitkom*-Studie an, ihr Smartphone schon einmal mit einem Wearable, wie einer Smartwatch oder einem Fitnessarmband, vernetzt zu haben.[17] Die dort erlangten Daten werden an das gekoppelte Smartphones gesendet, zum Teil gespeichert oder an Dienstanbieter übertragen.[18]

Die fortschreitende Verbesserung der Smartphones führte zu immer größeren Kapazitäten der verbauten bzw. erweiterbaren Datenspeichern. Die Speichergrößen aktuell angebotener Mobiltelefone reichen dabei von 8 bis 512 GB, wobei der ganz überwiegende Teil der Geräte Speichergrößen jenseits von 64 GB aufweist.[19] Smartphones kommen damit als mobile Datenträger ebenso in Betracht wie Laptops oder sonstige Speichermedien.[20] Die Geräte nutzen sog. Flash-Speicher, welche ggü. optischen oder magnetischen Datenträgern eine Besonderheit aufweisen. Eine Löschung der Daten findet bei diesen Speichern erst nach dem Überschreiben mit neuen Informationen statt, was eine Rekonstruktion gelöschter Daten oft möglich macht.[21] Mit der SIM-Karte[22] befindet sich ein weiterer relevanter Datenspeicher in Mobiltelefonen. Trotz bedeutend kleinerer Speicherkapazität, im Vergleich zum Gerätespeicher, werden auch heute noch Kontakt- und Anruflisten sowie Kurzmitteilungen auf SIM-Karten gespeichert.[23]

Während des laufenden Betriebes verarbeitet und speichert ein Smartphone ständig Nutzerdaten. Dies geschieht durch das Betriebssystem selbst oder durch Programme von Drittanbietern, sog. „Apps".[24] Das Betriebssystem Android bspw. ermittelt selbst dann fortwährend den Standort eines Smartphones, wenn der Nutzer annimmt, diese Funktion deaktiviert zu haben. Hierzu werden neben GPS-Daten auch WLAN und Bluetooth Informationen verwendet.[25]

Eine App kann alle Daten innerhalb des laufenden Programms verarbeiten und speichern. Hierzu zählen z. B. Starten und Beenden der App, Nutzungsdaten, Inhaltsdaten von Messangerdiensten wie WhatsApp oder mit Email-Clients empfangene Emails. Teilweise werden diese Daten zur Protokollierung über das Internet versendet.[26] Auch bei der Nutzung von Cloud-Diensten wie Dropbox, iCloud oder OneDrive werden, z. T. vom Nutzer unbemerkt und ungewollt, Daten auf anderen Geräten gespeichert bzw. mit anderen Nutzern geteilt.[27]

III. Bedeutung für das Ermittlungsverfahren

Für die Strafverfolgungsbehörden erlangen digitale Beweismittel und die Auswertung digitaler Kommunikationsinhalte immer größere Bedeutung.[28] Neben auswertbaren Computersystemen, hat sich das Smartphone zu einem wesentlichen Element der strafprozessualen Ermittlungen

---

12 Vgl. *Blechschmidt,* MMR 2018, 361.

13 Vgl. *Singelnstein,* NStZ 2012, 593 (598); *Rogge,* Der Kriminalist 2015, 29.

14 So z. B. ob und wann ein Benutzer zu Fuß, auf dem Fahrrad oder in einem Kfz unterwegs ist.

15 Vgl. *Christin/Reinhardt/Kanhere/Hollick,* The Journal of Systems and Software, 2011, 1928.

16 Vgl. *Lane/Miluzzo/Lu/Peebles/Choudhury/Campbell,* in: IEEE Commun. Mag. 2010, 140.

17 Vgl. *Bitkom,* Smartphone-Markt wächst um 3 Prozent auf 34 Milliarden Euro (Fn. 3).

18 Vgl. *Federrath,* in: Heinrich-Böll-Stiftung Sachsen/Lichdi, Digitale Schwellen, 2015, S. 57.

19 Vgl. aktuelle Chip Bestenliste unter https://www.chip.de/bestenlisten/Bestenliste-Handys--index/detail/id/900/#wrapper-ext (zuletzt abgerufen am 29.7.2019).

20 Unter Speichermedien sind hier externe Festplatten, USB-Sticks, CDS, DVDS und SD-Karten zu verstehen. Vgl. *Warken,* NZWiSt 2017, 289 (294).

21 In Einzelfällen ist es jedoch möglich auch diese Daten, durch aufwändige Verfahren, zu rekonstruieren. Vgl. *Rogge,* Der Kriminalist 2015, 29 (31 f.).

22 SIM steht für *Subscriber Identification Module.* Die Karte ist in europäischen Mobilfunknetzen erforderlich, um ein Mobiltelefon innerhalb des Netzes nutzen zu können. Vgl. https://wirtschaftslexikon.gabler.de/definition/sim-karte-52650/version-275768 (zuletzt abgerufen am 29.7.2019).

23 Vgl. *Rogge,* Der Kriminalist 2015, 29 (31 f.).

24 Der Begriff App ist eine Kurzform des englischen Begriffs *Application* was übersetzt Anwendung bedeutet und individuell installierbare Programme auf Smartphones bezeichnet. Vgl. *Federrath,* in: Heinrich-Böll-Stiftung Sachsen/Lichdi, Digitale Schwellen, S. 57.

25 Vgl. *Spehr,* Jeder Schritt zählt (Fn. 4).

26 Vgl. *Federrath,* in: Heinrich-Böll-Stiftung Sachsen/Lichdi, Digitale Schwellen, S. 58 f.

27 Vgl. a. a. O., S. 57.

28 Vgl. *Blechschmidt,* MMR 2018, 361 (363). Vgl. auch *Rogge,* Der Kriminalist 2015, 29.

entwickelt.[29] Daten wie E-Mails, Chatverläufe, Fotos oder Dokumente, aber auch der Verlauf besuchter Internetseiten geben in vielen Fällen Aufschluss über Tat und Täter. Daneben ermöglicht das Smartphone häufig den ungehinderten Zugriff auf die extern in einer Cloud gespeicherten Daten des Nutzers.[30] Das Smartphone wird als Tatmittel zum Aufzeichnen und Verbreiten von Videos oder Bildern mit strafrechtlich relevantem Inhalt genutzt.[31] Die gespeicherten (App-)Daten geben Ermittlungsbehörden Einblicke in Schlafphasen, Bewegungsaktivitäten oder den Standort des Gerätes. Es existiert kaum ein vergleichbares Objekt, dessen Auswertung in solchem Umfang Informationen über den Nutzer des Smartphones, sowie zu sozialen Kontakten, seinem Verhalten und möglicherweise auch Gedanken ermöglicht.[32] Draus kann, je nach Umfang und Inhalt der gewonnen Daten, ein sehr intensiver Eingriff in die Grundrechte des Betroffenen resultieren.[33]

IV. Grundrechtseingriff

Bei einem staatlichen Zugriff auf die Daten eines Smartphones können, aufgrund der Verschiedenartigkeit dieser Daten, unterschiedliche Grundrechte betroffen sein. Hierzu gehören das, insbesondere bei elektronischen Beweismitteln zum Tragen kommende, Recht auf Informationelle Selbstbestimmung (RiS) gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, sowie das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG.[34] Bei gegenständlicher Beschlagnahme eines Smartphones sowie bei einem Zugriff auf Daten, die bei einem IT-Dienstleister gespeichert sind, kommt weiterhin das Grundrecht auf Eigentum gem. Art. 14 GG in Betracht.[35] Sofern auf Kommunikationsdaten zugegriffen wird, sind ebenso die Grundrechte des jeweiligen Kommunikationspartners betroffen.[36] Die allgemeinen Verfahrensgrundrechte und -prinzipien, wie die Unschuldsvermutung, das Recht auf ein faires Verfahren und der Verhältnismäßigkeitsgrundsatz gelten selbstverständlich auch für die Erlangung und Verwertung elektronischer Beweismittel aus einem Smartphone.[37]

1. Das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG

Schon 1983 erkannten die Richter des *BVerfG* im sog. Volkszählungsurteil, dass es bei bestehenden und vor allem zukünftigen Bedingungen der automatischen elektronischen Datenverarbeitung (DV), in besonderem Maße des Schutzes personenbezogener Daten bedarf. Moderne DV-Systeme können Angaben über persönliche oder sachliche Verhältnisse einer Person praktisch unbegrenzt speichern und damit jederzeit verfügbar machen. Auswertung, Abgleich und Vernetzung dieser Daten kann zu einem vollständigen Persönlichkeitsprofil, mithin zu einem „gläsernen Menschen“ führen.[38] Diese Gefahr besteht insbesondere beim Zugriff auf Kommunikationsinhalte wie sie in Smartphones gespeichert sein können.[39] Die Richter begegneten dieser Gefahr mit der Anerkennung des RiS, dessen Schutzbereich durch die Befugnis des Einzelnen gekennzeichnet ist, grds. selbst über die Offenbarung persönlicher Lebenssachverhalte zu entscheiden.[40] Das RiS schützt damit den Einzelnen gegen informationsbezogene Maßnahmen, die für ihn weder überschaubar noch beherrschbar sind, was insbesondere dann der Fall ist, wenn Datenbestände für eine Vielzahl von Zwecken genutzt oder miteinander verknüpft werden können.[41] Eingriffe in das RiS werden damit rechtfertigungsbedürftig, wobei sich diese Rechtfertigung nur aus einem formellen Gesetz ergeben kann.[42] Als Auffangtatbestand umfasst das RiS alle Eingriffe, die auf Datenerhebung gerichtet sind, sofern diese nicht dem Schutzbereich speziellerer Grundrechte, wie z. B dem Fernmeldegeheimnis aus Art. 10 Abs. 1 GG unterfallen.[43] In Abgrenzung zum ebenfalls dem allgemeinen Persönlichkeitsrecht zuzuordnenden Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[44], umfasst der Schutzbereich des RiS jedoch nur offene und punktuelle Eingriffe im Rahmen der Datenerhebung.[45]

Das *BVerfG* präzisierte die Schranke des Art. 2 Abs. 1 GG im Hinblick auf die Grundsätze der Bestimmtheit und der Normenklarheit. Gesetzliche Regelungen, die einen Eingriff in das RiS legitimieren, müssen Anlass, Zweck und Grenzen eines Eingriffs bereichsspezifisch, präzise und normenklar festlegen. Der Betroffene muss die Rechtslage jederzeit erkennen und sich auf mögliche belastende Maßnahmen einstellen können. Die Verwendung unbestimmter Rechtsbegriffe darf nicht zu Ungewissheiten führen, welche die Vorhersehbarkeit und Justitiabilität des staatlichen Handelns gefährdet.[46] Weiterhin besteht das Gebot für die Legislative, die Eigenschaften moderner DV-Systeme und die sich daraus ergebenden Nutzungsmöglichkeiten zu beobachten, um gegebenenfalls eine Anpassung der rechtlichen Rahmenbedingungen zu initiieren.[47]

---

29 Vgl. Wenzel, NZWiSt 2016, 85 (88); So wurden im Rahmen eines Prozesses wegen des Verdachts der Unterstützung einer Terroristischen Vereinigung 9.000 Bilder auf einem einzigen Smartphone des Verdächtigen gesichert von denen eine Vielzahl Bezüge zum Islamischen Staat aufwies. Vgl. *BGH*, Beschl. v. 17.8.2017 – AK 34/17 = StraFo 2017, 470.

30 Vgl. *Momsen,* DRiZ 2018, 140.

31 Vgl. *Rogge,* Der Kriminalist 2015, 29.

32 Vgl. *Momsen,* DRiZ 2018, 140 (143).

33 Vgl. *Singelnstein,* NStZ 2012, 593 (598).

34 Vgl. *Warken,* NZWiSt 2017, 289 (292); *Singelnstein,* NStZ 2012, 593 (602).

35 Vgl. *Warken,* NZWiSt 2017, 289(293), die darauf verweist, dass in diesen Fällen auch das Eigentumsrecht des IT-Dienstleisters betroffen ist.

36 Vgl. ebd.

37 Vgl. *Warken,* NZWiSt 2017, 289(291).

38 Vgl. BVerfGE 65, 1 (42 f.).

39 Vgl. BVerfGE 124, 43 (63).; *Peters,* NZWiSt 2017, 465 (466).

40 Vgl. BVerfGE 65, 1; *Franzius,* ZJS 2015, 260; *Warken,* NZWiSt 2017, 289(292).

41 Vgl. BVerfGE 118, 168 (187).

42 Vgl. BVerfGE 65, 1; *Münch/Kunig*, GG, 6. Aufl. (2012), Art. 2 Rn. 38, 41.

43 Vgl. BVerfGE 115, 166 (187 ff.); *Singelnstein,* NStZ 2012, 593 (594); *Warken,* NZWiSt 2017, 289 (292).

44 Zur Entstehung dieses Grundrechts durch die Rechtsprechung des *BVerfG* vgl. BVerfGE 120, 274 (308 ff.).

45 Vgl. *Franzius,* ZJS 2015, 260 (262); *Singelnstein,* NStZ 2012, 593 (602).

46 Vgl. BVerfGE 120, 274 (316).

47 Vgl. BVerfGE 113, 29 (58).

2. Das Telekommunikationsgeheimnis gem. Art. 10 Abs. 1 GG

Das Telekommunikationsgeheimnis gem. Art. 10 Abs. 1 GG ist im Zusammenhang mit der Sicherung und Auswertung elektronischer Beweismittel ebenfalls von Bedeutung.[48] Es soll die Vertraulichkeit der individuellen Kommunikation zwischen Menschen schützen. Von Relevanz ist dies insbesondere, wenn räumliche Distanz die Nutzung von Telekommunikationsmedien bzw. -anbietern erforderlich macht, was die Gefahr eines Zugriffs Dritter auf die Kommunikationsdaten birgt.[49] Das Grundrecht schützt die freie Entfaltung der Persönlichkeit durch Kommunikation unter Nutzung von Telekommunikationsmitteln, unabhängig von der Art der übermittelten Inhalte und umfasst auch die Kommunikationsumstände wie z. B. Ort, Zeitpunkt, Dauer oder Beteiligte eines Kommunikationsvorgangs.[50] Bei der Nutzung eines Smartphones fällt eine Vielzahl dieser Daten an, die gespeichert und ggf. ausgewertet werden können. Das lässt Rückschlüsse auf das Kommunikations- und Bewegungsverhalten sowie ggf. auf das Vorhandensein von Beziehungen zwischen den Kommunikationsteilnehmern und deren Intensität zu.[51] Der Schutzbereich umfasst jedoch nur die laufende Kommunikation und endet sobald die Information endgültig beim jeweiligen Empfänger angekommen und der Übertragungsvorgang beendet ist.[52]

Nicht geschützt sind damit Daten, die nach Ende des Übertragungsvorgangs auf einem DV-Gerät im Herrschaftsbereich des Empfängers gespeichert werden. Diese unterfallen dem subsidiären Schutz des RiS.[53] Anruflisten, SMS, Browserverläufe, E-Mails etc., die auf dem Smartphone gespeichert sind, werden daher nicht von Art. 10 Abs. 1 GG erfasst.[54] Ausgenommen hiervon sind E-Mails, die auf zugangsgesicherten Mailservern eines Providers (zwischen)gespeichert sind und vom Empfänger noch nicht abgerufen wurden.[55]

V. Eingriffsermächtigung

Im vorgenannten Rahmen stehen den Ermittlungsbehörden auf Grundlage der Strafprozessordnung verschiedene Möglichkeiten zur Sicherung und Auswertung digitaler Spuren in Smartphones zur Verfügung. Als offene und punktuelle Maßnahme, sind hierzu insbesondere die §§ 94 ff. und § 110 StPO einschlägig.[56]

Mit Inkrafttreten der StPO im Jahr 1877 hatte sicher noch niemand auf Smartphones gespeicherte Daten im Blick, denen es am Merkmal der Körperlichkeit fehlt. Dennoch sind diese Normen, wie im Falle des § 94 StPO, seit über 100 Jahren beinahe unverändert.[57] Die Rechtsprechung des *BVerfG* hat mehrfach betont, dass Grundrechte, besonders im Hinblick auf sich ständig verändernde Möglichkeiten moderner DV-Systeme, entwicklungsoffen zu interpretieren sind.[58] Dies wirkt gleichzeitig auch auf die StPO als Eingriffsbefugnis, woraus folgt, dass auch diese Befugnisse, einer fortschrittlichen Auslegung zugänglich sind.[59] Obwohl das *BVerfG* die Sicherstellung von Emails auf Grundlage des § 94 StPO grds. für zulässig erachtet[60], eröffnet die bloße Auslegung historischer, für eine analoge Welt geschaffene Normen im modernen, digitalen Kontext, anstelle gesetzgeberischer Anpassungen jedoch Unsicherheitszonen. Dies birgt die Gefahr unterschiedlicher gerichtlicher Entscheidungen, sodass insbesondere die vom *BVerfG* geforderte Normenklarheit fehlt.

1. Sicherstellung und Beschlagnahme von Gegenständen gem. § 94 StPO

§ 94 StPO regelt die Sicherstellung von Gegenständen die als Beweismittel in Betracht kommen sowie die Beschlagnahme derselben, sofern diese nicht freiwillig herausgegeben werden.[61] Für eine Beschlagnahme ohne vorherige gerichtliche Anordnung, ist die Einholung einer richterlichen Bestätigung gem. § 98 Abs. 2 StPO obligatorisch.

Der im Wortlaut der Norm verwendeten Begriff „Gegenstände“, wird in der StPO nicht näher beschrieben. Er wird daher in der Rechtsprechung und dem Schrifttum unterschiedlich interpretiert.[62] Unstreitig ist, dass Smartphones körperliche Gegenstände sind, was sie zu tauglichen Objekten der Beschlagnahme macht.[63] Streitig ist indes, ob auch gespeicherte (Kommunikations-)Daten diesem Gegenstandsbegriff unterfallen. Während das *BVerfG* und Teile der Literatur[64] die Möglichkeit sehen auch gespeicherte Daten selbst zu beschlagnahmen, wird dies von anderen Autoren als Überdehnung der Wortlautgrenze abgelehnt.[65]

---

48 Vgl. *Warken,* NZWiSt 2017, 289 (292) unter Verweis auf *BVerfG*, Nichtannahmebeschl. v. 13.11.2010 – 2 BvR 1124/10 = WM 2011, 211.

49 Vgl. *Burghart,* in: Leibholz/Rinck, GG, 2018, Art. 10 Rn. 1.

50 Vgl. BVerfGE 67, 157 (172); 85, 386 (396); 115, 166 (183); 120, 274 (307). *Burghart,* in: Leibholz/Rinck, GG, Art. 10 Rn. 31; *Wenzel,* NZWiSt 2016, 85 (89).

51 Vgl. BVerfGE 115, 166 (183); *Burghart,* in: Leibholz/Rinck, GG, Art. 10 Rn. 31.

52 Vgl. BVerfGE 124, 43 (54); *Warken,* NZWiSt 2017, 289 (292).

53 BVerfGE 115, 166.

54 Vgl. *Wenzel,* NZWiSt 2016, 85 (89).

55 Vgl. BVerfGE 124, 43 (54 f.); *Burghart,* in: Leibholz/Rinck, GG, Art. 10, Rn. 31.

56 Vgl. *Blechschmidt,* MMR 2018, 361 (363); *Wenzel,* NZWiSt 2016, 85.

57 Vgl. *Menges,* in: LR-StPO, 27. Aufl. (2019), § 94 Entstehungsgeschichte; *Ruppert,* Jura 2018, 994.

58 Vgl. BVerfGE 106, 28 (36); 115, 166 (182); 120, 274 (307); 46, 120 (144).

59 Vgl. *Ruppert,* Jura 2018, 994.

60 Vgl. BVerfGE 124, 43 (58 f.).

61 Vgl. *Hartmann/Schmidt,* Strafprozessrecht, 5. Aufl. (2015), Rn. 416.

62 Vgl. *Bär,* Handbuch zur EDV-Beweissicherung, Bd. 13, 2007, Rn. 406.

63 Vgl. *Gercke,* in: HK-StPO, 6. Aufl. (2019), § 94 Rn. 17; *Menges,* in: LR-StPO, § 94 Rn. 11; *Bär,* Handbuch zur EDV-Beweissicherung, Rn. 405; *Hartmann/Schmidt,* Strafprozessrecht, Rn. 418; *Blechschmidt,* MMR 2018, 361 (364).

64 Vgl. BVerfGE 113, 29 (50); *BVerfG*, Nichtannahmebeschl. v. 25.7.2007 – 2 BvR 2282/06 2007 (Rn. 12), wodurch das *BVerfG* der Forderung nach einer fortschrittlichen Normauslegung nachkommt. Vgl. weiter *Hartmann/Schmidt,* Strafprozessrecht, Rn. 418; *Park,* Durchsuchung und Beschlagnahme, 4. Aufl. (2018), Rn. 804; *Blechschmidt,* MMR 2018, 361 (364).

65 Vgl. *Gercke,* in: HK-StPO, § 94 Rn. 18; *Roxin/Schünemann,* Strafverfahrensrecht, 28. Aufl. (2014), § 34 Rn. 4; *Cornelius,* in: Münchner Anwaltshandbuch IT-Recht, 3. Aufl. (2013), Teil 10 Rn. 465; *Bär,* Handbuch zur EDV-Beweissicherung, Rn. 407.

a) Voraussetzung der Beschlagnahme

Voraussetzung für die Beschlagnahme ist die potentielle Beweisbedeutung des Smartphones bzw. der darauf gespeicherten Daten, weshalb zunächst der Anfangsverdacht einer Straftat gem. § 152 Abs. 2 StPO vorliegen muss.[66] Damit ist ein Zugriff auf den umfassenden und teilw. sensiblen Datenbestand eines Smartphones unter den „[...]denkbar geringsten Voraussetzungen möglich[...]"[67]. Weiterhin müssen die Daten auf dem Smartphone für das Straf- bzw. Ermittlungsverfahren von Bedeutung sein. D.h., sie müssen mittelbar oder unmittelbar für die Tat oder die Tatumstände einen Beweis erbringen können.[68] Bei Smartphones genügt dabei schon der potentielle Beweiswert der gespeicherten Daten, um eine Beschlagnahme begründen zu können.[69] Jüngst urteilte jedoch das *LG Kiel*, dass sich aufgrund des Umfangs der auf den Geräten gespeicherten Daten, immer die Vermutung einer potentielle Beweisbedeutung dieser Daten anstellen lasse.[70] Die Vermutung der Beweisbedeutung müsse sich daher auf bisherige Ermittlungsergebnisse stützen und bereits im Vorfeld einer möglichen Durchsuchung bestehen. Die Beschlagnahme eines aufgefundenen Smartphones, das als Beweismittel nicht im Durchsuchungsbeschluss genannt werde, sei daher unzulässig.[71]

b) Beschlagnahme von Telekommunikationsdaten

Inhalts- und Verbindungsdaten können sowohl im Speicher als auch in der SIM-Karte moderner Smartphones abgelegt sein. Diese außerhalb eines laufenden Kommunikationsvorgangs gespeicherten Daten im Herrschaftsbereich des Betroffenen, unterliegen nicht dem Schutz des Telekommunikationsgeheimnisses aus Art. 10 Abs. 1 GG sondern dem des RiS aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. § 94 StPO stellt damit eine zulässige Ermächtigungsgrundlage für die Beschlagnahme dieser Daten dar.[72] Für Emails, die sich zum Zeitpunkt der Auswertung des Smartphones noch auf zugangsgesicherten Servern eines Providern befinden, gilt dies im Hinblick auf den Schutzbereich nicht. Diese sind bis zu ihrer endgültigen Ankunft im Herrschaftsbereich des Kommunikationsteilnehmers durch das Telekommunikationsgeheimnis geschützt.[73] Dennoch erkennt das *BVerfG* auch in diesem Fall § 94 StPO als zulässige Ermächtigungsgrundlage an, sofern der Eingriff offen und nur punktuell erfolgt.[74]

c) Auswertung des Smartphones

Für die Auswertung der nach § 94 StPO sichergestellten Gegenstände und Daten gibt es in der StPO keine einschlägigen Regelungen, weshalb sich die Maßnahmen am Zweck des Ermittlungsverfahrens und der Sicherung der Originalität des Beweismittels auszurichten haben.[75] Datenerhebung, -speicherung und -auswertung außerhalb des eigentliches Beweiszweckes verbieten sich daher. Gleichzeitig ist dem jeweiligen Datensatz von außen jedoch nicht anzusehen ob er beweiserheblich ist oder nicht, weshalb häufig zumindest eine Sichtung der Daten erforderlich ist. Die Auswertung von Smartphones kann, je nach Anforderung, auf unterschiedliche Weise erfolgen. Die Spanne reicht dabei vom einfachen Abfotografieren des Displays über den Einsatz sog. Forensik Software bis hin zum „Chip-Off"-Verfahren, bei dem einzelne Bauteile des Smartphones entfernt und anschließend mit einer Auswertungshardware verbunden werden.[76] Unter Auswertung ist die Inaugenscheinnahme des Dateninhalts zu verstehen.[77]

Durch die genannten Maßnahmen erlaubt die Beschlagnahme und Auswertung eines Smartphones nach § 94 Abs. 2 StPO den Zugriff auf einen großen heterogenen Datenbestand und damit die umfassende Gewinnung von Erkenntnissen, bis hin zur Bildung eines vollständigen Persönlichkeitsprofils des Nutzers. Damit gehen diese Maßnahmen auf Grundlage der geringsten Verdachtsform des Anfangsverdachtes weit über das ursprüngliche, mit einer Beschlagnahme bezweckte, Maß hinaus.[78] Die gesteigerten Möglichkeiten der Ausforschung führen zu deutlich sensibleren Einblicken und damit zu bedeutend intensiveren Eingriffen in die Grundrechte der Betroffenen. Die Eingriffe stützen sich dabei auf eine Ermächtigungsgrundlage, die seit Inkrafttreten der StPO unverändert Bestand hat, was einen Anpassungsbedarf insbesondere zur Begrenzung der Eingriffsintensität offensichtlich werden lässt.

Das *BVerfG* stellt in seinem Urteil zur Onlinedurchsuchung fest, dass mit der Infiltration eines komplexen informationstechnischen Systems, die entscheidende Hürde zur Ausspähung des Systems insgesamt genommen sei.[79] Die Auswertung eines Smartphones mithilfe forensischer Analysetools ermöglicht ebenfalls die vollumfängliche Ausspähung des Systems. Auch wenn dies, im Gegensatz zur Online-Durchsuchung, offen erfolgt und keine fortlaufende Überwachung ermöglicht, besteht im Hinblick auf den möglichen Umfang der gewonnenen Daten und damit der Intensität des Grundrechtseingriffs diesbezüglich zumindest eine Nähe zwischen der Auswertung von Smartphones und der Onlinedurchsuchung.[80]

2. Durchsicht von Papieren § 110 StPO

Der mögliche Umfang des Datenbestandes sowie die unterschiedlichen Arten von Daten auf einem Smartphone, stellen die Strafverfolgungsbehörden regelmäßig vor

66 Vgl. *Hartmann/Schmidt,* Strafprozessrecht, Rn. 421.
67 *Singelnstein,* NStZ 2012, 593 (598).
68 Vgl. BVerfGE 77, 1 (53); *Menges,* in: LR-StPO, § 94 Rn. 30; *Gercke,* in: HK-StPO, § 94 Rn. 28 f.
69 Vgl. *Ruppert,* Jura 2018, 994 (995).
70 *LG Kiel,* Beschl. v. 25.4.2016 – 7 Qs 24/16, in Anlehnung an *LG Berlin*, Beschl. v. 15.1.2004 – 518 Qs 44/03.
71 Vgl. *LG Kiel*, Beschl. v. 25.4.2016 – 7 Qs 24/16 (Rn. 18, 21).
72 *BVerfG*, Nichtannahmebeschl. v. 25.7.2007 – 2 BvR 2282/06 2007.
73 Vgl. BVerfGE 124, 43 (54 f.).
74 Vgl. BVerfGE 124, 43 (58 f.); *Blechschmidt,* MMR 2018, 361, (364); *Warken,* NZWiSt 2017, 417 (418).
75 Vgl. *Blechschmidt,* MMR 2018, 361 (364); *Gercke,* in: HK-StPO, § 94, Rn. 24.
76 Vgl. *Rogge,* Der Kriminalist 2015, 29 (31).
77 Vgl. *Zerbes/El-Ghazi,* NStZ 2015, 425 (427).
78 Vgl. *Singelnstein,* NStZ 2012, 593 (602).
79 Vgl. BVerfGE 120, 274 (308).
80 Vgl. *Momsen,* DRiZ, 2018, 140 (143).

Probleme. Die schiere Menge der Daten und die Komplexität der Smartphones lässt die, für eine Beschlagnahme geforderte, potentielle Beweisbedeutung auf den ersten Blick nicht erkennen. Daher kommt eine Beschlagnahme zu diesem Zeitpunkt nicht in Betracht. Jedoch gestattet § 110 Abs. 1 StPO der Staatsanwaltschaft, sowie auf deren Anordnung ihren Ermittlungspersonen, „[d]ie Durchsicht von Papieren des von der Durchsuchung Betroffenen […]“ um zu einem späteren Zeitpunkt eine Beschlagnahmeentscheidung treffen zu können.[81] Die Durchsicht von Papieren gilt daher als Teil der Durchsuchung[82] oder wird als vorläufige Sicherstellung[83] bezeichnet. Die Anwendung der Norm in Rechtsprechung und Praxis geht in zweifacher Hinsicht über den Wortlaut des Gesetzestextes hinaus. Zum einen sind nach dem *BVerfG* auch elektronische Datenträger vom Begriff „Papiere“ umfasst.[84] Zum anderen soll sich die Befugnis zur Durchsicht von Papieren auch auf Gegenstände erstrecken, die nicht auf dem Wege einer Durchsuchung in das Gewahrsam der Strafverfolgungsbehörden gelangt sind.[85] Damit ist die Durchsicht von Smartphones als Datenträger grds. zulässig.

Auch wenn die Durchsicht nach h.M. dem Schutz der Persönlichkeitsrechte des Betroffenen einer Durchsuchung dient[86], stellt sie sich in der Realität häufig als weitreichender Eingriff in dessen Lebensbereich dar.[87] Für die Bestimmung des sachlichen Umfangs der Maßnahme steht der Staatsanwaltschaft, respektive ihren Ermittlungspersonen, ein weiter Ermessenspielraum zu.[88] Damit erfolgt häufig ein ausgedehnter Zugriff auf alle im Smartphone befindlichen Daten und darüber hinaus, durch § 110 Abs. 3 StPO legitimiert, ggf. auch auf Cloud-Datenspeicher, sofern sie vom Smartphone aus erreichbar sind. Erschwerend kommt hinzu, dass dieser Zugriff aufgrund der technischen Gegebenheiten regelmäßig in den Diensträumen der Strafverfolgungsbehörde stattfinden muss[89], ohne dass der Betroffene die Möglichkeit hat persönliche oder für das Strafverfahren irrelevante Daten zurückzuhalten.[90] Eine solche Mitnahme wird z. B. dann erforderlich sein, wenn das Smartphone eine Zugangssicherung oder eine Verschlüsselung aufweist und diese erst durch technische Mittel überwunden werden muss.[91] Die Überwindung von digitalen Zugangssicherungen ist, ähnlich dem Öffnen verschlossener Behältnisse in der analogen Welt, im Rahmen der Durchsicht eine zulässige Maßnahme.[92]

Die in § 110 Abs. 3 StPO a. F. festgeschriebene Möglichkeit des Betroffenen an der Durchsicht teilzunehmen, wurde 2004 durch das JuMoG ersatzlos gestrichen.[93] Zwar könne sich nach Ansicht des *BVerfG* ein Anwesenheitsrecht auch aus Verhältnismäßigkeitserwägungen ergeben[94], die vorinstanzlichen Entscheidungen in dieser Sache zeigen jedoch die Abhängigkeit von der Beurteilung des jeweiligen Gerichtes. Auch die Durchsicht von Papieren rückt damit in die Nähe der verdeckten Maßnahmen gem. § 100a ff. StPO. So ist die Maßnahme dem Einzelnen zwar bekannt und damit Rechtschutz in Form gerichtlicher Überprüfung möglich[95], die fehlende Begrenzung der Durchsicht in sachlichem und zeitlichem Umfang sowie das nur vage zugestandene Anwesenheitsrecht durch die Rechtsprechung zeigen jedoch, dass der Durchsicht wesentliche Elemente einer offenen Maßnahme fehlen.[96] Darüber hinaus kann sich die Durchsicht von Kommunikationsdaten gegenüber dem jeweiligen Kommunikationspartner als verdeckte Maßnahme darstellen, sofern dieser nicht von der Maßnahme unterrichtet wird. Eine entsprechende Ermächtigung auch gegenüber unvermeidbar betroffenen Dritten, bspw. analog zu § 100b Abs. 3 S. 3 StPO, besteht jedoch nicht.

Auch die Maßnahme der Durchsicht von Papieren stammt aus einer Zeit, in der sie tatsächlich auf die in der Norm genannten Papiere beschränkt war. Zum Zeitpunkt ihrer Schaffung konnte der Gesetzgeber nicht die massive Eingriffsqualität vorhersehen, die sich aus der Digitalisierung sämtlicher Lebensbereiche, z. B. durch die Nutzung von Smartphones ergibt.[97]

3. Grundsatz der Verhältnismäßigkeit

Als übergeordnete Leitregel allen staatlichen Handelns wirkt auch im strafrechtlichen Ermittlungsverfahren der mit Verfassungsrang ausgestattete Grundsatz der Verhältnismäßigkeit.[98] Dies gilt sowohl für § 110 StPO als auch für § 94 StPO, obwohl den Ermittlungsbehörden nach dem reinen Wortlaut dieser Normen kein Ermessen zusteht.[99] Bei der Beschlagnahme und Auswertung von Smartphones sowie darauf befindlicher Daten setzt der Grundsatz der Verhältnismäßigkeit dem staatlichen Handeln aufgrund der besonderen Eingriffstiefe und Grundrechtsrelevanz Grenzen.[100] Insbesondere die hohe Ein-

---

81 Vgl. *Peters,* NZWiSt 2017, 465; *Blechschmidt,* MMR 2018, 361 (363).

82 Vgl. BGHSt 44, 265 (273); *Tsambikakis,* in: LR-StPO, § 110, Rn. 28; a.A. *Peters,* NZWiSt 2017, 465 (472).

83 Vgl. *BVerfG*, Nichtannahmebeschl. v. 28.4.2003 – 2 BvR 358/03 = NJW 2003, 2669; *Peters,* NZWiSt 2017, 465 (466).

84 Vgl. BVerfGE 113, 29 (51).; BT-Drs. 16/5846, S. 63. Trotz Ausweitung der Bedeutung des Begriffs „Papiere“ durch die Rechtsprechung sah der Gesetzgeber auch bei der letzten Reform des § 110 StPO im Jahr 2004 keine Veranlassung den Wortlaut zu verändern. Vgl. BT-Drs. 15/3482.

85 Vgl. *Tsambikakis,* in: LR-StPO, § 110 Rn. 21.

86 Vgl. *Tsambikakis,* in: LR-StPO, § 110 Rn. 1; *Gercke,* in: HK-StPO, § 110 StPO Rn. 1; *Hartmann/Schmidt,* Strafprozessrecht, Rn. 531.

87 Vgl. *Peters,* NZWiSt 2017, 465.

88 Vgl. *Tsambikakis,* in: LR-StPO, § 110 Rn. 28.

89 Vgl. *Zerbes/El-Ghazi,* NStZ 2015, 425 (426).

90 Vgl. *Peters,* NZWiSt 2017, 465 (467).

91 Vgl. *Momsen,* DRiZ 2018, 140, mit Verweis auf Nutzung einer PIN als "kleines Einmaleins des privaten Datenschutzes" und der sich schon daraus ergebenden technischen Schwierigkeiten für Strafverfolgungsorgane.

92 Vgl. *Zerbes/El-Ghazi,* NStZ 2015, 425 (427); *Meyer-Goßner/Schmitt,* StPO, 62. Aufl. (2019), § 110 Rn. 6.

93 Vgl. BGBl. I 2004, Nr. 45, S. 2201.

94 Vgl. BVerfGE 113, 29 (58).

95 Auch die Durchsicht ist als „vorläufige Sicherstellung“ gem. § 98 Abs. 2 StPO richterlich überprüfbar, vgl. *Herrmann/Soiné,* NJW 2011, 2922 (2925).

96 Vgl. *Peters,* NZWiSt 2017, 465 (469).

97 *Peters,* NZWiSt 2017, 465 (469 f.).

98 Vgl. BVerfGE 20, 162 (187); *Burghart,* in: Leibholz/Rinck, GG, Art. 20 Rn. 776; *Hartmann/Schmidt,* Strafprozessrecht, Rn. 431.

99 Vgl. *Hartmann/Schmidt,* Strafprozessrecht, Rn. 431; *Hauschild,* in: MüKo-StPO, 2014, § 94 Rn. 10.

100 *Park,* Durchsuchung und Beschlagnahme, Rn. 828.

griffsintensität erfordert eine enge Auslegung des Verhältnismäßigkeitsgrundsatzes.[101] Danach müssen die Maßnahme und der mit ihr einhergehende Grundrechtseingriff insgesamt in einem angemessenen Verhältnis zur Schwere der Straftat und der Stärke des Tatverdachts stehen. Eine nur leichte Straftat, eine geringe Beweisbedeutung der Daten oder ein nur vager Auffindeverdacht können einer Beschlagnahme und Auswertung eines Smartphones daher entgegenstehen.[102]

Über § 46 OWiG sind die Vorschriften der StPO auch im Ordnungswidrigkeitenverfahren anwendbar. Die hohe Eingriffsintensität im Hinblick auf die Auswertung eines Smartphones in Verbindung mit dem Verhältnismäßigkeitsgrundsatz dürften einer solchen Maßnahme jedoch grundsätzlich entgegenstehen.[103]

Die Beachtung des Verhältnismäßigkeitsgrundsatzes erfordert eine Beschränkung des Zugriffs auf den Datenbestand in sachlicher wie auch in zeitlicher Hinsicht. Die Strafverfolgungsbehörden sind daher verpflichtet, eine Erhebung nicht verfahrensrelevanter Daten zu vermeiden[104] und die Auswertung des Smartphones in kürzester Zeit durchzuführen.[105] In der Praxis wird sich besonders der letztgenannte Aspekt als schwierig erweisen. Moderne Smartphones stellen schon mit einfach verfügbaren Sicherungsmethoden wie einer PIN-Sperre die Strafverfolgungsbehörden vor große technische Probleme.[106] Fraglich ist daher schon in welchem zeitlichen Rahmen Ermittler, z.B. bei der Verfolgung eines niedrigschwelligen Vergehens versuchen dürfen die Sicherung eines Smartphones zu umgehen, ohne den Grundsatz der Verhältnismäßigkeit zu missachten.

Auch wenn Maßnahmen nach §§ 94 und 110 StPO als offene Maßnahmen mit nur punktuellem Eingriff gelten, reicht ihre Eingriffsintensität aufgrund des Umfangs der erhobenen Daten an die der verdeckten Maßnahmen der §§ 100a ff. StPO heran. Während bei den letztgenannten Bestimmungen der Grundsatz der Verhältnismäßigkeit in Form der Subsidiaritätsklauseln eine einfachgesetzliche Ausformung erhält[107], fehlt eine ähnliche Ausgestaltung für Sicherstellung und Durchsicht vollends.

4. Kernbereichsschutz

Neben dem Grundsatz der Verhältnismäßigkeit stellt der Schutz des Kernbereichs privater Lebensgestaltung die zweite wesentliche Begrenzung staatlicher Eingriffe, insbesondere bei der Auswertung elektronischer Daten dar. Unter Kernbereich wird ein letzter unantastbarer Bereich menschlicher Freiheit verstanden, welcher der Einwirkung der öffentlichen Gewalt, auch in Abwägung mit dem Informationsbedürfnis der Strafverfolgungsbehörden zur Sicherung einer funktionierenden Strafrechtspflege, nicht zugänglich ist.[108] Was konkret vom absolut geschützten Kernbereich umfasst wird, ist nicht abschließend geklärt.[109] Dem Kernbereich unterfällt nach dem *BVerfG* die Möglichkeit „[...]innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen[…]“ sowie die vertrauliche Kommunikation mit anderen.[110] Anhand der dargestellten technischen Möglichkeiten von Smartphones scheint es unbestritten, dass sich auf den Geräten Daten und Informationen finden lassen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Dies schließt die Beschlagnahme und Auswertung der Geräte nicht per se aus, macht aber eine Sichtung und Bestimmung möglicher Kernbereichsinhalte erforderlich, da der jeweilige Inhalt den Daten von außen nicht anzusehen ist.[111] Hier zeigt sich das Paradoxon des Kernbereichsschutzes. Um zu bestimmen was dem Kernbereich unterfällt, ist ggf. eine, wenn auch geringfügige, Verletzung eben dieses Kernbereichs erforderlich.[112] Der Gesetzgeber begegnete diesem Umstand für die heimliche Maßnahme der Online-Durchsuchung gem. § 100b StPO auf Erhebungs- und Auswertungsebene durch die gesetzlichen Regelungen zum Kernbereichsschutz in § 100d Abs. 3 StPO. Danach ist durch technische Vorkehrungen weitestgehend sicherzustellen, dass Daten, die dem Kernbereich privater Lebensgestaltung zuzuordnen sind, nicht erhoben werden bzw. unverzüglich zu löschen sind, falls eine Erhebung stattfand. [113]

Obwohl ein Eingriff durch Beschlagnahme und Auswertung von Smartphones, zumindest was Umfang und Informationsgehalt sichergestellter Daten anbelangt, im Vergleich zur Onlinedurchsuchung als ähnlich gravierend bezeichnet werden kann, fehlt für Beschlagnahme und Durchsicht von Papieren eine entsprechende einfachgesetzliche Regelung.

VI. Anpassungsbedarf/ Fazit

Die hohe Komplexität von Smartphones als IT-Systeme machen einen wirksamen Selbstschutz des durchschnittlichen Nutzers im Hinblick auf die gespeicherten Daten kaum möglich.[114] Smartphones erweisen sich für die Strafverfolgungsbehörden zunehmend als sehr gute Informationsquelle, da sie bei vollständiger Auswertung des Datenträgers ein umfassendes Persönlichkeitsbild des Betroffenen ermöglichen, was mit intensiven Eingriffen in dessen Grundrechtspositionen verbunden ist.

---

101 *Momsen,* DRiZ 2018, 140 (143).
102 Vgl. BVerfGE 96, 44 (51); BVerfGE 113, 29 (57); BVerfGE 124, 43 (66); *Singelnstein,* NStZ 2012, 593 (598).
103 ^Vgl. *Menges,* in: LR-StPO, § 94 Rn. 3; *Hartmann/Schmidt,* Strafprozessrecht, Rn. 413; a.A. *Ternig/Lellmann,* NZV 2016, 454, die eine Beschlagnahme und Auswertung eines Mobiltelefons zur Verfolgung einer Owi für zulässig erachten.
104 Vgl. *Singelnstein,* NStZ 2012, 593 (598).
105 Vgl. *Wenzel,* NZWiSt 2016, 85 (93) unter Verweis auf *AG Reutlingen*, Beschl. v. 5.12.2011 – 5 Gs 363/11 (Rn. 4).
106 Vgl. *Momsen,* DRiZ 2018, 140.
107 Vgl. *Gercke,* in: HK-StPO, § 100a Rn. 21.
108 Vgl. BVerfGE 109, 279 (313 ff.); *Gercke,* in: HK-StPO, vor § 94 Rn. 18; *Czerner,* in: Labudde/Spranger, Forensik in der digitalen Welt, 2017, S. 265 (273).
109 *Hartmann/Schmidt,* Strafprozessrecht, Rn. 426; *Menges,* in: LR-StPO, § 94 Rn. 77.
110 Vgl. BVerfGE 109, 279 (313).
111 *Hartmann/Schmidt,* Strafprozessrecht, Rn. 427.
112 Vgl. BverfGE 109, 279 (383), Sondervotum der Richterinnen *Jaeger* und *Hohmann-Dennhart*.
113 Vgl. BT-Drs. 18/12785, S. 56.
114 Vgl. BVerfGE 120, 274 (306).

Das *BVerfG* stellte bereits 2005 fest, dass der Gesetzgeber den Grundrechtsschutz bei staatlichen Ermittlungshandeln, ggf. durch Anpassung bestehender oder Schaffung ergänzender Regelungen effektiv sichern müsse.[115]

Im Hinblick auf die geforderte Normenklarheit und das Bestimmtheitsgebot ist zunächst an eine generelle Veränderung des Wortlauts der Normen zu denken. Der Anwendungsbereich der Beschlagnahme von Beweismitteln und der Durchsicht von Papieren wurde durch die Rechtsprechung immer weiter, z. T. über den Wortlaut hinaus, ausgedehnt. Eine Änderung der Bezeichnung „Papiere" in „Informationsträger" in § 110 StPO oder die Erweiterung des § 94 Abs. 1 StPO auf Daten könnten zur geforderten Normenklarheit beitragen.

Die hohe Eingriffsintensität ergibt sich nicht zuletzt aus der Tatsache, dass die Auswertung des Smartphones häufig nicht im Beisein des Betroffenen stattfindet. Der Betroffene hat damit keine Möglichkeit zu überprüfen, auf welche Daten tatsächlich zugegriffen wurde und ob der Zugriff für das zugrundliegende Ermittlungsverfahren tatsächlich erforderlich war. Ein grundsätzliches Anwesenheitsrecht des Betroffenen könnte die Eingriffsintensität verringern und gleichzeitig die Effektivität der Auswertung erhöhen, da der anwesende Betroffene nicht relevante Daten benennen und so eine langwierige Auswertetätigkeit aller im Smartphone gespeicherter Daten unterbleiben könnte. Zugleich würde dadurch der zeitliche Umfang der Maßnahme reduziert und so den Verhältnismäßigkeitsanforderungen genüge getan werden.

Ein weiterer Aspekt im Rahmen von Verhältnismäßigkeitsabwägungen stellt die Beschränkung der Zulässigkeit der Beschlagnahme und Auswertung von Smartphones nur für Ermittlungen bei bestimmten Straftaten dar. Diskussionen in der Literatur, die eine Smartphoneauswertung schon bei Ordnungswidrigkeiten als zulässig erachten, bis hin zu Forderungen, diese Maßnahmen nur unter den strikten Voraussetzungen des § 100a StPO als rechtmäßig anzusehen, zeigen exemplarisch den vorhandenen Regelungsbedarf. Ob für diese Beschränkung ein strikter Katalog oder bspw. mindestens ein Verbrechenstatbestand zu fordern ist, wäre in einem Gesetzgebungsverfahren mit Blick sowohl auf die Bedeutung der betroffenen Grundrechte und der Eingriffsintensität als auch auf das Erfordernis der Funktionstüchtigkeit der Strafrechtspflege, zu erörtern.

Den §§ 94 und 110 StPO fehlt in Bezug auf erlangte Daten eine einfachgesetzliche Regelung zum Schutz des Kernbereichs (analog zu § 110 d StPO). Insbesondere die in § 100d Abs. 2 StPO festgeschriebene Pflicht zur Löschung der Daten, Verwertungsverbote sowie der in § 100d Abs. 3 StPO geforderte Einsatz technischer Mittel kommen auch für die Durchsicht und Auswertung beschlagnahmter Smartphones in Betracht und könnten dazu beitragen die Eingriffsintensität der Maßnahme zu reduzieren.

Wie sich gezeigt hat, sind die derzeitigen Eingriffsermächtigungen der StPO nur bedingt geeignet, die tiefgreifenden Grundrechtseingriffe, die sich aus der Beschlagnahme und Auswertung von Smartphones ergeben, zu rechtfertigen. Die Anpassung der Eingriffsermächtigungen an die fortschreitende Digitalisierung aller Lebensbereiche, die sich insbesondere bei Smartphones zeigt, erscheint daher kriminalpolitisch geboten.

[115] Vgl. *BVerfG,* Urt. v. 12.4.2005 – 2 BvR 581/01 (Rn. 64).