Schriften zum Strafrecht

Band 419

Ein Update für den Kernbereichsschutz

Die Gefahr der Bildung von Persönlichkeitsprofilen bei der strafprozessualen Online-Durchsuchung

Von

Catharina Pia Conrad

Duncker & Humblot · Berlin

CATHARINA PIA CONRAD

Ein Update für den Kernbereichsschutz

Schriften zum Strafrecht

Band 419

Ein Update für den Kernbereichsschutz

Die Gefahr der Bildung von Persönlichkeitsprofilen bei der strafprozessualen Online-Durchsuchung

Von

Catharina Pia Conrad

Duncker & Humblot · Berlin

Die Rechtswissenschaftliche Fakultät der Universität Bremen hat diese Arbeit im Jahre 2022 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Erschienen bei Duncker & Humblot GmbH, Berlin
Satz: L101 Mediengestaltung, Fürstenwalde
Druck: CPI books GmbH, Leck
Printed in Germany

ISSN 0558-9126
ISBN 978-3-428-18925-0 (Print)
ISBN 978-3-428-58925-8 (E-Book)
DOI 10.3790/978-3-428-58925-8

Gedruckt auf alterungsbeständigem (säurefreiem) Papier entsprechend ISO 9706 ♾

Internet: http://www.duncker-humblot.de

Für meine Familie –
Sigrid, Matthias und Corinna Conrad

Vorwort

Dieses Dissertationsprojekt wurde im August 2022 abgeschlossen und von der Universität Bremen zur Prüfung angenommen. Das Promotionskolloquium fand im März 2023 statt.

Zwischen der Veröffentlichung der Dissertation und dem Promotionskolloquium erfolgte eine Kürzung des Titels und eine redaktionelle Überarbeitung.

An dieser Stelle möchte ich allen danken, die mich bei der Anfertigung dieser Dissertation unterstützt haben.

Besonderer Dank gilt den Betreuern dieser Dissertation Prof. Dr. Felix Herzog und Prof. Dr. Andreas Fischer-Lescano, die mir stets mit Rat und Tat zur Seite standen und mich bei der Umsetzung dieses Projekts unterstützt haben.

Weiterhin geht mein Dank an die Mitarbeitenden der Strafrechtslehrstühle an der Universität Bremen sowie an die Kolleg*innen vom Zentrum für Europäische Rechtspolitik (ZERP). Den fachlichen und freund*innenschaftlichen Austausch sowie das solidarische Miteinander und die motivierenden Worte in jeder Phase des Dissertationsprojekts haben die Arbeit und mich wesentlich geprägt. Namentlich zu nennen sind hier insbesondere Tore Vetter, Dr. Andreas Gutmann und Julia Gelhaar.

Außerdem möchte ich mich bei jenen außergewöhnlichen Frauen und Freundinnen bedanken, die mich zum Abschluss dieses Dissertationsprojektes getragen und dafür gesorgt haben, dass ich mich in jener schweren Zeit nicht verliere. Ohne sie wäre dieses Projekt nicht abgeschlossen worden.

Dieser Dank gebührt Dr. Hanna Söker, Elena Ewering, Christina Schmitz, Laura Fügemann, Dr. Nele Austermann, Laura Janßen, Sarah Heines, Sarah Haßdenteufel, Patricia Alcoberro Llivina, Leonie Rau und Pia Pinkenburg. Danke für jedes eurer Worte und Taten!

Mein größter Dank gilt meinen Eltern Matthias und Sigrid Conrad sowie meiner Schwester Corinna Conrad. Sie haben während Studium, Referendariat und Dissertation mitgefiebert, -gelitten und sich mitgefreut. Sie haben mir diese Dissertation ermöglicht. Ihnen ist sie gewidmet.

Esens, im Dezember 2023 *Catharina Pia Conrad*

Inhaltsverzeichnis

4. Kapitel

5. Kapitel

Einleitung

Diese Dissertation befasst sich mit der Gefahr der Bildung von Persönlichkeitsprofilen als Teil des Kernbereichs privater Lebensgestaltung am Beispiel der strafprozessualen Online-Durchsuchung. Für die Ermittlungsmaßnahme finden sich die unterschiedlichsten Begriffe wie „IT-Systemüberwachung“[1], „Ausspähen von Computer Dateien“[2] und „Zugriff auf informationstechnische Systeme“[3]. Mit ihr, so die Warnungen, gehen Gefahren der Rundumüberwachung,[4] Totalüberwachung[5] und der Bildung von Persönlichkeitsprofilen[6] einher. Was aber steckt hinter dieser Ermittlungsmaßnahme? Welche Gefahren birgt die Online-Durchsuchung tatsächlich? Was bedeuten sie und wie muss auf sie reagiert werden? All dies soll im Folgenden untersucht und geklärt werden.

Die Gefahr der Bildung von Persönlichkeitsprofilen ist bislang von Literatur und Rechtsprechung vernachlässigt worden. Lediglich die Feststellung, dass eine solche nicht bestehen dürfe,[7] wurde bis zum jetzigen Zeitpunkt durch die Rechtsprechung getroffen.

Diese einfache Feststellung allein kann jedoch bei einer Ermittlungsmaßnahme wie der Online-Durchsuchung nicht ausreichen. Denn sie erhebt Daten in einem neuen Ausmaß, indem sie in alle Lebensbereiche der betroffenen Person eindringt. So muss im Folgenden geklärt werden, was ein Persönlichkeitsprofil ist und wie mit ihm umgegangen werden muss. Grundsätzlich geht das Bundesverfassungsgericht davon aus, dass sich die Gefahr der Bildung von Persönlichkeitsprofilen aus einer Rundumüberwachung ergibt. Dabei kommt es insbesondere auf die Menge der erhobenen Daten an, die

---

[1] *Knierim/Oehmichen*, Quellen TKÜ und Online-Durchsuchung, in: Gesamtes Strafrecht aktuell, 375.

[2] LT-NRW Drucks., Ausschussprotokoll 14/292, S. 18; LT-NRW Drucks., Ausschussprotokoll 14/275, S. 18.

[3] *Roggan*, Gutachterliche Stellungnahme LT-Drucks. 14/0628, S. 6.

[4] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 323 = NJW 2004, 999.

[5] *Eschelbach*, in: SSW StPO, § 100b, Rn. 5.

[6] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 280 = NJW 2016, 1781.

[7] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 280 = NJW 2016, 1781; BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 323 = NJW 2004, 999.

sich aus einer längeren Zeitspanne der Überwachung verschiedener Lebensbereiche einer Person ergeben.[8]

Bereits diese pauschale Definition zeigt, dass in der Strafrechtswissenschaft bisher nicht ausreichend anerkannt wurde, welche Gefahren mit der Erhebung von Daten mittels der Online-Durchsuchung einhergehen. Dies soll sich mit dieser Ausarbeitung ändern und es soll eine präzisere Definition des Persönlichkeitsprofils entwickelt werden.

In der siebten Ausgabe der ZEIT des Jahres 2021[9] berichtete die Zeitung unter der Überschrift „Das Handy-Ich" über eine Studie, die sich in der Lage sieht, anhand der Smartphone-Nutzung innerhalb eines kurzen Zeitraums ein Persönlichkeitsprofil der Nutzer*innen mittels des Big-Five-Modells zu erstellen. Diese Studie zeigt eindrücklich, welche Möglichkeiten die Erfassung von Smartphone-Daten bietet und wie in kürzester Zeit das Innere einer Person nach außen getragen werden kann.[10] Diese technische Entwicklung soll mit dieser Ausarbeitung Eingang in die Strafrechtswissenschaft finden und es soll eine Reaktion auf dieses Phänomen entwickelt werden, an der es bislang fehlt.

Mit den neuen Möglichkeiten der Auswertung von IT-Geräten muss ein strafprozessualer Umgang gefunden werden, welcher in der Lage ist, die Rechte beschuldigter Personen weiterhin zu schützen und zu gewährleisten. Die Online-Durchsuchung ist gerade deswegen so brisant, weil sie, im Gegensatz zur klassischen Durchsuchung, heimlich durchgeführt wird und über einen längeren Zeitraum hinweg andauert. So ist es den Ermittlungsbehörden möglich, eine große Menge an Daten über die betreffende Person zu speichern und ihre Verhaltensmuster aufzudecken. Es stellt sich die Frage, welche Rückschlüsse aus der kompletten Überwachung eines IT-Systems auf die Persönlichkeit des*der Betroffenen gewonnen werden können und wie diese Erkenntnisse im Rahmen der Vorgaben zum Schutz des Kernbereichs der privaten Lebensgestaltung rechtlich geschützt werden können. Dabei ist ein besonderes Augenmerk auf den hohen Stellenwert zu richten, den ein informationstechnisches System im Leben eines*einer Jeden aufgrund des technischen Fortschritts hat. Es ist also auch zu prüfen, ob diese Situation eine

---

[8] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 280 = NJW 2016, 1781; BVerfG 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320, 350 f. = NJW 2006, 1939; BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 323 = NJW 2004, 999; BVerfG 16.07.1969 – 1 BvL 19/63, BVerfGE 27, 1, 6 = NJW 1969, 1707.

[9] *Drösser/Schütte*, Die ZEIT vom 11.02.2021, S. 46.

[10] *Stachel* et al., PNAS, Predicting personality from patterns of behavior collected with smartphones; online abzurufen über https://www.pnas.org/content/117/30/17680#ref-28 (zugegriffen am 14.4.2021).

Weiterentwicklung der Grundsätze zum Schutz des Kernbereichs der privaten Lebensgestaltung fordert.

Wesentliche Aufgabe soll es im Folgenden somit sein, das Recht in Einklang mit dem technischen Fortschritt zu bringen. Wenn der Gesetzgeber den Weg für die Nutzung des technischen Fortschritts im Rahmen der Strafverfolgung ebnet, muss dieser technische Fortschritt auch für den Schutz des Kernbereiches der privaten Lebensgestaltung genutzt werden.

Dafür muss eine Kontextualisierung zwischen der Menge der Daten und ihren Inhalten vorgenommen werden. Gerade in der Beziehung beider bestehen die größten Gefahren zur Bildung von Persönlichkeitsprofilen. Mit dieser Schnittstelle wird sich diese Ausarbeitung beschäftigen. Denn durch die Online-Durchsuchung lässt sich nicht nur eine erhebliche Menge an Daten generieren, sondern die Daten beinhalten auch Informationen zu allen Lebensbereichen der Betroffenen. In kürzester Zeit lassen sich erhebliche Persönlichkeitsstrukturen nachzeichnen, was beispielsweise bei einer Ermittlungsmaßnahme wie der akustischen Wohnraumüberwachung so zunächst nicht möglich wäre.

Das hat seinen Ursprung darin, dass es den Ermittlungsbehörden durch die Online-Durchsuchung ermöglicht wird, eine Ermittlungsmaßnahme einzusetzen, die sich nicht mehr auf den Inhalt eines einzelnen Datums konzentriert, sondern die in der Lage ist, durch eine Gesamtschau von Daten Persönlichkeitselemente aufzudecken. An dieser Stelle steigt die Gefahr der Bildung von Persönlichkeitsprofilen erheblich an.

In einem ersten Schritt wird das erarbeitet, was Rechtsprechung und Literatur bis dato nicht gelungen ist, eine Definition des Persönlichkeitsprofils.

Das folgende Kapitel beschäftigt sich sodann mit den Rechtsmaßstäben, an denen sich Maßnahmen, die die Gefahr der Bildung von Persönlichkeitsprofilen ermöglichen, messen lassen müssen. Hierfür folgt die Einordnung der Gefahr der Bildung von Persönlichkeitsprofilen, auf Basis der im ersten Kapitel entwickelten Definition, in den Kernbereich privater Lebensgestaltung.

Zum einen wird der Maßstab des Bundesverfassungsgerichts in Form des zweistufigen Schutzkonzepts dargestellt. Denn zur Verhinderung der Bildung von Persönlichkeitsprofilen kommt es im Wesentlichen auf eine Begrenzung der Daten bereits auf Erhebungsebene an. Darüber hinaus wird in diesem Kapitel dargestellt, warum die Rechtsprechung des Bundesverfassungsgerichts an dieser Stelle nicht vollends überzeugen kann und welche Vorgaben sich aus der Verfassung für die Gefahr der Bildung von Persönlichkeitsprofilen als Teil des Kernbereichs privater Lebensgestaltung stattdessen bei genauerer Untersuchung ergeben.

Nachdem die Anforderungen des Bundesverfassungsgerichts an den Kernbereich privater Lebensgestaltung dargestellt wurden, folgt eine Auseinandersetzung mit den europarechtlichen Vorgaben an die Gefahr der Bildung von Persönlichkeitsprofilen. Besondere Berücksichtigung wird dabei die Rechtsprechung des Europäischen Gerichtshofs zur Vorratsdatenspeicherung, die auf die Online-Durchsuchung übertragen werden kann, finden.

Das vierte Kapitel wird sich dann mit der konkreten Maßnahme, der Ermächtigung zur repressiven Online-Durchsuchung, auseinandersetzen. Dabei wird es um die historische Entwicklung der Online-Durchsuchung gehen. Dann wird dargestellt, welche Art der Daten, in welchem Umfang mittels der Online-Durchsuchung erhoben werden können, denn sie bilden das Fundament, auf das ein mögliches Persönlichkeitsprofil gestützt wird. Am Ende dieses Kapitels wird sich somit ein klarer Rahmen der Ermächtigung erkennen lassen.

In einem nächsten Schritt erfolgt eine Zusammenführung der zuvor genannten Aspekte. Die entwickelten Maßstäbe sollen nunmehr auf die konkrete Maßnahme angewendet werden. Nachdem in den vorherigen Kapiteln herausgestellt wurde, welche Besonderheiten sich für den Kernbereich privater Lebensgestaltung – gerade unter Berücksichtigung der Gefahren für die Bildung von Persönlichkeitsprofilen – ergeben und welche Vorgaben sowohl die Verfassung als auch das Unionsrecht treffen, um den Kernbereich zu schützen, wird untersucht, inwieweit diese Vorgaben vom Gesetzgeber durch Verfahrensvorschriften unter anderem in § 100d StPO eingehalten wurden.

Da sich der Gesetzgeber peinlichst genau an die Vorgaben des Bundesverfassungsgerichts gehalten hat und diese bereits nicht überzeugen konnten, wird in einem fünften Kapitel dargestellt, wie Sicherungen zum Schutz des Kernbereichs privater Lebensgestaltung im Verfahrensrecht aussehen müssen, um eine Datenerhebung auf das Nötigste zu reduzieren und so die Gefahr der Bildung von Persönlichkeitsprofilen zu verhindern.

Die Ausarbeitung hat es sich somit zur Aufgabe gemacht, eine angemessene Reaktion auf die Gefahren der Überwachung von IT-Systemen, wie sie beispielsweise von der zuvor genannten Studie aufgezeigt werden, zu finden. Hierfür braucht es einen neuen Umgang mit der Gefahr der Bildung von Persönlichkeitsprofilen als Teil des Kernbereichs privater Lebensgestaltung bei der strafprozessualen Online-Durchsuchung.

1. Kapitel

Der Begriff des Persönlichkeitsprofils

In diesem ersten Kapitel soll es zunächst um die Erarbeitung einer Definition der Gefahr der Bildung von Persönlichkeitsprofilen gehen.

Die Ermächtigung zur Online-Durchsuchung ist in der Lage eine erhebliche Menge an Daten zu generieren. Nicht nur das Bundesverfassungsgericht hat im Hinblick auf diese immensen Datenmengen die Gefahr der Bildung von Persönlichkeitsprofilen erkannt,[1] auch im Gesetzgebungsprozess wurde darauf hingewiesen, dass mittels der Online-Durchsuchung der betroffenen Person „beim Denken"[2] zugeschaut werden könne. Die Online-Durchsuchung dringt somit in intimste Lebensbereiche des*der Einzelnen ein.

Was ein solches Persönlichkeitsprofil konkret ist und inwieweit seine Erhebung verhindert werden kann, ist hingegen bis jetzt weitestgehend ungeklärt. Die Erarbeitung einer Definition des Persönlichkeitsprofils hat sich dieses Kapitel zur Aufgabe gemacht. Dabei wird es bei der Gefahr der Bildung von Persönlichkeitsprofilen regelmäßig um die Menge der Daten gehen, die erhoben werden. Für den wirksamen und effektiven Schutz vor der Gefahr der Bildung von Persönlichkeitsprofilen muss Begriff des Persönlichkeitsprofils zunächst definiert werden.

A. Bisherige Erkenntnisse über das Persönlichkeitsprofil

Große Probleme bereitet zunächst die Definition des Persönlichkeitsprofils als solchem. Zwar findet sich in der Rechtsprechung an einigen Stellen die Warnung vor der Gefahr der Bildung von Persönlichkeitsprofilen, welche mit der Menschenwürde nicht vereinbar sei,[3] eine genaue Definition des Begriffs des Persönlichkeitsprofils erfolgt allerdings nicht.

---

[1] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 280 = NJW 2016, 1781; BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 323 = NJW 2004, 999.

[2] *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 5.

[3] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 280 = NJW 2016, 1781; BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 323 = NJW 2004, 999.

Dammann legt den Fokus allein darauf, dass ein Persönlichkeitsprofil als eine Vorhersage des zukünftigen Verhaltens der betroffenen Person anzusehen sei.[4] Dass es in der Praxis keine Beispiele für ein verbotenerweise erstelltes Persönlichkeitsprofil gebe, sei ein Zeichen dafür, dass diesem Themenkomplex keine Relevanz zukomme.[5] Dies kann selbstredend nicht das Argument gegen eine Auseinandersetzung mit Persönlichkeitsprofilen sein. Zum einen stellt das Bundesverfassungsgericht zutreffend allein auf die „Gefahr" der Bildung von Persönlichkeitsprofilen und damit nicht auf deren tatsächliche Bildung ab. Zum anderen wurde mit der Online-Durchsuchung eine Ermittlungsmaßnahme geschaffen, die eine zuvor nicht gekannte Menge an Daten aus verschiedenen Lebensbereichen generieren kann,[6] sodass sich viele der Probleme in Bezug auf die Bildung von Persönlichkeitsprofilen zuvor so nicht gestellt haben. Aus diesem Grund lohnt sich für eine gelungene Definition des Persönlichkeitsprofils ein Blick in die Persönlichkeitspsychologie, da sich eine hinreichende Definition weder in der Rechtsprechung noch in der rechtswissenschaftlichen Literatur findet.

I. Übersicht über die Rechtsprechung

Das Bundesverfassungsgericht scheint davon auszugehen, dass die Gefahr der Bildung von Persönlichkeitsprofilen direkt mit einer Rundumüberwachung zusammenhängt, wenn es feststellt, dass eine Verletzung der Menschenwürde gegeben ist, „(…) wenn eine Überwachung derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können".[7]

Mit einer Rundumüberwachung gehe die Gefahr der Bildung eines Persönlichkeitsprofils einher. Somit kommt es nach Ansicht des Bundesverfassungsgerichts auf die Menge der Daten an, die bei (heimlichen) Ermittlungsmaßnahmen erhoben werden. Dabei spielt sowohl die zeitliche Komponente als auch die Erhebung von Daten aus unterschiedlichen Lebensbereichen eine Rolle. So sieht es auch *Warntjen*, der zutreffend davon ausgeht, dass eine Rundumüberwachung als eine Zusammenschau von Daten anzusehen ist, die die Lebenswirklichkeit der betroffenen Person aus verschiedenen Blickwinkeln erfasst.[8]

---

[4] *Dammann*, Der Kernbereich der privaten Lebensgestaltung, S. 151.

[5] *Dammann*, Der Kernbereich der privaten Lebensgestaltung, S. 151.

[6] Zur Gesamtschau der gesammelten Daten und der damit einhergehenden Gefahren mehr unter: 3. Kapitel B. I. 2. b).

[7] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 323 = NJW 2004, 999.

Das Bundesverfassungsgericht geht davon aus, dass der Mensch dann zu einem Objekt degradiert wird, wenn der Staat für sich in Anspruch nimmt, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren.[9] Später stellte das Gericht dann erneut fest, dass die umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger*innen nicht erlaubt ist. Die Erhebung und Verknüpfung entsprechender Daten kommt der Erstellung eines Persönlichkeitsprofils nahe und ermöglicht dadurch einen besonders intensiven Grundrechtseingriff.[10] Diese Formulierung legt den voreiligen Schluss nahe, dass die Gefahr der Bildung eines Persönlichkeitsprofils zwar ein intensiver Grundrechtseingriff ist, aber nicht zwangsläufig aufgrund einer Verletzung der Menschenwürde zu unterlassen ist. Zu einem späteren Zeitpunkt stellte das Gericht aber klar, dass Überwachungsmaßnahmen nicht derart umfassend sein dürfen, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des*der Betroffenen registriert werden und zur Grundlage eines Persönlichkeitsprofils gemacht werden können. Dies sei mit der Menschenwürde nicht vereinbar.[11]

Zusammenfassend lässt sich aus Sicht der Rechtsprechung somit sagen, dass es für die Gefahr der Bildung von Persönlichkeitsprofilen auf die Menge der Daten ankommt, die erhoben werden. Zu berücksichtigen ist dabei die Zeitspanne der Überwachung, aber auch die Erhebung unterschiedlicher Daten aus verschiedenen Lebensbereichen, die in der Lage sind, die Persönlichkeit eines Menschen zu registrieren und zu katalogisieren.[12]

Unklar bleibt indes, was ein Persönlichkeitsprofil ist und welche Art der Daten es braucht, um ein solches Persönlichkeitsprofil zu bilden. Hierbei kann die Persönlichkeitspsychologie Klarheit schaffen.

---

[8] *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung, S. 112.

[9] BVerfG 16.07.1969 – 1 BvL 19/63, BVerfGE 27, 1, 6 = NJW 1969, 1707.

[10] BVerfG 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320, 350 f. = NJW 2006, 1939.

[11] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 323 = NJW 2004, 999; BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 280 = NJW 2016, 1781.

[12] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 280 = NJW 2016, 1781; BVerfG 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320, 350 f. = NJW 2006, 1939; BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 323 = NJW 2004, 999; BVerfG 16.07.1969 – 1 BvL 19/63, BVerfGE 27, 1, 6 = NJW 1969, 1707.

II. Erkenntnisse der Persönlichkeitspsychologie

Ausgangspunkt eines Persönlichkeitsprofils ist der Begriff der Persönlichkeit. In der Persönlichkeitspsychologie wird davon ausgegangen, dass Merkmale, die Individuen voneinander unterscheiden, sogenannte Persönlichkeitsmerkmale sind. Die Persönlichkeit ist dabei die Gesamtheit aller Persönlichkeitsmerkmale.[13]

Ein Persönlichkeitsprofil ist dann die Beschreibung einer Person mittels verschiedener Eigenschaften,[14] durch die ein einzigartiges Persönlichkeitsprofil erstellt werden kann,[15] welches zeitlich stabil ist.[16] Oder genauer: Ein Persönlichkeitsprofil besteht aus den Eigenschaftswerten einer Person, durch deren Verhältnis zueinander die Individualität der betreffenden Person abgebildet wird.[17]

Dabei sind drei Prämissen im Umgang mit den Eigenschaften zu berücksichtigen:[18]

- Sie sind mit Verhaltensweisen verknüpft. Die Eigenschaft kann selbst nicht direkt beobachtet werden, sondern wird aus einem beobachteten Verhalten geschlossen.
- Eine Eigenschaft ist dann gegeben, wenn sie in unterschiedlichen Situationen beobachtet werden kann.
- Eine Eigenschaft kann einer Person erst dann zugeschrieben werden, wenn sie immer wieder vorkommt.[19]

Um die Persönlichkeit eines Menschen anhand seiner Eigenschaften abzubilden, gibt es in der Psychologie unterschiedliche Darstellungsweisen. Die Modelle der Eigenschaftsabbildung sind jene Modelle, die sich bemühen, die Gesamtheit einer Person möglichst genau darzustellen.[20] Am häufigsten ver-

---

13 *Schmitt/Altstötter-Gleich*, Differentielle Psychologie und Persönlichkeitspsychologie kompakt, S. 7.

14 *Neyer/Asendorpf*, Psychologie der Persönlichkeit, S. 24.

15 *Neyer/Asendorpf*, Psychologie der Persönlichkeit, S. 24.

16 *Neyer/Asendorpf*, Psychologie der Persönlichkeit, S. 26.

17 *Neyer/Asendorpf*, Psychologie der Persönlichkeit, S. 114.

18 *Schmitt/Altstötter-Gleich*, Differentielle Psychologie und Persönlichkeitspsychologie kompakt, S. 70; *Stemmler* et al., Differentielle Psychologie und Persönlichkeitsforschung, S. 55.

19 *Schmitt/Altstötter-Gleich*, Differentielle Psychologie und Persönlichkeitspsychologie kompakt, S. 70; *Stemmler* et al., Differentielle Psychologie und Persönlichkeitsforschung, S. 55.

20 *Schmitt/Altstötter-Gleich*, Differentielle Psychologie und Persönlichkeitspsychologie kompakt, S. 69.

wendet wird, nach dem aktuellen Stand der Wissenschaft, das Modell der „Big Five", auch Fünf-Faktoren-Modell (FFM) genannt.[21] Hierbei werden die Persönlichkeitseigenschaften eines Menschen anhand von fünf feststehenden Parametern bestimmt und ins Verhältnis zueinander gesetzt.[22] Namentlich sind das die Eigenschaften Neurotizismus, Extraversion, Verträglichkeit, Gewissenhaftigkeit und Offenheit (im Englischen: Neuroticism, Extraversion, Agreeableness, Conscientiousness und Openness, kurz: OCEAN).[23] Besonders ist an diesem Modell, dass es sich in verschiedenen Kulturen und Sprachgemeinschaften bewährt hat.[24]

Mittels solcher Eigenschaftskonzepte können zwei Ziele verfolgt werden. Zum einen können individuelle Unterschiede in der Ausprägung der Eigenschaften herausgearbeitet werden und das Modell ist damit in der Lage, Menschen zu beschreiben,[25] und zum anderen ist die Vorhersage von konkretem Verhalten denkbar.[26]

Im Ergebnis lässt sich sagen, dass unabhängig davon, welches der Eigenschaftskonzepte angewendet wird, Persönlichkeitsprofile durch diese gebildet werden können. Dabei kann durch die Anwendung der Konzepte die Individualität eines Menschen mittels Kategorisierung und Registrierung beschrieben werden. Außerdem ist es denkbar, das Verhalten der betroffenen Person vorherzusagen. Das kann dazu führen, dass Eigenschaften, die die betroffene Person selbst nicht wahrnimmt, deutlich präziser wiedergegeben werden können. Letztlich wird bei einem Eigenschaftsmodell, wie dem der „Big Five", das Innerste, was eine Person ausmacht, nach außen getragen.

B. Eine Definition des Persönlichkeitsprofils

Das Bundesverfassungsgericht geht davon aus, dass sich die Gefahr der Bildung von Persönlichkeitsprofilen aus einer Rundumüberwachung ergibt. Dabei kommt es insbesondere auf die Menge der erhobenen Daten an, die

---

21 *Schmitt/Altstötter-Gleich*, Differentielle Psychologie und Persönlichkeitspsychologie kompakt, S. 93.

22 *Schmitt/Altstötter-Gleich*, Differentielle Psychologie und Persönlichkeitspsychologie kompakt, S. 95.

23 *Schmitt/Altstötter-Gleich*, Differentielle Psychologie und Persönlichkeitspsychologie kompakt, S. 95; *Stemmler* et al., Differentielle Psychologie und Persönlichkeitsforschung, S. 293.

24 *Schmitt/Altstötter-Gleich*, Differentielle Psychologie und Persönlichkeitspsychologie kompakt, S. 93.

25 *Schmitt/Altstötter-Gleich*, Differentielle Psychologie und Persönlichkeitspsychologie kompakt, S. 99.

26 *Stemmler* et al., Differentielle Psychologie und Persönlichkeitsforschung, S. 63.

sich aus einer längeren Zeitspanne der Überwachung verschiedener Lebensbereiche einer Person ergeben.[27]

Gemäß dem Verständnis der Persönlichkeitspsychologie ist ein Persönlichkeitsprofil eine Beschreibung der Person mittels ihrer Eigenschaftswerte, durch deren Verhältnis zueinander die Individualität eines Menschen abgebildet wird.[28] Dadurch können die individuellen Unterschiede von Menschen herausgearbeitet werden. Grundsätzlich ist anhand solcher Profile auch die Vorhersage von konkretem, zukünftigem Verhalten denkbar.[29] Nicht verwechselt werden darf das Persönlichkeitsprofil mit den noch zu besprechenden Profiling-Daten.[30] Bei dem Prozess des Profiling erfolgt eine Bewertung des*r Betroffenen, während es bei der Bildung von Persönlichkeitsprofilen insbesondere auf die Menge der gesammelten Daten aus unterschiedlichen Lebensbereichen ankommt.[31] Durch die Erhebung einzelner Profiling-Daten besteht dann die Möglichkeit der Bildung von Persönlichkeitsprofilen.

Ein Persönlichkeitsprofil ist somit die Beschreibung einer Person mittels ihrer Eigenschaften. Ein solches Profil kann unabhängig von dem angewandten Eigenschaftsmodell anhand von Daten, aber auch mittels der Beobachtung des Verhaltens der betroffenen Person[32] erstellt werden, wobei ein Mensch in seinem Sein registriert und katalogisiert wird. Bei der Erstellung eines solchen Persönlichkeitsprofils wird die Gedanken- und Gefühlswelt, die einen Teil des Kernbereichs privater Lebensgestaltung darstellt, der betroffenen Person offengelegt und analysiert.

Abschließend kann festgestellt werden, dass die Bildung von Persönlichkeitsprofilen dann gegeben ist, wenn aufgrund der Menge der erhobenen Daten, die sich aus der Dauer der Überwachung oder der Erhebung von Daten aus verschiedenen Lebensbereichen ergeben kann (Rundumüberwachung), eine konkrete Beschreibung der Person möglich ist, sodass ihre Individualität offengelegt wird.

---

27 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 280 = NJW 2016, 1781; BVerfG 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320, 350 f. = NJW 2006, 1939; BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 323 = NJW 2004, 999; BVerfG 16.07.1969 – 1 BvL 19/63, BVerfGE 27, 1, 6 = NJW 1969, 1707.

28 *Neyer/Asendorpf*, Psychologie der Persönlichkeit, S. 114.

29 *Stemmler* et al., Differentielle Psychologie und Persönlichkeitsforschung, S. 63.

30 Vgl. hierzu: 3. Kapitel B. I. 2. a) bb).

31 *Schantz/Wolff*, Das neue Datenschutzrecht, S. 230.

32 *Neyer/Asendorpf*, Psychologie der Persönlichkeit, S. 98, 99, 101.

2. Kapitel

Entwicklung eines Rechtsmaßstabs für die Gefahr der Bildung von Persönlichkeitsprofilen

Nachdem zuvor eine Definition des Persönlichkeitsprofil erarbeitet wurde, ist nun ein Maßstab zu entwickeln, an denen sich jene staatlichen Maßnahmen messen lassen müssen, die die Gefahr der Bildung von Persönlichkeitsprofilen ermöglichen. Hierfür wird zunächst dargelegt, welche Anforderungen die Grundrechte an die Gefahr der Bildung von Persönlichkeitsprofile stellen. In einem nächsten Schritt wird dann erarbeitet, inwieweit unionsrechtliche Vorgaben Anwendung auf die Gefahr der Bildung von Persönlichkeitsprofilen finden.

A. Der Schutz des Kernbereichs der privaten Lebensgestaltung als verfassungsrechtlicher Maßstab

In diesem Abschnitt wird zunächst dargelegt, warum die Gefahr der Bildung vom Persönlichkeitsprofilen aus verfassungsrechtlicher Perspektive dem Kernbereich privater Lebensgestaltung zuzuordnen ist. Bei der Darstellung des verfassungsrechtlichen Maßstabes wird verdeutlicht, inwieweit das Konzept des Kernbereichs privater Lebensgestaltung eine Begrenzung der Menge der Datenerhebung vorsieht, um die Gefahr der Bildung von Persönlichkeitsprofilen zu verhindern. Dafür ist die Rechtsprechung des Bundesverfassungsgerichts zum Kernbereich privater Lebensgestaltung näher zu beleuchten, um anschließend deren Probleme bei der Gefahr der Bildung von Persönlichkeitsprofilen zu analysieren.

Das zweistufige Schutzkonzept des Bundesverfassungsgerichts kann insoweit nicht überzeugen, als dass es kaum Vorgaben zur Begrenzung der Daten auf Erhebungsebene enthält. Aus diesem Grund ist ein verfassungsrechtlicher Maßstab zu entwickeln, der einen Schutz des Kernbereichs privater Lebensgestaltung auch bei der Gefahr der Bildung von Persönlichkeitsprofilen ermöglicht und an dem sich zu einem späteren Zeitpunkt verfahrensrechtliche Schutzvorschriften messen lassen müssen.

I. Die Gefahr der Bildung von Persönlichkeitsprofilen als Teil des Kernbereichs privater Lebensgestaltung

In diesem Kapitel wird dargelegt, warum die Gefahr der Bildung von Persönlichkeitsprofilen dem Kernbereich private Lebensgestaltung zuzuordnen ist.

Wie bereits dargelegt, kann die Verhinderung der Gefahr der Bildung von Persönlichkeitsprofilen allein über eine Begrenzung der Daten erfolgen. Diese Begrenzung kann im deutschen Verfassungsrecht zum einen über den Verhältnismäßigkeitsgrundsatz und zum anderen durch den Schutz des Kernbereichs privater Lebensgestaltung gelingen.

Warum die Gefahr der Bildung von Persönlichkeitsprofilen primär dem Kernbereichsschutz zuzuordnen ist und neben dem Verhältnismäßigkeitsgrundsatz bestehen kann, wird im folgenden Abschnitt dargelegt.

1. Einordnung der Rechtsprechung

Weiterhin wird davon ausgegangen, dass die Gefahr der Bildung von Persönlichkeitsprofilen zwar die Menschenwürde verletze, aber unabhängig von dem ebenfalls aus der Menschenwürde erwachsenden Schutz des Kernbereichs privater Lebensgestaltung zu betrachten sei.[1] Begründet wird dies regelmäßig mit einer Passage aus dem Urteil zum großen Lauschangriff.[2] Hier heißt es:

> „Eine zeitliche und räumliche ‚Rundumüberwachung' wird regelmäßig schon deshalb unzulässig sein, weil die Wahrscheinlichkeit groß ist, dass dabei höchstpersönliche Gespräche abgehört werden. Die Menschenwürde wird auch verletzt, wenn eine Überwachung sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert und zur Grundlage eines Persönlichkeitsprofils werden können."[3]

Diese Aussage des Bundesverfassungsgerichts wird dahingehend verstanden, dass der Menschenwürdegehalt an dieser Stelle zwei Ansätze konstatiere:[4] den Schutz des Kernbereichs privater Lebensgestaltung und die Gefahr

---

[1] *Dammann*, Der Kernbereich der privaten Lebensgestaltung, S. 152; *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 137; *Hauck*, Heimliche Strafverfolgung und Schutz der Privatheit, S. 280; *Schwabenbauer*, Heimliche Grundrechtseingriffe, S. 293 ff.

[2] *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 137.

[3] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 323 = NJW 2004, 999.

[4] *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 137; *Dammann*, Der Kernbereich der privaten Lebensgestaltung, S. 152.

der Bildung von Persönlichkeitsprofilen. Der Schutz des Kernbereichs der privaten Lebensgestaltung sei getrennt von der Gefahr der Bildung von Persönlichkeitsprofilen zu betrachten, denn der Rundumüberwachung fehle es an dem konstituierenden Merkmal der Höchstpersönlichkeit.[5] Eine Trennung der beiden Punkte kann in diesem Abschnitt des Urteils allerdings nicht gesehen werden. Vielmehr wird deutlich, dass der Kernbereich privater Lebensgestaltung nicht trennscharf von der Gefahr der Bildung von Persönlichkeitsprofilen abgegrenzt werden kann. Dies ergibt sich aus der Systematik des Urteils, in dem sich diese Argumentation im Abschnitt zum Kernbereich wiederfindet. Es wurde gerade kein neuer, getrennter Argumentationspunkt des „Persönlichkeitsprofils" eröffnet.

Zumindest, und nichts Anderes wird aus der umstrittenen Passage des Urteils zum Lauschangriff deutlich, lässt sich die Gefahr der Bildung von Persönlichkeitsprofilen nicht klar vom Schutz des Kernbereichs privater Lebensgestaltung trennen. Zutreffend kann also zunächst davon ausgegangen werden, dass mit einer Rundumüberwachung, die die Gefahr der Bildung von Persönlichkeitsprofilen in sich trägt, mindestens auch die Gefahr besteht, punktuell höchstpersönliche und damit kernbereichsrelevante Informationen zu erheben.[6]

2. Gesamtschau der Daten

Eine besonders erhöhte und neue Gefahr der Bildung von Persönlichkeitsprofilen besteht bei der Online-Durchsuchung aufgrund der Menge an Daten, die erhoben werden können, seien sie auch auf den ersten Blick noch so irrelevant.[7] In ihrer Zusammenschau erhöhen sie die Gefahr der Bildung von Persönlichkeitsprofilen erheblich.

Wie noch darzustellen sein wird, ist es mittels der Online-Durchsuchung wie bei keiner anderen Ermittlungsmaßnahme möglich, Daten auf unterschiedliche Art und Weise und aus den verschiedensten Lebensbereichen zu erheben. Zum einen können sich auf einem IT-Gerät Daten befinden, die ein Äquivalent zu jenen Daten darstellen, die auch bei einer klassischen Durchsuchung hätten erhoben werden können. Diese können punktuell Kernbereichsrelevanz ausweisen. Zum anderen ist es aber auch möglich, durch eine Live-Überwachung diese Daten mittels eines Prozesses des Profiling zu Profiling-Daten zu verwerten. Dabei stammen die Daten aus den verschiedensten Lebensbereichen und können zusammengefügt werden. Bei diesen

[5] *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 137.

[6] *Baldus*, JZ 2008, 218, 220.

[7] Vgl.: *Lammer*, Verdeckte Ermittlungen im Strafprozeß, S. 90.

Profilingdaten, die das Ergebnis eines Profilingvorgangs sind, kommt es zunächst nicht auf den Informationsgehalt eines personenbezogenen Datums an, sondern die neue Information basiert auf der Interpretation dieser Daten.[8] Einem Datum liegen damit zwei Arten von Informationsgehalten zugrunde:

1. Der Ursprungsinhalt und die Kerninformation des Datums (A hält sich an Ort X auf).
2. Die Kerninformation im Kontext zu anderen Informationen, werden hier als Profilingdaten bezeichnet. Diese lassen Rückschlüsse auf die Eigenschaftsmerkmale einer Person zu. (A hält sich regelmäßig an Ort X mit B zum Zeitpunkt Y auf – dies ist je nach Menge der gesammelten Informationen dann erweiterbar auf Informationen wie Gesprächsinhalt et cetera. Aus diesen Kerndaten und eventuell bereits gebildeten Profilingdaten könnte sich folgendes Bild ergeben: Mit B pflegt A zwar nur eine oberflächliche Beziehung – erkennbar aufgrund der Dauer des Aufenthaltes an Ort X, der Länge des Treffens zum Zeitpunkt Y und aus der Häufigkeit der Treffen mit B –, dennoch zeigt A hier stets ein reges Interesse an B – Auswertung der Kommunikation. Im Ergebnis könnte dann ein Indiz für das Eigenschaftsmerkmal der Offenheit festgestellt werden.)

Daraus folgt: Mit jeder Kerninformation, die erhoben wird, insbesondere wenn sie ihren jeweiligen Ursprung in unterschiedlichen Lebensbereichen hat, steigen die Genauigkeit und auch die Menge an Profilingdaten, die entwickelt werden können. Am Ende eines solchen Profilingprozesses stehen dann neue Erkenntnisse in Bezug auf die Persönlichkeitseigenschaften eines Menschen. Hier steigt die Gefahr für den Kernbereich der privaten Lebensgestaltung immens.

Dass sich die Daten aus verschiedensten Lebensbereichen ergeben können, liegt daran, dass mit einer Online-Durchsuchung mehrere Ermittlungsmaßnahmen (anteilig) mitverwirklicht werden können. Daher seien an dieser Stelle einige Beispiele für Informationen genannt, die speziell bei einer Online-Durchsuchung erhoben werden können und deutlich machen, wie unterschiedlich die Kerninformationen bei einer Ermittlungsmaßnahme sein können: Fotos, Videos, Kontaktdaten, Kalendereinträge (auch von Ereignissen, die Jahre zurückliegen), Gesundheitsdaten von immer populärer werdenden Smartwatches, Suchmaschineneingaben, Kommunikation via Messenger-Diensten, Social-Media-Apps, GPS-Daten, die IP-Adresse, Online-Banking, Online-Shopping.[9] Auch Gelöschtes und Nichtgeäußertes kann nachvollzo-

[8] *Scholz*, in: NK zum Datenschutzrecht, Art. 4 Nr. 4, Rn. 6.

[9] Vgl. auch: *Großmann*, GA 2018, 439, 446; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 5.

gen werden.[10] Diese Daten können für sich genommen Ausfluss einer akustischen Wohnraumüberwachung, einer (Quellen-)TKÜ, einer Durchsuchung oder ähnlicher Maßnahme sein.[11] Anhand dieser Daten und Informationen ist es ein Leichtes, ein Persönlichkeitsprofil zu erstellen.[12] So wird auch in der Persönlichkeitsforschung davon ausgegangen, dass sich die Nutzung des Internets und mobiler Kommunikationsgeräte durch weite Teile der Bevölkerung hervorragend für die Persönlichkeitsforschung und deren Anwendungen nutzen lasse.[13]

Keine andere Ermittlungsmaßnahme ist in der Lage, einen auch nur vergleichbaren Umfang an Daten in kürzester Zeit zu erheben, die dann eine so weitreichende Lebensspanne betreffen.[14] Es kann, anders als bei der akustischen Wohnraumüberwachung, nicht nur das zum Zeitpunkt der Überwachung gesprochene Wort abgehört werden, sondern es können Daten erhoben werden, die bereits mehrere Jahre alt sind.[15] Jeder archivierte Chat oder die Notizen und Kalendereinträge von vor mehreren Jahren lassen sich so durch die Ermittlungsbehörden nachvollziehen. Mit der Ermittlungsmaßnahme der Online-Durchsuchung werden nicht nur Daten aus einem einzelnen Lebensbereich in den Fokus genommen, sondern verschiedenste Lebensbereiche, wenn nicht sogar alle, können durch die Ermittlungsbehörden überwacht und verknüpft werden.

Dies hat schließlich auch das Bundesverfassungsgericht erkannt, wenn es sagt, dass Online-Durchsuchungen

> „(…) oft gesamthaft über lange Zeit angesammelte Informationen, einschließlich höchstprivater Aufzeichnungen erfassen und dabei unter Umständen durch deren Verknüpfung sowie das Nach- und Mitverfolgen der Bewegungen im Internet auch geheim gehaltene Schwächen und Neigungen erschließen können, (…).“[16]

Dennoch hat das Bundesverfassungsgericht ein zweistufiges Schutzkonzept entwickelt, sodass eine Erhebung dieser Daten möglich ist.[17]

---

10 *Großmann*, GA 2018, 439, 447.

11 Vgl. hierzu: 2. Kapitel B. I. 2. c).

12 *Paa*, Der Zugriff der Strafverfolgungsbehörden auf das Private im Kampf gegen schwere Kriminalität, S. 62; *Eschelbach*, in: SSW StPO, § 100b, Rn. 5; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 5; *Mansdörfer*, GSZ 2018, 45, 47; mit weiteren beeindruckenden Studien: *Neyer/Asendorpf*, Psychologie der Persönlichkeit, S. 107 f.

13 *Neyer/Asendorpf*, Psychologie der Persönlichkeit, S. 103.

14 Vgl. auch: *Großmann*, GA 2018, 439, 450.

15 Vgl.: *Großmann*, GA 2018, 439, 446.

16 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 313 = NJW 2016, 1781.

17 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274 = NJW 2008, 822.

Zwar hat das Bundesverfassungsgericht bereits in einem Urteil von 1983 erkannt: „Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' Datum mehr."[18] Dennoch verkennt es in seinen Folgeentscheidungen, dass die Besonderheit der Online-Durchsuchung darin liegt, dass sie die Strafrechtswissenschaft durch ihre Ausgestaltung vor neue Probleme in Bezug auf den Kernbereichsschutz stellt, insbesondere die Gefahr der Bildung von Persönlichkeitsprofilen. Denn die Menge der vermeintlich irrelevanten und banalen Daten intensiviert die Gefahr der Bildung von Persönlichkeitsprofilen erheblich.

3. Persönlichkeitsprofilbildung als Ergebnis einer Rundumüberwachung

Es ist festzustellen, dass das Verbot der Bildung von Persönlichkeitsprofilen nicht nur vom Kernbereichsschutz nicht abzugrenzen ist, sondern darüber hinaus auch im Schutz des Kernbereichs der privaten Lebensgestaltung fußt und ihm zuzuordnen ist.[19] Dem wird zwar entgegengehalten, dass bei der Rundumüberwachung auch banale Informationen, ohne höchstpersönlichen Inhalt, die Gefahr der Bildung von Persönlichkeitsprofilen begründen können und deswegen das Verbot von Persönlichkeitsprofilen getrennt vom Schutz des Kernbereichs privater Lebensgestaltung zu sehen sei.[20] Dabei lässt diese Ansicht jedoch eine wesentliche Tatsache außer Acht. Richtig ist zwar, dass auch mit vermeintlich banalen Informationen ein Persönlichkeitsprofil gebildet werden kann, zu berücksichtigen ist allerdings, dass durch die Zusammenschau eben dieser banalen Informationen etwas Höchstpersönliches entstehen kann.[21] Das bedeutet, dass erst aus dem Ergebnis einer Rundumüberwachung, aus der sich die Gefahr der Bildung von Persönlichkeitsprofilen ergibt, auch die Verwirklichung des Tatbestandsmerkmals der Höchstpersönlichkeit folgt und das unabhängig davon, ob punktuell und für sich genommen höchstpersönliche Informationen erhoben worden sind. Das Produkt einer Rundumüberwachung, die Gefahr der Bildung von Persönlichkeitsprofilen, stellt als solches das konstitutive Merkmal der Höchstpersönlichkeit dar.

---

18 BVerfG 15.12.1983 – 1 BvR 209/83 u. a., BVerfGE, 65, 1, 45 = NJW 1984, 419.

19 *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung, 114, 128; *Bode*, Verdeckte strafprozessuale Ermittlungsmaßnahmen, S. 147, 162, 460; *Hong*, Der Menschenwürdegehalt der Grundrechte, S. 449.

20 *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 137.

21 *Hoffmann-Riem*, JZ 2008, 1009, 1020.

Im Übrigen darf nicht unberücksichtigt bleiben, dass es, sähe man die Gefahr der Bildung von Persönlichkeitsprofilen nicht als Teil des Kernbereichs privater Lebensgestaltung an, an Verfahrenssicherungen in der StPO fehlte. Auch für den Schutz des Kernbereichs privater Lebensgestaltung braucht es einfachgesetzliche verfahrensrechtliche Regelungen, um den Schutz der Menschenwürde zu gewährleisten.[22] Rechnete man die Gefahr der Bildung von Persönlichkeitsprofilen nicht dem Kernbereich privater Lebensgestaltung zu, fehlten solche Sicherungen.

Der Kernbereich der privaten Lebensgestaltung ist wie folgt zu definieren:

> „Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, und zwar ohne Angst, dass staatliche Stellen dies überwachen."[23]

Genau jene Informationen mit Kernbereichsrelevanz sind zunächst in der Lage, ein Persönlichkeitsprofil zu bilden. Diese braucht es aber nicht zwingend. Auch der Umfang der Informationen ist relevant. Insbesondere das unbewusste Erleben spielt im Rahmen des Persönlichkeitsprofils eine erhebliche Rolle. Wie oben bereits festgestellt, ist ein Persönlichkeitsprofil die Beschreibung einer Person mittels ihrer Eigenschaften. Hierbei kann die Gedanken- und Gefühlswelt der Person durch das Fünf-Faktoren-Modell offengelegt werden. Mittels Persönlichkeitsprofilen kann das herausgefunden und zusammengestellt werden, was die Definition des Kernbereichs privater Lebensgestaltung beschreibt. Das Persönlichkeitsprofil selbst stellt eine höchstpersönliche Information im Sinne des Kernbereichs privater Lebensgestaltung dar.

So geht auch *Warntjen* in seinem Kernbereichsmodell davon aus, dass das „erhöhte Rundumüberwachungspotential" ein Kriterium für die Frage sei, ob eine Ermittlungsmaßnahme den Kernbereich privater Lebensgestaltung berühren könne.[24] Dabei könne die Datenmenge ein Indiz für die Höchstpersönlichkeit sein.[25]

Präziser und zutreffend ist allerdings die Annahme, dass das Persönlichkeitsprofil einen Ausschnitt des Kernbereichs privater Lebensgestaltung be-

---

[22] Ständige Rechtsprechung mit weiteren Nachweisen: BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 277 = NJW 2016, 1781.

[23] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 313 = NJW 2004, 999.

[24] *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung, S. 128.

[25] *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung, S. 114, 128.

trifft.[26] Im Ergebnis kann demnach der Kernbereich privater Lebensgestaltung zum einen verletzt sein, wenn bei der Beobachtung einer Person eine solche Menge an Daten erhoben wird, dass so die Gefahr der Bildung von Persönlichkeitsprofilen besteht, und zum anderen, wenn eine Überwachung punktuell zu stark in die Tiefe geht, also die Information als solche bereits Kernbereichsrelevanz aufweist.[27]

Die Annahme, dass die Gefahr der Bildung von Persönlichkeitsprofilen als Teil des Kernbereichs privater Lebensgestaltung angesehen werden muss, ist nicht zuletzt in dem Grundgedanken des Kernbereichs selbst begründet. Bereits im Ersturteil zum Kernbereich der privaten Lebensgestaltung stellte das Bundesverfassungsgericht fest, dass der Kernbereich jener Bereich ist, welcher den Menschen als „geistig-sittliche" Person ausmache.[28] Was macht den Menschen als geistig-sittliche Person mehr aus, als die Abbildung seiner Persönlichkeit mittels einer Beschreibung und Darstellung seiner Eigenschaften, die in der Lage sind, die Gefühlswelt eines Menschen abzubilden? Mittels einer solchen Abbildung der Persönlichkeit wird der Mensch zu einem offenen Buch für die Ermittlungsbehörden.

Dem steht nicht entgegen, dass die ganz herrschende Meinung davon ausgeht, dass die Daten, die durch eine Online-Durchsuchung erhoben werden, dem Schutzbereich des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG angehören[29] und die Gefahr der Bildung von Persönlichkeitsprofilen bereits dem Schutzbereich unterfällt. Denn der Menschenwürdekern eines jeden Grundrechts beinhaltet den Kernbereich privater Lebensgestaltung,[30] sodass eine Abgrenzung zwischen dem im Einzelfall jeweils betroffenen Grundrecht und dem Kernbereich privater Lebensgestaltung nicht notwendig ist.

Im Ergebnis kann somit nicht nur die einzelne, punktuelle Information Kernbereichsrelevanz aufweisen, sondern auch die Gesamtschau von Daten kann kernbereichsrelevant sein, wenn die Gefahr der Bildung von Persönlichkeitsprofilen besteht. Aus diesem Grund ist die Gefahr der Bildung von Persönlichkeitsprofilen am Schutz des Kernbereichs privater Lebensgestaltung zu messen.

---

26 Vgl. auch: *Bode*, Verdeckte strafprozessuale Ermittlungsmaßnahmen, S. 147, 162, 460.

27 Vgl. auch: *Bode*, Verdeckte strafprozessuale Ermittlungsmaßnahmen, S. 460.

28 BVerfG 16.01.1957 – 1 BvR 253 56, BVerfGE 6, 32, 36.

29 *Di Fabio*, in: Dürig/Herzog/Scholz, Kommentar zum Grundgesetz, Art. 2 Abs. 1 Rdnr. 176; *Kunig/Kämmerer*, in: von Münch/Kunig, Grundgesetzkommentar; Art. 2 Rdnr. 75.

30 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 276 = NJW 2016, 1781.

4. Abgrenzung zum Verhältnismäßigkeitsgrundsatz

Die Gefahr der Bildung von Persönlichkeitsprofilen als Teil des Kernbereichsschutzes – und als Ergebnis einer Rundumüberwachung – ist vom Verhältnismäßigkeitsgrundsatz abzugrenzen. Zwar kann der Verhältnismäßigkeitsgrundsatz, unter anderem über den Gedanken des additiven Grundrechtseingriffs, der Menge der Daten Einhalt gebieten, allerdings unter anderen Voraussetzungen als der Kernbereich der privaten Lebensgestaltung.[31] Dabei können beide Gedanken nebeneinander bestehen.

Verhältnismäßigkeit und Kernbereich privater Lebensgestaltung schließen sich demnach nicht aus. Eine Begrenzung der Menge der Daten kann nebeneinander verlaufen. Während der Verhältnismäßigkeitsgrundsatz sich zunächst auf die Menge der Daten, die Verletzung unterschiedlicher Grundrechte und dann auf die Art der Daten bezieht, geht es beim Kernbereich privater Lebensgestaltung bei der Gefahr der Bildung von Persönlichkeitsprofilen allein um die Korrelation zwischen der Art der Daten und der Menge an Daten. Diese ist in der Lage, das Tatbestandsmerkmal der „Höchstpersönlichkeit“ zu verwirklichen.

Die Gefahr der Bildung eines Persönlichkeitsprofils aus einer Rundumüberwachung verwirklicht das Merkmal der Höchstpersönlichkeit und ist somit dem Kernbereich privater Lebensgestaltung des*der Einzelnen zuzuordnen. Diese Gefahr ist nicht über den Verhältnismäßigkeitsgrundsatz aufzulösen, auch wenn hier ebenfalls die Menge der Daten Berücksichtigung findet.

5. Zwischenergebnis

Das Problem der Gesamtschau der Daten zeigt deutlich, dass mit der Online-Durchsuchung eine Ermittlungsmaßnahme mit einer noch nie dagewesenen Eingriffsintensität geschaffen worden ist. Mit dieser Ermittlungsmaßnahme erhöht sich die Gefahr, den*die Betroffene*n zum Objekt des Strafverfahrens zu machen, wie bei keiner anderen Maßnahme.

Dabei ist die Gefahr der Bildung von Persönlichkeitsprofilen dem Kernbereich privater Lebensgestaltung zu zuordnen.

Da die Gefahr der Bildung von Persönlichkeitsprofilen insbesondere dann besteht, wenn im konkreten Einzelfall bei der Durchführung der Maßnahme eine solche Menge an Daten generiert wird, dass sie in einer Gesamtschau in der Lage ist, die Persönlichkeit der betroffenen Person mittels ihrer Eigen-

[31] Wann und unter welchen Voraussetzungen der Verhältnismäßigkeitsgrundsatz verletzt ist, kann hier nicht abschließend behandelt werden.

schaften zu beschreiben, und so die Individualität des Einzelnen offenlegt, muss zum Schutz des Kernbereichs privater Lebensgestaltung die Menge der Daten, die erhoben werden, begrenzt werden.

II. Entwicklung des Kernbereichs privater Lebensgestaltung in der Rechtsprechung

Der Kernbereich privater Lebensgestaltung hat seine Prägungen und Konkretisierungen insbesondere durch die Rechtsprechung des Bundesverfassungsgerichts erhalten. Aus diesem Grund sind jene Urteile zu untersuchen, die den Kernbereich der privaten Lebensgestaltung im Wesentlichen, gerade im Rahmen der Online-Durchsuchung, beeinflusst haben.

1. Das Elfes-Urteil

Seine erste Erwähnung findet der Kernbereich der privaten Lebensgestaltung in dem sogenannten „Elfes-Urteil“ aus dem Jahr 1957. Hier ging es zwar zunächst um die Ausreisefreiheit des Herrn Elfes, das Bundesverfassungsgericht legte jedoch auch folgenden Grundstein für die Begrifflichkeit des Kernbereichs der privaten Lebensgestaltung. Das Grundgesetz könne mit der „freien Entfaltung der Persönlichkeit“ (Art. 2 Abs. 1 GG) „(…) nicht nur die Entfaltung jenes Kernbereichs der Persönlichkeit gemeint haben, der das Wesen des Menschen als geistig-sittliche Person ausmacht (…).“[32] Die Formulierung aus Art. 2 Abs. 1 GG sei vielmehr nicht nur für sich genommen zu betrachten, sondern sie sei im Lichte des Art. 1 GG zu sehen und abzuleiten.[33]

Nach diesem ersten Urteil zum Kernbereich der privaten Lebensgestaltung ergibt sich dieser aus Art. 2 Abs. 1 GG im Lichte des Art. 1 GG und umfasst das Wesen des Menschen als solches mit allem, was ihn als geistig-sittliche Person ausmacht.

2. Die (zweite) Tagebuch-Entscheidung

In der zweiten Tagebuch-Entscheidung aus dem Jahr 1989 befasste sich das Bundesverfassungsgericht mit der Frage, ob tagebuchähnliche Aufzeichnungen des Beschuldigten im Strafverfahren herangezogen werden dürfen.[34]

---

[32] BVerfG 16.01.1957 – 1 BvR 253 56, BVerfGE 6, 32, 36.
[33] BVerfG 16.01.1957 – 1 BvR 253 56, BVerfGE 6, 32, 36.
[34] BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367 = NJW 1990, 563.

Grundsätzlich gewähre das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) dem*der Einzelnen die Befugnis, selbst zu entscheiden, wann und innerhalb welcher Grenzen er*sie persönliche Lebenssachverhalte offenbare. Dieses allgemeine Persönlichkeitsrecht gelte mit Ausnahme eines letzten unantastbaren Bereichs privater Lebensgestaltung aber nicht schrankenlos. Dieser letzte unantastbare Bereich der privaten Lebensgestaltung sei der öffentlichen Gewalt hingegen schlechthin entzogen[35] und Eingriffe seien nicht zu rechtfertigen.[36] Das ergebe sich aus dem Wesensgehalt der Grundrechte aus Art. 19 Abs. 2 GG und aus der Tatsache, dass der Kern der Persönlichkeit durch die unantastbare Würde des Menschen geschützt sei.[37] Ob es sich bei einem Sachverhalt um einen Eingriff in diesen Kernbereich handelt, müsse nach seinem inhaltlichen persönlichen Charakter und der Art der Intensität beurteilt werden.[38] Der Mensch als Person existiere, auch im Kern seiner Persönlichkeit, notwendigerweise in seinen sozialen Bezügen.[39] In dieser Entscheidung bestimmt das Bundesverfassungsgericht den Kernbereich der privaten Lebensgestaltung nach folgenden Kriterien:

Zum einen komme es darauf an, ob der*die Betroffene den Lebenssachverhalt geheim halten wolle. Denn wenn der Wille zur Geheimhaltung nicht bestehe, dann könne es sich in aller Regel auch nicht um einen Umstand handeln, der den Kernbereich berühre.[40] Außerdem komme es darauf an, wie höchstpersönlich der Inhalt der Aufzeichnung sei und in welcher Art und Intensität er aus sich heraus die Sphäre anderer oder die Belange der Gemeinschaft berühre.[41] Aufzeichnungen, die einen unmittelbaren Bezug zu begangenen Straftaten haben, seien hingegen nicht dem unantastbaren Bereich der privaten Lebensgestaltung zuzuordnen.[42]

Demnach könne bereits ein Bezug zur Tat bestehen, wenn der Beschuldigte in seinen Aufzeichnungen darlege, dass er unter seelischen Spannungszuständen leide und Schwierigkeiten mit Frauen habe. Sie stünde deswegen in Bezug zur Tat, weil sie Hinweise zur Vorgeschichte der Tat und der Persönlichkeit enthielten. Diese Bezüge finden sich nach Ansicht des Bundes-

---

35 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 374 = NJW 1990, 563.
36 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 373 = NJW 1990, 563.
37 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 373, 374 = NJW 1990, 563.
38 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 373, 374 = NJW 1990, 563.
39 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 374 = NJW 1990, 563.
40 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 374 = NJW 1990, 563.
41 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 374 = NJW 1990, 563.
42 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 375 = NJW 1990, 563.

verfassungsgerichts im Schuldprinzip wieder. Nur so könne gewährleistet werden, strafrechtliche Schuld und die richtige Strafhöhe zu bestimmen.[43] Das Schuldprinzip selbst finde seine Grundlage in der Menschenwürde.[44] Aus diesem Grund könnten sich die strafrechtlichen Ermittlungen nicht alleine auf das unmittelbare Tatgeschehen beziehen, sondern für eine interessensgerechte Urteilsfindung müsse auch die Persönlichkeit des*der Tatverdächtigen Teil der strafrechtlichen Ermittlungen werden.[45] Die Gedanken des*der Beschuldigten seien durch ihre Niederschrift bereits aus dem beherrschbaren Innenbereich entlassen und der Gefahr eines Zugriffs preisgegeben worden.[46] Eine Verletzung der Menschenwürde komme an dieser Stelle nicht in Betracht, da sie Grundlage für eine gerechte Bewertung des Tatgeschehens sei, was nicht zuletzt von Art. 1 Abs. 1 GG selbst – in Ausformung des Schuldprinzips – gefordert werde.[47]

Allerdings waren sich die Richter des Bundesverfassungsgerichts an dieser Stelle uneinig. Vier der Richter gingen davon aus, dass diese Art der Aufzeichnungen durchaus Teil des absolut geschützten Kernbereichs der privaten Lebensgestaltung seien, da sie ausschließlich innere Eindrücke und Gefühle wiedergäben, aber keinen unmittelbaren Bezug zur Straftat hätten.[48] Der Beschuldigte habe eine Auseinandersetzung mit dem eigenen Ich geführt, was vor fremden Augen und Ohren geschützt bleiben sollte.[49] Die Niederschrift enthalte keinerlei Hinweise auf die konkrete Straftat.[50] Außerdem sei die Unterscheidung zwischen Kernbereichsschutz und Abwägungsbereich praktisch aufgehoben, wenn davon ausgegangen werde, dass bereits Erkenntnisse über die Persönlichkeitsstruktur des Tatverdächtigten ausreichen, um den Schutz des Kernbereichs der privaten Lebensgestaltung zu versagen.[51] Denn wohl jede Information über die tatverdächtige Person sei in der Lage, Auskunft über die psychische Situation der Person zu geben.[52]

Dabei argumentieren diese anders urteilenden Richter damit, dass das Schuldprinzip lediglich besage, dass eine Person nur verurteilt werden dürfe, wenn ihre Schuld feststehe. Es könne aber nicht dazu genutzt werden, den

---

43 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 378 = NJW 1990, 563.
44 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 379 = NJW 1990, 563.
45 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 378 = NJW 1990, 563.
46 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 376, 377 = NJW 1990, 563.
47 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 379 = NJW 1990, 563.
48 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 382 = NJW 1990, 563.
49 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 381 = NJW 1990, 563.
50 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 382 = NJW 1990, 563.
51 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 382 = NJW 1990, 563.
52 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 382 = NJW 1990, 563.

Begriff des Kernbereichs der privaten Lebensgestaltung danach zu bestimmen, was zur Beantwortung der Schuldfrage vonnöten erscheine. Vielmehr müsse der Kernbereich von sich aus und vom „Personhaften“ her bestimmt werden. Alles andere führe zu einer Instrumentalisierung der Menschenwürde mittels des Schuldprinzips.[53]

Bereits hier ging das Bundesverfassungsgericht davon aus, dass es, um die Verwertbarkeit einer Information festzustellen, zunächst einer Kenntnisnahme und Durchsicht des Tagebuchs brauche. Allerdings sei dabei Zurückhaltung geboten.[54]

Zusammenfassend lässt sich sagen, dass der Kernbereich nach Ansicht des Bundesverfassungsgerichts zum einen nach dem Geheimhaltungswillen der betroffenen Person und zum anderen nach der Höchstpersönlichkeit des Inhalts der Aufzeichnung und der Art und Intensität, in der sie andere Belange und Bezüge der Gemeinschaft offenlegt, bestimmt werden kann. Eine Hälfte des Senats ging davon aus, dass straftatbezogene Aufzeichnungen nicht Teil des Kernbereichsschutzes seien. Straftatbezogene Aufzeichnungen können nach Ansicht dieser Richter auch jene Aufzeichnungen sein, die Teile der Persönlichkeit der beschuldigten Person offenlegen, da dies für die Beurteilung der Strafzumessung und der Schuld notwendig sei.[55]

Gem. § 15 Abs. 3 S. 3 BVerfGG a. F. führte eine Stimmengleichheit innerhalb des Senats damals noch dazu, dass ein Verstoß gegen das Grundgesetz nicht angenommen wurde. Eine solche Stimmengleichheit war bei diesem Urteil gegeben. Die abweichenden Richter gingen hingegen davon aus, dass Informationen, die nur mittelbaren Bezug zur Straftat aufweisen, nicht dem kernbereichsausschließenden Sozialbezug zuzuordnen seien.[56] Lasse man bereits den mittelbaren Bezug zu einer Straftat ausreichen und damit faktisch jede Information genügen, die Teile der Persönlichkeit der beschuldigten Person offenbart, dann sei der Kernbereich der privaten Lebensgestaltung im Kontext des Strafverfahrens hinfällig und entleert.[57] Dieser Ansicht ist zuzustimmen, dies darf durch den Schuldgrundsatz nicht ausgehebelt werden. Eine Information, der grundsätzlich ein kernbereichsrelevanter Charakter innewohnt, ist somit dann nicht dem Kernbereich privater Lebensgestaltung zuzuordnen, wenn sie einen unmittelbaren Straftatbezug aufweist. Dann weist die Information lediglich Sozialbezug auf.

---

[53] BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 383 = NJW 1990, 563.

[54] BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 375 = NJW 1990, 563.

[55] BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 378 = NJW 1990, 563.

[56] Vgl.: *Barrot*, Der Kernbereich privater Lebensgestaltung, S. 56; *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 62.

[57] So auch: *Barrot*, Der Kernbereich privater Lebensgestaltung, S. 56.

3. Verfassungsbeschwerde zur Wohnraumüberwachung

Eine weitere wichtige Entscheidung zum Kernbereich privater Lebensgestaltung ist ein Urteil des Bundesverfassungsgerichts aus dem Jahr 2004. Hier definierte und konkretisierte das Gericht den Begriff des Kernbereichs der privaten Lebensgestaltung nochmal näher. Auslöser war eine Verfassungsbeschwerde gegen die damals neu in die StPO eingeführte Ermittlungsmaßnahme des akustischen Lauschangriffs.

In dem Urteil stellte das Bundesverfassungsgericht fest, dass zur Unantastbarkeit der Menschenwürde die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung gehört.[58]

Nach Ansicht des Bundesverfassungsgerichts verletzt nicht jede akustische Überwachung von Wohnraum den Menschenwürdegehalt des Art. 13 Abs. 1 GG.[59] Eine Verletzung des Menschenwürdegehalts von Art. 13 Abs. 1 GG und Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG könne aber, abhängig von der Art und Weise der Durchführung der Maßnahme, zu einer Situation führen, in der die Menschenwürde verletzt werde.[60] Dem könne jedoch durch ausdrückliche rechtliche Regelungen entgegengewirkt werden.[61]

Die Menschenwürde als solche bedürfe als oberster Verfassungswert einer Konkretisierung. Dies geschehe in der Rechtsprechung durch die Ansehung des einzelnen Sachverhalts und der Bildung von Fallgruppen.[62] Der Begriff der Menschenwürde werde zumeist vom Verletzungsvorgang her beschrieben.[63] Derzeit bestimmten insbesondere Fragen des Schutzes der Identität und der psychisch-soziale Integrität die Auseinandersetzung über den Menschenwürdegehalt.[64] Der Mensch dürfe nicht zum bloßen Objekt der Staatsgewalt gemacht werden.[65] So dürfe ein*e Straftäter*in nicht unter Verletzung

---

[58] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279 = NJW 2004, 999.

[59] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279 = NJW 2004, 999.

[60] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 311 = NJW 2004, 999.

[61] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 311 = NJW 2004, 999.

[62] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 311 = NJW 2004, 999.

[63] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 312 = NJW 2004, 999.

[64] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 312 = NJW 2004, 999.

[65] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 312 = NJW 2004, 999.

seines*ihres verfassungsrechtlich geschützten sozialen Wert- und Achtungsanspruchs zum bloßen Objekt der Verbrechensbekämpfung und Strafvollstreckung gemacht werden.[66] Ein heimliches Vorgehen als solches untergrabe diesen Achtungsanspruch nicht.[67] Bei Beobachtungen sei aber ein unantastbarer Kernbereich privater Lebensgestaltung zu wahren.[68] Ein Eindringen in diesen Bereich sei nicht zu rechtfertigen.[69]

Zur Entfaltung der Persönlichkeit im Kernbereich der privaten Lebensgestaltung gehöre die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle, sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, und zwar ohne Angst, dass staatliche Stellen dies überwachen. Vom Schutz umfasst seien hiernach auch Gefühlsäußerungen, Äußerungen des unbewussten Erlebens sowie Ausdrucksformen der Sexualität. Dabei brauche auch die vertrauliche Kommunikation ein räumliches Substrat; dies erfordere einen absoluten Schutz des Verhaltens in diesen Räumen, nicht aber einen absoluten Schutz des Raumes selbst.[70] Dieser Schutz dürfe nicht relativiert werden.[71]

Die Maßnahme der akustischen Wohnraumüberwachung verstoße da gegen die Menschenwürde, wo der Kernbereich der privaten Lebensgestaltung nicht respektiert werde.[72] Ob der Kernbereich berührt werde, hier verweist das Bundesverfassungsgericht auf seine bestehende Rechtsprechung, hänge davon ab, ob der Inhalt höchstpersönlich sei. Dies stehe auch in Abhängigkeit dazu, inwieweit aus sich heraus auch die Sphäre anderer oder Belange der Gemeinschaft berührt werden.[73]

Art. 13 Abs. 3 GG beschreibe nicht ausdrücklich alle Grenzen, die es brauche, um den Kernbereich der privaten Lebensgestaltung absolut zu schüt-

---

[66] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 312 = NJW 2004, 999.

[67] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 313 = NJW 2004, 999.

[68] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 313 = NJW 2004, 999.

[69] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 313 = NJW 2004, 999.

[70] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 313, 314 = NJW 2004, 999.

[71] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 314 = NJW 2004, 999.

[72] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 314 = NJW 2004, 999.

[73] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 314 = NJW 2004, 999.

zen.[74] Erforderlich seien Regelungen, die unter Einhaltung der Normenklarheit sicherstellen, dass die Art und Weise der Durchführung der Maßnahme nicht zu einer Verletzung der Menschenwürde führe. Von vornherein müsse sichergestellt werden, dass die Maßnahme unterbleibe, wenn Anhaltspunkte bestehen, dass die Menschenwürde durch die Maßnahme verletzt würde. Führe die Maßnahme dann doch unerwartet zur Erhebung solcher Informationen, dann müsse sie abgebrochen werden und die Aufzeichnungen seien zu löschen. Eine Verwertung dieser Informationen im weiteren Strafverfahren sei ausgeschlossen.[75]

Ob zu erwarten sei, dass Informationen aus dem Kernbereich der privaten Lebensgestaltung erhoben werden, könne sich daraus ergeben, mit welcher Person der*die Betreffende kommuniziere und ob zu dieser Person ein besonderes Vertrauensverhältnis bestehe.[76] Eine Einschätzung sei aber auch bereits anhand der Art der Räumlichkeiten möglich[77] und danach, wer sich in dem zu überwachenden Raum aufhalte.[78]

Eine zeitliche und räumliche „Rundumüberwachung" sei regelmäßig schon deswegen ausgeschlossen, weil die Wahrscheinlichkeit groß sei, dass höchstpersönliche Gespräche abgehört würden.[79] Die Menschenwürde werde auch dann verletzt, wenn eine Überwachung sich über einen längeren Zeitraum erstrecke und so umfassend sei, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen der betroffenen Person registriert werden und zur Grundlage für ein Persönlichkeitsprofil gemacht werden können.[80]

Die damalige Ermächtigungsgrundlage der akustischen Wohnraumüberwachung und ihre Beweiserhebungs- und Verwertungsverbote tragen nach Ansicht des Bundesverfassungsgerichts dem Schutz des Kernbereichs der privaten Lebensgestaltung nicht in ausreichendem Maß Rechnung und seien aus

---

[74] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 316 = NJW 2004, 999.

[75] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 318 = NJW 2004, 999.

[76] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 319 = NJW 2004, 999.

[77] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 320, 321 = NJW 2004, 999.

[78] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 321 = NJW 2004, 999.

[79] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 323 = NJW 2004, 999.

[80] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 323 = NJW 2004, 999.

diesem Grund teilweise nicht mit der Verfassung vereinbar.[81] Der Vorschrift fehle es an einer Regelung, die den Abbruch der Maßnahme vorsehe, wenn in den absolut geschützten Kernbereich der privaten Lebensgestaltung eingegriffen werde. Dies ziehe auch Löschungspflichten und Verwertungsverbote nach sich.[82] Die Maßnahme müsse ganz unterbleiben, wenn Anhaltspunkte dafür bestehen, dass absolut geschützte Gespräche erfasst würden.[83]

Zusammenfassend lässt sich sagen, dass sich in dieser Entscheidung wesentliche Grundlagen für die spätere Rechtsprechung finden. Gleichzeitig wurde die bereits bestehende Rechtsprechung konkretisiert. So erfolgte die erste klare und eingängige Definition des Kernbereichs der privaten Lebensgestaltung, die auch heute die zumeist zitierte Definition darstellt.

Außerdem enthält das Urteil die wichtige Klarstellung, dass eine Ermittlungsmaßnahme nicht erfolgen darf, wenn von vornherein klar ist, dass die Würde des Menschen durch die Maßnahme verletzt würde.[84]

Weiterhin deutet sich bereits in diesem Urteil das später durch die Rechtsprechung zum IT-Grundrecht entwickelte zweistufige Schutzprinzip an. Auch bei der akustischen Wohnraumüberwachung kann es vorkommen, dass zunächst kernbereichsrelevante Informationen durch die Ermittlungsbehörden wahrgenommen werden.

> „Das mit der akustischen Wohnraumüberwachung verbundene Risiko des Eingriffs in den Kernbereich privater Lebensgestaltung kann verfassungsrechtlich nur hingenommen werden, wenn Vorkehrungen dagegen bestehen, dass keine weiteren Folgen aus ausnahmsweise erfolgten Verletzungen entstehen.“[85]

Hier formuliert das Bundesverfassungsgericht das erste Mal eine Inkaufnahme einer Verletzung des Kernbereichs der privaten Lebensgestaltung, wenn ein Verwertungsverbot besteht und eine Löschung erfolgt.

In Bezug auf die Rundumüberwachung bezieht das Bundesverfassungsgericht ebenfalls Stellung. Dabei geht es davon aus, dass eine Verletzung der Menschenwürde gegeben ist, wenn sich die Maßnahme über einen längeren Zeitraum erstreckt und in der Lage ist, nahezu lückenlos alle Bewegungen

---

[81] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 325 = NJW 2004, 999.

[82] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 328 = NJW 2004, 999.

[83] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 328 = NJW 2004, 999.

[84] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 318 = NJW 2004, 999.

[85] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 331 = NJW 2004, 999.

und Lebensäußerungen des*der Betroffenen zu registrieren, welche dann zur Grundlage für ein Persönlichkeitsprofil gemacht werden können.[86]

Die Richterinnen *Jaeger* und *Hohmann-Dennhardt* stellten in ihrer abweichenden Meinung allerdings fest, dass bei einer Privatwohnung zwar vermutet werden könne, dass in einen höchstpersönlichen Bereich eingedrungen werde. Allerdings erhalte man die Gewissheit erst, wenn die Abgeschlossenheit der Wohnung durchbrochen werde und man sich Kenntnis von dem verschaffe, was in ihr vorgehe. Dies habe zur Folge, dass zunächst ein Eingriff in den Kernbereich hingenommen werde, was Art. 79 Abs. 3 GG gerade verhindern wolle. Deswegen sei zumindest für Privatwohnungen, in denen der*die Beschuldigte sich mit Familienmitgliedern oder mit ersichtlich engen Vertrauten aufhalte, zu unterstellen, dass sie Raum für höchstpersönliche Kommunikation bieten. Aus diesem Grund genießen sie, dieser Meinung zufolge, umfassenden Schutz.[87]

4. Urteil zum IT-Grundrecht

Im Jahr 2008 beschäftigte sich das Bundesverfassungsgericht das erste Mal mit der Ermächtigungsgrundlage der Online-Durchsuchung. Das Urteil hatte eine Verfassungsbeschwerde gegen die Ermächtigungsgrundlage der Online-Durchsuchung im Verfassungsschutzgesetz NRW zum Gegenstand. Dabei erklärte das Bundesverfassungsgericht die Ausgestaltung der Ermächtigungsgrundlage für verfassungswidrig und nichtig.[88] Bekanntheit erlangt hat dieses Urteil insbesondere, weil hier das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht) präsentiert wurde. In dieses greife die Online-Durchsuchung ein.[89] Aber auch der Schutz des Kernbereichs privater Lebensgestaltung fand in diesem Urteil Berücksichtigung, indem das Gericht das für die Online-Durchsuchung einschlägige „zweistufige Schutzkonzept“ entwickelte.

Grundsätzlich müsse die Ermächtigungsgrundlage der Online-Durchsuchung Vorkehrungen zum Schutz des Kernbereichs der privaten Lebensgestaltung enthalten.[90] Für die Definition des Kernbereichs der privaten Le-

---

[86] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 323 = NJW 2004, 999.

[87] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 383, 384 = NJW 2004, 999.

[88] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 302 = NJW 2008, 822.

[89] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 302 = NJW 2008, 822.

[90] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 335 = NJW 2008, 822.

bensgestaltung griff das Bundesverfassungsgericht auf jene zurück, die es bereits im zuvor dargestellten Urteil zum großen Lauschangriff entwickelt hatte. Bei einem heimlichen Zugriff auf ein informationstechnisches System bestehe die Gefahr, dass solche Daten erhoben werden, die dem Kernbereich der privaten Lebensgestaltung zuzuordnen seien. Beispielhaft zählte das Gericht hier tagebuchähnliche Aufzeichnungen oder private Film- oder Tondokumente auf.[91]

Die Anforderungen der Verfassung an die konkrete Ausgestaltung des Kernbereichsschutzes hänge von der Art der Informationserhebung ab.[92]

Zunächst sei nach Möglichkeit sicherzustellen, dass Daten mit Kernbereichsbezug nicht erhoben werden. Geschehe dies dennoch, müsse dem auf der Auswertungsebene entgegengetreten werden. Die aufgefundenen und erhobenen Daten seien dann unverzüglich zu löschen und nicht verwertbar.[93] Der Kernbereichsschutz führe bereits bei der Datenerhebung zu praktischen Schwierigkeiten, denn es sei bei vielen Informationen unvorhersehbar (das Gericht nennt als Beispiel die Sprachtelefonie), welchen Inhalt die erhobenen Daten haben werden.[94] In solchen Fällen fordere die Verfassung aber nicht, den Zugriff aufgrund des Risikos von vornherein auf der Erhebungsebene zu unterlassen.[95] Denn der Kernbereichsschutz lasse sich in einem zweistufigen Schutzkonzept gewährleisten.[96] Die gesetzliche Regelung habe zunächst darauf hinzuwirken, dass die Erhebung solcher kernbereichsrelevanter Daten möglichst unterbleibe. Wenn es Anhaltspunkte dafür gebe, dass eine bestimmte Datenerhebung zu einer Berührung mit dem Kernbereich der privaten Lebensgestaltung führe, habe diese zu unterbleiben.[97] Zumeist werde sich dies aber vor oder während der Datenerhebung nicht klären lassen. Aus diesem Grund müsse ein geeignetes Verfahren entwickelt werden, welches in der Lage sei, den Belangen des*der Betroffenen hinreichend Rechnung zu

---

91 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 335 = NJW 2008, 822.

92 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 337 = NJW 2008, 822.

93 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 337 = NJW 2008, 822.

94 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 337, 338 = NJW 2008, 822.

95 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 338 = NJW 2008, 822.

96 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 338 = NJW 2008, 822.

97 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 338 = NJW 2008, 822.

tragen.[98] Wenn sich bei der Durchsicht ergebe, dass kernbereichsrelevante Daten erhoben worden seien, seien diese unverzüglich zu löschen. Eine Weitergabe oder Verwertung der Daten sei auszuschließen.[99]

Zwar hat das Bundesverfassungsgericht erneut festgestellt, dass der Kernbereichsschutz keiner Relativierung zugänglich ist,[100] dennoch enthält dieses Urteil mit der Entwicklung des zweistufigen Schutzkonzepts eine ebensolche Relativierung. Das Gericht nimmt mit der Einräumung der Möglichkeit der Erhebung von kernbereichsrelevanten Daten während der Durchführung der Online-Durchsuchung eine Kenntnisnahme von kernbereichsrelevanten Informationen bewusst in Kauf. Damit sind diese Daten der Staatsgewalt nicht mehr schlichtweg entzogen. Außerdem findet sich in dem zweistufigen Schutzkonzept nahezu keine Begrenzung der Daten auf der Erhebungsebene, sodass davon auszugehen ist, dass die Gefahr der Bildung von Persönlichkeitsprofilen bei dem Schutzkonzept unberücksichtigt geblieben ist.

5. Urteil zum BKAG

Ein weiteres Urteil, welches sich mit dem Kernbereich der privaten Lebensgestaltung beschäftigte, stammt aus dem Jahr 2016 und hatte ebenfalls die Online-Durchsuchung zum Gegenstand. Der Gesetzgeber hatte sich zunächst der Vorgaben des Urteils zum IT-Grundrecht angenommen und diese in einer Ermächtigungsgrundlage zur Online-Durchsuchung im BKAG umgesetzt.

Hier bekräftigte das Gericht erneut das bereits 2008 entwickelte zweistufige Schutzkonzept.[101]

Außerdem stellte es fest, dass der Schutz des Kernbereichs der privaten Lebensgestaltung nicht relativiert werden dürfe.[102] Dies bedeute jedoch nicht, dass jede tatsächliche Erfassung von höchstpersönlichen Informationen stets einen Verfassungsverstoß und eine Menschenrechtsverletzung begründe. Ein unbeabsichtigtes Eindringen in den Kernbereich könne nicht für jeden Fall von vornherein ausgeschlossen werden. Die Verfassung verlange für die Aus-

---

98 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 339 = NJW 2008, 822.

99 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 339 = NJW 2008, 822.

100 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 339 = NJW 2008, 822.

101 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220 = NJW 2016, 1781.

102 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 278 = NJW 2016, 1781.

gestaltung der Überwachungsbefugnisse eine Achtung des Kernbereichs als eine strikte, nicht frei durch Einzelfallerwägungen überwindbare Grenze.[103]

Hierfür müsse zum einen absolut ausgeschlossen werden, dass der Kernbereich zum Ziel staatlicher Ermittlungsmaßnahmen gemacht werde und diese Informationen in irgendeiner Weise verwertet oder zur Grundlage von Ermittlungen werden.[104]

Die Durchführung der Ermittlungsmaßnahme müsse zum anderen dem Kernbereichsschutz auf zwei Ebenen Rechnung tragen.[105] Auf der ersten Ebene müsse nach Möglichkeit sichergestellt werden, dass kernbereichsrelevante Daten nicht erhoben werden. In jedem Fall sei der Abbruch der Maßnahme vorzusehen, wenn erkennbar werde, dass eine Überwachung in den Kernbereich privater Lebensgestaltung eindringen werde.[106] Auf der zweiten Ebene sei dann eine Auswertung und Verwertung durch eine unabhängige Stelle vorzunehmen, die über die Löschung und Verwertbarkeit der höchstpersönlichen Daten entscheide.[107]

Außerdem stellte das Gericht erneut fest, dass es mit der Menschenwürde unvereinbar sei, wenn sich die Überwachung über einen längeren Zeitraum erstrecke und so umfassend sei, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des*der Betroffenen registriert werden und so zur Grundlage eines Persönlichkeitsprofils gemacht werden können. Beim Einsatz moderner und heimlicher Ermittlungsmaßnahmen müssten die Sicherheitsbehörden mit Rücksicht auf das dem additiven Grundrechtseingriff innewohnenden Gefährdungspotenzial handeln und sie hätten Sorge dafür zu tragen, dass die Überwachung insgesamt beschränkt bleibe.[108]

---

[103] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 278 = NJW 2016, 1781.

[104] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 278 = NJW 2016, 1781.

[105] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 278, 279 = NJW 2016, 1781.

[106] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 279 = NJW 2016, 1781.

[107] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 280 = NJW 2016, 1781.

[108] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 280 = NJW 2016, 1781.

III. Analyse der Rechtsprechung im Hinblick auf die Gefahr der Bildung von Persönlichkeitsprofilen

Die historische Entwicklung des Kernbereichs privater Lebensgestaltung lässt sich in zwei Phasen einteilen. Die erste Phase geht bis zur Entscheidung über die akustische Wohnraumüberwachung und entwickelte eine Definition des Begriffs des Kernbereichs privater Lebensgestaltung. Demnach gehört zum Kernbereich der privaten Lebensgestaltung „(…) die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, und zwar ohne die Angst, dass staatliche Stellen dies überwachen."[109]

In einer zweiten Phase, die mit dem Urteil zur akustischen Wohnraumüberwachung beginnt, entwickelte das Bundesverfassungsgericht das zweistufige Schutzkonzept, mit dem es sich von der ursprünglichen Idee eines absolut geschützten Kernbereichs privater Lebensgestaltung entfernte und eine Begrenzung der Erhebung der Daten weitestgehend auf Verwertungsebene vornahm.

Für die Gefahr der Bildung von Persönlichkeitsprofilen als Teil der Kernbereichs ergibt sich aus dem zweistufigen Schutzkonzept insbesondere ein Problem: Die mangelnde Begrenzung der Daten. Es erfolgt keine Begrenzung der Daten auf Ebene der Erhebung – mit der fernliegenden Ausnahme, es werden allein kernbereichsrelevante Daten erhoben, was bei Anwendung der Rechtsprechung des Bundesverfassungsgerichts nie der Fall sein dürfte –, sodass der Erhebung einer solchen Menge an Daten, die ein Persönlichkeitsprofil ermöglichen, keine klaren Grenzen gesetzt werden.

Nach dem zweistufigen Schutzkonzept erfolgt eine Begrenzung der Daten bei der Frage nach der strafprozessualen Verwertbarkeit. Eine solche Beurteilung der Zuweisung zum Kernbereich erfolgt, anders als man sich es erhoffen würde, nicht auf Grundlage der Menge der bereits erhobenen Daten, sondern es wird punktuell kontrolliert, ob einzelne Daten beziehungsweise Informationen dem Kernbereich privater Lebensgestaltung zu zuordnen sind. Wie zuvor dargelegt, verkennt das Bundesverfassungsgericht in Gänze, dass bereits die gesamte Menge der Daten, wenn die Gefahr der Bildung von Persönlichkeitsprofilen besteht, dem Kernbereich privater Lebensgestaltung angehört.

Mit dieser Rechtsprechungsentwicklung hat sich das Bundesverfassungsgericht weitestgehend von seiner ursprünglichen Idee des Kernbereichs entfernt. Diese umfasste, dass die Feststellung, ob es sich um einen Sachverhalt

[109] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 313 = NJW 2004, 999.

handelt, der in den Kernbereich eingreift, sich nach seinem persönlichen Charakter und der Art der Intensität beurteilt,[110] dass der Mensch notwendigerweise in seinen sozialen Bezügen existiert[111] und der Kernbereich das ist, was das Wesen des Menschen als geistig-sittliche Person ausmacht[112], wozu letztlich auch die Auseinandersetzung mit dem eigenen Ich gehört.[113]

Die Annahme, die Bewertung eines Eingriffs in den Kernbereich der privaten Lebensgestaltung lasse sich nicht allein anhand einer einzelnen Information vornehmen, sondern könne auch in der Kontextualisierung mehrere Daten erfolgen, ist nach damaliger Rechtsprechung denkbar gewesen und in Ansätzen bereits erfolgt.[114]

Auch wenn das Bundesverfassungsgericht in seiner Rechtsprechung die Gefahren für die Bildung von Persönlichkeitsprofilen anhand der erhobenen Menge der Daten erkannt hat,[115] so ist es nicht gewillt, diese Gefahr auf Erhebungsebene im zweistufigen Schutzkonzept zu berücksichtigen, sondern weist lediglich auf diese Gefahr hin, ohne effektiven Schutz zu fordern oder zu schaffen.

Das Bundesverfassungsgericht verkennt somit in all seinen Entscheidungen, dass die Gefahr der Bildung von Persönlichkeitsprofilen dem Kernbereich privater Lebensgestaltung zuzuordnen ist. Der Maßstab des Bundesverfassungsgerichts für die Gefahr der Bildung von Persönlichkeitsprofilen ist somit auf das zweistufige Schutzkonzept begrenzt und eine weitere Begrenzung der Datenmenge erfolgt nicht.

IV. Weitreichender Maßstab über Art. 1 Abs. 1 GG als das zweistufige Schutzkonzept des Bundesverfassungsgerichts

Da das zweistufige Schutzkonzept keine Begrenzung der Daten auf der Erhebungsebene, mit Ausnahme der alleinigen Erhebung von kernbereichsre-

---

110 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 373, 374 = NJW 1990, 563.

111 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 374 = NJW 1990, 563.

112 BVerfG 16.01.1957 – 1 BvR 253 56, BVerfGE 6, 32, 36.

113 BVerfG 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367, 381 = NJW 1990, 563.

114 Wie beispielsweise in: BVerfG 15.12.1983 – 1 BvR 209/83 u. a., BVerfGE, 65, 1, 45 = NJW 1984, 419.

115 BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 323 = NJW 2004, 999. BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 280 = NJW 2016, 1781.

levanten Daten durch eine Online-Durchsuchung, vorsieht, ist nunmehr ein Maßstab zu entwickeln, an dem sich Verfahrensvorschriften zum Schutz des Kernbereichs privater Lebensgestaltung messen lassen müssen.

Unabhängig von der Frage, ob die Gefahr der Bildung von Persönlichkeitsprofilen dem Kernbereich zuzuordnen ist oder aber seine Grundlage direkt in der Menschenwürde liegt, besteht Einigkeit darüber, dass die Gefahr der Bildung von Persönlichkeitsprofilen an Art. 1 Abs. 1 GG zu messen ist.

Zutreffend geht das Bundesverfassungsgericht davon aus, dass sich der Schutz des Kernbereichs privater Lebensgestaltung aus dem Menschenwürdekern des jeweils betroffenen Grundrechts ergibt.[116] Das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG schützt den*die Einzelne vor der Erhebung, Kenntnisnahme, Speicherung, Verwendung, Weitergabe und Veröffentlichung von persönlichen Daten[117] und damit auch vor der Erhebung von Daten mittels der Online-Durchsuchung. Darüber hinaus ist die betroffene Person bei einer Online-Durchsuchung auch in seinem IT-Grundrecht verletzt. Aus dem Menschenwürdekern der informationellen Selbstbestimmung und dem IT-Grundrecht ergibt sich somit der Kernbereich privater Lebensgestaltung, der die Gefahr der Bildung von Persönlichkeitsprofilen bei der Online-Durchsuchung mitumfasst.

Wie zuvor dargelegt, erkennt das Bundesverfassungsgericht zutreffend, dass die Gefahr der Bildung von Persönlichkeitsprofilen nicht bestehen darf und gegen die Menschenwürde verstößt,[118] belässt es jedoch bei dieser vagen Formulierung.

Im ersten Kapitel wurde dargelegt, dass die Gefahr der Bildung von Persönlichkeitsprofilen dann besteht, wenn im Rahmen der konkreten Maßnahme eine solche Menge an Daten generiert werden kann, dass die Möglichkeit besteht, dass eine konkrete Beschreibung der Person ermöglicht und ihre Individualität offengelegt wird.

Da die Menschenwürde unantastbar ist und der Kernbereich privater Lebensgestaltung absolut – wobei hier angemerkt sei, dass diese Absolutheit mit dem zweistufigen Schutzkonzept doch erheblich ins Wanken geraten ist – geschützt ist, darf der Fall, dass die Möglichkeit einer Profilbildung

---

116 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 276 = NJW 2016, 1781.

117 Vgl. mit weiteren Nachweisen aus der Rechtsprechung: *Di Fabio*, in: Dürig/Herzog/Scholz, Kommentar zum Grundgesetz, Art. 2 Abs. 1 Rdnr. 176.

118 BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 323 = NJW 2004, 999; BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 280 = NJW 2016, 1781.

besteht, schlichtweg nicht eintreten. Es ist mit Art. 1 Abs. 1 GG unvereinbar, wenn die Gefahr der Bildung von Persönlichkeitsprofilen besteht.

Zur Absicherung dieses Rechts einer einzelnen Person braucht es Sicherungen, die einer solchen Gefahr vorbeugen. Die Gefahr der Bildung von Persönlichkeitsprofilen – und das verkennt das Bundesverfassungsgericht in seinen Entscheidungen gänzlich – besteht bereits auf der Erhebungsebene. Art. 1 Abs.1 GG fordert, dass eine solche Menge an Daten, die die Gefahr der Bildung von Persönlichkeitsprofilen ermöglicht, nicht erhoben wird.

Aus diesem Grund darf der Kernbereich nicht nur punktuell durch die Vermeidung der Verwertung einzelner Daten geschützt werden, sondern es braucht darüber hinaus eine normierte Begrenzung der Menge der Daten auf der Ebene der Datenerhebung beim Kernbereich privater Lebensgestaltung, um der Gefahr der Bildung von Persönlichkeitsprofilen wirksam begegnen zu können.

An dieser Stelle muss beim Bundesverfassungsgericht ein Umdenken stattfinden. Konsequenterweise kann im Rahmen einer Verfassungsbeschwerde zur Online-Durchsuchung die Gefahr der Bildung von Persönlichkeitsprofilen gem. Art. 2 Abs. 1, Art. 1 Abs. 1 GG gerügt werden, wenn die in Rede stehende Maßnahme in der Lage war, ein Persönlichkeitsprofil zu bilden. Der alleinige Verweis darauf, dass ein solche Gefahr nicht bestehen darf, reicht nicht aus und wird einem effektiven Menschenwürdeschutz nicht gerecht.

V. Gefahrenbegriff

Unklar ist, ab wann die „Gefahr" besteht, dass ein Persönlichkeitsprofil gebildet werden kann. Grundsätzlich ist es in einem Strafverfahren unumgänglich, Teile der Persönlichkeit offenzulegen. Dies ist ein wesentlicher Teil von Ermittlungsarbeit. Gerade für die Darlegung eines Motives oder für die Strafzumessung wird es sich oftmals nicht vermeiden lassen, auch Eigenschaften der betroffenen Person herauszuarbeiten. Wichtig ist an dieser Stelle allerdings, dass dabei kein vollständiges Abbild der Persönlichkeit geschaffen wird, sondern nur Anteile einer Persönlichkeit dargestellt werden.[119]

Dies darf nach zutreffender Ansicht des Bundesverfassungsgerichts nur bis zur Grenze eines kompletten Persönlichkeitsprofils erfolgen.[120]

---

[119] Davon ausgehend, dass sich im Strafverfahren mit der ganzen Persönlichkeit auseinandergesetzt wird: *Benda*, in: FS Geiger, S. 42.

[120] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 280 = NJW 2016, 1781; BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 323 = NJW 2004, 999.

Grundsätzlich sind alle Informationen in der Lage, Grundlage eines Persönlichkeitsprofils zu werden. Bei der Gefahr der Persönlichkeitsprofilbildung geht es um den Umfang der erhobenen Informationen.

Der Begriff der Gefahr meint nicht die tatsächliche Anordnung, also die formale Ermächtigung zur Erhebung der Daten zur Schaffung eines Persönlichkeitsprofils.[121] Der Begriff der Gefahr beinhaltet die konkrete Gefahr im Einzelfall. Denn die abstrakte Gefahr der Bildung von Persönlichkeitsprofilen wohnt der Online-Durchsuchung als solcher bereits inne. Diese ist jedoch auch bei anderen Ermittlungsmaßnahmen denkbar, insbesondere wenn mehrere Maßnahmen nebeneinander angeordnet werden. Aus diesem Grund bedarf es einer konkreten Gefahr, es muss also verhindert werden, dass in einem solchen Umfang Daten erhoben werden, dass anhand deren ein Persönlichkeitsprofil erstellt werden kann.

Besteht im Einzelfall eine konkrete Gefahr, dass eine solche Menge an Daten erhoben wird, dass ein umfassendes Persönlichkeitsprofil erstellt werden kann, welches nicht nur einzelne Eigenschaften der Persönlichkeit abbildet, sondern die Gesamtpersönlichkeit widerspiegelt, dann besteht die Gefahr der Bildung eines Persönlichkeitsprofils.

Somit kommt es wesentlich auf die Menge der Daten an, die erhoben werden. Um der Gefahr der Bildung von Persönlichkeitsprofilen effektiv entgegentreten zu können, müssen sich Sicherungen finden, die bereits der Erhebung von Daten Grenzen setzen. Sicherungsvorschriften auf Ebene der Verwertung können eine konkrete Gefahr der Bildung von Persönlichkeitsprofilen nicht mehr verhindern.

Rechtsmaßstab einer Maßnahme, die im Einzelfall eine konkrete Gefahr der Bildung von Persönlichkeitsprofilen ermöglicht, ist der sich aus Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 GG – in Gestalt des IT-Grundrechts – ergebene Kernbereich privater Lebensgestaltung. Hiernach muss die Menge der erhobenen Daten, abgesichert durch verfahrensrechtliche Vorschriften, soweit begrenzt werden, dass die konkrete Gefahr der Bildung von Persönlichkeitsprofilen zu keinem Zeitpunkt im Verfahren besteht.

B. Unionsrechtlicher Maßstab

Nachdem dargestellt wurde, wie es sich mit dem Schutz der höchstpersönlichen Daten auf Grundrechtsebene verhält, ist zu überlegen, inwieweit dieser Schutz der höchstpersönlichen Daten durch europarechtliche Erwägungen

[121] A.A. wohl: *Hauck*, Heimliche Strafverfolgung und Schutz der Privatheit, S. 280.

ergänzt oder überlagert wird und die Gefahr der Bildung von Persönlichkeitsprofilen auf unionrechtlicher Ebene Berücksichtigung findet.

Hierfür wird zunächst dargestellt, inwieweit die Grundrechtecharta überhaupt in verfassungsrechtliche Fragen eingebunden werden kann.

In einem nächsten Schritt wird sodann geprüft, wie durch die Gefahr der Bildung von Persönlichkeitsprofilen in die Grundrechtecharta eingegriffen wird, ob ein möglicher Eingriff gerechtfertigt werden kann und welches europäische Sekundärrecht Einfluss auf die Gefahr der Bildung von Persönlichkeitsprofilen bei der strafprozessualen Online-Durchsuchung nimmt.

Am Ende des Kapitels wird dann dargelegt, warum das vom Bundesverfassungsgericht entwickelte Schutzniveau bei der Online-Durchsuchung hinter dem des Europäischen Gerichtshofs zurückbleibt, sodass die Grundrechtecharta direkte Anwendung findet.

I. Möglichkeiten zur Einbeziehung des Unionsrechts

Die Frage nach dem Verhältnis zwischen den Grundrechten des Grundgesetzes und dem Unionsrecht hat das Bundesverfassungsgericht in seinen Entscheidungen zum „Recht auf Vergessen I und II“ behandelt.

Geht es bei dem zu beurteilenden Sachverhalt um einen solchen, bei dem auf die Wirksamkeit oder die Gültigkeit von Unionsrecht ankommt, dann obliegt diese Entscheidung gem. Art. 267 Abs. 3 AEUV dem Europäischen Gerichtshof.[122] Kommt es hierauf nicht an, ist zwischen zwei Optionen der Einbeziehung von Unionsrecht in das Grundgesetz zu unterscheiden. Zum einen ist die direkte Anwendung, aufgrund des Anwendungsvorrangs des Europarechts, in Form der Unionsgrundrechte möglich[123] oder die Grundrechte des Grundgesetzes sind im Licht der Grundrechtecharta auszulegen.[124]

Die unmittelbare Anwendung von Unionsgrundrechten kommt zum einen dann in Betracht, wenn der Europäische Gerichtshof deren Auslegung bereits geklärt hat oder die anzuwendenden Rechtsgrundsätze aus sich heraus offenkundig sind.[125] Wesentliches Unterscheidungskriterium ist, ob es sich bei dem in Rede stehenden Sachverhalt um einen solchen handelt, der vollständig vereinheitlichtes Unionsrecht betrifft, dann kann eine unmittelbare Anwendung der Unionsgrundrechte erfolgen, oder gestaltungsoffenes Unions-

122 BVerfG 06.11.2019 – 1 BvR 16/13, BVerfGE 152, 152, 182 = NJW 2020, 300.

123 BVerfG Beschl. 06.11.2019 – 1 BvR 276/17, BVerfGE 152, 216 = NJW 2020, 314.

124 BVerfG 06.11.2019 – 1 BvR 16/13, BVerfGE 152, 152 = NJW 2020, 300.

125 BVerfG Beschl. 06.11.2019 – 1 BvR 276/17, BVerfGE 152, 216, 244 = NJW 2020, 314.

recht, dann kommt nur eine Auslegung der grundgesetzlichen Grundrechte im Lichte des Unionsrechts in Betracht.[126] Indiz hierfür kann sein, ob der europäische Gesetzgeber eine Regelung mittels Verordnung oder Richtlinie geschaffen hat. Grundsätzlich kann bei der Verabschiedung einer Richtlinie durch den europäischen Gesetzgeber davon ausgegangen werden, dass dieser keine vollständige Vereinheitlichung von Regelungsstandards anstrebte, sondern den Mitgliedstaaten Gestaltungsfreiräume belassen wollte.[127] Auch der Wortlaut der entsprechenden unionsrechtlichen Norm kann Aufschluss darüber geben, ob sie auf die Ermöglichung von Vielfalt und der Geltendmachung verschiedener Wertungen abzielt – keine unmittelbare Anwendung – oder aber von dem Ziel einer gleichförmigen Rechtsanwendung getragen ist.[128]

Dennoch bleiben die Grundrechte des Grundgesetzes hinter dem Unionsrecht, aufgrund des Anwendungsvorrangs, ruhend in Kraft.[129] Sie können nur insoweit durch das Unionsrecht überlagert werden, als deren Schutzversprechen in der Substanz erhalten bleibt.[130] Über Art. 23 Abs. 1 GG lässt sich die Prüfungskompetenz des Bundesverfassungsgerichts ableiten zu untersuchen, ob ein deutsches Fachgericht vollvereinheitlichtes Unionsrecht richtig angewendet hat.[131]

Zum anderen kann eine unmittelbare Prüfung der Grundrechtecharta dann geboten sein, wenn Anhaltspunkte dafür bestehen, dass ausnahmsweise die grundgesetzlichen Grundrechte den Schutz des Unionsrechts nicht gewährleisten und das zu prüfende innerstaatliche Recht der Durchführung des Unionsrechts dient.[132] Die grundsätzliche Vermutung der Mitgewährung von Unionsrecht durch die grundgesetzlichen Grundrechte greift dann nicht mehr, wenn und soweit das maßgebliche Schutzniveau keine Entsprechung im Grundgesetz und seiner Auslegung durch die Rechtsprechung hat.[133]

Eine mittelbare Einbeziehung von unionsrechtlichen Erwägungen in die grundgesetzlichen Grundrechte kommt nebstdem bei gestaltungsoffenem

---

126 BVerfG Beschl. 06.11.2019 – 1 BvR 276/17, BVerfGE 152, 216, 246 = NJW 2020, 314.

127 BVerfG Beschl. 06.11.2019 – 1 BvR 276/17, BVerfGE 152, 216, 231 = NJW 2020, 314.

128 BVerfG Beschl. 06.11.2019 – 1 BvR 276/17, BVerfGE 152, 216, 247 = NJW 2020, 314.

129 BVerfG Beschl. 06.11.2019 – 1 BvR 276/17, BVerfGE 152, 216, 235 = NJW 2020, 314.

130 BVerfG Beschl. 06.11.2019 – 1 BvR 276/17, BVerfGE 152, 216, 235 = NJW 2020, 314.

131 BVerfG Beschl. 06.11.2019 – 1 BvR 276/17, BVerfGE 152, 216, 237 f. = NJW 2020, 314.

132 BVerfG 06.11.2019 – 1 BvR 16/13, BVerfGE 152, 152, 179 = NJW 2020, 300.

133 BVerfG 06.11.2019 – 1 BvR 16/13, BVerfGE 152, 152, 181 = NJW 2020, 300.

Unionsrecht in Betracht. Danach sind die Grundrechte im Lichte der Charta und der EMRK auszulegen. Dies ergibt sich aus der Völker- und Europarechtsfreundlichkeit des Grundgesetzes gem. Art. 1 Abs. 2, 23 Abs. 1, 24, 25, 26, 59 Abs. 2 GG, denn bei der Auslegung und der Fortentwicklung des Grundrechtsschutzes sind der internationale Menschenrechtsschutz und die europäische Grundrechtstradition zu berücksichtigen.[134]

Diese Grundsätze hat das Bundesverfassungsgericht für Konstellationen zwischen Dritten entwickelt, bei denen die Grundrechte beziehungsweise. die Grundrechtecharta zwischen den Bürger*innen im Wege der mittelbaren Drittwirkung ihre Wirkung entfalten. Da es sich hierbei um allgemeine Grundsätze zur Wirkung des Unionsrechts auf die grundgesetzlichen Grundrechte geht, steht nicht zu befürchten, dass diese in einem Verhältnis zwischen Bürger*innen und Staat anders ausfallen würden.

Zusammenfassend lässt sich somit sagen, dass es für die unmittelbare Anwendung von Unionsgrundrechten zur Prüfung der Verfassungsmäßigkeit einer Norm oder eines Einzelfalls unionsrechtlich vollständig vereinheitlichte Regelungen braucht oder das unionsrechtliche Schutzniveau über das grundrechtliche Schutzniveau hinausgehen muss.

In den übrigen Fällen sind die grundgesetzlichen Grundrechte im Lichte der Charta und der EMRK völker- und europarechtsfreundlich auszulegen.

II. Verstoß gegen Unionsrecht: Die Gefahr der Bildung von Persönlichkeitsprofilen bei der Online-Durchsuchung

In einem nächsten Schritt muss somit gefragt werden, ob bei der Frage nach dem Schutz des*der Einzelnen vor der Gefahr der Bildung von Persönlichkeitsprofilen auf europarechtlicher Ebene im Rahmen einer verfassungsrechtlichen Prüfung Unionsrecht direkt anzuwenden ist oder ob die im vorherigen Kapitel dargelegten grundrechtlichen Gewährleistungen im Lichte dessen auszulegen sind. Eine direkte Anwendung kommt dann in Betracht, wenn es sich beim Schutz vor der Gefahr der Bildung von Persönlichkeitsprofilen im Rahmen der Ermittlungsmaßnahme der Online-Durchsuchung um einen offenkundigen unionsrechtlichen Rechtssatz handelt oder das Schutzniveau des Unionsrechts keine grundrechtliche Entsprechung hat.

[134] BVerfG 06.11.2019 – 1 BvR 16/13, BVerfGE 152, 152, 177 = NJW 2020, 300.

1. Art. 8, 7 Grundrechte Charta

Die Gefahr der Bildung von Persönlichkeitsprofilen bei der Online-Durchsuchung muss sich im Wesentlichen an Art. 8 GRC i. V. m. Art. 7 GRC messen lassen.[135]

Art. 8 GRC schützt, wie auch Art. 16 AEUV, die personenbezogenen Daten. Zu den personenbezogenen Daten gehören alle Informationen die der Privatsphäre, einschließlich der Intimsphäre, zuzuordnen sind.[136]

Ein Eingriff in den Schutzbereich ist dann gegeben, wenn eben diese Daten verarbeitet werden.[137] Ein Verarbeitungsprozess umfasst die Erhebung, Speicherung, Benutzung, Sperrung oder Löschung von personenbezogenen Daten.[138] Wie bereits zuvor dargestellt, ist die Verarbeitung von personenbezogenen Daten gerade primäres Ziel der Online-Durchsuchung. Durch sie entstehen erhebliche Datenmengen, wie im zweiten Kapitel bereits dargestellt. Bei einem solchen Verarbeitungsprozess können durch eine Gesamtbetrachtung der Daten genaue Schlüsse auf das Privatleben der betroffenen Person gezogen werden, wie auf die Gewohnheiten des täglichen Lebens oder das soziale Umfeld. Dies stellt einen besonders schwerwiegenden Eingriff in Art. 8 GRC i. V. m. Art. 7 GRC dar, da dieser Eingriff bei der betroffenen Person das Gefühl erzeugen kann, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist.[139] Diese Möglichkeit der Erstellung eines Profils der betroffenen Person stellt eine genauso sensible Information dar wie der Inhalt einer Kommunikation selbst.[140] Die Speicherung von Verkehrs- und Standortdaten kann eine Vielzahl von Informationen wie sexuelle

---

135 Art. 7 und Art. 8 GRC stehen nach der Rechtsprechung des EuGH dabei wohl in Idealkonkurrenz nebeneinander, während ein Teil der Literatur davon ausgeht, dass Art. 8 GRC lex specialis ist. Siehe mit weiteren Nachweisen: *Bernsdorff*, in: NK Charta der Grundrechte der Europäischen Union, Art. 8 Rn. 13; *Wolff*, in: Frankfurter Kommentar EUV GRC AEUV, Art. 8 GRC Rn. 3, 62.

136 EuGH 13.01.2010 – C-92/09 – Schecke, Slg. 2020, I – 11063 Rn. 52 = EuZW 2010, 939.

137 EuGH 13.01.2010 – C-92/09 – Schecke, Slg. 2020, I – 11063 Rn. 52 = EuZW 2010, 939.

138 *Jarass*, in: Jarass, Charta der Grundrechte der Europäischen Union, Art. 8 Rn. 9; *Wolff*, in: Frankfurter Kommentar EUV GRC AEUV, Art. 8 GRC Rn.19.

139 EuGH 08.04.2014 – C-293/12, C-594/12 – Digital Rights Irland Ltd und Seitlinger u. a. Rn. 26 f, 37 = NJW 2014, 2169; EuGH 21.12.2016 – C-203/15, C-698/15 – ele2 Sverige AB/Post- och telestyrelsen und Secretary of State for the Home Department/Watson u. a. Rn. 100 = NJW 2017, 717; EuGH 06.10.2020 – C-623/17 – privacy International Rn. 71 = GSZ 2021, 36.

140 EuGH 08.04.2014 – C-293/12, C-594/12 – Digital Rights Irland Ltd und Seitlinger u. a. Rn. 37 = NJW 2014, 2169; EuGH 21.12.2016 – C-203/15, C-698/15 – ele2 Sverige AB/Post- och telestyrelsen und Secretary of State for the Home Depart-

Orientierung, politische Meinung, religiöse, philosophische, gesellschaftliche oder andere Überzeugungen oder den Gesundheitszustand offenbaren.[141]

Eine Rechtfertigung solcher Eingriffe ist gem. Art. 8 GRC denkbar, wenn aufgrund einer gesetzlichen Grundlage ein legitimes Ziel im Sinne des Art. 8 Abs. 2, Art. 52 Abs. 1 S. 2 GRC erreicht werden soll und die Einschränkung verhältnismäßig ist. Somit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.[142]

In Betracht kommt im Rahmen der strafprozessualen Online-Durchsuchung die Aufklärung von begangenen schweren Straftaten. Das Ziel der Verarbeitung von personenbezogenen Daten zum Zwecke der Strafverfolgung von schweren Straftaten hat der Europäische Gerichtshof bereits in seinen Entscheidungen zur Vorratsdatenspeicherung grundsätzlich als legitimes Ziel mit der Begründung, dass Bekämpfung schwerer Kriminalität letztlich zur öffentlichen Sicherheit beitrage, anerkannt.[143] Allerdings können mit dem Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten nur „nicht schwere" Eingriffe in die Grundrechte der Art. 7, 8 GRC gerechtfertigt werden, denn die Bekämpfung, auch von besonders schwerer Kriminalität, kann nicht mit einer Bedrohung der nationalen Sicherheit gleichgesetzt werden.[144]

Im Rahmen der Verhältnismäßigkeitsprüfung kommt es in einem nächsten Schritt darauf an, dass die Belange „ausgewogen gewichtet"[145] werden und die Einschränkungen in Bezug auf die personenbezogenen Daten auf das absolut Notwendigste reduziert werden.[146] Dabei ist die geheime Informa-

---

ment/Watson u. a. Rn. 99 = NJW 2017, 717; EuGH 05.04.2022 – C-140/20 – G. D./Commissioner of An Garda Síochána Rn. 44 = EuZW 2022, 536.

[141] EuGH 05.04.2022 – C-140/20 – G. D./Commissioner of An Garda Síochána Rn. 45 = EuZW 2022, 536.

[142] Ständiger Rechtsprechung des EuGH u. a.: EuGH 21.12.2016 – C-203/15, C-698/15 – ele2 Sverige AB/Post- och telestyrelsen und Secretary of State for the Home Department/Watson u. a. Rn. 94 = NJW 2017, 717.

[143] EuGH 08.04.2014 – C-293/12, C-594/12 – Digital Rights Irland Ltd und Seitlinger u. a. Rn. 41 = NJW 2014, 2169; EuGH 05.04.2022 – C-140/20 – G. D./Commissioner of An Garda Síochána Rn. 48 = EuZW 2022, 536.

[144] EuGH 05.04.2022 – C-140/20 – G. D./Commissioner of An Garda Síochána Rn. 59, 63= EuZW 2022, 536. EuGH 2022 Rdnr. 59, 63

[145] EuGH 13.01.2010 – C-92/09 – Schecke, Slg. 2020, I – 11063 Rn. 77 = EuZW 2010, 939.

[146] EuGH 13.01.2010 – C-92/09 – Schecke, Slg. 2020, I – 11063 Rn. 77 = EuZW 2010, 939; EuGH 21.12.2016 – C-203/15, C-698/15 – ele2 Sverige AB/Post- och telestyrelsen und Secretary of State for the Home Department/Watson u. a. Rn. 96, 108 = NJW 2017, 717; EuGH 06.10.2020 – C-623/17 – privacy International Rn. 67 =

tionserhebung als ein besonders intensiver Eingriff in Art. 8 GRC anzusehen, was auf der Ebene der Verhältnismäßigkeit Berücksichtigung finden muss.[147] Bei Daten, die erhebliche Auskünfte über die betroffene Person zulassen, ist der Gestaltungsspielraum des Gesetzgebers erheblich eingeschränkt und unterliegt einer strikten Kontrolle.[148] Dabei müssen durch den Gesetzgeber Regelungen getroffen werden, die Regeln für die Tragweite und die Anwendung der fraglichen Maßnahme vorsehen und Mindestanforderungen aufstellen, sodass die betroffene Person über ausreichend Garantien verfügt, die Schutz vor Missbrauch sowie Schutz vor dem Zugang Unberechtigter zu den Daten ermöglicht.[149] Es braucht klare und präzise Regeln, die die Tragweite des Eingriffs in Art. 7, 8 GRC regeln, der besonderen Schwere des Eingriffs gerecht werden und die Beschränkung auf das absolut Notwendige ermöglichen.[150] In diesem Zusammenhang bekräftigte der Europäische Gerichtshof in einer Entscheidung von 2022 erneut: „Angesichts des sensiblen Charakters der Informationen, die sich aus den Verkehrs- und Standortdaten ergeben können, ist deren Vertraulichkeit nämlich von entscheidender Bedeutung für das Recht auf Achtung des Privatlebens."[151] Aus diesem Grund ist die anlasslose Vorratsdatenspeicherung solcher Daten wegen der Schwere des Eingriffs auch bei schwerer Kriminalität nicht gerechtfertigt.[152]

Anderes gilt hingegen – zur Bekämpfung von schwerer Kriminalität –, wenn eine Speicherung von Verkehr- und Standortdaten gezielt auf Grundlage objektiver und nichtdiskriminierender Kriterien über einen auf das absolut Notwendige begrenzten Zeitraum stattfindet und einer gerichtlichen Kontrolle unterliegt.[153]

GSZ 2021, 36; EuGH 05.04.2022 – C-140/20 – G. D./Commissioner of An Garda Síochána Rn. 52, 53 = EuZW 2022, 536.

147 EuGH 08.04.2014 – C-293/12, C-594/12 – Digital Rights Irland Ltd und Seitlinger u. a. Rn. 37 = NJW 2014, 2169; *Jarass*, in: Jarass Charta der Grundrechte der Europäischen Union, Art. 8 Rn. 17; *Wolff*, in: Frankfurter Kommentar EUV GRC AEUV, Art. 8 GRC Rn. 47.

148 EuGH 08.04.2014 – C-293/12, C-594/12 – Digital Rights Irland Ltd und Seitlinger u. a. Rn. 48 = NJW 2014, 216.

149 Ständige Rechtsprechung des EuGH – zuletzt: EuGH 06.10.2020 – C-623/17 – privacy International Rn. 54 = GSZ 2021, 36.

150 Ständige Rechtsprechung des EuGH – zuletzt: EuGH 06.10.2020 – C-623/17 – privacy International Rn. 54 = GSZ 2021, 36.

151 EuGH 05.04.2022 – C-140/20 – G. D./Commissioner of An Garda Síochána Rn. 65 = EuZW 2022, 536.

152 EuGH 05.04.2022 – C-140/20 – G. D./Commissioner of An Garda Síochána Rn. 65 = EuZW 2022, 536.

153 EuGH 05.04.2022 – C-140/20 – G. D./Commissioner of An Garda Síochána Rn. 67 = EuZW 2022, 536.

Zusammenfassend ist somit zusagen, dass aufgrund der Daten, die bei einer Online-Durchsuchung erhoben und verarbeitet werden – von vergleichbarer Art und Umfang wie bei der Vorratsdatenspeicherung –, die Online-Durchsuchung in Art. 7, 8 GRC eingreift. Allerdings ist eine Rechtfertigung dieses Eingriffs nicht per se ausgeschlossen, auch wenn erhebliche Gefahren für die Persönlichkeitsrechte der betroffenen Person bestehen. In Bezug auf die Verhinderung der Gefahr der Bildung von Persönlichkeitsprofilen sieht auch Art. 8 GRC – wie die grundgesetzlichen Grundrechte – erhebliche Verfahrensvoraussetzungen vor. Dabei ist bei der Online-Durchsuchung darauf zu achten, dass aufgrund der Gefahren für die Persönlichkeitsrechte des*der Einzelnen nur solche Daten erhoben werden, die sich auf das absolut Notwendige beschränken. Dies muss mittels klarer und präziser Verfahrensregelungen abgesichert werden.

Da Art. 8 GRC spezieller ist, läuft Art. 52 Abs. 3 GRC leer und die EMRK findet in diesem Zusammenhang keine Anwendung.[154]

2. Richtlinie (EU) 2016/680 [DSRL-JI]

Eine Eingrenzung der Erhebung der Datenmenge kann über die DSRL-JI[155] erfolgen. Eine Begrenzung der zu erhebenden Daten, durch welche die Gefahr der Bildung von Persönlichkeitsprofilen ausgelöst wird, erfolgt über Art. 4 Abs. 1 lit. b, c. Durch diese Bestimmung kommt auch die bereits dargestellte Vorgabe des Europäischen Gerichtshofs zum Ausdruck, wonach Daten nicht über das nötige Maß hinaus erhoben werden dürfen.

Die DSRL-JI hat es sich gem. Art. 1 Abs. 2 lit. b zur Aufgabe gemacht, im Sinn der Art. 8 GRC und Art. 16 Abs, 1 AEUV natürlichen Personen gegenüber Behörden und der Justiz, die aus dem Anwendungsbereich der DS-GVO[156] gem. Art. 2 Abs. 2 lit. d DS-GVO bei der Strafverfolgung ausdrücklich ausgenommen sind, Schutz der personenbezogenen Daten zu gewähren.

---

154 *Wolff*, in: Frankfurter Kommentar EUV GRC AEUV, Art. 8 GRC Rn. 3.

155 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates ABl. L 119 v. 4.5.2016, S. 89–131.

156 Verordnung (EU) 20/6/67ß des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Warenverkehr und zu Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung), ABl. L 119 v. 4.5.2016, S. 1–88.

Die DSRL-JI findet dann sachlich Anwendung, wenn es um die Verarbeitung von personenbezogenen Daten Lebender geht, die DS-GVO nicht eingreift, keine spezielleren datenschutzrechtlichen Regelungen des Bundes bestehen und die Verarbeitung nicht ausschließlich persönlichen oder familiären Tätigkeiten dient.[157] Der DSRL-JI kommt insoweit eine Auffangfunktion zu[158]

Die Richtlinie wurde in weiten Teilen bereits im dritten Teil des Bundesdatenschutzgesetzes (BDSG) umgesetzt.

a) Verstoß gegen allgemeine Verarbeitungsgrundsätze

Im Rahmen der Umsetzung der Richtlinie wurde Art. 4, der die Grundsätze zur Verarbeitung von personenbezogenen Daten bestimmt, in § 47 BDSG weitestgehend wortgleich umgesetzt. Dabei ist die Formulierung an Art. 5 DS-GVO angelehnt und kann auf Art. 4 der DSRL-JI übertragen werden. Die Erhebung von Daten, welche eine Erstellung von Persönlichkeitsprofilen ermöglichen, verstößt gegen den Verarbeitungsgrundsatz der Datenminimierung aus Art. 4 Abs. lit. c der DRSL-JI.

Die Grundsätze zur Datenverarbeitung finden sich in § 47 BDSG, zu ihnen gehören, die Rechtmäßigkeit, die Verarbeitung nach Treu und Glauben und die Zweckbindung sowie die Datenminimierung.

Eine erste Einschränkung der zu erhebenden Daten nimmt die DRSL-JI mit dem Grundsatz der Zweckbindung aus Art. 4 Abs. 1 lit. b DRSL-JI, der wie Art. 5 Abs. 1 lit. b DS-GVO zu verstehen ist, vor. Die Zweckbindung umfasst die Zweckfestlegung und dann die anschließende Bindung an diesen Zweck. Dabei genügt zur Zweckfestlegung nicht, wenn allein die Nennung von einem der Rechtfertigungsgründe, beispielweise Ermittlung einer schweren Straftat, erfolgt. Er muss als solcher hinreichend bestimmt sein, um einer gewisse Begrenzungsfunktion zu entsprechen. Zweckbindung meint darüber hinaus, dass sich der*die Verantwortliche für die Verarbeitung sich innerhalb dieses Rahmens bewegen muss.[159]

Eine Umsetzung dieses Grundsatzes, findet sich neben dem BDSG als lex specialis in § 100e Abs. 3 Nr. 4 StPO. Danach muss die Anordnung der Online-Durchsuchung die Art der zu erhebenden Daten angeben und aufzeigen, inwieweit sie von Nutzen für das Verfahren sind. Gem. § 100e Abs. 6 StPO

---

157 *Lauber/Rönsberg*, in: Handbuch Europäisches und deutsches Datenschutzrecht, S. 105.

158 *Schantz*, in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 349.

159 *Mantz/Marosi*, in: Handbuch Europäisches und deutsches Datenschutzrecht, S. 62.

ist dann unter engen Voraussetzungen die Zweckänderung normiert. Für alle weiteren Verarbeitungsprozesse von personenbezogenen Daten, findet sich in § 483 StPO eine Vorgabe, die die Zweckfestlegung und -bindung vorsieht.

In Art. 4 Abs. 1 lit. c DSRL-JI wird der Grundsatz der Datenminimierung vorgeschrieben. Dies bedeutet, dass personenbezogenen Daten dem Zweck angemessen und erheblich sowie auf das für die Verarbeitung notwendige Maß beschränkt sein müssen.[160]

Diesbezüglich ist der Wortlaut des § 47 BDSG nicht derselbe wie in der JI-Richtlinie. Zwar war die wortgleiche Übernahme noch in der Ausgangsdrucksache geplant.[161] Diese wurde jedoch mit der Beschlussempfehlung des Innenausschusses[162] geändert. Im Bericht des Innenausschusses wird als Grund hierzu ausgeführt, man wolle die deutsche Fassung näher an die deutsche Rechtssprache heranführen. Dies gelte für die Formulierungen „maßgeblich" und „übermäßig", die anders umschrieben werden sollen.[163] Unabhängig von einer Bewertung der Änderung des Wortlauts muss davon ausgegangen werden, dass es sich hierbei lediglich um redaktionelle Änderungen handelt, die Bedeutung und die Umsetzung der DSRL-JI, aber beibehalten wird.

Der Grundsatz der Datenminimierung findet dann Anwendung, wenn eine gewisse Menge von Daten vorhanden ist.[164] Dabei setzt er eine rechtmäßige Datenverarbeitung und eine rechtmäßige Zweckbestimmung der Datenverarbeitung voraus.[165] Die Erhebung der personenbezogenen Daten muss dem Zweck angemessen sein, was nicht die Verhältnismäßigkeit im engeren Sinne meint, sondern die ihr vorgelagerte Frage der Zuordnung zum Zweck.[166] Wesentlich ist hierbei, dass die Verarbeitung auf das notwendige Maß beschränkt wird. Prinzipiell sind so wenig Daten wie möglich zu erheben, zu verarbeiten und zu nutzen.

Für die Online-Durchsuchung findet sich in der StPO keine Vorschrift, die den Grundsatz der Datenminimierung vorsieht. Es verbleibt hier lediglich der für jede staatliche Maßnahme geltende Verhältnismäßigkeitsgrundsatz. Eine Begrenzung der Daten aus der StPO heraus ist allein über § 100d StPO, der Vorgaben zum Schutz des Kernbereichs privater Lebensgestaltung, denkbar,

---

160 *Mantz/Marosi*, in: Handbuch Europäisches und deutsches Datenschutzrecht, S. 62.

161 BT-Drucks., 18/11325, S. 47.

162 BT-Drucks., 18/12084.

163 BT-Drucks. 18/12144, S. 7.

164 *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 420.

165 *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 420.

166 *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 421.

diese Begrenzung entspricht jedoch nicht dem Sinn und Zweck der Vorgabe aus lit. c, da sie zunächst nur auf jene Daten Anwendung findet, die unmittelbaren Kernbereichsbezug aufweisen. Hier findet somit § 47 Nr. 3 BDSG Anwendung und wird nicht durch speziellere Vorschriften verdrängt.

Darüber hinaus sieht Art. 8 DSRL-JI, der in § 47 Nr. 1 BDSG Berücksichtigung gefunden hat, vor, dass eine Verarbeitung personenbezogener Daten nur dann rechtmäßig ist, wenn und so weit die Verarbeitung zur Realisierung einer der Zwecke erforderlich ist und auf Grundlage des Rechts der Union oder der Mitgliedstaaten erfolgt.[167] Damit stellt die Richtlinie klar, dass es sich um ein Verbotsprinzip mit Erlaubnisvorbehalt handelt. Die Verarbeitung von personenbezogenen Daten ist somit grundsätzlich verboten, kann aber durch eine Ermächtigung erlaubt werden.[168] Es braucht eine Rechtsgrundlage, die ihrerseits den Anforderungen der Erforderlichkeit und der Zweckbindung genügt.[169] Eine solche Ermächtigung zur Datenverarbeitung stellt § 100b StPO dar.

Besteht die Gefahr, dass durch eine strafprozessuale Online-Durchsuchung ein Persönlichkeitsprofil gebildet werden kann, wurden die Verarbeitungsgrundsätze der DRSL-JI aus Art. 4 Abs. 1 lit. b und c, welche in § 47 Nr. 2, 3 BDSG umgesetzt wurden und im Lichte der Art. 7, 8 GRC auszulegen sind, nicht berücksichtigt. Unter dem Gesichtspunkt der Zweckbindung und der Datenminimierung dürfen nur jene Daten erhoben werden, die auf das absolut Notwendigste reduziert sind. Dies ist nicht der Fall, wenn durch die Datenmengen Persönlichkeitsprofile ermöglicht werden.

b) Verstoß gegen das Verbot des Profilings

Darüber hinaus sieht die Richtlinie gem. Art. 10, 11 i. V. m. Art. 3 Nr. 4 einen grundsätzlichen Schutz der betroffenen Person gegenüber den Behörden vor Profiling vor.

Zur Begriffsbestimmung heißt es in Art. 3 Nr. 4 der Richtlinie, Profiling sei „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten (…)". Hierunter kann die Gefahr der Bildung von Persönlichkeitsprofilen nicht subsumiert werden. Denn diese besteht, wenn die Beschreibung einer Person mittels ihrer Eigenschaften droht und einen Menschen in seinem Sein registriert und katalogisiert wird. Bei der Erstellung

167 *Schwichtenberg*, in: Kühling/Buchner, DSGVO BDSG, § 47 BDSG Rn. 5.
168 *Schwichtenberg*, DuD 2016, 605, 605 f.
169 *Schwichtenberg*, in: Kühling/Buchner, DSGVO BDSG, § 47 BDSG Rn. 5.

eines Persönlichkeitsprofils wird die Gedanken- und Gefühlswelt der betroffenen Person offengelegt und analysiert.

Bei der Gefahr der Bildung von Persönlichkeitsprofilen kommt es somit nicht auf die Art der Verarbeitung – automatisch oder manuell –, sondern auf die Art und den Umfang der gewonnenen Daten, die einer Rundumüberwachung dienen, an. Ziel des Vorgangs des Profilings ist hingegen, die Bewertung von Persönlichkeitsmerkmalen, um Verhalten zu analysieren und vorherzusagen,[170] an dessen Ende dann möglichweise ein Persönlichkeitsprofil gebildet werden kann, nicht aber zwingend gebildet werden muss.[171] Die Begriffe des Profilings und die Gefahr der Bildung von Persönlichkeitsprofilen dürfen somit nicht synonym verwendet werden und sind klar voneinander abzugrenzen. Art. 11 DSRL-JI verbietet die „ausschließlich" automatisierte Verarbeitung – einschließlich Profiling – nicht aber die Ermöglichung von Persönlichkeitsprofilen. Die automatische Verarbeitung von Daten – so wohl der bisherige Stand der praktischen Umsetzung – spielt für die Ermittlungsmaßnahme der Online-Durchsuchung (noch) keine Rolle. Nicht auszuschließen ist hingegen, dass mit dem Fortschritt der Technik auch im Rahmen der Online-Durchsuchung Algorithmen entwickelt werden, die beschuldigte Personen anhand von zuvor festgelegten Kategorien im Sinne des Art. 10 DSRL-JI bewerten. Dies ist aber nicht Gegenstand der Arbeit, wäre aber zu gegebener Zeit zu berücksichtigen.

3. E-privacy Richtlinie 2002/58

Die Richtlinie 2002/58/EG (e-privacy Richtlinie)[172] kann nicht zur Verfestigung von Unionsrecht bei der Gefahr der Bildung von Persönlichkeitsprofilen im Rahmen der strafprozessualen Online-Durchsuchung herangezogen werden.

Bei der zuvor dargestellten Rechtsprechung zur Schutzwirkung des Art. 8 GRC befasste sich der Europäische Gerichtshof mit der Vorratsdatenspeicherung, welche in Art. Art. 15 Abs. 1 der Richtlinie 2002/58/EG durch den europäischen Gesetzgeber ausdrücklich zugelassen wurde.

---

[170] *Johannes/Weinhold*, in: Das neue Datenschutzrecht bei Polizei und Justiz, § 1 Rn. 168.

[171] Das Profil als Ergebnis von Profiling ansehend wohl auch die Richtlinie selber in Rn. 51 der Erwägungsgründen.

[172] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und dem Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) ABl. L 201 v. 31.7.2002, S. 37–47.

Adressat*innen der Richtlinie sind gem. Art. 3 die Betreiber*innen von elektronischen Kommunikationsdiensten, die öffentliche Kommunikationsnetze in der Gemeinschaft bereitstellen und personenbezogene Daten verarbeiten.

Gemäß Art. 5 haben die Mitgliedstaaten den Schutzauftrag, die Vertraulichkeit der mittels öffentlichen Kommunikationsnetze übertragenen Nachrichten zu gewährleisten. Insbesondere ist das Mithören, Abhören und Speichern sowie andere Arten des Abfangens und Überwachens von Nachrichten zu untersagen. Auch Verkehrsdaten, die verarbeitet und gespeichert werden, sind gem. Art. 6 nach der Übertragung der Nachricht durch die Betreiber*innen zu löschen oder zu anonymisieren.

Die Richtlinie verpflichtet die Mitgliedstaaten, Betreiber*innen mittels nationalen Rechts, die Vertraulichkeit der Daten – unter anderem im Sinne der Art. 5, 6 – zu gewährleisten. Ausnahmen von dieser Verpflichtung der Betreiber*innen dürfen gem. Art. 15 Abs. 1 der Richtlinie 2002/58/EG zum Zwecke der Strafverfolgung gemacht werden. Diese Ausnahme gilt der Vorratsdatenspeicherung, hiernach sollen die Kommunikationsdienstleister*innen entgegen ihrer Pflicht, unter anderem aus Art. 5, 6 der Richtlinie, Verkehrsdaten und andere Informationen speichern. Für die Online-Durchsuchung braucht es eine solche Ausnahme hingegen nicht; Ermittlungsbehörden sind bei der Online-Durchsuchung nicht auf die Mitwirkung der Kommunikationsdienstleister*innen angewiesen, da das Abfangen von Informationen auf dem IT-Gerät selbst außerhalb ihres Machtbereichs liegt.

III. Gleichrangiges Schutzniveau von grundgesetzlichen Grundrechten und der Grundrechtecharta

Eine Online-Durchsuchung, die in der Gestalt Daten erhebt, dass Persönlichkeitsprofile gebildet werden können, greift in den Schutzbereich der Art. 7, 8 GRC ein. Dieser Eingriff ist als besonders schwerwiegend einzustufen, da bei einer Online-Durchsuchung durch eine Gesamtbetrachtung der Daten genaue Schlüsse auf das Privatleben der betroffenen Person gezogen werden können und bei der betroffenen Person das Gefühl erzeugt werden kann, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist.[173]

[173] EuGH 08.04.2014 – C-293/12, C-594/12 – Digital Rights Irland Ltd und Seitlinger u. a. Rn. 26 f., 37 = NJW 2014, 2169; EuGH 21.12.2016 – C-203/15, C-698/15 – ele2 Sverige AB/Post- och telestyrelsen und Secretary of State for the Home Department/Watson u. a. Rn. 100 = NJW 2017, 717; EuGH 06.10.2020 – C-623/17 – privacy International Rn. 71 = GSZ 2021, 36.

Ein solcher Eingriff kann zwar mit der Strafverfolgung von besonders schwerer Kriminalität gerechtfertigt werden, hierfür muss die Datenerhebung allerdings auf das absolut Notwendigste reduziert werden. Dieser Grundsatz hat über die Umsetzung der DSRL-JI ins BDSG insoweit Berücksichtigung gefunden, als dass die Verarbeitungsgrundsätze des Art. 4 der DSRL-JI in § 47 BDSG übernommen wurden. Für die Gefahr der Bildung von Persönlichkeitsprofilen sind gem. § 47 Nrn. 2, 3 BDSG der Grundsatz der Zweckbindung und der Datenminimierung zu berücksichtigen.

Damit gehen die Forderungen des Europäischen Gerichtshofs deutlich weiter als die des Bundesverfassungsgerichts, welches eine Begrenzung der Daten bei der Online-Durchsuchung wohl nur durch punktuelle Kernbereichsrelevanz oder den allgemeinen Verhältnismäßigkeitsgrundsatz vornimmt. Aus diesem Grund finden Art. 7, 8 GRC auf die Online-Durchsuchung direkte Anwendung, da das Schutzniveau der Charta hier höher einzustufen ist als der grundgesetzliche Grundrechtsschutz.

§ 47 BDSG setzt Art. 4 der DSRL-JI um, die die Verarbeitung von personenbezogenen Daten unter anderem durch die Strafverfolgungsbehörden regelt. Damit wird bei der Verarbeitung von personenbezogenen Daten Unionsrecht durchgeführt.

Die DSRL-JI kann aber nicht als vollharmonisiertes und vereinheitlichtes Unionsrecht angesehen werden. Zwar finden sich in den Erwägungsgründen der DSRL-JI Anhaltspunkte für den Willen zu einer Harmonisierung. So heißt es zum Beispiel im Erwägungsgrund vier: Es bedürfe „des Aufbaus eines soliden und kohärenteren Rechtsrahmens für den Schutz personenbezogener Daten in der Union, die konsequent durchgesetzt werden." Ein solcher Harmonisierungsgedanke ergibt sich ferner aus dem Erwägungsgrund sieben nach dem die Rechte und Freiheiten einer Person bei der Verarbeitung personenbezogener Daten im repressiven sowie im präventiven Bereich „in allen Mitgliedstaaten gleichwertig geschützt werden" sollen. Auch im Zusammenspiel mit der DS-GVO, der nach einhelliger Meinung bereits der Status der Vollharmonisierung zukommt, – ließe sich ein vereinheitlichtes Unionsrecht gut begründen. So sind die DS-GVO und die DSRL-JI nicht immer klar voneinander abzugrenzen und ihnen liegen letztlich – mit Ausnahme des Transparenzgebotes – dieselben datenschutzrechtlichen Grundsätze zu Grunde. Im Rahmen der DS-GVO sind wesentliche Vorschriften als gefestigt anzusehen. Diese Erwägungen können auf die DSRL-JI übertragen werden.

Entscheidendes Argument gegen vollharmonisiertes Unionsrecht bei der Anwendung der DSRL-JI auf die strafprozessuale Online-Durchsuchung ist jedoch, dass die DSRL-JI, anders als beispielsweise die e-privacy Richtlinie oder auch die DS-GVO, keine konkreten Vorgaben für eine heimliche Er-

mittlungsmaßnahme trifft. Sie setzt die Möglichkeit solcher Maßnahmen zwar voraus, allerdings trifft sie über die Verarbeitungsgrundsätze hinaus keine weiteren Vorgaben insbesondere zur Erhebung der Daten. Sie ist in den Teilen, die Vorgaben für die Online-Durchsuchung machen, auf die Verwertbarkeit beschränkt, auch wenn es wie bei dem Grundsatz der Datenminimierung Überschneidungen gibt.[174]

Wie oben bereits dargelegt, geht das Bundesverfassungsgericht in seiner bisherigen Rechtsprechung zur Gefahr der Bildung von Persönlichkeitsprofilen nicht davon aus, dass es bei dem Schutz des Kernbereichs privater Lebensgestaltung einer Begrenzung der Menge der Daten über die punktuelle Kernbereichsrelevanz hinaus bedarf.

Damit bleibt es klar hinter dem Schutzniveau des Europäischen Gerichtshofs bei einem Eingriff in Art. 7, 8 GRC zurück. Solange das Bundesverfassungsgericht seine Rechtsprechung in diesem Kontext nicht ändert, ist das Schutzniveau der Grundrechtecharta wohl höher als die des Grundgesetzes und die Grundrechtecharta würde direkte Anwendung finden.

Danach können insbesondere die Erwägungen und Vorgaben des Europäischen Gerichtshofs zur Vorratsdatenspeicherung auf die Gefahr der Bildung von Persönlichkeitsprofilen bei der Online-Durchsuchung übertragen werden. Denn wie bei der Gefahr der Bildung von Persönlichkeitsprofilen, liegt das Kernproblem bei der Vorratsdatenspeicherung in der Menge und der Vielfalt der Daten, die kontinuierlich erhoben und gespeichert werden. Dass sich die Grundsätze nicht nur auf die Vorratsdatenspeicherung beziehen, hat der Europäische Gerichtshof in seinem Urteil von 2020 klargestellt: „Die gleichen Fragen stellen sich auch für andere Arten der Verarbeitung von Daten (…)“[175]

Bei der Online-Durchsuchung gilt dasselbe, was der Europäische Gerichtshof bereits für die Vorratsdatenspeicherung festgestellt hat:

> „Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden, etwas auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren.“[176]

---

[174] So zutreffend auch: *Müller/Schwabenbauer*, in: Handbuch des Polizeirechts, Rn. 393. Zum selben Ergebnis in Bezug auf das Bayerische Verfassungsschutzgesetz, zu dessen Überprüfung auch die Online-Durchsuchung gehört: BVerfG 26.04.2022 – 1 BvR 1619/17 = NJW 2022, 1583.

[175] EuGH 06.10.2020 – C-623/17 – privacy International Rn. 61 = GSZ 2021, 36.

[176] EuGH 08.04.2014 – C-293/12, C-594/12 – Digital Rights Irland Ltd und Seitlinger u. a. Rn. 27 = NJW 2014, 2169; EuGH 21.12.2016 – C-203/15, C-698/15 –

Aus diesem Grund kann die Rechtsprechung zur Vorratsdatenspeicherung in diesem Bereich in Gänze auf die Online-Durchsuchung übertragen werden.

Der Gesetzgeber unterliegt bei der Einhaltung dieser Grundsätze der strikten Kontrolle durch die Rechtsprechung.[177] Nach der klaren und eindeutigen Rechtsprechung des Europäischen Gerichtshofs „(…) *muss* eine nationale Regelung, die mit einem Eingriff in die in Art. 7 und 8 der Charta verankerten Grundrechte verbunden ist, jedoch den Anforderungen entsprechen, die sich aus der in den Rn. 65, 67 und 68 des vorliegenden Urteils angeführten Rechtsprechung ergeben."[178] Rn. 68 legt fest, dass klare und präzise Regelungen getroffen werden, die gewährleisten, dass der Eingriff auf das absolut Notwendige beschränkt wird.[179] Eine solche feste Normierung der Beschränkung findet sich in der StPO zur Online-Durchsuchung, die das Bundesverfassungsgericht als verfassungsmäßig eingestuft hat, nicht. Damit ist das vom Europäische Gerichtshof geforderte Schutzniveau höher als das des Bundesverfassungsgerichts.

Nach der hier vertretenen Ansicht, die davon ausgeht, dass es für den Schutz des Kernbereichs privater Lebensgestaltung nach den verfassungsrechtlichen Grundrechten ebenfalls eines weitreichenderen Schutzes bedarf, als er durch das Bundesverfassungsgericht gewährleistet wird, kann von einem gleichrangigen Schutzniveau zwischen Grundrechtecharta und verfassungsrechtlichen Grundrechten ausgegangen werden. Wie im Abschnitt zuvor dargelegt, ist der verfassungsrechtliche Maßstab für die Gefahr der Bildung von Persönlichkeitsprofilen bei der Online-Durchsuchung durch das Bundesverfassungsgericht unzutreffend bestimmt worden. Die Grundrechtecharta findet in diesem Fall nicht direkt Anwendung, die grundrechtlichen Vorgaben zum Kernbereich privater Lebensgestaltung sind lediglich im Lichte der Grundrechtecharta, insbesondere unter Berücksichtigung der Rechtsprechung des Europäischen Gerichtshofs zur Vorratsdatenspeicherung, auszulegen.

Folgte man der Rechtsprechung des Bundesverfassungsgerichts, bliebe das Grundgesetz hinter dem Schutzniveau der Grundrechte zurück und diese würden Anwendung finden.

---

ele2 Sverige AB/Post- och telestyrelsen und Secretary of State for the Home Department/Watson u. a. Rn. 98 = NJW 2017, 717.

177 EuGH 08.04.2014 – C-293/12, C-594/12 – Digital Rights Irland Ltd und Seitlinger u. a. Rn. 48 = NJW 2014, 2169.

178 Hervorhebung durch die Verfasserin. EuGH 06.10.2020 – C-623/17 – privacy International Rn. 76 = GSZ 2021, 36.

179 EuGH 06.10.2020 – C-623/17 – privacy International Rn. 68 = GSZ 2021, 36.

3. Kapitel

Die Online-Durchsuchung

Im folgenden Kapitel wird eine grundsätzliche Vorstellung und Darstellung der strafprozessualen Online-Durchsuchung erfolgen, um eine Einordnung der Ermittlungsmaßnahme zu ermöglichen.

Bereits im Jahr 2007 stellte *Schlegel* fest, dass sich die Online-Durchsuchung in einem Dilemma, richtigerweise einem Trilemma, zwischen dem technisch Möglichen, dem sicherheitspolitisch Notwendigen und dem gesellschaftlich Wünschenswerten befindet.[1] Diesem Trilemma mussten sich Politik, Justiz und Gesellschaft also stellen. Dieses Kapitel beschäftigt sich mit der Historie der Online-Durchsuchung und stellt nachfolgend die Ermächtigungsgrundlage der Online-Durchsuchung dar.

Insbesondere soll hierbei in einem ersten, historischen Teil herausgearbeitet werden, warum die Online-Durchsuchung von Politik und Gesellschaft als sicherheitspolitisch notwendig erachtet wurde und wie sie sich entwickelt hat. Diese historische Herleitung kann mögliche grundsätzliche Probleme der Online-Durchsuchung offenbaren und erste Umgangsmöglichkeiten und Lösungsansätze aufzeigen, die es dann später zu diskutieren und vertieft zu behandeln gilt. Im Mittelpunkt dieser Betrachtung wird dabei immer der Schutz des Kernbereichs der privaten Lebensgestaltung stehen. Auch soll dargelegt werden, welche neuen und bis jetzt unbearbeiteten Probleme die Maßnahmen mit sich bringen, die sich bereits in ihrer Historie herauskristallisiert haben.

Nachfolgend wird zunächst eine grundsätzliche Darstellung der Online-Durchsuchung in der StPO erfolgen. In diesem Teil der Bearbeitung soll ein erster Rahmen der Online-Durchsuchung mitsamt seinen Problemen abgesteckt werden, der zu einem späteren Zeitpunkt auf die Gefahr der Bildung von Persönlichkeitsprofilbildung hin zu untersuchen ist. Hier wird ein großer Schwerpunkt auf der Art der Daten liegen, die mittels einer Online-Durchsuchung erhoben werden können, denn sie sind die Basis aus der ein Persönlichkeitsprofil gebildet werden kann. Bereits hier wird deutlich werden, dass die Online-Durchsuchung nahezu in alle Lebensbereiche des*der Nutzer*in eindringt und dadurch in ganz speziellem Maße Daten generiert.

---

[1] *Schlegel*, GA 2007, 648, 663.

A. Historische Entwicklung

Schon im Jahr 1992 erkannte *Bär*, dass die Veränderungen in der Informationsgesellschaft die Ermittlungsbehörden immer häufiger dazu zwingen, auf Computerdaten als Beweismittel zurückzugreifen. Dies beschränke sich nach seiner Ansicht nicht nur auf die Computerkriminalität, sondern gelte für alle Deliktsformen. Aus diesem Grund forderte er dazu auf, die Strafverfolgungsbehörden sowohl mit dem technischen Wissen und den benötigten Geräten auszustatten als auch entsprechende Ermächtigungsgrundlagen zu entwickeln. Denn die in der StPO normierte Fixierung auf körperliche Gegenstände werde den Anforderungen nicht mehr gerecht. Außerdem stellte er fest, dass unklar sei, welche Rolle die Durchsuchung bei der Gewinnung von Computerdaten spiele.[2] Bereits hier wird deutlich, welchen Herausforderungen sich die Strafprozessordnung mit dem Beginn der Verbreitung von Computern stellen musste und auch immer noch stellen muss. Klar wird dabei auch, dass die schnelle Entwicklung der Informationstechnik zu einem immer größeren Handlungszwang der Gesetzgebung führte.

Im Folgenden soll nun dargestellt werden, wie sich diese Forderung nach einer entsprechenden Ermächtigungsgrundlage seit 1992 entwickelt hat, bevor am 24.08.2017 die strafprozessuale Online-Durchsuchung in Kraft getreten ist.

I. Erste Überlegungen auf Bundesebene

Die ersten Überlegungen zur Online-Durchsuchung auf Bundesebene waren durch unterschiedliche Herangehensweisen geprägt. Die erste Online-Durchsuchung fand 1995 auf einer Mailbox statt. Während sich die Gesetzgebung mit der konkreten Ausgestaltung einer neuen Ermächtigungsgrundlage zur Online-Durchsuchung beschäftigte, ging es in der Rechtsprechung vordergründig darum herauszufinden, ob bereits Ermächtigungsgrundlagen bestehen und in welche Grundrechte durch eine solche Online-Durchsuchung eingegriffen wird. All diese parallel stattfindenden Entwicklungen werden im Folgenden dargestellt.

1. Online-Durchsuchung auf einer Mailbox

Im Jahr 1995 musste sich der Bundesgerichtshof das erste Mal mit der Problematik eines heimlichen Zugriffs auf ein technisches Gerät von außen auseinandersetzen. Hierbei ging es um den heimlichen Zugriff auf eine Mail-

[2] *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, S. 509.

box. Bei einer Wohnungsdurchsuchung hatten die Ermittelnden Aufzeichnungen mit Passwörtern und Telefonnummern sichergestellt. Sie gingen davon aus, dass es sich dabei um Anschlüsse zu passwortgeschützten Mailboxen handelte, auf denen Texte und Zahlenmaterial abgelegt seien, die den Beschuldigten als Arbeitsgrundlage dienten.[3] Bereits hier gab es die Überlegung, ob ein solcher Zugriff auf die Rechtsgrundlagen der Beschlagnahme und der Durchsuchung (§§ 94 ff., 102 ff. StPO) gestützt werden könne. Dies wurde vom Gericht mit Hinweis auf den Sinn und Zweck der Durchsuchung abgelehnt. Es gehe nicht um die Sicherstellung körperlicher Gegenstände oder das körperliche Eindringen in Wohnungen und andere Räume.[4] Dennoch müsste, so der Bundesgerichtshof, die Grundgedanken der Durchsuchung auch auf diese (neue) Ermittlungsmaßnahme Anwendung finden. Dies ergebe sich bereits aus der sachlichen Nähe der beiden Maßnahmen zueinander. Außerdem müsste bei dieser neuen Maßnahme erhöhte Anforderungen an die Verhältnismäßigkeit gestellt werden, weil sie, anders als die „klassische" Durchsuchung, heimlich erfolge.[5] Im Ergebnis sah das Gericht die Ermächtigungsgrundlage der Telefonüberwachung gem. § 100a S. 1 Nr. 1c, S. 2 a. F. StPO[6] als unzweifelhaft gegeben an.[7] Dies stieß in der Literatur auf erhebliche Kritik, es gebe für das Einwählen auf eine Mailbox schlicht und ergreifend keine Ermächtigungsgrundlage.[8] Grund sei zum einen, dass allein das Online-Einwählen in eine Mailbox nicht dem Fernmeldeverkehr zuzuordnen sei. Zum anderen sei kein „Überwachen" gegeben, wenn die Mailbox

---

[3] BGH 31.07.1995 – 2 BJs 94/94-6 u. a. = NJW 1997, 1934.

[4] BGH 31.07.1995 – 2 BJs 94/94-6 u. a. = NJW 1997, 1934.

[5] BGH 31.07.1995 – 2 BJs 94/94-6 u. a. = NJW 1997, 1934.

[6] § 100a StPO in der Fassung vom 28.10.1994

„1 Die Überwachung und Aufzeichnung des Fernmeldeverkehrs darf angeordnet werden, wenn bestimmte Tatsachen den Verdacht begründen, daß jemand als Täter oder Teilnehmer

1. (…)

c) Straftaten gegen die öffentliche Ordnung (§§ 129 bis 130 des Strafgesetzbuches, § 92 Abs. 1 Nr. 7 des Ausländergesetzes),

(…)

begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat, und wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

2 Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, daß sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder daß der Beschuldigte ihren Anschluß benutzt."

[7] BGH 31.07.1995 – 2 BJs 94/94-6 u. a. = NJW 1997, 1934.

[8] *Palm/Roy*, NJW 1997, 1904, 1905; *Bizer*, DuD 1996, 627.

nur einmalig abgehört werde.[9] Die Ermächtigung beschränke sich auch lediglich auf einen einmaligen Zugriff, da ein mehrfacher Zugriff auf eine Mailbox dem Richtervorbehalt der Durchsuchung aus § 105 StPO widerspreche.[10]

Diese Sicht ist zutreffend. Zwar wurde der Begriff des *Fernmeldeverkehrs* in der StPO in der Fassung vom 17.12.1997 durch das Begleitgesetz zum Telekommunikationsgesetz durch den Begriff der *Telekommunikation* ersetzt, dies stellt allerdings nur eine terminologische Änderung dar.[11] Der Begriff der Telekommunikation wird durch den Gesetzgeber in § 3 Nr. 16 a. F. TKG als „(…) der technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen (…)" definiert.[12] Sind die Nachrichten allerdings nur auf der Mailbox gespeichert, findet kein Kommunikationsvorgang mehr statt, sodass auch kein Fernmeldeverkehr beziehungsweise keine Telekommunikation mehr aufgezeichnet werden kann.[13]

Im Ergebnis ist daher festzuhalten, dass sich bereits hier die Nähe zur Durchsuchung zeigte und ein Umgang mit dieser Tatsache sich schon damals als schwer erwies.

2. Erste Erwähnung einer Online-Durchsuchung

Was folgte, war eine Auseinandersetzung mit dem Thema in der Politik. Als Reaktion auf die Terroranschläge vom 11.09.2001 wurde ein Sicherheitspaket mit Änderungen des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes, des Bundesgrenzschutzgesetzes, des BKA-Gesetzes und des Ausländergesetzes verabschiedet.[14]

Die erste namentliche Erwähnung der Online-Durchsuchung findet sich in einer Dienstanweisung *Schilys*.[15] Das von ihm geführte Bundesinnenministe-

---

[9] *Bizer*, DuD 1996, 627.

[10] BGH 31.07.1995 – 2 BJs 94/94-6 u. a. = NJW 1997, 1934.

[11] *Palm/Roy*, NJW 1997, 1904.

[12] Heute § 3 Nr. 22 TKG: „Telekommunikation" der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen, (…).

[13] Vgl.: *Palm/Roy*, NJW 1997, 1904; *Bizer*, DuD 1996, 627.

[14] Gesetz zur Bekämpfung des internationalen Terrorismus vom 09.01.2002, Bundesgesetzblatt Jahrgang 2002 Teil I Nr. 3, 11.01.2002.

[15] *Rosenbach*, Spiegel 2007, Digitale Spaltung; online abzurufen über http://www.spiegel.de/spiegel/print/d-52109100.html (zugegriffen am 22.8.2018); *Rath*, TAZ 2007, Online-Schnüffeln ohne Freibrief?; online abzurufen über https://www.taz.de/

rium soll 2005 eine Dienstanweisung an das Bundesamt für Verfassungsschutz geleitet haben, in der Zugriffe auf den Server oder den PC auch bei abgeschlossener Kommunikation vorgesehen waren. Auch sei die Rede von verdeckten Zugriffen auf PCs oder Server gewesen.[16] Eine Rückverfolgung und eine sichere Feststellung des Wortlautes dieser Dienstvorschrift ist nicht mehr möglich, sodass auf Medienberichte aus dieser Zeit zurückgegriffen werden muss.

3. Online-Durchsuchung als klassische Durchsuchung?

Erstmals breite öffentliche Aufmerksamkeit wurde der Online-Durchsuchung im Jahr 2006 zuteil. Im Februar 2006 beschloss ein Ermittlungsrichter am Bundesgerichtshof, dass eine Durchsuchung des PC-Datenbestandes eines Beschuldigten ohne dessen Wissen von § 102 StPO gedeckt sei.[17] Dabei wurde den Ermittlungsbehörden gestattet, von außen ein Programm auf dem Computer des Beschuldigten zu installieren und so die Daten zur Durchsicht an die Ermittlungsbehörden zu übertragen.[18] Dabei stehe die Heimlichkeit der Maßnahme einer Anwendbarkeit von § 102 StPO nicht entgegen, da die Durchsuchung keine Maßnahme sei, die nach ihrer Rechtsnatur offen durchgeführt werden müsse.[19] Außerdem sei dem Fortschritt in der Informationsgesellschaft dadurch Rechnung zu tragen, dass keine überhöhten Anforderungen an die Bestimmtheit einer Norm zu stellen seien.[20] Grundsätzlich erlaube der Richtervorbehalt nur einen einmaligen Zugriff, es sei denn, dem stünden technische Schwierigkeiten entgegen. Ein erneuter Zugriff sei außerdem möglich, wenn die Maßnahme mit einer herkömmlichen umfangreichen Durchsuchung vergleichbar sei, bei der diese ebenfalls innerhalb einer Durchsuchungsaktion fortgesetzt werde.[21] Tatsächlich wurde die Maßnahme nicht durchgeführt.[22]

Archiv-Suche/!287008&s=Online-Durchsuchung&SuchRahmen=Print/ (zugegriffen am 22.8.2018).

16 *Rosenbach*, Spiegel 2007, Digitale Spaltung; online abzurufen über http://www.spiegel.de/spiegel/print/d-52109100.html (zugegriffen am 22.8.2018); *Rath*, TAZ 2007, Online-Schnüffeln ohne Freibrief?; online abzurufen über https://www.taz.de/Archiv-Suche/!287008&s=Online-Durchsuchung&SuchRahmen=Print/ (zugegriffen am 22.8.2018).

17 BGH 21.02.2006 – 3 BGs 31/06, 60 = StV 2007, 60.

18 BGH 21.02.2006 – 3 BGs 31/06 = StV 2007, 60.

19 BGH 21.02.2006 – 3 BGs 31/06, 61 = StV 2007, 60.

20 BGH 21.02.2006 – 3 BGs 31/06, 61 = StV 2007, 60.

21 BGH 21.02.2006 – 3 BGs 31/06, 63 = StV 2007, 60.

22 BT-Drucks., 16/3973, Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE, S. 2.

Kernproblem dieses Beschlusses war die Frage, ob es sich bei der Durchsuchung um eine zwingend offene Maßnahme handelt oder ob sie auch heimlich möglich ist. Zwingend für die Offenheit der Durchsuchung sprechen die Anwesenheitsrechte aus § 106 StPO. Diese fordern zwar keine Anwesenheitspflicht, dennoch können Beschuldigte so ihr Kontrollrecht ausüben.[23] Dem wurde damals in der Literatur entgegengehalten, dass es sich bei den §§ 106, 107 StPO um reine Ordnungsvorschriften handle,[24] die keine Rechtsfolgen begründen und keine Tatbestandsvoraussetzungen der Durchsuchung darstellen würden.[25] Außerdem genüge es diesen Ordnungsvorschriften, wenn der*die Betroffene nach Abschluss der Ermittlungen eine Mitteilung gem. § 107 StPO erhalte.[26] An dieser Stelle ist lediglich festzuhalten, dass Rechtsprechung und Teile der Literatur bis zu diesem Zeitpunkt davon ausgingen, dass eine Online-Durchsuchung auf Grundlage der Regelungen zur Durchsuchung gem. §§ 102 ff. StPO möglich sei. Unter der Online-Durchsuchung, die zu diesem Zeitpunkt auf die Ermächtigungsgrundlage der Durchsuchung gestützt wurde, verstand man demnach die Installation eines Computerprogrammes von außen auf dem Computer des*der Beschuldigten, um die darauf abgelegten Dateien zu kopieren und zur Durchsicht an die Ermittlungsbehörden zu übertragen.[27] Ziel war es, wie bei der klassischen Durchsuchung, beweiserhebliche Dateien zu sichern und diese gegebenenfalls sicherzustellen.[28]

4. Kehrtwende am Bundesgerichtshof

Nur zehn Monate später erfolgte dann die Kehrtwende am Bundesgerichtshof. Am 25.11.2006 beschloss ein Ermittlungsrichter, dass die heimliche Ausforschung eines Computers nicht von § 102 StPO gedeckt sei.[29] Grund hierfür sei, dass es sich bei der Durchsuchung um einen körperlichen und nicht um einen elektronischen Vorgang handle. Außerdem sei die Durchsuchung eine auf Offenheit angelegte Maßnahme. Auch bei der weitesten Auslegung der Norm könne sie nicht als Rechtsgrundlage herangezogen werden.[30] Dieser Beschluss des BGH-Ermittlungsrichters wurde vom 3. Strafse-

---

23 *Beulke/Meinighaus*, StV 2006, 63, 64.

24 *Hegmann*, in: BeckOK StPO, § 106, Rn. 3; a.A. *Hauschild*, in: MüKO StPO, § 106, Rn. 1.

25 *Hofmann*, NStZ 2005, 121, 124.

26 *Graf*, DRiZ 1999, 281, 285.

27 BGH 21.02.2006 – 3 BGs 31/06, 60 = StV 2007, 60; *Beulke/Meinighaus*, StV 2006, 63, 64; *Hofmann*, NStZ 2005, 121.

28 *Graf*, DRiZ 1999, 281, 285.

29 BGH 25.11.2006 – 1 BGs 184/06, 175 = MMR 2007, 174.

30 BGH 25.11.2006 – 1 BGs 184/06, 175 = MMR 2007, 174.

nat bestätigt.[31] Auch hier wurde festgestellt, dass es an der erforderlichen Befugnisnorm fehle. Das liege daran, dass die rechtmäßige Durchsuchung die Anwesenheit der betroffenen Person fordere, wodurch die Maßnahmen offengelegt werden. Grund hierfür sei, dass die Vorschriften der §§ 106, 107 StPO zwingendes Recht darstellen und nicht zur Disposition der Ermittlungsbeamt*innen stehen.[32]

Nachdem sich nun die Rechtsprechung und die Mehrheit der Lehre gegen die Anwendung der Vorschrift zur Durchsuchung auf die Online-Durchsuchung ausgesprochen hatten, blieb die Forderung nach einer neuen gesetzlichen Grundlage im Raum stehen.[33]

5. Das „Programm zur Stärkung der Inneren Sicherheit"

Parallel zu dieser Rechtsprechungsentwicklung wurde auch die Politik tätig, indem am 09.11.2006 der Haushaltsausschuss des Deutschen Bundestags das „Programm zur Stärkung der Inneren Sicherheit" (PSIS) mit einem Gesamtvolumen von 132 Mio. EURO beschloss.[34] Mit diesem Programm sollte, als Reaktion auf Kofferbombenanschläge auf Regionalzüge nach Koblenz und Dortmund, der fortbestehenden Bedrohungslage entgegengetreten werden.[35] Ziel war es, mögliche künftige Täter*innen abzuschrecken und das Sicherheitsgefühl in der Bevölkerung zu stärken.[36] In Anlage 2b, Maßnahme 3, fordert das PSIS die „(…) technische Fähigkeit, entfernte PC auf verfahrensrelevante Inhalte hin untersuchen zu können, ohne selbst am Standort des Geräts anwesend zu sein".[37]

---

[31] BGH 31.01.2007 – StB 18/06, BGHSt 51, 211 = MMR 2007, 237.

[32] BGH 31.01.2007 – StB 18/06, BGHSt 51, 211, 213 = MMR 2007, 237.

[33] *Bär*, MMR 2007, 239, 242.

[34] *Bundesministerium des Inneren* 2006, Grünes Licht im Haushaltsausschuss für BMI-Programm zur Stärkung der Inneren Sicherheit; online abzurufen über https://web.archive.org/web/20090102161912/http://www.bmi.bund.de/Internet/Content/Nachrichten/Pressemitteilungen/2006/11/Programm__zur__Staerkung__der__Inneren__Sicherheit.html (zugegriffen am 20.11.2020).

[35] BT-Drucks., 16/3973, Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE, S. 1.

[36] *Bundesministerium des Inneren* 2006, Grünes Licht im Haushaltsausschuss für BMI-Programm zur Stärkung der Inneren Sicherheit; online abzurufen über https://web.archive.org/web/20090102161912/http://www.bmi.bund.de/Internet/Content/Nachrichten/Pressemitteilungen/2006/11/Programm__zur__Staerkung__der__Inneren__Sicherheit.html (zugegriffen am 20.11.2020).

[37] Auch hier muss auf die Sekundärquelle einer Bundestagsdrucksache verwiesen werden, da das PSIS als solches nicht mehr einzusehen ist: BT-Drucks., 16/3973, Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE, S. 1.

Durch eine Kleine Anfrage der FDP im Jahr 2007 wurde die Online-Durchsuchung erneut Thema auf der bundespolitischen Bühne.[38] In diesem Zuge stellte sich heraus, dass das BKA zu diesem Zeitpunkt, auf Grundlage von § 2 Abs. 6 Nr. 3 BKAG, die technische Umsetzbarkeit einer Online-Durchsuchung im Rahmen eines Entwicklungsprozesses prüfte. Dabei wurde das bewusste Offenlassen von Sicherheitslücken, also die Nutzung von sogenannten Zero-Day-Exploits, als Mittel zur Infiltrierung des Systems allerdings nicht angestrebt.[39] Nach damaliger Ansicht der Bundesregierung unterscheide sich die Online-Durchsuchung von der Beschlagnahme eines Rechners dadurch, dass bei einer Beschlagnahme Daten, die sich auf dem Arbeitsspeicher des Rechners befinden, nicht erlangt werden können.[40] Außerdem gab es nach Ansicht der Bundesregierung bereits Ermächtigungsgrundlagen zur Online-Durchsuchung im Bundesverfassungsschutzgesetz, dem Gesetz über den militärischen Abschirmdienst und dem Gesetz über den Bundesnachrichtendienst.[41]

Der *Spiegel* berichtete 2009, dass mehr als 2 500 Online-Durchsuchungen durch den Bundesnachrichtendienst durchgeführt worden seien. Diese erfolgten zumeist mittels Keyloggern, aber auch durch Trojaner.[42]

6. Zusammenfassung

Zusammenfassend lässt sich sagen, dass es bei den ersten Überlegungen zur Online-Durchsuchung zumeist um einen einmaligen Zugriff auf die Systeme ging, bei dem lediglich die Daten kopiert werden sollten. Auf eine „Überwachung" über einen längeren Zeitraum hinweg war die Online-Durchsuchung zunächst nicht angelegt. Mit dieser Tatsache und der daraus resultierenden Nähe zur „klassischen" Durchsuchung, die sich in der Rechtsprechung und der Literatur immer wieder herauskristallisierte, lässt sich auch der Ursprung des Wortes Online-Durchsuchung erklären. Somit wurde

---

38 BT-Drucks., 16/3972, Antwort der Bundesregierung auf die Kleine Anfrage der FDP, S. 1.

39 BT-Drucks., 16/3972, Antwort der Bundesregierung auf die Kleine Anfrage der FDP, S. 1.

40 BT-Drucks., 16/3972, Antwort der Bundesregierung auf die Kleine Anfrage der FDP, S. 3.

41 BT-Drucks., 16/4803, Schriftliche Fragen mit den in der Woche vom 19. März 2007 eingegangenen Antworten der Bundesregierung, 8, 9. Als Ermächtigungsgrundlagen wurden hierbei angegeben: Bundesverfassungsschutz: § 9 I, 8 II BVerfSchG; Militärische Abschirmdienste: §§ 5, 4 I MADG i. V. m. § 9 I, 8 II BVerfSchG; Bundesnachrichtendienst: § 3 BNDG.

42 *Stark*, Spiegel 2009, Digitale Spionage; online abzurufen über http://www.spiegel.de/spiegel/print/d-64497190.html (zugegriffen am 31.5.2021).

Anfang der 2000er Jahre davon ausgegangen, dass durch die Online-Durchsuchung nur unwesentlich mehr Daten gesichert würden als bei der „klassischen“ Durchsuchung. Eine mögliche Kernbereichsproblematik wurde bis dato von der Gesetzgebung nicht erkannt und berücksichtigt.

II. Entwicklung in der Literatur

Spätestens seit den Beschlüssen des Bundesgerichtshofes war die Online-Durchsuchung als Thema nun auch in der Literatur und bei den Organen der Strafverfolgung angekommen.

Zu Beginn wurde unter diese Maßnahme sowohl das heimliche Ausspähen der Daten von einem IT-System als auch die komplette Kopie des IT-Systems mittels eines Internetzugangs subsumiert.[43] Teilweise wurde dabei zwischen der Online-Durchsuchung und einer Echtzeitüberwachung unterschieden.[44] Diese Unbestimmtheit ergab sich wohl vor allem aus der Tatsache, dass nicht deutlich wurde, wie die Maßnahme, welche noch in ihren Kinderschuhen steckte, technisch umgesetzt werden würde. Die Ausführungen in der Literatur waren somit noch recht unbestimmt, weshalb eine abstrakt-generelle Auseinandersetzung mit diesem Thema stattfand.

1. Besteht eine Ermächtigungsgrundlage für die Online-Durchsuchung?

Im repressiven Bereich stellte man sich in der Literatur nicht nur die Frage nach der Verfassungsmäßigkeit der Maßnahmen, sondern vordergründig die nach einer Ermächtigungsgrundlage, die der Bundesgerichtshof, wie bereits dargestellt, schnell beantwortet hatte. Dabei stand in der Literatur die Anwendbarkeit der §§ 102 (ggf. analog), 100a (a. F.) und 110a (a. F.) StPO im Vordergrund.

Eine Strömung innerhalb der Strafrechtswissenschaft widersprach einer Anwendung der Vorschriften über die Durchsuchung (§§ 102 ff. StPO) mit dem Argument des Bundesgerichtshofs, dass es sich bei der Durchsuchung zwingend um eine offene Maßnahme handle und die Online-Durchsuchung diesem Grundsatz aufgrund ihrer Heimlichkeit widerspreche.[45] Eine zuwi-

---

[43] *Hornung*, DuD 2007, 575; *Buermeyer*, HRRS 2007, 154, 160; *Schlegel*, GA 2007, 648, 650.

[44] *Rux*, JZ 2007, 285, 288.

[45] *Valerius*, JR 2007, 275, 277; *Beulke/Meinighaus*, in: FS Widmaier, 70; *Hornung*, DuD 2007, 575, 576; *Buermeyer*, HRRS 2007, 154, 158; *Rux*, JZ 2007, 285, 290; *Kudlich*, JA 2007, 391, 393; *Jahn/Kudlich*, JR 2007, 57, 59.

der laufende Ansicht hielt dem jedoch entgegen, dass es sich bei der Online-Durchsuchung sogar um die mildere Maßnahme gegenüber der „klassischen" Durchsuchung handle.[46] Außerdem müsse die Person, die sich des Internets bediene, mit vielfältigen Angriffen auf ihr System rechnen, darunter auch solchen, die vom Staat ausgehen.[47] § 100a StPO a. F. (Überwachung der Telekommunikation) komme als taugliche Ermächtigungsgrundlage nicht in Betracht, da die Überwachung eines IT-Gerätes nicht unter den Begriff der Telekommunikation falle.[48]

Eine weitere Strömung stellte sich aus rechtspolitischer Sichtweise die Frage nach der Notwendigkeit der Online-Durchsuchung im repressiven Bereich. Denn hier sei insbesondere zu bedenken, dass die Einführung der Online-Durchsuchung ihr Ziel, die Bekämpfung von Terrortaten, gar nicht erreichen könne. IT-Systeme könnte effektiv mit Sicherheitsmechanismen ausgestattet werden und gerade Terrorist*innen, die in der Lage seien, Anschläge im großen Ausmaß zu planen und durchzuführen, seien auch im Stande, sich vor Spionagesoftwares zu schützen.[49] Eine Online-Durchsuchung ermögliche lediglich die Verfolgung von „virtuellen Eierdieben".[50]

§ 161 StPO als Generalklausel auf die Online-Durchsuchung anzuwenden, dürfe schon aufgrund der hohen Eingriffsintensität in Grundrechte nicht erfolgen.[51] Die Frage des Eingriffs in Grundrechte war eine der meist diskutierten, sollte es künftig zu einer Einführung der Online-Durchsuchung kommen.

2. Online-Durchsuchung als Eingriff in Art. 13 GG?

Eine Ansicht ging davon aus, dass die Online-Durchsuchung in Art. 13 GG eingreife, da auch das „virtuelle Betreten" der Wohnung in den Schutzbereich des Art. 13 GG falle.[52] Deshalb müssten die Verfahrensvorschriften des Art. 13 GG in Bezug auf dieses „virtuelle Betreten" angepasst und damit die Verfassung geändert werden.[53] Andere siedelten dieses Problem der Sen-

---

46 *Hofmann*, NStZ 2005, 121, 124.

47 *Hofmann*, NStZ 2005, 121, 124.

48 *Hornung*, DuD 2007, 575, 576; a. A. und für die Anwendung des § 100a a. F.: *Hofmann*, NStZ 2005, 121, 125; *Jahn/Kudlich*, JR 2007, 57, 61.

49 *Beulke/Meinighaus*, in: FS Widmaier, 72; *Buermeyer*, HRRS 2007, 154, 166.

50 *Buermeyer*, HRRS 2007, 154, 165.

51 *Hofmann*, NStZ 2005, 121; *Beukelmann*, StraFo 2008, 1, 3; *Jahn/Kudlich*, JR 2007, 57, 60.

52 *Valerius*, JR 2007, 275, 280.

53 *Valerius*, JR 2007, 275, 280; *Hornung*, DuD 2007, 575, 578; *Rux*, JZ 2007, 285, 295; *Kudlich*, JA 2007, 391, 394; *Jahn/Kudlich*, JR 2007, 57, 60.

sibilität der Daten allerdings nicht im Bereich des Wohnungsbegriffes an, sondern sahen hierin einen Eingriff in den absoluten Kernbereich der privaten Lebensgestaltung.[54] Einige gingen daher primär von einem Eingriff in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG aus.[55]

Warnend wurde in der Literatur darauf hingewiesen, dass über die IT-Geräte wesentliche Inhalte über deren Nutzer*innen gespeichert und protokolliert würden und die Maßnahme zu einer weitreichenden Überwachung dieser Nutzer*innen führen könne, die die Qualität von Persönlichkeitsprofilen erreichen könne.[56] Dies sei insbesondere gegeben, weil der Computer „praktisch nichts vergisst".[57]

Im Ergebnis lässt sich wohl sagen, dass grundsätzlich Einigkeit bestand, dass es an einer Ermächtigungsgrundlage fehlt. Eine Normierung müsste sich erheblichen verfassungsrechtlichen Problemen stellen. Dabei gab es zwei Ansätze: Zum einen könnten die Schranken des Art. 13 GG erweitert werden, um deren Gedanken auf die Online-Durchsuchung zu übertragen. Dann müsse aber auch die Verfassung geändert werden.[58] Zum anderen könnte, weil Art. 13 GG nicht immer Anwendung finde, ein Eingriff in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG zu bejahen sein.[59] Unabhängig davon, welcher Eingriff bejaht werde, sei dennoch stets der Kernbereich der privaten Lebensgestaltung zu berücksichtigen.[60] Außerdem müsste im politischen Diskurs auch zur Debatte stehen, ob eine Online-Durchsuchung überhaupt notwendig sei.[61]

3. Zusammenfassung

Festzuhalten ist, dass sich der Begriff der „Online-Durchsuchung" durchgesetzt hatte, ungeachtet dessen, ob es sich um eine eigentliche Überwachung – diese technische Möglichkeit wurde erkannt – oder um eine reine

---

54 *Beukelmann*, StraFo 2008, 1, 4; *Hornung*, DuD 2007, 575, 577; *Schlegel*, GA 2007, 648, 661 f.; *Rux*, JZ 2007, 285, 291; *Kutscha*, NJW 2007, 1169, 1171.

55 *Hornung*, DuD 2007, 575, 579; *Schlegel*, GA 2007, 648, 660.

56 *Valerius*, JR 2007, 275, 279; *Beukelmann*, StraFo 2008, 1, 6; *Rux*, JZ 2007, 285.

57 *Beukelmann*, StraFo 2008, 1.

58 *Valerius*, JR 2007, 275, 280; *Hornung*, DuD 2007, 575, 578; *Rux*, JZ 2007, 285, 295; *Kudlich*, JA 2007, 391, 394; *Jahn/Kudlich*, JR 2007, 57, 60.

59 *Hornung*, DuD 2007, 575, 579; *Schlegel*, GA 2007, 648, 660.

60 *Beukelmann*, StraFo 2008, 1, 4; *Hornung*, DuD 2007, 575, 577; *Schlegel*, GA 2007, 648, 661 f.; *Rux*, JZ 2007, 285, 291; *Kutscha*, NJW 2007, 1169, 1171.

61 *Beulke/Meinighaus*, in: FS Widmaier, 72; *Buermeyer*, HRRS 2007, 154, 166.

„Spiegelung“ der Daten handelte, welche der Beschlagnahme eines Computers nahesteht.

Bis zu diesem Zeitpunkt bestand in der Strafrechtswissenschaft Uneinigkeit darüber, ob die Strafprozessordnung eine Online-Durchsuchung bereits deckte. Des Weiteren wurde auch der Diskurs über den Eingriff in Grundrechte durch eine Online-Durchsuchung intensiv geführt, ohne dass an dessen Ende ein Ergebnis stand. Insbesondere ein Eingriff in Art. 13 GG wirkte unausgegoren und konnte nicht überzeugen. Es brauchte also eine erste Verankerung der Online-Durchsuchung im Gesetz, um die Rechtsprechung und die Rechtswissenschaft „voranzubringen“.

III. Verfassungsschutzgesetz Nordrhein-Westfalen

Mit der Änderung des Verfassungsschutzgesetzes Nordrhein-Westfalen und der darin enthaltenen Einführung einer Online-Durchsuchung betrete man rechtliches Neuland[62] – so die Einschätzung des dortigen Haupt- und Innenausschusses zu Beginn des Gesetzgebungsprozesses in Bezug auf den Zugriff auf informationstechnische Systeme. 2006 erfolgte eine erste Normierung der „Online-Durchsuchung“ im Verfassungsschutzgesetz Nordrhein-Westfalen. Hier hieß es in § 5 VSG NRW a. F.:

„*§ 5*

Befugnisse

(1) …

(2) Die Verfassungsschutzbehörde darf nach Maßgabe des § 7 zur Informationsbeschaffung als nachrichtendienstliche Mittel die folgenden Maßnahmen anwenden:

…

11. heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel. Soweit solche Maßnahmen einen Eingriff in das Brief-, Post- und Fernmeldegeheimnis darstellen bzw. in Art und Schwere diesem gleichkommen, ist dieser nur unter den Voraussetzungen des Gesetzes zu Artikel 10 Grundgesetz zulässig; …“

Im Folgenden wird es nun darum gehen, das Gesetzgebungsverfahren darzustellen, um einen ersten Überblick über die Probleme im Zusammenhang mit dieser verdeckten Ermittlungsmaßnahme zu erhalten. Später folgte dann eine Verfassungsbeschwerde gegen diese Norm. Es liegt also nahe, auch dieses Urteil näher zu beleuchten.

---

62 LT-NRW Drucks., Ausschussprotokoll 14/275, S. 1.

1. Gesetzgebungsverfahren

Grundgedanke des von der Landesregierung am 03.07.2006 zur ersten Lesung eingebrachten Entwurfs des „Gesetzes zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen“ (Verfassungsschutzgesetz Nordrhein-Westfalen – VSG NRW) war es, der „Bedrohung durch den islamistischen Terrorismus“, insbesondere nach den Anschlägen in Marokko, Spanien und London, zu begegnen.[63] Dabei sollte die Norm des § 5 Abs. 2 Nr. 11 VSG NRW a. F. die Befugnis für die „(…) legendierte Teilnahme an Chats, Auktionen und Tauschbörsen, die Feststellung der Domaininhaber, die Überprüfung der Homepagezugriffe, das Auffinden verborgener Webseiten sowie der Zugriff auf gespeicherte Computerdaten (…)“[64] schaffen.

a) Kontroversen um den Gesetzesentwurf

Von der Landesregierung wurden mögliche verfassungsrechtliche Probleme nur im Zusammenhang mit dem Recht auf informationelle Selbstbestimmung und dem Bestimmtheitsgebot erkannt.[65] Die Annahme eines Verstoßes gegen das Recht auf Unverletzlichkeit der Wohnung durch einen solchen verdeckten Angriff auf ein IT-System über das Internet sei hingegen nach Ansicht des damaligen Innenministers Nordrhein-Westfalens, *Wolf*, „völlig abwegig“.[66] Die Opposition (*Rudolph* für die SPD) wies allerdings bereits zu diesem Zeitpunkt darauf hin, dass es sich bei der in dem Gesetzentwurf formulierten Ermächtigung nicht mehr um die reine Beobachtung der aktuellen Kommunikation handle, sondern zum ersten Mal auf Inhalte des IT-Systems zugegriffen werde, was insbesondere mit Art. 13 GG nicht zu vereinbaren sei.[67] Bei der Norm handle es sich nach *Düker* um einen Eingriff in den Kernbereich der Privatsphäre, welchem in der Norm nicht genügend Rechnung getragen werde. Aus diesem Grund sei dieser Gesetzentwurf nicht mit der Verfassung zu vereinbaren.[68]

Es folgte am 19.10.2006 eine öffentliche Anhörung verschiedener Gutachter*innen zu dem geplanten Gesetzesentwurf. Auch hier wurde klar, dass sich der Gesetzesentwurf in Bezug auf die Online-Durchsuchung erheblicher Kritik stellen musste. Der gemeinsame Tenor war, dass ein solcher Zugriff

63 LT-NRW Drucks., 14/2211, S. 1.
64 LT-NRW Drucks., 14/2211, S. 17.
65 LT-NRW Drucks., 14/2211, S. 17.
66 LT-NRW Drucks., Plenarprotokoll 14/36, S. 3952.
67 LT-NRW Drucks., Plenarprotokoll 14/36, S. 3954.
68 LT-NRW Drucks., Plenarprotokoll 14/36, S. 3956.

auf den Computer über das Internet nicht mit Art. 13 GG vereinbar sei.[69] Außerdem wurde von den Gutachter*innen auf die großen Probleme im Zusammenhang mit dem Kernbereich der privaten Lebensgestaltung hingewiesen.[70]

Zum einen wurde in den jeweiligen Stellungnahmen thematisiert, dass die Beobachtung der Kommunikation in den Schutzbereich des Art. 10 GG eingreifen könnte. Sollte dem nicht so sein, dann wäre zumindest ein Eingriff in das Recht auf informationelle Selbstbestimmung zu berücksichtigen.[71] Außerdem sei darauf hinzuweisen, dass der Zugriff auf Computer auch in Art. 13 GG eingreifen könne.[72] Sollte eine Maßnahme aus Nr. 11 des Gesetzentwurfes in den unantastbaren Kernbereich der privaten Lebensgestaltung eingreifen, so würde eine Überwachung gänzlich ausscheiden.[73] Aufgrund der bereits entwickelten Erwägungen zum Schutz des Kernbereichs der privaten Lebensgestaltung sei es notwendig, den Gesetzesentwurf um solche Normen zu ergänzen, die diese Daten schützen. Abgeleitet werden könnten diese Grundsätze demnach unter anderem aus der Rechtsprechung zur akustischen Wohnraumüberwachung.[74]

Dennoch beschloss der Innenausschuss am 09.11.2006 die Annahme des Gesetzesentwurfes.[75] Die Änderungsanträge der SPD wurden abgelehnt. Die CDU und die FDP, die damaligen Regierungsparteien, reagierten auf die Kritik der Gutachter*innen ebenfalls mit einem Änderungsantrag. In diesem Antrag wurde festgestellt, dass die Befugnisse (hierunter auch § 5 Abs. 2 Nr. 11 VSG NRW a. F.) das Recht auf informationelle Selbstbestimmung in erheblicher Art und Weise tangieren. Diesem Umstand wolle man mit „(…) entsprechenden Evaluierungspflichten versehen mit einer Befristung (…)“ entgegentreten.[76] Dieser Änderungsantrag wurde am 19.12.2006

---

69 LT-NRW Drucks., Ausschussprotokoll 14/275, S. 5.

70 LT-NRW Drucks., Ausschussprotokoll 14/275, S. 7, 14, 19, 23, 33.

71 *Schwarz*, Gutachterliche Stellungnahme, LT-Drucks. 14/0650, S. 5; *Huster*, Gutachterliche Stellungnahme zur LT-Drucks., NRW Stellungnahme 14/0641, S. 3.

72 *Schwarz*, Gutachterliche Stellungnahme, LT-Drucks. 14/0650, S. 5; *Huster*, Gutachterliche Stellungnahme, LT-Drucks., 14/0641, S. 4; *Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen*, Gutachterliche Stellungnahme, LT-Drucks., 14/0625, S. 7.

73 *Schwarz*, Gutachterliche Stellungnahme, LT-Drucks. 14/0650, S. 7; das Problem zwar erkennend, aber für nicht anwendbar haltend, weil solche Daten nicht Ziel der Maßnahme seien: *Bundesamt für Verfassungsschutz*, Gutachterliche Stellungnahme, LT-Drucks., 14/0639, S. 7.

74 *Roth*, Gutachterliche Stellungnahme, LT-Drucks., 14/0645, S. 19; *Roggan*, Gutachterliche Stellungnahme, LT-Drucks., 14/0628, S. 7.

75 LT-NRW Drucks., Ausschussprotokoll 14/297, S. 19.

76 LT-NRW Drucks., 14/3133, S. 2.

angenommen.[77] Am 20.12.2006 erfolgte dann die Verkündung des Gesetzes in der Form des Regierungsentwurfes und mit Einarbeitung des Änderungsantrags.[78]

Zusammenfassend lässt sich sagen, dass schon im Gesetzgebungsverfahren viele verfassungsrechtliche Bedenken bestanden, denen durch die Regierungsparteien lediglich durch Evaluierungspflichten Rechnung getragen wurde. Letztlich wurde ein Gesetz verkündet, bei dem trotz der Neugestaltung einer Eingriffsbefugnis, die es so zuvor noch nicht in Deutschland gegeben hatte, innerhalb des Gesetzgebungsverfahrens nicht genügend Raum für Diskussion gegeben wurde. Außerdem ist besonders darauf hinzuweisen, dass bereits im Gesetzgebungsverfahren erkannt wurde, dass die Norm den Grundsätzen zum Schutz des Kernbereichs der privaten Lebensgestaltung nicht gerecht wurde.[79] Es fehlte an jeglicher Vorsorge zum Schutz des Kernbereiches. So kann vermutet werden, dass hier bewusst abgewartet wurde, welchen verfassungsrechtlichen Rahmen das Bundesverfassungsgericht für den Kernbereich privater Lebensgestaltung bei der Online-Durchsuchung abstecken würde.

b) Unklarheiten bei der Begriffsbestimmung

Unübersichtlich bleibt des Weiteren, wohl aufgrund der Unklarheiten über die praktische Umsetzbarkeit und die Zielsetzung der Maßnahme, die Begrifflichkeit dieser neuen Ermächtigungsgrundlage. So finden sich in den Gesetzgebungsunterlagen unterschiedliche Begrifflichkeiten für eine solche neu geschaffene Befugnisnorm. In der Norm selbst ist die Rede von einem „heimlichen Zugriff auf informationstechnische Systeme".

Zu den verschiedenen Begriffen in den Gesetzgebungsunterlagen für den Vorgang dieser verdeckten Ermittlungsmaßnahme gehören etwa der „Zugriff auf Daten"[80], das „heimliche Eindringen in fremde Rechnersysteme"[81], das

---

[77] *Landtag NRW*, Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen; online abzurufen über https://www.landtag.nrw.de/portal/WWW/Webmaster/GB_II/II.2/Suche/Landtagsdokumentation_ALWP/Suchergebnisse_Ladok.jsp?view=berver&mn=16301f3cae9&wp=14&w=native%28%27id%3D%27%271402306%2F0100%27%27+%27%29 (zugegriffen am 12.11.2020).

[78] Gesetz- und Verordnungsblatt für das Land NRW Nr. 38, S. 620; *Huster*, Gutachterliche Stellungnahme, LT-Drucks., 14/0641, S. 4.

[79] *Roth*, Gutachterliche Stellungnahme LT-Drucks., 14/0645, S. 19; *Roggan*, Gutachterliche Stellungnahme, LT-Drucks., 14/0628, S. 7.

[80] *Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen*, Gutachterliche Stellungnahme, LT-Drucks., 14/0625, S. 9.

[81] *Gusy*, Gutachterliche Stellungnahme, LT-Drucks., 14/0629, S. 6.

„Ausspähen von Computer Dateien“[82] oder das „Hacken von Computern“.[83] Außerdem finden sich Umschreibungen wie „Maßnahmen im Internet und Zugriff auf gespeicherte Computerdaten“[84], ONI-Maßnahmen (Offensive Nutzung des Internets)[85] und der Begriff „Zugriff auf informationstechnische Systeme“.[86] Die letztgenannte Bezeichnung der Rechtsgrundlage entspricht auch der geläufigen Formulierung in der heutigen Zeit. Die Aufzählung der verschiedenen Begrifflichkeiten zeigt deutlich, dass es bei der Schaffung der Ermächtigungsgrundlage insgesamt unklar war, was unter dieser Befugnis genau zu verstehen ist und wie sie durchgeführt werden kann und soll. So ist zum einen das Zielobjekt der Maßnahme nach diesen Formulierungen unklar. Teilweise wird nur von der „Nutzung des Internets“ gesprochen, während sich die Begriffe „Rechner“ oder „Computer(s)“ wohl nur auf den Personalcomputer als solchen beziehen, während wiederum der Begriff des „IT-Systems“ grundsätzlich deutlich weiter zu verstehen ist. Zum anderen ist allen voran der Begriff des Hackens ungenau. Fraglich ist hierbei, welches Vorgehen es beim Hacken braucht. Ist auch ein Hacken gegeben, wenn sich mittels eines Zugriffs von außen Zugang zum Zielobjekt verschafft wird (beispielsweise durch die Eingabe des Passwortes ohne technische Hilfsmittel)? Dann könnte auf einen Personalcomputer auch heimlich eingedrungen werden, ohne sich des „klassischen Hackens“ zu bedienen. Das „Ausspähen von Dateien“ ist wohl auch von außen auf ein System denkbar. „Maßnahmen im Internet“ können alle Maßnahmen sein, sogar unabhängig von einem konkreten IT-System, welches infiltriert werden soll.

Zu keinem Zeitpunkt war in dem Gesetzgebungsverfahren allerdings die Rede von einer „Online-Durchsuchung“. Zwar stand die Frage, ob eine solche neu eingeführte Maßnahme gegen Art. 13 GG verstoße, regelmäßig im Mittelpunkt des politischen Diskurses, dennoch blieb es lediglich bei einer solchen Parallelziehung.

2. Entscheidung des Bundesverfassungsgerichts

Die Ermächtigungsgrundlage des § 5 Abs. 2 Nr. 11 VSG NRW a. F. wurde dann, so wie es sich bereits in den Stellungnahmen angedeutet hatte, für

---

[82] LT-NRW Drucks., Ausschussprotokoll 14/292, S. 18; LT-NRW Drucks., Ausschussprotokoll 14/275, S. 18.

[83] *Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen*, Gutachterliche Stellungnahme, LT-Drucks., 14/0625, S. 9.

[84] *Huster*, Gutachterliche Stellungnahme, LT-Drucks., 14/0641, S. 3.

[85] *Bundesamt für Verfassungsschutz*, Gutachterliche Stellungnahme, LT-Drucks., 14/0639, S. 5.

[86] *Roggan*, Gutachterliche Stellungnahme, LT-Drucks., 14/0628, S. 6.

verfassungswidrig erklärt, weil sie mit Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG nicht vereinbar sei.[87] In dieser Entscheidung wurde das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG (IT-Grundrecht) entwickelt.[88]

Das Bundesverfassungsgericht erkennt in § 5 Abs. 2 Nr. 11 VSG NRW a. F. zwei Befugnisse, zum einen die des heimlichen Beobachtens und sonstigen Aufklärens des Internets und zum anderen die des heimlichen Zugriffs auf informationstechnische Systeme.[89] Dabei bestehe das Internet aus verschiedenen informationstechnischen Systemen und stelle auch selbst ein informationstechnisches System dar. Unter der erstgenannten Befugnis sei zu verstehen, dass die Verfassungsschutzbehörde die Inhalte der Internetkommunikation zur Kenntnis nehmen dürfe.[90]

a) Der „Zugriff auf informationstechnische Systeme"

Die heutige Online-Durchsuchung ist damit der zweiten Maßnahme, des Zugriffs auf informationstechnische Systeme, zuzuordnen. Wichtig ist nun die erste klare Definition des heimlichen Zugriffs auf informationstechnische Systeme. Nach Ansicht des Bundesverfassungsgerichts ist hierunter „(…) eine technische Infiltration zu verstehen, die etwa Sicherheitslücken des Zielsystems ausnutzt oder über die Installation eines Spähprogramms erfolgt"[91]. Ziel dieser Maßnahme sei dabei, die Überwachung der Nutzung des IT-Geräts, Speichermedien durchzusehen oder sogar das System selbst fernzusteuern.[92] Hier taucht mit Verweis auf die damals aktuelle Diskussion in der Rechtswissenschaft zum ersten Mal der Begriff der Online-Durchsuchung auf.[93]

Begründet wurde die Verfassungsbeschwerde durch die Beschwerdeführer*innen unter anderem damit, dass keine hinreichenden Vorkehrungen zum

---

87 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274 = NJW 2008, 822.

88 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274 = NJW 2008, 822.

89 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 276 = NJW 2008, 822.

90 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 277 = NJW 2008, 822.

91 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 276 = NJW 2008, 822.

92 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 276 = NJW 2008, 822.

93 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 277 = NJW 2008, 822.

Schutz des Kernbereichs der privaten Lebensgestaltung geschaffen worden seien. Außerdem sei die gesetzliche Eingriffsschwelle zu niedrig angesetzt.[94]

Die Bundesregierung nahm in der Anhörung an, dass sich die Online-Durchsuchung durch das wiederholte Eindringen oder das länger andauernde Verweilen in einem Rechner einer Überwachung annähere.[95] Sie ging davon aus, dass die Online-Durchsuchung aufgrund ihrer Eingriffstiefe unter einen Richtervorbehalt zu stellen und mit einer grundsätzlichen Benachrichtigungspflicht zu versehen sei.[96]

Die sächsische Landesregierung ging nicht davon aus, dass die „Online-Durchsuchung" in den Kernbereich der privaten Lebensgestaltung eingreife, weil der*die Einzelne nicht auf eine höchstpersönliche Kommunikation auf dem Personalcomputer angewiesen sei.[97]

Das Bundesverfassungsgericht hielt die Verfassungsbeschwerde gegen § 5 Abs. 2 Nr. 11 VSG NRW a. F. für begründet und erklärte die Norm in beiden Alternativen für verfassungswidrig und nichtig.[98] Begründet wurde dies mit der Verletzung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht).[99] Damit seien die vorgesehenen Eingriffe nicht verfassungsrechtlich gerechtfertigt. Außerdem genüge die Normierung des Eingriffs in informationstechnische Systeme nicht dem Gebot der Normenklarheit, die Anforderungen an den Verhältnismäßigkeitsgrundsatz seien nicht gewahrt und es werden keine hinreichenden Vorkehrungen zum Schutz des Kernbereichs der privaten Lebensgestaltung getroffen.[100]

---

[94] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 291 = NJW 2008, 822.

[95] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 293 = NJW 2008, 822.

[96] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 293 = NJW 2008, 822.

[97] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 296 = NJW 2008, 822.

[98] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 302 = NJW 2008, 822.

[99] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 302 = NJW 2008, 822.

[100] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 302 = NJW 2008, 822.

b) Das IT-Grundrecht

Mit der Benennung des IT-Grundrechts sollte der neuartigen Gefährdung der Persönlichkeit durch die neue Informationstechnik Rechnung getragen werden.[101] So werden, dem Bundesverfassungsgericht zufolge, die Personalcomputer, die sich in nahezu jedem Haushalt befinden, unter anderem dazu genutzt, eigene persönliche Angelegenheiten zu verwalten und zu archivieren. Diese Art der Nutzung von IT-Geräten habe so zu einer erheblichen Bedeutungssteigerung für die Persönlichkeitsentfaltung geführt.[102] Eine daraus resultierende Persönlichkeitsgefährdung ergebe sich insbesondere daraus, dass diese informationstechnischen Systeme nicht nur in der Lage seien, bewusst angelegte Daten durch den*die Nutzer*in zu speichern, sondern auch über die Fähigkeit verfügen, durch einen eigenständigen Datenverarbeitungsprozess selbstständig Daten zu produzieren, welche das Verhalten und die Eigenschaften der Nutzer*innen offenlegen.[103] Die Erhebung dieser Daten könne bei einer Auswertung durch Dritte weitreichende Rückschlüsse auf die Persönlichkeit des*der Nutzer*in zulassen und auch eine Profilbildung werde hierdurch ermöglicht.[104] Zum Schutz vor dieser Gefährdung reichen die Art. 10 und 13 GG nicht aus.[105] So schütze Art. 10 Abs. 1 GG lediglich die Übermittlung von Informationen an individuelle Empfänger*innen mittels des Telekommunikationsverkehrs, nicht aber die Vertraulichkeit und Integrität der IT-Systeme selbst.[106] Art. 13 Abs. 1 GG könne durch die Online-Durchsuchung dann betroffen sein, wenn die Ermittlungsbehörden zum Zwecke der physischen Manipulation des IT-Systems in die Räumlichkeiten der Wohnung eindrängen. Denkbar wäre eine Verletzung auch dann, wenn sich das IT-System in der Wohnung befinde und dazu genutzt werde, Vorgänge innerhalb der Wohnung zu überwachen.[107]

---

[101] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 303 = NJW 2008, 822.

[102] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 304 = NJW 2008, 822.

[103] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 305 = NJW 2008, 822.

[104] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 305 = NJW 2008, 822.

[105] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 306 = NJW 2008, 822.

[106] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 307 = NJW 2008, 822.

[107] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 310 = NJW 2008, 822.

Das IT-Grundrecht solle den persönlichen und privaten Lebensbereich der Grundrechtsträger*innen vor staatlichen Zugriffen im Bereich der Informationstechnik schützen.[108] Dieses Grundrecht finde Anwendung bei Systemen, die alleine oder aufgrund ihrer technischen Vernetzung dazu in der Lage seien, die personenbezogenen Daten des*der Betroffenen offenzulegen oder aus diesen ein aussagekräftiges Bild über die Persönlichkeit abzubilden.[109] Das Grundrecht beinhalte zum einen die Pflicht, dass die erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben, zum anderen müsse gewährleistet werden, dass die Leistungen und Funktionen des angegriffenen Systems sowie dessen Speicherinhalte nicht von Dritten genutzt werden können.[110] Der Schutz der Systeme sei aber nicht schrankenlos, ein Eingriff könne sowohl durch präventive Zwecke als auch durch Strafverfolgungszwecke gerechtfertigt werden. An einer solchen verfassungsmäßigen Grundlage fehle es aber hier.[111]

Außerdem fehle es der Norm an hinreichenden gesetzlichen Vorkehrungen, die Eingriffe in den unantastbaren Kernbereich der privaten Lebensgestaltung vermeiden.[112] So sei es möglich, dass bei einem heimlichen Zugriff auf ein informationstechnisches System persönliche Daten erhoben werden, die diesem Kernbereich zuzuordnen seien. Denn es können sich auf einem IT-Gerät sowohl Daten befinden, die Höchstpersönliches beinhalten, weil sie von dem*der Betroffenen selbst angelegt und gespeichert worden seien, aber auch solche, die auf dem Wege der Telekommunikation übermittelt worden seien.[113] Da der*die Betroffene aufgrund der Heimlichkeit der Ermittlungsmaßnahme keine Möglichkeit habe, auf die Wahrung seines*ihres Rechts auf einen unantastbaren Kernbereich der privaten Lebensgestaltung hinzuwirken, bedürfe es besonderer gesetzlicher Vorkehrungen, um diesem Ungleichgewicht entgegenzuwirken.[114] Der Kernbereich müsse zunächst dadurch abgesichert werden, dass Daten, die einen Bezug zu diesem aufweisen, soweit

---

[108] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 313 = NJW 2008, 822.

[109] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 314 = NJW 2008, 822.

[110] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 314 = NJW 2008, 822.

[111] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 315 = NJW 2008, 822.

[112] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 335 = NJW 2008, 822.

[113] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 335 = NJW 2008, 822.

[114] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 336 = NJW 2008, 822.

dies möglich sei, nicht erhoben werden. Da es aber unvermeidbar sein könne, Daten mit Kernbereichsbezug zu erheben, müsse ein hinreichender Schutz auf der Ebene der Auswertung gefunden werden. Dabei müssen diese Daten unverzüglich gelöscht und ihre Verwertung ausgeschlossen werden.[115] Auf technischer Ebene solle gewährleistet werden, dass kernbereichsrelevante Daten gar nicht erst erhoben werden, indem technische Such- oder Ausschlussmechanismen zu ihrer Bestimmung programmiert werden. Dieses Vorgehen komme aber zu schnell an seine technischen Grenzen, sodass allein diese Maßnahme dem Kernbereichsschutz nicht genüge.[116] Aus diesem Grund müsse ein zweistufiges Schutzkonzept eingehalten werden.[117] Auf der ersten Erhebungsebene sei darauf hinzuwirken, dass die Erhebung der kernbereichsrelevanten Daten, beispielsweise durch technische Sicherungen, unterbleibe.[118] Könne dies nicht gewährleistet werden, müsse durch geeignete Verfahrensvorschriften sichergestellt werden, dass die Intensität der Kernbereichsverletzung auf ein Minimum reduziert werde.[119] Dem solle im Rahmen einer Durchsicht der Daten in Bezug auf ihre Kernbereichsrelevanz Rechnung getragen werden. Sollte sich bei dieser Durchsicht herausstellen, dass kernbereichsrelevante Daten erhoben wurden, seien diese unverzüglich zu löschen und ihre Verwertung sei auszuschließen.[120] Dieses Schutzkonzept werde von § 5 Abs. 2 Nr. 11 VSG NRW i. V. m. § 4 Abs. 1 G10 nicht eingehalten. Es werde lediglich normiert, dass nicht mehr benötigte Daten zu löschen seien. Dies reiche nicht aus und führe zur Nichtigkeit der Norm.[121]

Im Kern liegen dieser Entscheidung also folgende, für die weitere Ausarbeitung wichtige, Aussagen zugrunde: Die Online-Durchsuchung ist an dem Grundrecht der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Geräte zu messen. Dabei muss der Kernbereichsschutz durch ein zweistufiges Schutzkonzept gewährleistet werden. Dieses Schutzkonzept umfasst auf der Erhebungsebene, dass kernbereichsrelevante Daten nach Möglichkeit nicht erhoben werden und dass auf der Auswertungsebene

---

115 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 337 = NJW 2008, 822.

116 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 337 = NJW 2008, 822.

117 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 338 = NJW 2008, 822.

118 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 338 = NJW 2008, 822.

119 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 338 = NJW 2008, 822.

120 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 339 = NJW 2008, 822.

121 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 339 = NJW 2008, 822.

kernbereichsrelevante Daten gelöscht werden, um sicherzustellen, dass sie nicht verwertet werden.[122]

c) Kritik in der Literatur

In der Literatur wurde dieses Urteil unterschiedlich aufgenommen. Einigkeit bestand jedoch darüber, dass es sich bei dieser Entscheidung um eine geschichtlich wegweisende handle.[123] Dabei wurde unter anderem von *Erd* zutreffend festgestellt, dass das Bundesverfassungsgericht mit diesem Urteil die Grundlage für die grundsätzliche Zulässigkeit der Online-Durchsuchung geschaffen habe.[124] Gleichzeitig werde dem Gesetzgeber auch eine enorme Aufgabe hinterlassen, denn wie es technisch und im Verfahren gewährleistet werden könne, dass Daten, die dem Kernbereich der privaten Lebensgestaltung zuzuordnen seien, nicht erhoben werden, werde nicht konkret festgelegt und bedürfe aus diesem Grund einer Konkretisierung durch den jeweiligen Bundes- oder auch Landesgesetzgeber.[125] Die Entscheidung führe zudem zu praktischen und personellen Problemen.[126] Die Aufgabe werde durch den technischen Fortschritt und die damit einhergehende wachsende Menge an Daten nicht leichter. Es bedürfe in der Weiterentwicklung der Ermächtigung zur Online-Durchsuchung auch einer wesentlichen Entwicklung der konkreten Vorschrift.[127]

Von Seiten der Rechtswissenschaft wurde in Bezug auf das Urteil zudem kritisch angemerkt, dass es der Neuschaffung eines Grundrechts und einer weiteren Ausprägung des allgemeinen Persönlichkeitsrechts nicht bedurft habe.[128] Außerdem wurde kritisiert, dass die dogmatische Würdigung des Rechts auf informationelle Selbstbestimmung nicht gelinge, weil bereits die reine Erhebung von personenbezogenen Daten in dieses Recht eingreife.[129]

Die Einwände gegen die Entwicklung des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Geräte können nicht überzeugen. Denn damit wurde, wie auch die Weiterentwicklung der Online-Durchsu-

---

122 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 339 = NJW 2008, 822.

123 *Erd*, KJ 2008, 118, 120; *Hornung*, CR 2008, 299; *Böckenförde*, JZ 2008, 925; *Hömig*, JURA 2009, 207.

124 *Erd*, KJ 2008, 118, 123.

125 *Erd*, KJ 2008, 118, 126; *Hornung*, CR 2008, 299, 304; *Böckenförde*, JZ 2008, 925.

126 *Hornung*, CR 2008, 299, 304.

127 *Hornung*, CR 2008, 299, 306.

128 *Sachs/Krings*, JuS 2008, 481, 483, 486; *Hornung*, CR 2008, 299, 306.

129 *Hornung*, CR 2008, 299, 301.

chung zeigt, konsequent und richtig auf die immer schneller fortschreitende Entwicklung im informationstechnischen Bereich reagiert. Mit diesem Urteil hat das Bundesverfassungsgericht einen wichtigen und ausbaufähigen Grundstein für die Absicherung der Bürger*innen gegen staatliches Eindringen in ihre technischen Geräte geschaffen. In diesem Zusammenhang ist, insbesondere wegen des Bezugs zur weiterführenden Ausarbeitung, auf die Tatsache hinzuweisen, dass das Bundesverfassungsgericht bereits hier die Gefahr der Erstellung von Persönlichkeitsprofilen der Nutzer*innen des auszuspähenden Geräts erkannt hat und auf diese hinweist.[130] Im Folgenden ist aus diesem Grund zu untersuchen, ob sich diese Gefahr durch den technischen Fortschritt intensiviert hat und wie mit dieser möglichen Intensivierung umzugehen ist. Das Urteil hat einen ersten Rahmen vorgegeben, um diesem technischen Fortschritt zu begegnen.

d) Zwischenresümee zur ersten Normierung der Online-Durchsuchung

Bereits die Ungenauigkeit im Umgang mit der Begrifflichkeit zu § 5 Abs. 2 Nr. 11 VSG NRW a. F. zeigt, dass der Gesetzgebung eine unreife und unausgegorene Idee in Bezug auf die Online-Durchsuchung zugrunde lag. Diese präventive und unbestimmte Ermächtigungsgrundlage, die schon seit geraumer Zeit Teil des wissenschaftlichen Diskurses war, wurde zutreffend vom Bundesverfassungsgericht zurechtgestutzt.

Im Ergebnis hat das Urteil des Bundesverfassungsgerichts, nach einer angeregten Diskussion in der Literatur und insbesondere auch im Gesetzgebungsverfahren, zu einer grundsätzlichen Zulässigkeit der Online-Durchsuchung geführt. Im selben Atemzug wurden auch klare Vorgaben an den Gesetzgeber gestellt, die es nun umzusetzen galt, um eine Online-Durchsuchung zu legitimieren. Die Richtung dieser neuen Ermittlungsmaßnahme war von nun an klar bestimmt durch die Entwicklung des neuen Grundrechtes und durch die aufgestellten Anforderungen zum Umgang mit Daten, die den Kernbereich der privaten Lebensgestaltung berühren. Viele Einwände der Opposition und der Gutachter*innen, die im Gesetzgebungsverfahren von § 5 Abs. 2 Nr. 11 VSG NRW a. F. vorgebracht worden waren, wurden auch vom Bundesverfassungsgericht als erheblich eingestuft und begründeten die Verfassungswidrigkeit der Vorschrift. Die zuvor in der Literatur geführte Diskussion, in welches Grundrecht durch die Online-Durchsuchung eingegriffen wird, konnte sich nun auf kritische Punkte konzentrieren. Außerdem kommt diesem Urteil eine Klarstellungsfunktion zu, indem deutlich gemacht wird,

[130] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 305 = NJW 2008, 822.

dass es einer Verfassungsänderung, wie sie gefordert wurde,[131] nicht bedarf und dass es auf eine Anwendung des Art. 13 GG nicht ankommt. Wesentliche Probleme, die von der Literatur erkannt und diskutiert worden waren, wurden vom Bundesverfassungsgericht aufgegriffen und ermöglichten somit auch eine Weiterentwicklung in der Rechtswissenschaft. Der Gesetzgeber konnte nun auf Grundlage dieser Rechtsprechung weiterarbeiten.

IV. Bundeskriminalamtsgesetz

Nachdem auf Bundesebene das PSIS beschlossen worden war, gelangten im Juli 2007 die ersten Gerüchte um die Neufassung des BKAG an die Öffentlichkeit. Angestoßen wurden diese dadurch, dass der sogenannte „Schäuble-Entwurf" öffentlich wurde.[132] Hier soll es geheißen haben:

> „(…), das BKA dürfe, ohne Wissen des Betroffenen durch den automatisierten Einsatz technischer Mittel aus informationstechnischen Systemen Daten erheben, soweit die Abwehr der dringenden Gefahr oder die Verhütung von Straftaten auf andere Weise aussichtslos oder wesentlich erschwert wäre."[133]

Erst am 16.04.2008 wurde der Referentenentwurf, welcher einen neuen § 20k BKAG für die Online-Durchsuchung vorsah, beschlossen.[134] Dieser wurde dann als Gesetzentwurf (Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt) am 04.06.2008 in den Bundestag eingebracht.[135]

Dieser führte zur Reform des BKAG und trat am 01.01.2009 einen Tag nach Verkündung im Bundesgesetzblatt am 31.12.2008 in Kraft.[136] Allerdings wurde damit die Online-Durchsuchung erneut einer Verfassungsbeschwerde ausgesetzt und im Anschluss modifiziert. Dieser Gang der Online-Durchsuchung ist näher zu beleuchten, da sich hier wesentliche Neuerungen finden, die auch in die aktuelle Fassung der Online-Durchsuchung in der StPO Eingang gefunden haben.

---

131 *Kudlich*, JA 2007, 391.

132 *Erd*, KJ 2008, 118, 121.

133 *Lutz/Jungholt*, Welt Online 2007, Online-Razzia: Schäuble legt Entwurf vor; online abzurufen über https://www.welt.de/wams_print/article1027727/Online-Razzia-Schaeuble-legt-Entwurf-vor.html (zugegriffen am 11.2.2019).

134 *Böckenförde*, JZ 2008, 925, 934.

135 BT-Drucks., 16/10121.

136 BGBl. I 2008 I, 3083.

1. Erstes Gesetzgebungsverfahren

Ziel der Neuerung des BKAG war auch hier die Bekämpfung des internationalen Terrorismus.[137] In § 20k BKAG a. F. sollte unter der Überschrift „verdeckter Eingriff in informationstechnische Systeme" die Online-Durchsuchung geregelt werden. Im Gesetzentwurf hieß es hierzu:

„*§ 20k*

Verdeckter Eingriff in informationstechnische Systeme

(1) Das Bundeskriminalamt darf ohne Wissen des Betroffenen mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben, wenn bestimmte Tatsachen die

Annahme rechtfertigen, dass eine Gefahr vorliegt für

1. Leib, Leben oder Freiheit einer Person oder

2. solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen

oder den Bestand des Staates oder die Grundlagen der Existenz

der Menschen berührt.

Eine Maßnahme nach Satz 1 ist auch zulässig, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass ohne Durchführung der Maßnahme in näherer Zukunft ein Schaden eintritt, sofern bestimmten Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für eines der in Satz 1 genannten Rechtsgüter hinweisen. Die Maßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung nach § 4a erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre.

(2) Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand von Wissenschaft und Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand von Wissenschaft und Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) Bei jedem Einsatz des technischen Mittels sind zu protokollieren:

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,

2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

---

[137] BR-Drucks., 404/08, S. 1; BT-Drucks., 16/10121, S. 1.

4. die Organisationseinheit, die die Maßnahme durchführt.

Die Protokolldaten dürfen nur verwendet werden, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach Absatz 1 rechtmäßig durchgeführt worden ist. Sie sind bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann automatisiert zu löschen, es sei denn, dass sie für den in Satz 2 genannten Zweck noch erforderlich sind.

(4) Die Maßnahme darf sich nur gegen eine Person richten, die entsprechend § 17 oder § 18 des Bundespolizeigesetzes verantwortlich ist. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(5) Die Maßnahme nach Absatz 1 darf nur auf Antrag des Präsidenten des Bundeskriminalamtes oder seines Vertreters durch das Gericht angeordnet werden. Bei Gefahr im Verzuge kann die Anordnung durch den Präsidenten des Bundeskriminalamtes oder seinen Vertreter getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit diese Anordnung nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

(6) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Namen und Anschrift,
2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes, sowie
4. die wesentlichen Gründe.

Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Anordnungsvoraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(7) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erhobene Daten sind unverzüglich von zwei Bediensteten des Bundeskriminalamtes, von denen einer die Befähigung zum Richteramt hat, auf kernbereichsrelevante Inhalte durchzusehen. Daten, die den Kernbereich privater Lebensgestaltung betreffen, dürfen nicht verwertet werden und sind unverzüglich zu löschen. Bestehen Zweifel, ob Daten dem Kernbereich privater Lebensgestaltung zuzurechnen sind, sind diese zu löschen oder unverzüglich dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit oder Löschung der Daten vorzulegen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr

erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt."[138]

Mit diesem Gesetzentwurf stand zum ersten Mal eine konkrete Ermächtigungsgrundlage auf Bundesebene für die Online-Durchsuchung zur politischen Debatte, mit der sich der Gesetzgeber dem technischen Fortschritt stellen wollte. Ziel der neu geschaffenen Ermächtigungsgrundlage war die Erhebung von Daten, die *nicht mehr* Gegenstand einer laufenden Kommunikation sind oder *nicht* für die Telekommunikation vorgesehen sind,[139] oder positiv formuliert: Alle Daten, die sich auf dem IT-System befinden, es sei denn, sie sind der laufenden Kommunikation zuzuordnen. Damit eröffnet die Ermächtigungsgrundlage die Möglichkeit einer weitreichenden Ausforschung eines IT-Systems. Nicht mitumfasst sein soll hingegen der Zugriff auf Kameras oder Mikrofone.[140] In dieser Befugnis soll allerdings das Kopieren von Dateien von der Festplatte eines Rechners und der Einsatz von Keyloggern enthalten ein.[141] Außerdem gehört zu den Protokollierungspflichten aus Abs. 3 auch die Pflicht anzugeben, ob die Maßnahme zur einmaligen Durchsicht oder zur kontinuierlichen Überwachung genutzt werden soll.[142] Es war also hier erstmalig eine Überwachung des IT-Systems vorgesehen und gewollt. In Bezug auf die Regelungen zum Schutz des Kernbereichs der privaten Lebensgestaltung in Abs. 7 ist klar die Umsetzung der ersten Vorgaben des Bundesverfassungsgerichts aus dem Urteil zum VSG NRW zu erkennen. Die Beurteilung der Kernbereichsrelevanz sollte nach diesem ersten Entwurf durch zwei Bedienstete des Bundeskriminalamtes, von denen einer*eine die Befähigung zum Richteramt hat, erfolgen.[143]

Nach der ersten Beratung am 25.09.2008 folgte am 10.11.2008 die Beschlussempfehlung und der Bericht des Innenausschusses. Dieser beinhaltete zwei wesentliche Änderungen in Bezug auf die Online-Durchsuchung. Zum einen wurde empfohlen, in Abs. 2 S. 2 und 3 das Wort „Wissenschaft" zu streichen, sodass das eingesetzte Mittel zur Online-Durchsuchung sich nur noch am Stand der Technik messen lassen müsse. Des Weiteren wurde empfohlen, dem Kernbereichsschutz mehr Rechnung zu tragen und nicht nur die zwei Beamt*innen des Bundeskriminalamtes über die Kernbereichsrelevanz entscheiden zu lassen, sondern darüber hinaus auch die*den Datenschutzbeauftragte*n, der*die von der Behörde selbst weisungsfrei sei, zu beteiligen.

---

138 BT-Drucks., 16/10121, S. 9, 10; so auch schon in: BR-Drucks., 404/08, S. 15–17.

139 BR-Drucks., 404/08, S. 68; BT-Drucks., 16/10121, S. 28.

140 BT-Drucks., 16/10121, S. 28; BR-Drucks., 404/08, S. 68.

141 BR-Drucks., 404/08, S. 69, 70; BT-Drucks., 16/10121, S. 29.

142 BR-Drucks., 404/08, S. 72; BT-Drucks., 16/10121, S. 30.

143 BR-Drucks., 404/08, S. 75; BT-Drucks., 16/10121, S. 31.

Sollte bei diesen Beteiligten Uneinigkeiten über die Kernbereichsrelevanz aufkommen, seien die Daten einem Gericht vorzulegen.[144] Mit diesen Zusätzen sei nun auch dem vom Bundesverfassungsgericht geforderten Kernbereichsschutz Genüge getan.[145] Die Opposition rügte jedoch, dass die Vorschrift immer noch nicht dem Kernbereichsschutz gerecht werde, insbesondere weil die Beamt*innen des Bundeskriminalamtes dem Ermittlungsinteresse der Behörde zu nahe stünden. Dies könne auch nicht durch die Beteiligung des*der Datenschutzbeauftragten verhindert werden. Im Übrigen sei eine solche Ermächtigungsgrundlage wie die der Online-Durchsuchung grundsätzlich nicht erforderlich.[146]

Dennoch wurde das Gesetz am 25.12.2008 mit Einarbeitung der Beschlussempfehlung des Innenausschusses verkündet.

Zusammenfassend lässt sich sagen, dass mit dieser Normierung die Online-Durchsuchung ihren finalen Schliff bekommen hat. Die Maßnahme wurde in ihren wesentlichen Punkten konkretisiert und Verfahrensvorschriften wurden entwickelt, die der Eingriffstiefe deutlich gerechter wurden. Fest steht spätestens ab diesem Zeitpunkt, dass sich die Maßnahme, zumindest in Bezug auf das BKAG, auf alle Daten erstreckt, die sich auf dem IT-System befinden, mit Ausnahme derjenigen, die der laufenden Telekommunikation unterfallen, und dass es sich bei dieser Maßnahme um eine heimliche Überwachung handelt. Mit dieser Normierung wurde daher ein wesentlicher Grundstein der Online-Durchsuchung gelegt und die weiteren Normierungen orientieren sich an dieser ersten konkreten Regelung der Online-Durchsuchung. Wie bereits aufgezeigt, war aber auch diese Normierung nicht frei von verfassungsrechtlichen Bedenken. Aus diesem Grund sah sich auch das neue BKAG einer Verfassungsbeschwerde ausgesetzt.

2. Entscheidung des Bundesverfassungsgerichts

Am 20.04.2016, acht Jahre nach der Verkündung des neuen BKAG, erfolgte dann das Urteil des Bundesverfassungsgerichtes, welches die Vorschriften zumindest grundsätzlich für mit der Verfassung vereinbar erklärte.[147]

Zunächst stellte das Gericht fest, dass ein Eingriff in den Kernbereich der privaten Lebensgestaltung mit keinem entgegenstehenden Interesse aufgewo-

144 BT-Drucks., 16/10822, Beschlussempfehlung und Bericht Innenausschuss, S. 3.
145 BT-Drucks., 16/10822, Beschlussempfehlung und Bericht Innenausschuss, S. 8.
146 BT-Drucks., 16/10822, Beschlussempfehlung und Bericht Innenausschuss, S. 9.
147 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220 = NJW 2016, 1781.

gen werden könne.[148] Daher dürfe der Kernbereich nicht zum Ziel von staatlichen Ermittlungen gemacht werden. Um dies zu gewährleisten, müssen zunächst Vorkehrungen getroffen werden, die eine unbeabsichtigte Miterfassung von Kernbereichsinformationen nach Möglichkeit ausschließen. Auf der zweiten Ebene seien dann Vorkehrungen zu treffen, die bei der Auswertung und der Verwertung der Daten den Eingriff in den Kernbereich minimieren.[149] Dabei müsse gerade auf der zweiten Ebene sichergestellt werden, dass die erfassten Daten durch eine unabhängige Stelle gesichtet und gefiltert werden.[150] Insbesondere sei es mit der Menschenwürde unvereinbar, wenn sich eine Überwachungsmaßnahme über einen längeren Zeitraum erstrecke und so umfassend sei, dass alle Bewegungen und Lebensäußerungen der Betroffenen registriert werden und zur Grundlage von Persönlichkeitsprofilen werden können.[151]

Dies bedeute für die mit der Verfassungsbeschwerde angegriffene Norm der Online-Durchsuchung gem. § 20k BKAG konkret, dass diese bei verfassungskonformer Auslegung mit der Verfassung vereinbar sei, aber die Regelungen zum Schutz des Kernbereichs der privaten Lebensgestaltung noch nicht ausreichend berücksichtigt seien.[152] Die Online-Durchsuchung greife, wie auch schon in der zuvor dargestellten Bundesverfassungsgerichtsentscheidung klargestellt, in das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme ein und sei in ihrer Intensität vergleichbar mit einem Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung.[153] Das Gericht stellte fest, dass nicht nur tagebuchähnliche Aufzeichnungen und andere Verkörperungen des höchstpersönlichen Lebensbereichs auf einem IT-Gerät gespeichert würden, sondern auch die höchstpersönliche Kommunikation zumeist über elektronische Kommunikationsdienste oder internetbasierte Netzwerke stattfinde.[154]

---

[148] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 276 = NJW 2016, 1781.

[149] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 278 = NJW 2016, 1781.

[150] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 280 = NJW 2016, 1781.

[151] 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 280 = NJW 2016, 1781.

[152] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 303 = NJW 2016, 1781.

[153] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 304 = NJW 2016, 1781.

[154] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 304 = NJW 2016, 1781.

In Bezug auf den Schutz des Kernbereichs der privaten Lebensgestaltung genügten die Regelungen damit nicht den verfassungsrechtlichen Anforderungen.[155] Zwar weise die Ermittlungsmaßnahme der Online-Durchsuchung auch eine gewisse Nähe zur Wohnraumüberwachung auf, dennoch sei der Kernbereichsschutz bei der Online-Durchsuchung noch stärker als bei der Wohnraumüberwachung auf die Auswertungs- und Verwertungsphase zu verschieben.[156] Dies müsse durch die Filterung der Daten durch eine unabhängige Stelle erfolgen.[157] Dabei genügen die Regelungen auf der Ebene der Datenerhebung den verfassungsrechtlichen Vorgaben.[158] Allerdings fehle es auf der zweiten Ebene an einer unabhängigen Kontrolle der Daten, die in der Lage sei, dafür zu sorgen, dass die kernbereichsrelevanten Daten gegenüber der Behörde nicht offenbart werden.[159] Eine Sichtung durch Beamt*innen des Kriminalamtes selbst genüge dieser Vorgabe nicht.

Allerdings gab es auch abweichende Meinungen innerhalb des Gerichts. Dabei wurde in einem dieser Sondervoten davon ausgegangen, dass die Forderung nach der Errichtung einer „unabhängigen Stelle“ zum nachgelagerten Kernbereichsschutz zu weit gehe.[160]

Zusammenfassend lässt sich sagen, dass der Eingriff in die Rechte des*der Betroffenen in seiner Intensität vergleichbar ist mit einem Eingriff in das Recht der Unverletzlichkeit der Wohnung.[161] Hier schließt sich nunmehr ein Kreis und mit dieser Klarstellung konnten sich auch diejenigen zufriedengeben, die bereits zu Beginn der Diskussion um die Online-Durchsuchung erhebliche Parallelen zur Durchsuchung gesehen hatten. Besonders hervorzuheben ist aber, dass seit der ersten Normierung zur Sicherung des Kernbereichsschutzes im BKAG a. F. der Standard des Kernbereichsschutzes bei der Online-Durchsuchung noch einmal erheblich erhöht wurde und nun, nach diesem zweiten Urteil des Bundesverfassungsgerichtes aus dem Jahr 2016, in weiten Teilen der Verfassung genügte. Dennoch sah das Bundesverfassungs-

---

155 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 306 = NJW 2016, 1781.

156 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 306 = NJW 2016, 1781.

157 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 307 = NJW 2016, 1781.

158 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 308 = NJW 2016, 1781.

159 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 308 = NJW 2016, 1781.

160 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 369 = NJW 2016, 1781.

161 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 304 = NJW 2016, 1781.

gericht noch Handlungsbedarf und stellte die Forderung nach einer von der ermittelnden Behörde unabhängigen Stelle auf.[162]

Mit dieser Entscheidung war ein erheblicher Schritt hin zur Legitimation der Online-Durchsuchung getan.

Das Bundesverfassungsgericht erklärte das Gesetz nicht für nichtig, sondern gab dem Gesetzgeber bis zum 01.07.2018 Zeit zur Nachbesserung.

3. Das neue BKAG

Am 14.02.2017 wurde dann der „*Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtsgesetzes*" von den Fraktionen CDU/CSU und SPD in den Bundestag eingebracht.[163]

In diesem Gesetzesentwurf heißt es in:

„*§ 49*

Verdeckter Eingriff in informationstechnische Systeme

(1) Das Bundeskriminalamt darf ohne Wissen der betroffenen Person mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass eine Gefahr vorliegt für

1. Leib, Leben oder Freiheit einer Person oder
2. solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt.

Eine Maßnahme nach Satz 1 ist auch zulässig, wenn

1. bestimmte Tatsachen die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Schädigung der in Satz 1 genannten Rechtsgüter eintritt oder
2. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums die in Satz 1 genannten Rechtsgüter schädigen wird.

Die Maßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung nach § 5 erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre.

(2) Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

---

[162] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 307 = NJW 2016, 1781.

[163] BT-Drucks., 18/11163.

2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) Die Maßnahme darf sich nur gegen eine Person richten, die entsprechend § 17 oder § 18 des Bundespolizeigesetzes verantwortlich ist. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(4) Die Maßnahme nach Absatz 1 darf nur auf Antrag der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung durch das Gericht angeordnet werden.

(5) Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,
3. Art, Umfang und Dauer der Maßnahme,
4. der Sachverhalt sowie
5. eine Begründung.

(6) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sowie
4. die wesentlichen Gründe.

Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Anordnungsvoraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die aufgrund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(7) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach Absatz 1 erlangt worden sind, sind dem anordnenden Gericht unverzüglich vorzulegen. Das Gericht entscheidet unverzüglich über die Verwertbarkeit oder Löschung. Daten, die den Kernbereich privater Lebensgestaltung betreffen, dürfen nicht verwertet werden und sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der

Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist sechs Monate nach der Benachrichtigung nach § 74 oder sechs Monate nach Erteilung der gerichtlichen Zustimmung über das endgültige Absehen von der Benachrichtigung zu löschen. Ist die Datenschutzkontrolle nach § 69 Absatz 1 noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren.

(8) Bei Gefahr im Verzug kann die Präsidentin oder der Präsident des Bundeskriminalamtes oder ihre oder seine Vertretung im Benehmen mit der oder dem Datenschutzbeauftragten des Bundeskriminalamtes über die Verwertung der Erkenntnisse entscheiden. Bei der Sichtung der erhobenen Daten kann sie oder er sich der technischen Unterstützung von zwei weiteren Bediensteten des Bundeskriminalamtes bedienen, von denen einer die Befähigung zum Richteramt haben muss. Die Bediensteten des Bundeskriminalamtes sind zur Verschwiegenheit über die ihnen bekannt werdenden Erkenntnisse, die nicht verwertet werden dürfen, verpflichtet. Die gerichtliche Entscheidung nach Absatz 7 ist unverzüglich nachzuholen."

Diese Vorschrift weist im Vergleich zur ersten Normierung der Online-Durchsuchung im BKAG vier wesentliche Veränderungen auf:

Zum einen wurde in Abs. 1 S. 2 der Norm die Gefahrenlage ausdrücklich geregelt, damit es keiner verfassungskonformen Auslegung bedarf.[164]

Zum anderen wurden in Abs. 5 die formalen Anforderungen an die Anordnung geregelt.

Die wohl wichtigste Änderung findet sich in Abs. 7, in dem es heißt, dass nun ein Gericht als unabhängige Stelle über die Kernbereichsrelevanz der Daten entscheidet.

Außerdem trifft Abs. 8 Regelungen, die dem BKA bei Gefahr in Verzug Handlungsmöglichkeiten an die Hand geben sollen.[165]

Mit diesem Gesetzestext hat der Gesetzgeber die Vorgaben des Bundesverfassungsgerichts in das BKAG eingefügt und dieser bildet den aktuellen Standard der Diskussion um die Online-Durchsuchung im präventiven Bereich auf Bundesebene ab. Die Online-Durchsuchung hat, gerade mit Blick auf den Schutz des Kernbereichs der privaten Lebensgestaltung, bis heute eine enorme Entwicklung genommen. Spätestens nach der Bundesverfassungsgerichtsentscheidung zum VSG NRW war klar, dass der Kernbereichsschutz eine erhebliche Rolle bei der Umsetzung der Online-Durchsuchung spielen würde, sogar so sehr, dass auch die erste Ausgestaltung des BKAG (und insgesamt die zweite Normierung der Online-Durchsuchung) nicht dem verfassungsrechtlich geforderten Schutzniveau entsprach.

164 BT-Drucks., 18/11163, S. 118.
165 BT-Drucks., 18/11163, S. 118.

Schlussendlich lässt sich sagen, dass es sich bei dieser Ausgestaltung der Vorschrift um die vorerst letzte Normierung der Online-Durchsuchung im präventiven Bereich handelt. Weitere Beanstandungen durch das Bundesverfassungsgericht sind zunächst nicht zu erwarten. So hat der Gesetzgeber schrittweise eine Ermächtigungsgrundlage der Online-Durchsuchung geschaffen, die insbesondere im Rahmen des Kernbereichsschutzes die verfassungsrechtlichen Vorgaben des Bundesverfassungsgerichts ausreizt. Dieser Gedanke, dass diese Ermächtigungsgrundlage das Mindestmaß des verfassungsrechtlich Vorgegebenen enthält, sollte in den folgenden Ausführungen immer berücksichtigt werden.

Nach dieser Entscheidung folgte dann die Einführung der Online-Durchsuchung in die StPO.

V. Einführung der Online-Durchsuchung in die Strafprozessordnung

An die vorangegangene Darstellung der Normierung der Online-Durchsuchung im präventiven Bereich schließt nun jene über die Einführung der Online-Durchsuchung in die StPO an. Was im Jahr 1995 mit der „Online-Durchsuchung“ auf einer Mailbox begann, sollte nun sein vorläufiges Ende in einer festen Verankerung der Online-Durchsuchung als Ermittlungsmaßnahme in der StPO finden. Bereits in seinem Urteil zum VSG NRW stellte das Bundesverfassungsgericht fest, dass eine Online-Durchsuchung auch im repressiven Bereich grundsätzlich zulässig ist.[166]

1. Gesetzgebungsverfahren

Am 30.12.2016 ließ die Bundesregierung dem Bundesrat den *Entwurf eines Gesetzes zu effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens* zukommen.[167] Ziel dieses Gesetzes war es zunächst, die strafprozessualen Vorschriften auf ihre Tauglichkeit, Zeitgemäßheit und Effektivität hin zu überprüfen, um das Strafverfahren zu vereinfachen und zu beschleunigen.[168] In diesem Gesetzentwurf, der am 22.02.2017 auch in den Bundestag eingebracht wurde,[169] war weder die Quellen-TKÜ noch die Online-Durchsuchung vorgesehen.

---

[166] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 270 = NJW 2016, 1781.

[167] BR-Drucks., 796/16.

[168] BR-Drucks., 796/16, S. 1; BT-Drucks., 18/11277, S. 1.

[169] BT-Drucks., 18/11277.

Erst in der Formulierungshilfe der Bundesregierung für einen Änderungsantrag am 15.05.2017 im Ausschuss für Recht und Verbraucherschutz fand sich die strafprozessuale Online-Durchsuchung, im Übrigen in der Fassung, in der sie auch beschlossen wurde, im politischen Diskurs wieder.[170]

In der Begründung hierzu hieß es, dass der erhöhten Nutzung von IT-Geräten durch die Bürger*innen Rechnung getragen werden müsse.[171] Dabei sei die Online-Durchsuchung zu verstehen als „(…) der verdeckte staatliche Zugriff auf fremde informationstechnische Systeme über Kommunikationsnetze mittels einer Überwachungssoftware".[172] Hier wurde klargestellt, zum ersten Mal auch in dieser Deutlichkeit, dass durch die Ermittlungsmaßnahme der Online-Durchsuchung das IT-System umfassend überwacht und seine Speichermedien ausgelesen werden.[173] Es handelt sich also faktisch um eine länger andauernde Überwachung, bei der nicht nur Daten einmalig und punktuell „gespiegelt" werden, sondern wodurch das gesamte Nutzungsverhalten einer Person offengelegt wird.[174] So könne man sich mit dieser Maßnahme einen potenziell großen und aussagekräftigen Datenbestand verschaffen.[175]

Deswegen habe das Bundesverfassungsgericht die Eingriffsintensität der Online-Durchsuchung für vergleichbar mit der Wohnraumüberwachung befunden und aus diesem Grund könnten die Voraussetzungen für die akustische Wohnraumüberwachung in weiten Teilen auf die Online-Durchsuchung übertragen werden. Dies gelte insbesondere auch für den Katalog ausreichend schwerer Straftaten.[176]

a) Anhörung der Sachverständigen

Eine Anhörung von Sachverständigen fand bereits am 31.05.2017 statt, also 16 Tage nach dem Bekanntwerden des Änderungsantrags im Ausschuss für Recht und Verbraucherschutz. In dieser Anhörung wurde erhebliche Kritik an der Online-Durchsuchung geäußert. Zum einen wurde mehrfach die Gefahr, die mit der Infiltrierung eines IT-Systems einhergeht, betont. Denn sobald Sicherheitslücken bewusst offengelassen beziehungsweise genutzt werden, können diese nicht nur durch den Staat zur Strafverfolgung oder zur Abwehr von Gefahren genutzt, sondern eben auch von Dritten instrumenta-

170 BT-Drucks., Ausschussdrucksache 18(6)334.
171 BT-Drucks., Ausschussdrucksache 18(6)334, S. 15.
172 BT-Drucks., Ausschussdrucksache 18(6)334, S. 15.
173 BT-Drucks., Ausschussdrucksache 18(6)334, S. 16, 23.
174 BT-Drucks., Ausschussdrucksache 18(6)334, S. 23.
175 BT-Drucks., Ausschussdrucksache 18(6)334, S. 24.
176 BT-Drucks., Ausschussdrucksache 18(6)334, S. 24.

lisiert werden.[177] Als besonders problematisch wurde angesehen, dass die Online-Durchsuchung einen sehr intensiven Eingriff darstellt, da man ein digitales Abbild des Lebens der Betroffenen erstellen könne.[178] IT-Systeme könnten in der heutigen Zeit einen ausgelagerten „Teil des Gehirns"[179] darstellen. Auch deswegen gehe der im Entwurf genannte Straftatenkatalog zu weit[180] und sei nicht an die strafprozessualen Gegebenheiten angepasst worden.[181] Dieser Argumentation wurde entgegengehalten, dass der Straftatenkatalog nicht zu weit gefasst sei, da eine solche Ermittlungsmaßnahme im Verhältnis nur selten in der Praxis angewendet werde[182] und die Gerichte ohnehin sehr genau arbeiten würden, weshalb eine ausartende Anwendung der Online-Durchsuchung unwahrscheinlich sei.[183] Kritisiert wurde außerdem, die Formulierung leide an einem erheblichen Grad der Unbestimmtheit[184] und die Regelungen zu den Berufsgeheimnisträger*innen seien unzureichend.[185] Diesen vielen Kritikpunkten wurde, insbesondere aus der Praxis im Bereich der inneren Sicherheit, entgegengehalten, dass es solcher Instrumentarien wie der Online-Durchsuchung für eine effektive Strafverfolgung bedürfe, denn die Beschlagnahme des IT-Geräts führe eben nicht zu damit vergleichbaren Ergebnissen.[186]

---

[177] *Chaos Computer Club* et al., Stellungnahme zur Bundestagsdrucksache 18/11272, S. 6; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 6, 21; *Sinn*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 10.

[178] *Deutscher Anwaltsverein durch den Ausschuss Strafrecht*, Stellungnahme zur Bundestagsdrucksache 18/11272, S.13; *Sinn*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 10.

[179] *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 5.

[180] *Deutscher Anwaltsverein durch den Ausschuss Strafrecht*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 13; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 12; *Bundesbeauftragte für Datenschutz und Informationsfreiheit Voßhoff*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 6.

[181] *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 10.

[182] *Greven*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 6; *Vizepräsident des Bundeskriminalamts Henzler*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 10, 11; *Krauß*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 10, 11.

[183] *Huber*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 4.

[184] *Deutscher Anwaltsverein durch den Ausschuss Strafrecht*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 15; a.A.: *Huber*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 7, 8.

[185] *Deutscher Anwaltsverein durch den Ausschuss Strafrecht*, Stellungnahme zur Bundestagsdrucksache 18/11272, S.18; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 23.

[186] *Greven*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 1; *Vizepräsident des Bundeskriminalamts Henzler*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 2, 3, 6; *Huber*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 2; *Krauß*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 2, 3.

b) Inkrafttreten der Maßnahme

Am 20.06.2017 wurden dann die Beschlussempfehlung und der Bericht des Ausschusses für Recht und Verbraucherschutz vorgelegt.[187] Dieser entspricht auch in seiner Begründung in Bezug auf die Online-Durchsuchung dem Änderungsantrag der Regierungsfraktionen vom 15.05.2017. Die Abstimmung erfolgte am 22.06.2017 im Bundestag.[188] Nach der Unterrichtung des Bundesrates wurde das Gesetz am 23.08.2017 trotz Widerstands, beispielsweise durch den Ausschuss für Agrarpolitik und Verbraucherschutz,[189] verkündet[190] und trat am Folgetag in Kraft. Damit war die erste repressive Online-Durchsuchung innerhalb eines Zeitraums von etwas mehr als drei Monaten geboren.

Die Entstehung der strafprozessualen Online-Durchsuchung ist insbesondere aus zwei Gründen problematisch, die es auch im weiteren Verlauf noch zu berücksichtigen gilt. Zum einen ist die Online-Durchsuchung sehr schnell und mit wenig Beratungszeit im Plenum über einen Änderungsantrag der Regierungsfraktionen in die StPO eingeführt worden und zum anderen wurde, wohl bedingt durch diese Schnelligkeit, kaum ein Unterschied zur präventiven Normierung im BKAG vorgenommen.

Unabhängig von der Frage, ob eine solche repressive Online-Durchsuchung für die Praxis überfällig war, lässt sich zusammenfassend sagen, dass es bedenklich ist, wie diese Ermächtigungsgrundlage in den Gesetzgebungsprozess eingebracht wurde.[191] Die Einbringung einer solch einschneidenden Ermächtigungsgrundlage durch einen Änderungsantrag legt den Verdacht nahe, dass die Bundesregierung diese möglichst schnell und insbesondere, ohne die Aufmerksamkeit der Öffentlichkeit zu erregen, umsetzen wollte. Dabei ist fraglich, ob es sich bei dem Änderungsantrag der Regierungsfraktionen überhaupt noch um einen Änderungsantrag nach § 82 Abs. 1 GO BT handelte oder ob dieser nicht vielmehr eine neue Gesetzesinitiative darstellte.[192] Ordnet man dieses Vorgehen in den politischen Kontext ein, wird deutlich, dass die Bundesregierung kurz vor dem Ende der Legislaturperiode stand und diese Ermächtigungsgrundlage wohl noch schnell umsetzen wollte, um dies

187 BT-Drucks., 18/12785.

188 BT-Plenarprotokoll 18/240, S. 24594 D.

189 BR-Drucks., 527/1/17.

190 Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens v. 17.8.2017, BGBl. I, S. 3202–3213.

191 *Deutscher Anwaltsverein durch den Ausschuss Strafrecht*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 3, 4; *Roggan*, StV 2017, 821.

192 *Deutscher Anwaltsverein durch den Ausschuss Strafrecht*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 3, 4; *Roggan*, StV 2017, 821.

als Erfolg ihrer Regierungszeit verbuchen zu können. Dies geschah somit auch vor dem Hintergrund der kommenden Neuwahlen, die am 24.09.2017 stattfanden.

Letztlich ist der Gesetzestext in der StPO (§§ 100b ff. StPO) weitestgehend deckungsgleich mit dem des § 49 BKAG, mit der Ausnahme, dass die präventive Norm in Abs. 1 Nrn. 1 und 2 eine Gefahr für die Rechtsgüter Leib, Leben, Freiheit einer Person oder solcher Rechtsgüter der Allgemeinheit, deren Bedrohung die Grundlage oder den Bestand des Bundes oder eines Landes oder die Grundlage der Existenz der Menschen berührt, fordert, während man sich bei der repressiven Maßnahme der StPO für den Straftatenkatalog der akustischen Wohnraumüberwachung entschied. Die Wortlautnähe der beiden Normen ist nicht zuletzt darauf zurückzuführen, dass man sich bereits beim Verfassen des Gesetzestextes zum BKAG an den Bundesverfassungsgerichtsurteilen aus den Jahren 2008 und 2016 orientiert hat[193] und auch in der Gesetzesbegründung zur strafprozessualen Online-Durchsuchung regelmäßig auf diese verweist.[194]

Der Umgang mit beziehungsweise die Ignoranz gegenüber den Zweifeln der Gutachter*innen in allen Gesetzgebungsverfahren zur Online-Durchsuchung führt dazu, dass sich die Online-Durchsuchung auch nach diesem langen Entwicklungsprozess noch immer erheblicher Kritik ausgesetzt sieht. Letztendlich ist dieses Gesetz nichts weiter als ein politischer „Schnellschuss", bei dem für die repressive Ermächtigungsgrundlage vom Bundesverfassungsgericht und seinen Urteilen aus den Jahren 2008 und 2016 abgeschrieben wurde.

2. Verfassungsbeschwerden

Sowohl die FDP als auch die Gesellschaft für Freiheitsrechte (GFF) haben gegen die Online-Durchsuchung Verfassungsbeschwerde eingereicht.

Zum einen bringen die Beschwerdeführenden vor, dass der Straftatenkatalog zu umfangreich und damit unverhältnismäßig sei.[195] Außerdem seien die Regelungen zum Kernbereichsschutz in § 100d Abs. 1–3 StPO und diejeni-

---

193 BT-Drucks., 18/11163.

194 Siehe.: BT-Drucks., 18/12785, S. 46 ff.

195 *Gazeas*, Verfassungsbeschwerde gegen die Regelungen der Strafprozessordnung zur Online-Durchsuchung und Quellen-Telekommunikationsüberwachung; online abzurufen über https://www.fdp.de/sites/default/files/uploads/2018/08/20/fdp-vfb-gazeas-zusammenfassung.pdf (zugegriffen am 19.9.2019); *Strate/Ventzke* 2018, Beschwerdeschrift Verfassungsbeschwerde; online abzurufen über https://freiheitsrechte.org/home/wp-content/uploads/2018/08/GFF_Verfassungsbeschwerde_Staatstrojaner_anonym.pdf (zugegriffen am 19.2.2019).

gen zum Schutz der Berufsgeheimnisträger unzureichend.[196] Des Weiteren werde das 2008 entwickelte IT-Grundrecht verletzt, wenn Sicherheitslücken (Zero-Day-Exploits) eines IT-Systems zur Durchführung einer Online-Durchsuchung oder einer Quellen-TKÜ ausgenutzt werden.[197]

Hier bleibt abzuwarten, wie das Bundesverfassungsgericht entscheidet. Auf die Gefahr der Bildung von Persönlichkeitsprofilen gehen die Verfassungsbeschwerden nicht konkret ein.

VI. Zwischenresümee

Die Online-Durchsuchung stand seit ihrer technischen Umsetzbarkeit im Diskurs von Politik und Justiz. Dabei lässt sich der Ursprung des Wortes Online-Durchsuchung mit der Tatsache erklären, dass sich diese Ermittlungsmaßnahme bereits in ihrem Entwicklungsprozess mit der „klassischen" Durchsuchung messen lassen musste und immer wieder Vergleiche zu dieser hergestellt wurden.[198] In den Anfängen der Online-Durchsuchung standen die Heimlichkeit der Maßnahme und der Fernzugriff auf das Gerät im Mittelpunkt. Der Überwachungsgesichtspunkt charakterisierte sich erst im Urteil des Bundesverfassungsgerichts zum VSG NRW heraus.[199] Hierbei wurde dann die Möglichkeit von Profilbildungen erkannt und ein zweistufiges Schutzkonzept zur Sicherung des Kernbereichs der privaten Lebensgestaltung entwickelt.[200] Auch das neu gefasste BKAG konnte den Ansprüchen an den Kernbereichsschutz nicht gerecht werden und auch hier musste nachgebessert werden. Diese Ansprüche wurden nach Ansicht des Gesetzgebers mit der Einführung eines neuen BKAG und der Normierung der Online-Durchsuchung in der StPO erfüllt. Ob diese Regelungen zum Kernbereich privater Lebensgestaltung nun nach Ansicht des Bundesverfassungsgerichts genügen, bleibt abzuwarten.

---

196 *Gazeas*, Verfassungsbeschwerde gegen die Regelungen der Strafprozessordnung zur Online-Durchsuchung und Quellen-Telekommunikationsüberwachung; online abzurufen über https://www.fdp.de/sites/default/files/uploads/2018/08/20/fdp-vfb-gazeas-zusammenfassung.pdf (zugegriffen am 19.9.2019).

197 *Strate/Ventzke* 2018, Beschwerdeschrift Verfassungsbeschwerde; online abzurufen über https://freiheitsrechte.org/home/wp-content/uploads/2018/08/GFF_Verfassungsbeschwerde_Staatstrojaner_anonym.pdf (zugegriffen am 19.2.2019).

198 Beginnend mit der Rechtsprechung zur Mailboxabfrage, über die Frage nach einer bestehenden Ermächtigungsgrundlage in der StPO bis hin zu den Verfassungsgerichtsentscheidungen und der Gesetzgebung zur StPO.

199 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274 = NJW 2008, 822.

200 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274 = NJW 2008, 822.

Die Formulierungen in der Entscheidung aus dem Jahr 2008 zum VSG NRW sprachen bereits von einer Weiterentwicklung der Informationstechnik.[201] Zu dieser Zeit waren es lediglich die „Personalcomputer", die sich in jedem Haushalt befanden. Nun, mehr als 10 Jahre später, hat die Entwicklung einen weiteren Schritt gemacht und nahezu jede*r Bürger*in ist im Besitz eines Smartphones. Es sind nicht mehr nur die nebensächlichen Dinge, die an „Personalcomputern" getätigt werden, sondern es werden höchstpersönliche bis triviale Daten und damit alle Arten von Daten auf diesen „ausgelagerten Teil des Gehirns"[202] übertragen und diesem Teil des Gehirns werden Denkleistungen überlassen. Diese reichen beispielsweise von der einfachen, wiederholten Erinnerung bis zur personalisierten Werbung.[203] So haben auch die späteren Entscheidungen des Bundesverfassungsgerichts gezeigt, dass eine Weiterentwicklung insbesondere in Bezug auf den Kernbereichsschutz stattgefunden hat. Nach der Einführung der Online-Durchsuchung in das VSG NRW hat eine erste Normierung des Kernbereichsschutzes in das BKAG a. F. Eingang gefunden, welche dann mit der Einführung einer unabhängigen Stelle (in Form des*der Ermittlungsrichter*in) im BKAG noch einmal präzisiert wurde. Dies verdeutlicht, dass wahrgenommen wurde, dass mit dem technischen Fortschritt auch die Nutzer*innen geschützt werden müssen. So heißt es im Bundesverfassungsgerichtsurteil zum BKAG:

> „Mit der Menschenwürde unvereinbar ist es, wenn eine Überwachung sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können."[204]

Diese Erkenntnis besteht schon länger, ist aber heute mehr denn je ein Problem. Denn es schließt sich die Frage an, ob dies bereits bei einer Online-Durchsuchung geschehen kann und wie dann damit umzugehen ist. Kann dieses vom Bundesverfassungsgericht 2008 in Bezug auf das VSG NRW entwickelte zweistufige Schutzkonzept auch in der heutigen Zeit und unter diesen Gesichtspunkten noch bestehen oder muss es eine Anpassung erfahren? Die historische Entwicklung der Online-Durchsuchung lehrt, dass der Kernbereichsschutz ihr Kernproblem ist. So hat dieser Schutz in der ersten Normierung noch keine Berücksichtigung gefunden. Im Laufe der Zeit sind dann immer detailliertere Verfahrensvorschriften entwickelt worden. Bis jetzt konnte die Gesetzgebung den Kernbereichsschutz, trotz der immer schneller fortschreitenden Möglichkeiten der Informationstechnik, wohl hinreichend

---

201 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 303 = NJW 2008, 822.

202 *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 5.

203 Mehr zu der Art der Daten, die erhoben werden unter: B. I. 2. a).

204 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 280 = NJW 2016, 1781.

berücksichtigen. Dennoch bleibt nun die Frage, ob ein weiterer Schritt, eine weitere Entwicklung gemacht werden muss, um diesem Fortschritt gerecht zu werden. Die Historie und lange Entwicklung der Ermächtigungsgrundlage der Online-Durchsuchung offenbart, dass Gesellschaft und Politik eine solche Ermittlungsmaßnahme als sicherheitspolitisch notwendig erachten. Diese Notwendigkeit, das zeigen die Ausführungen zuvor, wird seit jeher mit der neuen Gefahr des internationalen Terrorismus begründet. Später sind dann Überlegungen hinzugekommen, die Gefahren im technischen Fortschritt und damit verbundenen neuen „kriminellen" Möglichkeiten sehen.

Im Folgenden ist das Ergebnis der beschriebenen historischen Entwicklung, also die aktuelle Normierung der strafprozessualen Online-Durchsuchung de lege lata zu untersuchen. Dabei soll herausgefunden werden, ob der Gesetzgeber mit dieser einen tragfähigen Ausweg aus den zuvor von Rechtsprechung und Wissenschaft dargelegten Problemen gefunden hat.

B. Rechtsrahmen der Online-Durchsuchung

Zunächst gilt es nun, die Online-Durchsuchung *de lege lata* genauer zu beleuchten. Die Ausführungen zum Gesetzgebungsverfahren haben gezeigt, dass es den Regierungsparteien hier hauptsächlich um eine schnelle Umsetzung des Gesetzesvorhabens ging. Dabei sind in § 100b StPO die Ermächtigungsgrundlage der Online-Durchsuchung, in den §§ 100d StPO i. V. m. 100a Abs. 5, 6 StPO die technischen Anforderungen an die Ermittlungsmaßnahme und in § 100e StPO das Verfahren der Online-Durchsuchung geregelt.

An dieser Stelle der Bearbeitung wird es darum gehen zu bestimmen, welche Daten mittels einer Online-Durchsuchung erhoben werden können. Denn diese Daten sind es, die die Grundlage für mögliche Persönlichkeitsprofile des*der Nutzer*in des IT-Gerätes bilden. Der Inhalt und der Umfang dieser Daten wird letztlich der ausschlaggebende Punkt in der Beurteilung der Wahrscheinlichkeit der Bildung von Persönlichkeitsprofilen sein. Aus diesem Grund ist es elementar, klar zu benennen, welche Daten erhoben werden können und dürfen. Eine übergeordnete Rolle spielt hier, wie sich die Online-Durchsuchung zu anderen Ermittlungsmaßnahmen verhält. Schwierigkeiten wird dabei insbesondere die Abgrenzung zur akustischen und optischen Wohnraumüberwachung und die Nutzung von Peripheriegeräten bereiten. Des Weiteren wird zu berücksichtigen sein, dass bereits eine Online-Durchsuchung mehrere Ermittlungsmaßnahmen in sich vereinen kann. Hierin ist eine weitere Gefahr zu erkennen, die es im Folgenden zu untersuchen gilt.

I. Ermächtigungsgrundlage

Die Maßnahme wurde im August 2017 gem. § 100b StPO als neue Ermittlungsmaßnahme in die StPO unter der Überschrift „Online-Durchsuchung“ aufgenommen. § 100b StPO stellt nun die Ermächtigungsgrundlage der repressiven Online-Durchsuchung dar. Die Tatbestandsmerkmale sind:

1. Verdacht,
2. Straftat nach Abs. 2 (Katalogtat),
3. Schwere der Tat auch im Einzelfall,
4. Subsidiaritätsklausel,
5. Verhältnismäßigkeit.

Alle fünf Tatbestandsmerkmale müssen kumulativ gegeben sein.

Nach der Gesetzesbegründung ist unter der Online-Durchsuchung „(…) der verdeckte staatliche Zugriff auf fremde informationstechnische Systeme mit dem Ziel, deren Nutzung zu überwachen und gespeicherte Inhalte aufzuzeichnen (…)“[205], zu verstehen. Der Begriff der „Durchsuchung“ ist somit irreführend, da es sich bei der Ermittlungsmaßnahme vielmehr um eine „IT-System*überwachung*“ handelt.[206] Der Einfachheit halber und dem Titel der Vorschrift entsprechend, wird jedoch auch in den folgenden Ausführungen weiter von der Online-Durchsuchung gesprochen.

Die Online-Durchsuchung dient also der Erhebung von Daten und der Überwachung des Nutzungsverhaltens des*der Beschuldigten. Diese Feststellung bedarf einer erheblichen Konkretisierung.

1. Das informationstechnische System

Zunächst ist der Begriff des informationstechnischen Systems, welches das Eingriffsobjekt der Ermächtigungsgrundlage darstellt, zu definieren.

In der Gesetzesbegründung zur Online-Durchsuchung in der StPO findet sich keine nähere Definition des IT-Systems. Es ist lediglich die Rede von dessen Allgegenwart. „Dies gilt vor allem für die Nutzung mobiler Geräte in Form von Smartphones oder Tablet-PCs.“[207] Damit nimmt die Gesetzesbegründung keine abschließende Aufzählung vor und eine Begrenzung des Begriffs des IT-Systems im strafrechtlichen Sinn erfolgt nicht. Wie zuvor

---

205 BT-Drucks., 18/12785, S. 54.

206 Vgl.: *Knierim/Oehmichen*, Quellen TKÜ und Online-Durchsuchung, in: Gesamtes Strafrecht aktuell, 375; *Freiling/Safferling/Rückert*, JR 2018, 9, 13.

207 BT-Drucks., 18/12785, S. 46.

bereits dargestellt, ist der Wortlaut des Gesetzestextes der Ermächtigungsgrundlage in der Strafprozessordnung weitestgehend deckungsgleich mit jenem aus dem präventiven Bereich. Dies ist darauf zurückzuführen, dass letztlich beide Ermächtigungsgrundlagen auf den Urteilen des Bundesverfassungsgerichts zur Online-Durchsuchung aus den Jahren 2008 und 2016 beruhen.[208] Außerdem finden sich auch in der Gesetzesbegründung zur StPO Verweise auf die präventive Ermächtigungsgrundlage.[209] Aufgrund der übrigen Verweise auf die präventive Online-Durchsuchung im BKAG ist davon auszugehen, dass auch an dieser Stelle der dort verwendete Begriff des IT-Systems gemeint ist.

a) Der Ursprung des Begriffs des IT-Systems

An dieser Stelle ist zu untersuchen, wo der Begriff des IT-Systems seinen Ursprung hat und wie er sich entwickelt hat. In der Gesetzesbegründung zum BKAG (2016) verweist der Gesetzgeber zunächst auf die alte Regelung des BKAG (2008).[210] Die Gesetzesbegründung zum alten BKAG geht wiederum davon aus, dass der Begriff des informationstechnischen Systems dem des § 2 Abs. 2 Nr. 1 BSIG-Errichtungsgesetz (Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik) entspricht.[211] In der Gesetzesbegründung zum alten BKAG (2008) heißt es: „Der Begriff des informationstechnischen Systems entspricht § 2 Abs. 2 Nr. 1 des BSI-Errichtungsgesetzes (BSIG) und ist bewusst weit gewählt, um alle nach der Rechtsprechung des Bundesverfassungsgerichts schutzbedürftigen informationstechnische Systeme zu erfassen.“[212] In § 2 Abs. 1 BSI-Errichtungsgesetz wird der Begriff der Informationstechnik so definiert: „Die Informationstechnik im Sinne dieses Gesetzes umfasst alle technischen Mittel zur Verarbeitung oder Übertragung von Informationen.“ Die erste Gesetzesbegründung zum BSI-Errichtungsgesetz, welches vom 01.01.1991 bis zum 19.08.2009 galt, enthielt somit bereits in § 2 Abs. 2 Nr. 1 BSI-Errichtungsgesetz den Begriff des informationstechnischen Systems. Das heute geltende Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BSI-Gesetz) hat im Jahr 2009 die Formulierung des § 2 Abs. 2 aus dem Errichtungsgesetz übernommen. Damit hat der Begriff des informationstechnischen Systems seinen Ursprung zunächst nicht im Urteil des Bundesverfassungsgerichts von 2008, sondern er ist bereits seit den 1990er Jahren Teil des deutschen Rechts-

208 BT-Drucks., 18/11163.
209 BT-Drucks., 18/12785, S. 46 ff.
210 BT-Drucks., 18/11163, S. 118.
211 BT-Drucks., 16/10121, S. 29.
212 BT-Drucks., 16/10121, S. 29.

systems und steht seither für ein technisches Mittel, welches Informationen verarbeitet und überträgt.[213] Bereits im Jahr 1990 ist der Gesetzgeber demnach davon ausgegangen, dass die Definition der Informationstechnik weit zu fassen ist, um auch die künftigen Entwicklungen auf dem Gebiet der Informationstechnik mitumfassen zu können.[214]

b) Der Begriff des IT-Systems des Bundesverfassungsgerichts

Der Definition des IT-Systems aus dem BSI-Errichtungsgesetz hat sich das Bundesverfassungsgericht dann im Jahr 2008 bei der Entwicklung des IT-Grundrechtes zunächst weitestgehend angeschlossen. In der Weiterentwicklung sind dennoch einige Einschränkungen durch das Gericht vorgenommen worden. So hat das Bundesverfassungsgericht festgestellt, dass nicht jedes informationstechnische System, das personenbezogene Daten erzeugen, verarbeiten oder speichern kann, des Schutzes durch eine eigenständige persönlichkeitsrechtliche Gewährleistung bedürfe.[215] Im Umkehrschluss bedeutet dies, dass ein IT-System im mindesten dazu in der Lage sein muss, personenbezogene Daten zu erzeugen, sie zu verarbeiten oder zu speichern. Für den Schutz durch das IT-Grundrecht bedürfe es aber weiterer Überschneidungen mit den Lebensbereichen der einzelnen Person, sodass der punktuelle Bezug zu einem bestimmten Lebensbereich der*des Betroffenen nicht ausreiche.[216] Eine weitere Definition hat das Bundesverfassungsgericht in seiner Entscheidung nicht vorgenommen. Somit hat sich das Bundesverfassungsgericht für einen engen Begriff des IT-Systems entschieden.

c) Der strafprozessuale Begriff des IT-Systems

Nun stellt sich die Frage, ob der Begriff des IT-Systems aus dem IT-Grundrecht derselbe ist, wie jener der strafprozessualen Ermächtigungsgrundlage. Denn dies würde ein spürbares Spannungsverhältnis zwischen erforderlicher Weite und notwendiger Begrenzung darstellen.[217] Das Problem hat seinen Ursprung in der bereits ausführlich dargestellten Entwicklung der Online-Durchsuchung. Das Bundesverfassungsgericht hat im Jahr 2008 das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Sys-

---

213 BT-Drucks., 11/7029, S. 7.

214 BT-Drucks., 11/7029, S. 7.

215 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 313 = NJW 2008, 822.

216 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 313 = NJW 2008, 822.

217 *Hauck*, in: Löwe-Rosenberg, § 100a, Rn. 104.

teme entwickelt,[218] und an dieses angelehnt wurde dann die Online-Durchsuchung in das BKAG aufgenommen.[219] Der Begriff des informationstechnischen Systems entwickelte sich also in Korrelation zwischen dem Grundrechtsschutz und der Ermittlungsmaßnahme. Das Bundesverfassungsgericht war damit mittelbar an der Begriffsbestimmung beteiligt und hat ihn mitgeprägt.

In der strafrechtlichen Literatur wird davon ausgegangen, dass unter einem IT-System alle technischen Geräte zu verstehen sind, die über eine Steuerung, Programme, Aufzeichnungsmöglichkeiten und Datenleitungen verfügen und in ein LAN mit eingebunden sind,[220] also alle Systeme, die in der Lage sind, Informationen zu erheben, zu verarbeiten und Ergebnisse auszugeben oder weiterzuleiten, und damit Kommunikationszwecken dienen.[221] Damit sei die Norm „entwicklungsoffen" gefasst worden.[222] Nach heutiger Auffassung passen unter den Begriff des IT-Systems zunächst Klassiker, namentlich der Personalcomputer[223], das Smartphone[224] und auch elektrische Geräte, die der Kommunikation in der Wohnung oder in Kraftfahrzeugen dienen.[225] Dazu können demnach auch Geräte wie der SMART-TV oder andere SMART-Home-Geräte (wie beispielsweise ALEXA) gehören.[226] Im Zuge einer Durchsuchung auf diesen Geräten ist es grundsätzlich auch zulässig, auf Server zuzugreifen. Aus diesem Grund darf auch auf Cloud-Speicherdienste oder virtuelle Festplatten zugegriffen werden.[227] Mitumfasst sind außerdem externe Systeme, die der Datenspeicherung dienen. Damit ist der

---

218 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274 = NJW 2008, 822.

219 BT-Drucks., 18/11163.

220 *Knierim/Oehmichen*, Quellen TKÜ und Online-Durchsuchung, in: Gesamtes Strafrecht aktuell, Rn. 63.

221 *Graf*, in: BeckOK StPO, § 100b, Rn. 7; *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 107.

222 *Graf*, in: BeckOK StPO, § 100b, Rn. 7.

223 So auch schon in: BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274 = NJW 2008, 822.

224 Hier noch als „Telekommunikationsgeräte" bezeichnet: BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 304 = NJW 2008, 822; BT-Drucks., 18/12785, S. 46.

225 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 304 = NJW 2008, 822.

226 *Knierim/Oehmichen*, Quellen TKÜ und Online-Durchsuchung, in: Gesamtes Strafrecht aktuell, 378; *Löffelmann*, GSZ 2020, 244; *Blechschmitt*, MMR 2018, 361, 362.

227 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 303 = NJW 2016, 1781.

Zugriff auf Internetforen, Online-Shoppingportale und soziale Netzwerke möglich.[228]

Allerdings ist eine weite Definition des IT-Systems – und damit anders als die Definition des Bundesverfassungsgerichts –, welche unabhängig von den Bezugspunkten zum Lebensbereich besteht, vorzugswürdig. Dem liegt ein rechtspolitischer und letztlich dem Verhältnismäßigkeitsgebot innewohnender Gedanke zugrunde, wonach die Rechte der einzelnen Person nicht vernachlässigt werden dürfen. Denn hielte man den Begriff des IT-Geräts bei der Ermächtigungsgrundlage eng, dann fehlte es an einem zur Ermittlungszielerreichung gleich geeigneten, aber milderen Mittel, in Form eines weniger eingriffsintensiven IT-Systems. Das Smartphone stellt in der Regel das eingriffsintensivere IT-System dar als beispielsweise der mit dem WLAN verbundene Wecker oder auch andere SMART-Home Geräte – dies gilt nicht für sprachgesteuerte Geräte wie ALEXA etc. Nähme man den mit dem WLAN verbundenen Wecker aus dem Begriff des IT-Systems heraus, wäre eine Unverhältnismäßigkeit innerhalb der Maßnahme nicht denkbar und es müsste auf das eingriffsintensivere Gerät zurückgegriffen werden. Denn die IT-Geräte, die einen intensiven Eingriff in das IT-Grundrecht bedeuten – wie der PC, das Smartphone oder das Tablet –, wären dann die einzigen Geräte, die berücksichtigt werden könnten. Dem könnte entgegengehalten werden, dass ein enger IT-Systembegriff zur Folge hätte, dass es an einem „verhältnismäßigen" IT-Gerät fehlte und die Maßnahme mangels Verhältnismäßigkeit nicht durchgeführt werden könnte. Dem kann wiederum mit dem Beispiel des Weckers widersprochen werden: So könnte es den Ermittlungsbehörden bei der Ermittlungsarbeit zur Aufklärung eines Tötungsfalles um die Information des „Aufstehens" der tatverdächtigen Person gehen. Hierfür reicht grundsätzlich die Überwachung des Weckers aus. Auf diesem sind deutlich weniger Informationen über die Person gespeichert und eine Online-Durchsuchung auf diesem Gerät kann gegenüber einem Smartphone als milder eingestuft werden. Auf jenem sind in der Regel deutlich mehr Informationen gespeichert und es besteht eine höhere Gefahr für die betroffene Person. Rechtspolitisch ist es also erstrebenswert, den Wecker an dieser Stelle nutzen zu können. Aus diesem Beispiel kann jedoch nicht geschlossen werden, dass, mangels eines milderen Mittels, die Online-Durchsuchung auf dem Smartphone nicht durchgeführt werden dürfte. Es käme dann auf die Angemessenheit der Maßnahme an, die in diesem Beispiel wohl gegeben wäre. Es spricht also vieles dafür, einen weiten Begriff des IT-Geräts für die strafprozessuale Online-Durchsuchung zu verwenden und damit auch den mit dem WLAN verbundenen Wecker als Eingriffsobjekt zuzulassen.

---

228 *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 109; *Roggan*, StV 2017, 821, 826.

Dennoch kommen auch weiterhin andere Grundrechte wie Art. 13 GG oder auch Art. 2 Abs. 1 GG in Betracht. Bleibt man bei dem Beispiel rund um den mit dem WLAN verbundenen Wecker, wird hier in aller Regel auch Art. 13 GG Anwendung finden. Dies gilt insbesondere dann, wenn er sich in der Wohnung befindet und die Sprachsteuerung aktiviert ist. Damit ist zwischen dem Begriff des IT-Systems aus dem IT-Grundrecht und der strafprozessualen Definition zu unterscheiden. Der Begriff des IT-Systems umfasst in der StPO, wie schon in den 1990er Jahren angedacht und von der heutigen Literatur beschrieben, alle Systeme, die Daten verarbeiten, speichern oder erzeugen. Dies ergibt sich zum einen aus der Gesetzesbegründung und zum anderen sorgt es für eine effektivere Anwendung des Verhältnismäßigkeitsgrundsatzes, und das ohne weitere Einschränkungen.

2. Daten

Ebenfalls richtungsweisend ist die Frage nach den Daten, die erhoben werden können und dürfen. Diese Daten sind später in der Bearbeitung auf ihren Kernbereichsschutz hin zu untersuchen und bilden die Grundlage eines Persönlichkeitsprofils. Grundsätzlich kann auf alle auf dem informationstechnischen System gespeicherten Informationen zugegriffen werden.[229] Dabei findet eine zeitliche oder inhaltliche Begrenzung der Überwachung zunächst nicht statt.[230]

a) Arten der zu gewinnenden Daten

Nur spärlich wird in der Gesetzesbegründung dargestellt, welche Erkenntnisse sich aus der Online-Durchsuchung konkret ergeben können und welche Beweise tatsächlich gesichert werden sollen. Denkbar sind grundsätzlich zwei Arten. Zum einen können solche Daten erhoben werden, die auch bei einer „klassischen" Durchsuchung zu Tage getreten wären. Zum anderen können diese Daten dann aber auch in einen Kontext gesetzt werden, sodass nach einem Auswertungsprozess Profilingdaten entstehen.

aa) Daten als Äquivalent zur „klassischen" Durchsuchung

Im Fokus einer Online-Durchsuchung können zunächst jene Daten stehen, welche sich zum Zeitpunkt der Maßnahme auf dem Gerät befinden und als

229 *Knierim/Oehmichen*, Quellen TKÜ und Online-Durchsuchung, in: Gesamtes Strafrecht aktuell, 375; BT-Drucks., 18/12785, S. 54.

230 *Freiling/Safferling/Rückert*, JR 2018, 9, 13; *Bruns*, in: KK, § 100b, Rn. 5.

einzelnes Datum gespeichert sind.[231] Ziel ist dabei, ein Äquivalent zur Situation vor der Digitalisierung zu schaffen.[232] Beispielsweise sind Aktenordner und sonstige Aufzeichnungen, die sich vor dem Zeitalter der Digitalisierung noch in der Wohnung befanden, nun in digitaler Form auf dem IT-System beziehungsweise verschiedenen Servern, auf die mittels des IT-Systems zugegriffen werden kann, gespeichert. So findet das Banking in der heutigen Zeit auf den IT-Geräten statt und kaum noch jemand hat den klassischen Kontoauszugsordner bei sich zuhause im Regal stehen. Um also auch weiterhin auf diese Daten zugreifen und diese in einem Strafverfahren verwerten zu können, brauchte es aus Sicht der Ermittlungsbehörden eine Maßnahme,[233] die im Stande ist, diese Situation wiederherzustellen. Für diese Art der Daten würde es genügen, eine punktuelle und konkrete Durchsuchung nach einem bestimmten Datum durchzuführen. An dieser Stelle wäre dann das Datum für sich genommen für das Strafverfahren relevant und es bräuchte keine Überwachung des IT-Geräts. Um diesem Äquivalenzgedanken Rechnung tragen zu können, würde also eine einmalige „Durchsuchung" des IT-Systems genügen und die Norm bräuchte keinen Überwachungscharakter.

bb) Profiling-Daten

Ein Überwachungscharakter, der explizit in der Gesetzesbegründung zur Online-Durchsuchung aufgeführt wird,[234] führt zu der weiteren Art der Daten. Der Gesetzgeber hat sich also mit der Zeit von dem ursprünglichen Gedanken der Äquivalenz entfernt hin zu einer Überwachung des IT-Systems. An dieser Stelle intensiviert sich der Eingriff erheblich. In der Konsequenz findet eine „Live-Überwachung" des Nutzungsverhaltens der betroffenen Person statt.[235] Mit eben dieser Überwachung ist es den Ermittlungsbehörden über einen längeren Zeitraum möglich, das Verhalten einer Person zu überwachen, zu beobachten und letztlich auch zu analysieren, und all dies unter Berufung auf nur eine Ermittlungsmaßnahme. Es kann durch die Ermittlungsbehörden beobachtet werden, wie sich eine Person in einzelnen Situationen verhält und wie sie mit ihnen umgeht. Damit können im Rahmen der Online-Durchsuchung zwei Arten der Daten erhoben werden. Zum einen

231 BT-Drucks., 18/12785, S. 54.

232 Zunächst auch Grundgedanke in der Gesetzesbegründung: BT-Drucks., 18/12785, S. 46.

233 *Greven*, Stellungnahme zur Ausschussdrucksache 18(6)334; *Vizepräsident des Bundeskriminalamts Henzler*, Stellungnahme zur Bundestagsdrucksache 18/11272; *Huber*, Stellungnahme zur Ausschussdrucksache 18(6)334.

234 BT-Drucks., 18/12785, S. 54.

235 Zum Begriff siehe: *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 5.

jene Daten, die sich ohnehin auf dem IT-Gerät befinden und bei einer Beschlagnahme zu Tage getreten wären,[236] und zum anderen jene Daten, die aufgrund der Überwachung des IT-Geräts erhebliche Rückschlüsse auf das Verhalten der betroffenen Person und damit auf ihre Persönlichkeit zulassen.

Wie *Buermeyer* schon in seiner Stellungnahme zur Gesetzesbegründung der Online-Durchsuchung feststellte, kann dem*der Betroffenen bei dieser Art der Daten beim Denken zugeschaut werden.[237] Hierbei geschieht Folgendes: Die zuerst genannten Daten können durch die Überwachung des IT-Geräts in den Kontext der Lebenssituation der betroffenen Person gesetzt werden. Damit kann die Persönlichkeit einer Person schnell und effektiv erfasst werden. Wie handelt eine Person wann und warum? Das lässt sich bei diesen kontextbezogenen Daten schnell festlegen und lässt weitreichende Schlüsse auf das zu, was das Wesen eines jeden Menschen ausmacht. Vergleichbar sind diese Daten mit jenen, die sich nach Art. 4 Nr. 4 DS-GVO aus dem Prozess des Profiling ergeben. Dort heißt es:

> „‚Profiling' jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen".

Profiling im Sinne der Datenschutz-Grundverordnung meint einen Prozess der Datenverarbeitung,[238] bei dem Bestände von personenbezogenen Daten ausgewertet und analysiert werden und auf deren Grundlage dann die Bewertung von Persönlichkeitsmerkmalen vorgenommen wird.[239] Es kommt nicht auf den Informationsgehalt eines personenbezogenen Datums an, sondern die neue Information basiert auf der Interpretation dieser Daten.[240] Durch ihre Verknüpfung gehen die neu gewonnenen Daten über die Summe der Einzelinformationen hinaus.[241] Aus diesen Daten können dann erhebliche Rückschlüsse auf das Privat- und Berufsleben der betroffenen Person gezogen werden, so etwa auf das soziale Umfeld und die Beziehung zu anderen Per-

---

236 Sinn und Zweck einer Online-Durchsuchung wäre es in diesen Fällen, die immer häufiger vorkommende Verschlüsselung zu umgehen, siehe: *Vizepräsident des Bundeskriminalamts Henzler*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 6.

237 *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 5.

238 *Buchner*, in: Kühling/Buchner, Kommentar zur DSGVO/BDSG, Art. 4 Nr. 4, Rn. 1.

239 *Schantz/Wolff*, Das neue Datenschutzrecht, Rn. 274.

240 *Scholz*, in: NK zum Datenschutzrecht, Art. 4 Nr. 4, Rn. 6.

241 *Scholz*, in: NK zum Datenschutzrecht, Art. 4 Nr. 4, Rn. 6.

sonen, Gewohnheiten des täglichen Lebens, das Konsumverhalten et cetera.[242]

Auch diese Art der Daten kann durch eine Online-Durchsuchung entstehen, indem das IT-Gerät überwacht wird und über einen längeren Zeitraum verschiedene Daten gesammelt werden, welche dann in einer neuen Zusammensetzung erhebliche Rückschlüsse auf die betroffene Person zulassen. Allerdings besteht nur eine Vergleichbarkeit der gewonnenen Daten aus der Online-Durchsuchung mit dem Begriff des Profiling aus der Datenschutz-Grundverordnung und es darf keine Gleichsetzung der Begrifflichkeiten erfolgen. Denn das Profiling selbst beschreibt lediglich einen Prozess, welcher gem. Art. 4 Nr. 4 DS-GVO in einer automatisierten Verarbeitung besteht;[243] das Ergebnis dieser Verarbeitung in Form der Profilingdaten kann bei der strafprozessualen Online-Durchsuchung jedoch auch auf manuelle Art und Weise entstehen. Wesentlich ist an dieser Stelle also nicht der Prozess als solcher, sondern das Ergebnis dieses Prozesses in Form der Profilingdaten. Grundsätzlich ist es auch denkbar, ein solches Profiling bereits nach einer punktuellen Online-Durchsuchung durchzuführen, wobei die Überwachung eines Geräts wohl gewinnbringender und insbesondere effizienter ist. Die Online-Durchsuchung lässt durch ihren Überwachungscharakter und ohne eine Einschränkung der Daten auf abstrakter Ebene der Ermächtigungsgrundlage zunächst einmal eine solche Profiling-Datengewinnung zu.

Grundsätzlich ist die Erstellung einzelner Profilingdaten, selbstredend je nach Inhalt, zunächst nicht als verfassungsrechtlich problematisch einzustufen, denn dass aus einzelnen Informationen Rückschlüsse auf die Person des*der Täter*in gezogen werden, ist dem Strafprozessrecht zunächst nicht fern und wohnt jeder strafprozessualen Ermittlungsmaßnahme inne. Aus einer Observation kann geschlossen werden, wo sich die betreffende Person gerne aufhält, und auch Rückschlüsse auf das warum können gezogen werden. Aus einer Telekommunikationsüberwachung kann geschlossen werden, wann und warum der*die Tatverdächtige mit wem kommuniziert et cetera. All diese einzelnen Profilingdaten für sich genommen stellen noch keine verfassungsrechtliche Problematik dar. Erst die Erzeugung vieler und unterschiedlicher Profilingdaten kann aufgrund der Gefahr zur Bildung von Persönlichkeitsprofilen womöglich, dies gilt es später zu untersuchen, Kernbereichsrelevanz aufweisen.

---

242 *Scholz*, in: NK zum Datenschutzrecht, Art. 4 Nr. 4, Rn. 7.

243 *Buchner*, in: Kühling/Buchner, Kommentar zur DSGVO/BDSG, Art. 4 Nr. 4, Rn. 5.

Damit sind der Art der Daten, die erhoben werden dürfen, zunächst keine Grenzen gesetzt und die Erhebung jeglicher Daten ist grundsätzlich durch die Ermächtigungsgrundlage gedeckt.[244]

b) Datengewinnung mittels Peripheriegeräten

Weiterhin problematisch ist, auf welche Weise diese Art der Daten gewonnen wird. Denn die Daten aus einer Online-Durchsuchung können sich aus verschiedenen, spezielleren Ermittlungsmaßnahmen zusammensetzen. Dies resultiert vor allem aus der Tatsache, dass die überwiegende Anzahl der IT-Geräte mit Peripheriegeräten wie Mikrofon und Kamera ausgestattet sind. Dabei ist in einem ersten Schritt die aktive und die passive Aktivierung der Geräte zu unterscheiden.

aa) Aktivierung der Peripheriegeräte durch die Ermittlungsbehörden

Die überwiegende Meinung geht zutreffend davon aus, dass ein heimliches Aktivieren der Kamera und des Mikrofons und damit die aktive Aktivierung der Geräte durch die Ermittlungsbehörden nicht von der Ermittlungsmaßnahme der Online-Durchsuchung gedeckt ist. Dies ergibt sich bereits aus dem Wortlaut der Norm, wonach Daten nur „daraus", also aus dem informationstechnischen System selbst, erhoben werden dürfen. Dies schließt eine aktive Inbetriebnahme des Systems aus.[245] Es handelt sich somit eindeutig nicht um Inhalte, die auf dem System, wie von der Gesetzesbegründung verlangt,[246] gespeichert sind, sondern vielmehr wird durch die Ermittlungsbehörde selbst die Speicherung herbeigeführt. Die Daten stammen nicht mehr aus der Benutzung des Geräts durch den*die Nutzer*in, sondern werden von den Behörden künstlich herbeigeführt.

---

244 So auch: *Bruns*, in: KK, § 100b, Rn. 5.

245 *Schmitt*, in: Meyer-Goßner/Schmitt, § 100b, Rn. 2; *Gercke*, in: Heidelberger Kommentar, § 100b, Rn. 11; *Großmann*, GA 2018, 439, 443; *Knierim/Oehmichen*, Quellen TKÜ und Online-Durchsuchung, in: Gesamtes Strafrecht aktuell, 376; *Singelnstein/Derin*, NJW 2017, 2646, 2647; *Roggan*, StV 2017, 821, 826; *Singelnstein*, verfassungsblog 2017, Hacken zur Strafverfolgung? Gefahren und Grenzen der strafprozessualen Online-Durchsuchung; online abzurufen über https://verfassungsblog.de/hacken-zur-strafverfolgung-gefahren-und-grenzen-der-strafprozessualen-online-durchsuchung/ (zugegriffen am 12.11.2020); a.A.: *Bruns*, in: KK, § 100b, Rn. 5.

246 BT-Drucks., 18/12785, S. 54.

bb) Die passive Kenntnisnahme durch Peripheriegeräte

Denkbar ist außerdem die passive Kenntnisnahme von Daten durch die Ermittlungsbehörden mittels Peripheriegeräten. Die Gesetzesbegründung geht davon aus, dass mittels einer Online-Durchsuchung das Nutzungsverhalten der betroffenen Person überwacht werden kann und gespeicherte Inhalte aufgezeichnet werden dürfen.[247] Der Gesetzeswortlaut besagt, dass sich die Daten aus dem informationstechnischen System ergeben müssen. Die wohl überwiegende Meinung geht davon aus, dass dies auch den Live-Zugriff mitumfasst, sodass in der Konsequenz die passive Kenntnisnahme von Peripheriegeräten auch in der Online-Durchsuchung enthalten ist.[248] Hierfür wichtig ist der Begriff der gespeicherten Inhalte, welcher sich aus der Gesetzesbegründung ergibt.[249] In Frage steht somit also, ob auch die Aufzeichnung der Daten, die mittels Peripheriegeräten erhoben werden, als solche „gespeicherten Inhalte" angesehen werden können.

Dargestellt werden soll diese Problematik am Beispiel eines Videotelefonats via Skype. Hier werden durch den*die Nutzer*in sowohl die Kamera als auch das Mikrofon genutzt und aktiviert. Dabei findet eine Live-Übertragung des Telefonats statt. Das Gespräch als solches wird nicht für den*die Benutzer*in erkennbar langfristig auf dem IT-System gespeichert. Anders als beispielweise bei Sprachnachrichten oder versendeten Videos, die durch das IT-Gerät zumeist langfristig und für den*die Benutzer*in sichtbar gespeichert werden, erfolgt bei einem Videotelefonat eine solche langfristige Speicherung zumeist nicht. Es stellt sich also die Frage, ob auch solche Inhalte, die beispielsweise bei einem Videotelefonat entstehen, von der Online-Durchsuchung gedeckt sind, wenn sie nicht für den*die Nutzer*in sichtbar und langfristig gespeichert werden. *Hauck* geht davon aus, dass der Begriff der gespeicherten Inhalte aus der Gesetzesbegründung jener ist, der sich auch in § 3 Abs. 4 Nr. 1 BDSG a. F. wiederfindet.[250] Die Speicherung ist demnach „(…) das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung". Selbstredend sei für die strafprozessuale Definition das Kriterium der personenbezogenen Daten nicht ausschlaggebend.[251] Diese Definition der Speicherung aus dem Bundesdatenschutzgesetz stammt aus dem Jahr 1984,[252]

247 BT-Drucks., 18/12785, S. 54.

248 *Roggan*, StV 2017, 821, 825; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, 5; *Bruns*, in: KK, § 100b, Rn. 5.

249 BT-Drucks., 18/12785, S. 54.

250 *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 106.

251 *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 106.

252 BT-Drucks., 10/1180, S. 4.

wurde aber nicht in das neue Bundesdatenschutzgesetz übernommen. In der alten Fassung des Gesetzes wurde die Speicherung, wie auch heute, als ein Teil der Verarbeitung definiert. In der alten Fassung fand allerdings eine zusätzliche Definition des Begriffs der Speicherung statt. Mit der Datenschutzgrundverordnung wurde diese Definition angepasst und man entschied sich auf Ebene der Europäischen Union gegen die bis dahin in Deutschland normierte systematische Definition des Verarbeitens und für eine beispielhafte Definition.[253] Allerdings wird auch weiterhin auf diese Definition verwiesen[254] und sie kann auch immer noch zu Rate gezogen werden. Auch die Inhalte eines Videotelefonats werden kurzfristig im Arbeitsspeicher des Geräts gespeichert, damit stellen sie gespeicherte Inhalte im Sinne der Gesetzesbegründung dar und ergeben sich somit, dem Wortlaut der Ermächtigungsgrundlage entsprechend, aus dem IT-System. Auch nach *Haucks* Argumentation, bei der die Speicherung bereits das „Erfassen" der Daten mitumfasst, handelt es sich bei Daten aus einem Videotelefonat um gespeicherte Daten im Sinne der Gesetzesbegründung. Damit kommt es bei der Online-Durchsuchung nicht auf eine durch den*die Nutzer*in sichtbare, langfristige Speicherung an.

Anderer Ansicht scheint hingegen der Gesetzgeber selbst zu sein, wenn er in der Gesetzesbegründung zwischen jenen Daten differenziert, die durch die offene Durchsuchung nach den §§ 94 ff., 102 ff. StPO erhoben werden können, und solchen, die sich aus einer heimlichen Telekommunikationsüberwachung ergeben.[255] Ein Unterschied zur Quellen-TKÜ wird bei der Online-Durchsuchung somit auch an dieser Stelle vorgenommen, sodass davon ausgegangen werden kann, dass sowohl die Quellen-TKÜ als auch die Online-Durchsuchung die Erhebung der laufenden Kommunikation zulassen und die Online-Durchsuchung lediglich ein „Mehr" zur Quellen-TKÜ darstellt.[256] Diesen Schluss legt auch die Gesetzesbegründung nahe, die davon ausgeht, dass bei der Online-Durchsuchung nicht nur neu hinzukommende Kommunikationsinhalte – wie bei der Quellen-TKÜ –, sondern alle auf dem IT-System gespeicherten Inhalte überwacht werden.[257] Damit ist die passive Kenntnisnahme von Daten mittels Peripheriegeräten grundsätzlich denkbar und gewollt. Für das Beispiel der Videotelefonie bedeutet dies, unabhängig davon, ob man diese nun unter die „gespeicherten Inhalte" subsumiert oder nicht,

253 *Roßnagel*, in: NK zum Datenschutzrecht, Art. 4 Nr. 2, Rn. 4.

254 *Roßnagel*, in: NK zum Datenschutzrecht, Art. 4 Nr. 2, Rn. 19.

255 BT-Drucks., 18/12785, S. 54.

256 *Köhler*, in: Meyer-Goßner/Schmitt, § 100b, Rn. 1; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 9; *Knierim/Oehmichen*, Quellen TKÜ und Online-Durchsuchung, in: Gesamtes Strafrecht aktuell, 375; *Freiling/Safferling/Rückert*, JR 2018, 9, 13.

257 BT-Drucks., 18/12785, S. 54.

dass sie eine Quellen-TKÜ darstellt und damit auch unter die Online-Durchsuchung fällt.

cc) Aktivierung des Peripheriegeräts durch das Gerät selbst

Im nächsten Schritt stellt sich dann allerdings das Problem, wie mit Situationen umzugehen ist, in denen das IT-Gerät weder durch den*die Nutzer*in noch durch die Ermittlungsbehörden aktiviert wird. Das Argument der herrschenden Meinung kommt schnell dort an seine Grenzen, wo das IT-Gerät selbst, ohne Wissen des*der Betroffenen Daten via Peripheriegeräte erhebt. So kann eine Unterscheidung in der Person des*der Aktivierenden nicht mehr zu Rate gezogen werden, wenn es um sprachgesteuerte IT-Geräte wie beispielsweise ALEXA geht, denn diese Art des Geräts hört immer zu.[258] Dies reicht bei einer Liveüberwachung des IT-Geräts bereits aus, um von den Ermittlungsbehörden wahrgenommen und gespeichert zu werden. Möglich wäre es, dass sich eine solche Sprachsteuerung auch in der Zukunft weiterverbreitet und ihr noch mehr Gewicht zukommt. Aber auch andere Situationen sind denkbar, in denen sich der*die Nutzer*in nicht über die Aktivierung des Peripheriegeräts bewusst ist und dies auch nicht durch eindeutige Einstellungen zugelassen hat. Folgt man jedoch streng dem zuvor genannten Wortlautargument, reicht es aus, dass die aktivierende Person nicht den Ermittlungsbehörden zugeordnet werden kann. Erhebt ein IT-Gerät also selbst und ohne Wissen des*der Betroffenen Daten mittels der Peripheriegeräte, sind diese Daten von der Ermächtigungsgrundlage ebenfalls mitumfasst.

c) Daten aus spezielleren Ermittlungsmaßnahmen

Auch bei der passiven Kenntnisnahme der Peripheriegeräte bleibt die Problematik der möglichweise mitverwirklichten Ermittlungsmaßnahmen bestehen. Die passive Wahrnehmung von Audiodateien beim Einschalten des Mikrofons kann sowohl einen kleinen Lauschangriff im Sinne des § 100f StPO als auch, abhängig von dem Aufenthaltsort der betroffenen Person, einen großen Lauschangriff gem. § 100c StPO darstellen. Auch eine Quellen-TKÜ kann, wie zuvor dargestellt, bereits mitverwirklicht werden. Dies gilt auch für einige weitere Ermittlungsmaßnahmen, die als speziellere Ermächtigungsgrundlagen in Betracht kommen.

In diesem Zusammenhang können einige Beispiele zur Verdeutlichung genannt werden:

[258] Hierzu mit einer genaueren Auseinandersetzung und weiteren Nachweisen: *Blechschmitt*, MMR 2018, 361, 362.

Sollten die Ermittlungsbehörden beispielsweise ein Telefonat über das Internet in der Wohnung des*der Betroffenen mithören, bei dem persönliche Informationen ausgetauscht werden, und somit gleichzeitig passiv an der Aktivierung des Mikrofons des IT-Geräts teilnehmen, wäre die einschlägige Norm die der Quellen-TKÜ gem. § 100a StPO. Problematisch ist dabei, ob in Art. 13 GG eingegriffen wird, wenn das Telefonat in der Wohnung erfolgt und Bildmaterial, wie bei der Videotelefonie, aufzeichnet.

Noch deutlicher wird das Problem allerdings bei dem folgenden Beispiel: Der*die Betroffene nimmt ein Sprachmemo auf, um sich später an diesen eventuell sehr persönlichen Gedanken erinnern zu können. Hier wäre wohl die akustische Wohnraumüberwachung gem. § 100c StPO die einschlägige Ermittlungsgrundlage und nicht die Online-Durchsuchung als solche.

Auch wäre es denkbar, dass der*die Betroffene ein Video in der Wohnung aufnimmt, das persönlichen Inhalt hat und Vorgänge in der Wohnung offenlegt. Hier könnte man als spezielle Ermächtigungsgrundlage an die in der StPO bewusst nicht geregelte optische Wohnraumüberwachung denken.

Diese Beispiele zeigen, dass bereits durch eine Online-Durchsuchung mehrere speziellere Ermächtigungen verwirklicht werden können, wenn die Kenntnisnahme von Daten mittels Peripheriegeräten in der Online-Durchsuchung mitumfasst ist, sei es auch nur bei einer passiven Kenntnisnahme.

aa) Quellen-TKÜ

Als erste mitverwirklichte Ermittlungsmaßnahme bei passiver Kenntnisnahme von Daten mittels Peripheriegeräten ist an die Quellen-TKÜ zu denken. Wie bereits oben dargestellt, wird sie als ein „Weniger“ im Vergleich zur Online-Durchsuchung angesehen.[259] Auch der Gesetzgeber geht hiervon aus, wenn er sagt, dass „nicht nur neu hinzukommende Kommunikationsinhalte“[260] Teil der Online-Durchsuchung seien.

Eine Mitverwirklichung der Quellen-TKÜ ist also zunächst einmal gewollt und eine Abgrenzung zur Online-Durchsuchung erfolgt somit nur in eine Richtung. Denn eine Quellen-TKÜ ist immer dann gegeben, wenn laufende Kommunikation aufgezeichnet wird, aber keine Online-Durchsuchung, also die Erhebung weiterer Daten aus einem IT-Gerät, stattfindet. Aus diesem Grund bedarf es auch keiner gesonderten Anordnung der Quellen-TKÜ,

---

[259] *Köhler*, in: Meyer-Goßner/Schmitt, § 100b, Rn. 1; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 9; *Knierim/Oehmichen*, Quellen TKÜ und Online-Durchsuchung, in: Gesamtes Strafrecht aktuell, 375; *Freiling/Safferling/Rückert*, JR 2018, 9, 13.

[260] BT-Drucks., 18/12785, S. 54.

wenn aktuelle Kommunikationsinhalte in Form einer funktionalen Äquivalenz zur herkömmlichen TKÜ durch die Ermittlungsbehörden erhoben werden. Die Daten aus einer Quellen-TKÜ können damit Teil einer Online-Durchsuchung sein.

bb) Wohnraumüberwachung

Grundsätzlich kann als die intensivste möglicherweise mitumfasste Ermittlungsmaßnahme die Wohnraumüberwachung angesehen werden. Dabei soll die Online-Durchsuchung auch an Art. 13 Abs. 1 GG zu messen sein, wenn sich das betroffene IT-System in der Wohnung befindet und so bestimmte Vorgänge in dieser überwacht werden.[261] In Betracht kommen durch die Kenntnisnahme der Peripheriegeräte sowohl die optische als auch die akustische Überwachung des Wohnraums der betroffenen Person. Dabei ist im Folgenden zu untersuchen, ob beide Formen des Spähangriffs mit Art. 13 GG vereinbar sind.

(1) Optische Wohnraumüberwachung

Unter anderem wäre es denkbar, eine optische Wohnraumüberwachung – aufgrund der passiven Kenntnisnahme der Daten bei der Aktivierung der Kamera – durchzuführen. Allerdings ist eine repressive optische Wohnraumüberwachung gem. Art. 13 Abs. 3 GG nicht mit der Verfassung vereinbar. Nach Art. 13 Abs. 3 GG ist zu repressiven Zwecken lediglich die akustische Wohnraumüberwachung vorgesehen, die optische Wohnraumüberwachung ist hingegen nur aus präventiven Gründen denkbar.[262]

Aus diesem Grund ist dafür Sorge zu tragen, dass bei der Online-Durchsuchung keine Überwachung erfolgt, bei der durch eine passive Kenntnisnahme mittels der Kamera Vorgänge innerhalb der Wohnung wahrgenommen werden können. Ein solches Vorgehen stellt nach Art. 13 Abs. 3 GG einen unzulässigen repressiven Spähangriff auf einen Wohnraum dar,[263] der nicht gerechtfertigt werden kann. Dies führt zu erheblichen Abgrenzungsproblemen und der Frage, wann ein solcher verfassungsrechtlich unzulässiger optischer Spähangriff gegeben ist: Können Vorgänge in der Wohnung bereits durch ein Videotelefonat wahrgenommen werden und wie ist mit Videos umzugehen,

261 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 310 = NJW 2008, 822; a.A.: *Freiling/Safferling/Rückert*, JR 2018, 9, 20; *Hauck*, in: Löwe-Rosenberg, § 100a, 9.

262 *Papier*, in: Herzog/Scholz/Klein, Art. 13, Rn. 83; *Bruns*, in: KK, § 100b, Rn. 5; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 4.

263 *Roggan*, StV 2017, 821, 826; *Soiné*, NStZ 2018, 497, 504.

die Vorgänge in der Wohnung wahrnehmen lassen, aber bereits zeitlich länger zurückliegen und auf dem IT-Gerät langfristig gespeichert sind? Zur Beantwortung dieser Fragen ist zunächst zu berücksichtigen, ob mittels einer Online-Durchsuchung grundsätzlich ein Eingriff in das Wohnungsgrundrecht möglich ist. Sodann ist darzustellen, ob die einzelnen Fallgruppen, die eine optische Wohnraumüberwachung darstellen könnten, auch tatsächlich in den Schutzbereich des Wohnungsgrundrechts eingreifen und ob ein solcher Eingriff durch die Schranke des Art. 13 Abs. 3 GG gerechtfertigt werden kann.

(a) Möglichkeit des Eingriffs in Art. 13 GG

Grundsätzlich greifen solche Maßnahmen in Art. 13 Abs. 1 GG ein, die einen Einblick in die Vorgänge in die Wohnung ermöglichen und die der natürlichen Wahrnehmung von außerhalb des geschützten Bereichs entzogen sind.[264] Dabei ist das Schutzgut die räumliche Sphäre, in der sich das Privatleben entfaltet.[265] So ist nach Ansicht der Bundesverfassungsgerichts ein Anwendungsfall, der in den Schutzbereich des Art. 13 Abs. 1 GG falle „(…) die Infiltration eines informationstechnischen Systems, das sich in einer Wohnung befindet, um mit Hilfe dessen bestimmte Vorgänge innerhalb der Wohnung zu überwachen (…)“[266]. Dem ist zuzustimmen. Der Schutzbereich des Art. 13 Abs. 1 GG ist bereits eröffnet, wenn Vorgänge in der Wohnung mittels des IT-Geräts durch die Ermittlungsbehörden wahrgenommen werden können. Dies gilt unabhängig davon, dass der Schutz des Art. 13 GG allein nicht ausreicht, um die Integrität von IT-Systemen zu wahren.[267] Auch genügt es als alleiniges Kriterium für die Eröffnung des Schutzbereiches nicht, dass sich das IT-Gerät in der Wohnung der betroffenen Person befindet. Die Infiltration muss vielmehr einen Bezug zur Wohnung haben.[268] Ein Eingriff in das Wohnungsgrundrecht ist unter anderem dann gegeben, wenn der Staat in die Wohnung eindringt oder aber in dieser verweilt.[269] Die Abs. 3

---

264 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 310 = NJW 2008, 822.

265 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 310 = NJW 2008, 822.

266 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 310 = NJW 2008, 822.

267 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 310 = NJW 2008, 822.

268 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 310 = NJW 2008, 822; *Kunig*, in: Münch/Kunig, Art. 13, Rn. 17; a. A.: *Schlegel*, GA 2007, 648.

269 BVerfG 26.05.1993 – 1 BvR 208/93, BVerfGE 89, 1, 12 = NJW 1993, 2035.

und 4 legen nahe, dass Abs. 1 vor der Informationserlangung über das Geschehen in der Wohnung schützt.[270]

Hauck geht hingegen davon aus, dass bei einer Online-Durchsuchung grundsätzlich kein Eingriff in Art. 13 GG gegeben sei, weil es darauf ankomme, der Wohnung die Möglichkeit zu entziehen, sie als Rückzugsort zu nutzen. Lausch- und Spähangriffe seien deswegen an Art. 13 GG zu messen, weil sie in der Lage seien, *alle* Informationen aus der Wohnung zu erheben und damit der Wohnung den Status als Rückzugsort in Gänze zu entziehen.[271] Für einzelne Informationen, die sich aus der Wohnung ergeben, genüge der Schutz des allgemeinen Persönlichkeitsrechts.[272]

Diese Argumentation kann nicht überzeugen. Insbesondere können durch eine Online-Durchsuchung gerade nicht nur einzelne Rechnerinformationen erhoben werden, wie von *Hauck* darlegt,[273] sondern es ist, wie bereits oben dargestellt, denkbar, dass mittels einer Online-Durchsuchung und der passiven Kenntnisnahme der Peripheriegeräte auch Vorgänge innerhalb der Wohnung wahrgenommen werden. Diese, wenn auch passive, Wahrnehmung der Vorgänge kann grundsätzlich einen Eingriff in Art. 13 GG darstellen, weil sie in der Lage ist, Vorgänge innerhalb der Wohnung zu offenbaren, und die betroffene Person in der Wahrnehmung ihrer Wohnung als Rückzugsort beeinträchtigen kann. Für die Einordnung als optische Wohnraumüberwachung bedarf es nicht der Entziehung der Wohnung als Rückzugsort in Gänze. Bei einem Eingriff in das Wohnungsgrundrecht kommt es vielmehr darauf an, ob die betroffene Person in ihrer räumlich abgeschirmten Privatsphäre beeinträchtigt wird.[274] Die Durchführung einer optischen Wohnraumüberwachung mittels der Online-Durchsuchung ist vom Tatbestand der Ermächtigungsgrundlage zwar nicht von vornherein ausgeschlossen, allerdings dürfen entsprechende Daten nicht erhoben werden. Aus diesem Grund ist eine Online-Durchsuchung abzubrechen, wenn optische Vorgänge in der Wohnung durch die Ermittlungsbehörden wahrgenommen werden können. Ein gegenteiliges Verhalten ist als verfassungswidrig einzustufen. Wann genau eine verfassungswidrige optische Wohnraumüberwachung gegeben ist, unterliegt einigen Abgrenzungsproblemen. Für eine optische Wohnraumüberwachung mittels der Online-Durchsuchung kommen die Fallgruppen der Videotelefonie,

---

270 *Kunig*, in: Münch/Kunig, Art. 13, Rn. 17; *Kühne*, in: Sachs, GG Kommentar, Art. 13, Rn. 22.

271 *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 8.

272 *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 8.

273 *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 8.

274 *Kluckert*, in: BeckOK GG, Art. 13, 5a; BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 310 = NJW 2008, 822.

welche auch bei der Quellen-TKÜ zu berücksichtigen ist, und jene der auf dem IT-Gerät gespeicherten Videos in Betracht.

(b) Eingriff durch Kenntnisnahme von Videotelefonie

Die passive Kenntnisnahme der Kamera durch die Ermittlungsbehörden bei einem Videotelefonat in der Wohnung kann grundsätzlich einen Eingriff in Art. 13 Abs. 1 GG darstellen.[275] Das Videotelefonat stellt hierbei einen Vorgang innerhalb der Wohnung dar. Während der passiven Kenntnisnahme der Kamera bei einem Videotelefonat verweilen die Ermittlungspersonen in der Wohnung der betroffenen Personen und überwachen sie. Sie erhalten dabei optische Informationen über die Wohnung mittels eines technischen Geräts und greifen damit in die räumlich geschützte Privatsphäre der betroffenen Person ein. Diese Beeinträchtigung besteht unabhängig von dem Inhalt des Gesprächs.

Gerechtfertigt werden kann ein solcher Eingriff in Art. 13 Abs. 1 GG im repressiven Bereich nur durch Abs. 2 (Durchsuchung) oder Abs. 3 (akustische Wohnraumüberwachung). Da es sich bei dem Eingriff der Kenntnisnahme von Videoübertragungen aus der Wohnung um keine der genannten Alternativen handelt, kann ein solcher Eingriff nicht gerechtfertigt werden. Denkbar wäre, sollte dies technisch möglich sein, allein die Tonspur nach den Voraussetzungen des Abs. 3 zur Kenntnis zu nehmen.

(c) Eingriff durch die Erhebung von gespeicherten Videos

Weiterhin muss gefragt werden, wie mit Videos umzugehen ist, die sich in einem gespeicherten Format auf dem IT-Gerät befinden. Damit ist die Live-Überwachung der Kamera, die zuvor dargestellt wurde, von der Erhebung solcher Videos abzugrenzen, die zwar in der Wohnung entstanden sind und auch Vorgänge aus der Wohnung abbilden, sich aber lediglich gespeichert auf dem Gerät befinden. Dabei muss an dieser Stelle unterschieden werden zwischen jenen Videos, die im Anordnungszeitraum entstehen, und solchen, die zeitlich vor der Online-Durchsuchung entstanden sind. Ein Beispiel wären solche Videos, die vor dem Anordnungszeitraum der Online-Durchsuchung während einer Geburtstagsparty in der Wohnung der betroffenen Person aufgenommen wurden.

275 Vgl.: *Roggan*, StV 2017, 821, 826.

(aa) Videoaufnahmen während des Anordnungszeitraums

Bruns geht davon aus, dass die Erhebung von Videos, die auf dem IT-Gerät gespeichert sind, „ohne Zweifel" zulässig sei.[276] Es ist allerdings fraglich, ob Zweifel an dieser Stelle nicht doch durchaus ihre Berechtigung haben. Denn auch diese Art der Videos ist grundsätzlich im Stande, Vorgänge innerhalb der Wohnung wiederzugeben, die eigentlich der natürlichen Wahrnehmung von außen entzogen sind, – im Übrigen unabhängig von ihrer Kernbereichsrelevanz.[277] Unklar ist, warum eine solche Wahrnehmung der Vorgänge innerhalb der Wohnung keinen Eingriff in Art. 13 GG darstellen soll. Denkbar wäre allenfalls, darauf abzustellen, dass die betreffende Person keinen Gebrauch davon macht, die Aufnahme zu löschen und sie weiterhin bewusst auf dem IT-Gerät speichert. Darin ist allerdings keine Einwilligung in den Eingriff zu sehen, zumal die betreffende Person von dem Eingriff in ihr Grundrecht gar keine Kenntnis hat. Videos, die in der Wohnung entstanden sind und die Wahrnehmung von Vorgängen in dieser zulassen, sind als nicht verwertbar einzustufen und dürfen bereits nicht erhoben werden.[278] Dies gilt zunächst für solche Videos, die während des Anordnungszeitraums in der Wohnung der betroffenen Person entstehen und Vorgänge in der Wohnung preisgeben. Auch hier verweilen die Ermittlungspersonen heimlich in der Wohnung, während die betroffene Person diese als privaten Rückzugsort nutzt. In dieser Fallkonstellation kommt der Überwachungscharakter der Maßnahme ebenfalls zum Tragen. Eine gegenteilige Auffassung würde im Übrigen die Gefahr bergen, dass das Verbot der optischen Live-Überwachung durch eine Auswertung der wenige Sekunden später erfolgenden Speicherung der Daten umgangen wird. Wie bei der Videotelefonie greift auch bei den gespeicherten Videos innerhalb des Anordnungszeitraums keine der Schranken des Art. 13 GG, sodass die Kenntnisnahme von Videos, die im Anordnungszeitraum in der Wohnung der betroffenen Person entstanden sind, nicht gerechtfertigt werden kann.

(bb) Gespeicherte Videos

Insbesondere problematisch ist der Umgang mit jenen Videos, die sich bereits seit längerer Zeit auf dem IT-Gerät befinden und vor dem Anordnungszeitraum auf diesem gespeichert wurden. Denn der Schutz des Art. 13 Abs. 1 GG kann sich nicht ohne zeitliche Grenze entfalten, da sonst das

276 *Bruns*, in: KK, § 100b, Rn. 5.

277 Formulierung aus: BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 310 = NJW 2008, 822.

278 Vgl.: *Soiné*, NStZ 2018, 497, 504.

Grundrecht aus Art. 13 GG zu weit ausgedehnt würde. Um von einem Eingriff in Art. 13 GG ausgehen zu können, müssen aktuelle Vorgänge in der Wohnung wahrgenommen werden können, also solche, die sich während des Anordnungszeitraums in der Wohnung abspielen. Bei der Kenntnisnahme dieser älteren Videos werden keine aktuellen Vorgänge in der Wohnung abgebildet. Es fehlt somit bei dieser Konstellation an einem Überwachungscharakter, die Ermittlungsbehörden verweilen nicht in der Wohnung, sondern nehmen Vorgänge in der Wohnung nachträglich zur Kenntnis.

(d) Zusammenfassung

Zusammenfassend lässt sich sagen, dass repressive optische Wohnraumüberwachungen nicht gerechtfertigt werden können und als verfassungsrechtlich unzulässig anzusehen sind. Dies erstreckt sich auch auf die Online-Durchsuchung. Für die optische Wohnraumüberwachung macht es im Ergebnis keinen Unterschied, ob Vorgänge aus der Wohnung live mitgeschnitten werden oder ob sie sich gespeichert auf dem IT-System befinden. Allerdings muss unterschieden werden zwischen Videos, die während des Anordnungszeitraums auf dem IT-Gerät gespeichert werden, und solchen, die sich bereits über einen längeren Zeitraum auf dem IT-Gerät befinden. Die Systematik des Art. 13 GG zeigt deutlich, dass die optische Wohnraumüberwachung bewusst nicht als Ermittlungsmaßnahme zu repressiven Zwecken mitaufgenommen wurde. Denkbar wäre somit allenfalls, eine akustische Wahrnehmung der Vorgänge in der Wohnung mittels der Online-Durchsuchung durchzuführen, indem lediglich die Tonspur der Videos erhoben wird.

(2) Akustische Wohnraumüberwachung

Weiterhin ist zu berücksichtigen, dass die Ermittlungsbehörden mittels einer Online-Durchsuchung und des passiven Zugriffs auf das Mikrofon des IT-Geräts eine akustische Wohnraumüberwachung durchführen. Eine solche ist zu repressiven Zwecken grundsätzlich denkbar. Art 13 Abs. 3 GG definiert die Schranke für einen solchen Eingriff so, dass nach den Vorgaben akustische Daten erhoben werden dürfen, welche Lebensvorgänge aus der Wohnung offenbaren.

Eine akustische Wohnraumüberwachung ist gegeben, wenn durch technische Mittel akustische Vorgänge in der Wohnung wahrgenommen werden können, die der Wahrnehmung von außen grundsätzlich entzogen sind.[279] Wenn bei der passiven Kenntnisnahme der Mikrofone des IT-Geräts akusti-

[279] BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 310 = NJW 2008, 822.

sche Vorgänge in der Wohnung wahrgenommen werden können, stellt dies einen Eingriff in Art. 13 Abs. 1 GG dar, dessen Schranken sich für die repressive akustische Wohnraumüberwachung aus Art. 13 Abs. 2, 3 GG ergeben. Da die Online-Durchsuchung dieselben Eingriffsvoraussetzungen hat wie die akustische Wohnraumüberwachung, ist die Schranke des Art. 13 Abs. 3 GG umgesetzt worden.[280]

(a) Das Verhältnis zwischen akustischer Wohnraumüberwachung und Online-Durchsuchung

Das Verhältnis zwischen den Ermittlungsmaßnahmen der Online-Durchsuchung und der akustischen Wohnraumüberwachung ist in der Literatur noch nicht abschließend geklärt. An dieser Stelle wird von *Bruns* vertreten, dass die passive Kenntnisnahme der Mikrofonmitschnitte auch von der Online-Durchsuchung gedeckt sei, denn der Gesetzgeber habe eine Gleichsetzung von Online-Durchsuchung und akustischer Wohnraumüberwachung vorgenommen.[281]

Zunächst ist aber festzuhalten, dass es sich hier nicht um deckungsgleiche Maßnahmen handelt. Trotz derselben Anordnungsvoraussetzungen sind die Ermittlungsmaßnahme der akustischen Wohnraumüberwachung und die der Online-Durchsuchung voneinander zu trennen. Welche der beiden Maßnahmen intensiver ist, richtet sich nach dem jeweiligen Einzelfall – in der Regel wird dies aber wohl die Online-Durchsuchung sein. Die Möglichkeiten der Datenerhebung sind bei der Online-Durchsuchung deutlich vielseitiger als bei der akustischen Wohnraumüberwachung. Die Rechtsprechung geht lediglich von einer Vergleichbarkeit der beiden Maßnahmen aus.[282] Aus diesem Grund kann nicht davon ausgegangen werden, dass bei der Anordnung einer Online-Durchsuchung auch automatisch eine akustische Wohnraumüberwachung mit angeordnet wird.

(b) Notwendigkeit der Anordnung einer akustischen Wohnraumüberwachung bei passiver Kenntnisnahme der Mikrofone?

Es drängt sich in diesem Zusammenhang die Frage auf, ob es für die passive Kenntnisnahme der Mikrofone von IT-Geräten einer gesonderten Anordnung in Form der akustischen Wohnraumüberwachung gem. § 100e StPO

280 Zum Problem der Umsetzung der Subsidiaritätsklausel siehe: B. I.

281 *Bruns*, in: KK, § 100b, Rn. 5.

282 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 269, 274, 307, 312, 329 = NJW 2016, 1781.

bedarf. Denn wird das Mikrofon eines IT-Systems, welches sich in der Wohnung des*der Nutzer*in befindet, wahrgenommen, handelt es sich faktisch um die akustische Kenntnisnahme der Vorgänge in der Wohnung und damit um eine akustische Wohnraumüberwachung.

Unter anderem geht *Soiné* davon aus, dass es in einem solchen Fall die gesonderte Anordnung der akustischen Wohnraumüberwachung brauche. Nur dann seien Raumgespräche als verwertbar anzusehen.[283] Diesbezüglich argumentiert *Graf*, dass die Daten nicht auf dem IT-System gespeichert werden, sie aus diesem Grund bereits nicht mehr von der Online-Durchsuchung mitumfasst seien und es deswegen auf die Anordnung einer akustischen Wohnraumüberwachung nicht ankomme.[284] Dies kann aber, wie bereits oben dargestellt, nicht überzeugen, da auch diese Daten zu den gespeicherten Informationen eines IT-Geräts gehören.[285]

Folgte man der Ansicht *Soinés*, wäre die Unterscheidung zwischen aktiver und passiver Kenntnisnahme des Mikrofons hinfällig. Dächte man diese Ansicht zu Ende, dürften die Ermittlungsbehörden nicht nur das Mikrofon passiv zur Kenntnis nehmen, sondern auch eine Aktivierung wäre – über die Ermächtigungsgrundlage der akustischen Wohnraumüberwachung – denkbar. Eine Online-Durchsuchung ermächtigt, wie zuvor dargestellt, nur zu einer passiven Kenntnisnahme der Mikrofone. In Abgrenzung hierzu ermächtigt die akustische Wohnraumüberwachung zu der aktiven Aktivierung von technischen Mitteln zur akustischen Überwachung innerhalb des Wohnraums. Die beiden Ermittlungsmaßnahmen haben demnach unterschiedliche Zielrichtungen und sind in der Erreichung ihres jeweiligen Ziels nicht gleich effektiv. Während die akustische Wohnraumüberwachung allein das gesprochene Wort innerhalb der Wohnung aufzeichnet, zielt die Online-Durchsuchung auf Daten auf dem IT-Gerät ab. Die Online-Durchsuchung kann somit Anteile einer akustischen Wohnraumüberwachung enthalten, stellt aber keine solche Ermittlungsmaßnahme dar. Es bedarf somit keiner gesonderten Anordnung der akustischen Wohnraumüberwachung zur passiven Kenntnisnahme von Mikrofonen von IT-Geräten. Dass eine Ermittlungsmaßnahme Anteile einer anderen Ermittlungsmaßnahme beinhaltet, ist nicht ungewöhnlich. So kann eine akustische Wohnraumüberwachung auch Anteile einer Observation beinhalten. In der Abgrenzung zwischen der Online-Durchsuchung und der akustischen Wohnraumüberwachung verläuft die Grenze dort, wo es den Ermittlungsbehörden auf eine faktische akustische Wohnraumüberwachung ankommt. Wenn das primäre Ziel der Ermittlungsarbeit die Erfassung des gesprochenen Wortes in der Wohnung ist und nicht im wesent-

283 *Soiné*, NStZ 2018, 497, 504; *Graf*, in: BeckOK StPO, § 100b, Rn. 55.
284 *Graf*, in: BeckOK StPO, § 100b, 55.
285 Vgl.: B. I. 2.

lichen Daten aus dem IT-Gerät erhoben werden sollen, dann bedarf es auch der Anordnung einer akustischen Wohnraumüberwachung. Dies kann beispielsweise der Fall sein, wenn sprachgesteuerte IT-Geräte wie Alexa das gesamte akustische Geschehen innerhalb der Wohnung aufzeichnen[286] und es den Ermittlungsbehörden gerade hierauf ankommt.

Die Online-Durchsuchung greift somit bei der passiven Kenntnisnahme in Art. 13 Abs. 1 GG ein und erfüllt die Schranken des Art. 13 Abs. 3 GG, ist aber nicht als eine akustische Wohnraumüberwachung anzusehen. Es bedarf im Grundsatz keiner gesonderten Anordnung.[287]

(c) Verletzung des Zitiergebots

Da die Online-Durchsuchung, wie oben dargestellt, auch in das Wohnungsgrundrecht aus Art. 13 GG eingreift, indem sie die akustische Wahrnehmung von Vorgängen in der Wohnung ermöglicht, stellt sich nun die Frage, ob der Gesetzgeber gegen das Zitiergebot aus Art. 19 Abs. 1 S. 2 GG verstoßen hat,[288] indem er in Art. 17 des Gesetzes zur effektiven und praxistauglicheren Ausgestaltung des Strafverfahrens lediglich Art. 10 GG zitiert, in welchen durch die Quellen-TKÜ eingegriffen werde.[289] Auch in der Gesetzesbegründung verweist der Gesetzgeber lediglich auf einen Eingriff in Art. 13 GG in Bezug auf die bereits geregelte akustische Wohnraumüberwachung.[290] Allein die Nennung des Artikels in der Gesetzesbegründung reicht zur Einhaltung des Zitiergebots nicht aus.[291] Dass eine Online-Durchsuchung in Art. 13 GG eingreifen kann, wenn Vorgänge innerhalb der Wohnung wahrgenommen werden können, hat das Bundesverfassungsgericht bereits 2008 festgestellt.[292] Nicht berücksichtigt werden kann hierbei, dass nicht jede Online-Durchsuchung tatsächlich in das Wohnungsgrundrecht eingreift. Bereits die Möglichkeit der Einschränkung des Grundrechts bei Anwendung des Gesetzes reicht aus, um das Zitiergebot auszulösen.[293] So ist Sinn und Zweck

---

286 Zur Bedeutsamkeit von Smart-Home-Geräten für die Strafverfolgung vgl.: *Blechschmitt*, MMR 2018, 361.

287 Hiervon unberührt bleibt die Frage, ob eine akustische Wohnraumüberwachung (§ 100c StPO) mittels der Infiltrierung eines IT-Systems erfolgen darf.

288 Hiervon ausgehend: *Roggan*, StV 2017, 821, 826.

289 BGBl. I 2017, 3202.

290 BT-Drucks., 18/12785, S. 48.

291 *Dreier*, in: Grundgesetz Kommentar, Art. 19, Rn. 20.

292 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 310 = NJW 2008, 822; a.A.: *Freiling/Safferling/Rückert*, JR 2018, 9, 20; *Hauck*, in: Löwe-Rosenberg, § 100a, 9.

293 *Remmert*, in: Herzog/Scholz/Klein, Art. 19, Rn. 40.

des Zitiergebots eine Warn- und Besinnungsfunktion des Gesetzgebers,[294] außerdem soll sichergestellt werden, dass nur wirklich gewollte Eingriffe in Grundrechte erfolgen.[295] Der Gesetzgeber hat so über das Zitiergebot eine Rechenschaffenspflicht[296] und muss Grundrechtseingriffe ausdrücklich als solche zu erkennen geben.[297]

Das Bundesverfassungsgericht hat für die Notwendigkeit des Zitiergebots aus Art. 19 Abs. 1 S. 2 GG verschiedene Ausnahmen angenommen. Unter anderem geht es davon aus, dass offensichtliche Grundrechtseingriffe nicht zitiert werden müssen.[298] Bei offenkundigen Grundrechtseingriffen habe der Gesetzgeber diese bereits im Rahmen von Diskussionen wahrgenommen und sei sich ihrer bewusst.[299]

Unabhängig von der Frage, ob es nicht auch bei der Offensichtlichkeit der Grundrechteinschränkung eine Zitation des eingeschränkten Grundrechts braucht,[300] kann hier nach den zuvor vorgenommenen Ausführungen schon nicht von einer Offensichtlichkeit die Rede sein. Sowohl in der Rechtsprechung als auch in der Wissenschaft fehlt es an einer einhelligen Meinung, wann und wie mittels der Online-Durchsuchung in Art. 13 GG eingegriffen wird. Aus diesem Grund hätte sich der Gesetzgeber auf diesen Grundrechtseingriff besinnen müssen, wie es gerade Sinn und Zweck des Zitiergebots ist. Innerhalb des Gesetzgebungsprozesses wurde in verschiedenen Stellungnahmen auf einen möglichen Eingriff in Art. 13 GG hingewiesen.[301] Da Art. 13 GG dennoch nicht zitiert wurde, bleibt zu befürchten, dass sich der Gesetzgeber des Eingriffs nicht bewusst war. In jedem Fall ist aber eine Offenkundigkeit des Grundrechtseingriffs auszuschließen.

Auch eine Ausnahme über ein Wiederholungsgesetz kommt hier nicht in Betracht. Dieser vom Bundesverfassungsgericht entwickelten Ausnahme vom Zitiergebot liegt die Annahme zu Grunde, dass, wenn sich Beschrän-

---

294 Mit weiteren Nachweisen aus der Rechtsprechung: BVerfG 07.12.2011 – 2 BvR 2500/09, 2 BvR 1857/10, BVerfGE 130, 1, 39 = NJW 2012, 907.

295 BVerfG 04.05.1983 – 1 BvL 46/80, 1 BvL 47/80, BVerfGE 64, 72, 79 = NJW 1983, 2869.

296 BVerfG 04.05.1983 – 1 BvL 46/80, 1 BvL 47/80, BVerfGE 64, 72, 79 = NJW 1983, 2869.

297 BVerfG 25.05.1956 – 1 BvR 190/55, BVerfGE 5, 13, 16 = NJW 1956, 986.

298 BVerfG 30.05.1973 – 2 BvL 4/73, 185, 189 = NJW 1973, 1363.

299 BVerfG 30.05.1973 – 2 BvL 4/73, 185, 189 = NJW 1973, 1363.

300 Hierzu unter anderem kritisch: *Dreier*, in: Grundgesetz Kommentar, Art. 19, Rn. 27; *Kaiser*, Auf Schritt und Tritt – die elektronische Aufenthaltsüberwachung, S. 189.

301 *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 4; *Sinn*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 12.

kungen lediglich wiederholen, sie nicht erneut zitiert werden müssen.[302] Auch nach dieser Ansicht ist es allerdings notwendig, dass dem „bisherigen Recht fremde Möglichkeiten des Eingriffs in Grundrechte“[303] zitiert werden. Bei der Online-Durchsuchung handelt es sich um eine der StPO neuen Ermächtigungsgrundlage. Auch diese Ausnahme kann auf die Online-Durchsuchung somit keine Anwendung finden.

Gleiches gilt für die Ausnahme des mittelbaren Grundrechtseingriffs. Nach dieser Ausnahme bezieht sich das Zitiergebot nur auf finale Grundrechtseingriffe klassischer Art.[304] Nach Ansicht des Bundesverfassungsgerichts richtet sich der Geltungsbereich des Art. 19 Abs. 1 S. 2 GG nicht an andere grundrechtsrelevante Maßnahmen wie Inhaltsbestimmungen und Regelungsaufträge, welche die Verfassung dem Gesetzgeber zur Konkretisierung des Grundrechtsschutzes zugewiesen hat.[305] Bei der Online-Durchsuchung handelt sich um einen finalen Grundrechtseingriff und nicht um eine Inhaltsbestimmung, sodass auch diese Ausnahme des Bundesverfassungsgerichts keine Anwendung finden kann.

Des Weiteren gehört Art. 13 GG auch zu jenen Grundrechten, die grundsätzlich der Zitierpflicht unterfallen.[306]

Aus diesem Grund ist das Gesetz zur effektiven und praxistauglichen Ausgestaltung des Strafverfahrens als verfassungswidrig einzustufen, da es Art. 13 GG nicht zitiert.[307]

cc) Beschlagnahme des IT-Geräts

Besondere Nähe weist die Online-Durchsuchung zur herkömmlichen Durchsuchung beziehungsweise zur Sicherstellung, Beschlagnahme und der darauf oftmals folgenden Durchsicht von Papieren auf. Dem Ursprung der Vorschrift entsprechend, können bei der Online-Durchsuchung auch Anteile einer „klassischen“ Wohnungsdurchsuchung und insbesondere der Beschlagnahme enthalten sein. Diese beiden Maßnahmen sind auch jene, die durch den Namen der Ermittlungsmaßnahme suggeriert werden.

---

302 BVerfG 25.05.1956 – 1 BvR 190/55, BVerfGE 5, 13, 16 = NJW 1956, 986.

303 BVerfG 25.05.1956 – 1 BvR 190/55, BVerfGE 5, 13, 16 = NJW 1956, 986.

304 Vgl. mit weiteren Nachweisen: *Dreier*, in: Grundgesetz Kommentar, Art. 19, Rn. 21.

305 BVerfG 04.05.1983 – 1 BvL 46/80, 1 BvL 47/80, BVerfGE 64, 72, 81 = NJW 1983, 2869.

306 *Dreier*, in: Grundgesetz Kommentar, Art. 19, Rn. 26.

307 Vgl. auch: *Roggan*, StV 2017, 821, 826.

Nach einer Durchsuchung der Wohnung oder einer Person, was eine offene Maßnahme darstellt, ist es denkbar, Gegenstände i. S. d. § 94 StPO sicherzustellen oder zu beschlagnahmen und unter anderem elektronische Speichermedien durchzusehen. Kommt es den Ermittlungsbehörden also auf die Erlangung eines bestimmten Fotos, Videos oder einer anderen Datei, von der sie Kenntnis haben, dass sie sich auf dem IT-Gerät befindet, an, ist zunächst die Beschlagnahme des IT-Geräts als die mildere Maßnahme gegenüber der Online-Durchsuchung durchzuführen.[308] Dies ist darin begründet, dass es sich bei der Beschlagnahme um eine offene Maßnahme handelt, die einer heimlichen Maßnahme, wie der Online-Durchsuchung, vorzuziehen ist. Außerdem wohnt der Beschlagnahme gerade kein Überwachungscharakter inne, dem aufgrund der Dauer und der Heimlichkeit der Maßnahme erheblich höhere Grundrechtsrelevanz zukommt. Bei einer herkömmlichen Durchsuchung ist nur eine punktuelle Durchsicht des Geräts möglich und es wird gezielt nach einzelnen Daten gesucht. Gem. § 110 Abs. 3 StPO ist auch die Online-Sichtung von Daten möglich.[309] Bei der Online-Durchsuchung kommt es hingegen auf die dauerhafte Überwachung des Geräts an, nicht auf das Auffinden eines einzelnen Datums.[310] Dies macht bereits die Gesetzesbegründung deutlich, wenn sie die Online-Durchsuchung als eine Maßnahme definiert, die die Nutzung des Geräts durch die betroffene Person überwacht und gespeicherte Inhalte aufzeichnet.[311] Der Gesetzgeber grenzt die Online-Durchsuchung ganz bewusst von der Beschlagnahme ab.[312] Ziel einer Online-Durchsuchung ist die Überwachung des Nutzungsverhaltens einer Person und nicht die einmalige punktuelle Durchsicht des IT-Geräts.[313] Hieraus ergibt sich die Nähe zur akustischen Wohnraumüberwachung, sie erfolgt ebenfalls heimlich und dient der Überwachung einer Person. Auch bei einer akustischen Wohnraumüberwachung erhoffen sich die Ermittlungspersonen Informationen, die den*die Täter*in belasten, ohne im Vorhinein eine konkrete Beschreibung gesuchter Daten vornehmen zu können. Gleiches ist der Grundgedanke der Online-Durchsuchung. Ein IT-Gerät soll überwacht werden, um aus der Überwachung des Nutzungsverhaltens Informationen über die Tat zu erlangen. Das lässt auch § 100e Abs. 2 StPO erkennen, indem die Vorschrift deutlich macht, dass sich eine Online-Durchsuchung über einen längeren Zeitraum hinweg erstreckt.

---

308 Zu der Unterscheidung beider Maßnahmen siehe bereits: BVerfG 11.05.2007 – 2 BvR 543/06, 322.

309 Genauer hierzu: *Zerbes/El-Ghazi*, NStZ 2015, 425, 428.

310 Vgl.: *Freiling/Safferling/Rückert*, JR 2018, 9, 13; *Knierim/Oehmichen*, Quellen TKÜ und Online-Durchsuchung, in: Gesamtes Strafrecht aktuell, S. 375.

311 BT-Drucks., 18/12785, S. 54.

312 BT-Drucks., 18/12785, S. 54.

313 BT-Drucks., 18/12785, S. 54.

Da die Ermächtigungsgrundlage der Online-Durchsuchung vorsieht, dass Daten aus dem IT-Gerät erhoben werden, was dem Wortlaut entsprechend zunächst die Erhebung einer einzelnen Information mitumfasst, geht *Hauck* davon aus, dass die Befugnisnorm der Online-Durchsuchung teleologisch zu reduzieren sei.[314] Es gehe nach seiner Ansicht bei der Online-Durchsuchung nicht um eine umfassende Datenerhebung, die im Übrigen aufgrund der Gefahr einer Totalüberwachung nicht mit Art. 1 GG vereinbar sei, sondern zugriffsrelevant sei lediglich das einzelne Datum, dem in einem Ermittlungsverfahren erheblicher Beweiswert zukommt.[315] Dass die Gefahren der Totalüberwachung bei einer Online-Durchsuchung sehr hoch sind, wird noch zu einem späteren Zeitpunkt zu berücksichtigen sein. Eine solche Gefahr führt aber nicht zu einer grundsätzlichen Verfassungswidrigkeit beziehungsweise zu der Notwendigkeit einer verfassungskonformen Auslegung mittels einer teleologischen Reduktion der Online-Durchsuchung, auch wenn ein Überwachungscharakter angenommen wird. Einer solchen Auslegung widerspricht des Weiteren die Tatsache, dass die Online-Durchsuchung auf Dauer angelegt ist. Dies bräuchte es, wollte man nur eine einzelne Information erlangen, zumeist nicht. Vielmehr würde dafür ein einmaliger Zugriff auf das IT-Gerät ausreichen.

Somit kommt es der Online-Durchsuchung gerade nicht auf eine einmalige Durchsicht des Geräts und der Erhebung eines einzelnen Datums, von dem die Ermittlungsbehörden wissen, dass es sich auf dem IT-Gerät befindet, an. Hierfür reichen weiterhin die Beschlagnahme und das Auslesen der Daten gem. § 110 StPO als einschlägige Ermächtigungsgrundlagen aus. Sie sind stets subsidiär zur Online-Durchsuchung. Eine Online-Durchsuchung stellt somit kein Äquivalent zur Beschlagnahme dar und darf auch nicht als solche behandelt werden. Meinte die Online-Durchsuchung eine tatsächliche „Durchsuchung“ beziehungsweise Durchsicht der Papiere mittels der Infiltrierung des IT-Systems, hätte keine neue Ermittlungsmaßnahme geschaffen werden müssen. Denn Ziel der Online-Durchsuchung ist nicht das Auffinden einzelner Daten.

Die Online-Durchsuchung enthält zwar insoweit Anteile einer Beschlagnahme und der Durchsicht von Papieren, als dass sie es ebenfalls ermöglicht, dass einzelne Daten ausgewertet werden. Durch ihren Überwachungscharakter ist sie allerdings deutlich weitreichender als die reine, einmalige Durchsicht des IT-Geräts.

---

314 *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 109.

315 *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 110.

dd) Weitere Ermittlungsmaßnahmen

Bei der Online-Durchsuchung können außerdem Anteile anderer Ermittlungsmaßnahmen mitverwirklicht werden wie beispielsweise einer Observation.

Auch hier wäre es nun denkbar, je nach mitverwirklichter Ermittlungsmaßnahme, die Voraussetzungen und Maßstäbe der einzelnen Ermittlungsmaßnahmen anzuwenden. Dies würde jedoch zu erheblichen Ungenauigkeiten in der Praxis führen, weil pro Online-Durchsuchung wohl auch immer die Voraussetzungen anderer Ermittlungsmaßnahmen mitgeprüft werden müssten. Außerdem würde bei diesem Modell verkannt, dass die Ermittlungsbehörden die Peripheriegeräte nur passiv mitnutzen können und somit nicht, wie bei den womöglich verwirklichten anderen Ermittlungsmaßnahmen, die Kontrolle über deren Einsatz haben. Eine Online-Durchsuchung beinhaltete damit zumeist lediglich Anteile andere Ermittlungsmaßnahmen. Berücksichtigt werden muss im Übrigen, dass es sich bei der Online-Durchsuchung um die (mit) intensivste aller Maßnahmen in der StPO handelt. Aus diesem Grund sind an sie auch die höchsten Anforderungen zu stellen, sodass die Voraussetzungen der verschiedenen Ermittlungsmaßnahmen eher heranzuziehen sind. Sind die Voraussetzungen der Online-Durchsuchung gegeben, werden auch jene der eingriffsschwächeren Maßnahmen erfüllt sein. Dies befreit selbstredend nicht von einer Verhältnismäßigkeitsprüfung im Einzelfall, sodass stets die mildere Ermittlungsmaßnahme durchzuführen ist. Die Online-Durchsuchung darf an dieser Stelle nur die ultima ratio darstellen.[316]

Durch die Mitverwirklichung anderer Ermittlungsmaßnahmen intensiviert sich die Online-Durchsuchung und somit der Grundrechtseingriff. Insbesondere kann durch eine Online-Durchsuchung in verschiedene Grundrechte eingegriffen werden, was erhebliche Auswirkungen auf die Verhältnismäßigkeit der Maßnahme im konkreten Einzelfall hat. In der weiteren Ausarbeitung wird demnach auf der Ebene des Kernbereichsschutzes zu beachten sein, dass auch diese Daten aus der passiven Beobachtung der Peripheriegeräte erhoben werden können und dürfen. Durch die Möglichkeit der Mitverwirklichung verschiedener Ermittlungsmaßnahmen stammen auch die erhobenen Daten aus den verschiedensten Lebensbereichen der betroffenen Person. Dies ermöglicht eine breite Erfassung ihrer Lebenswirklichkeit und leistet so einen erheblichen Beitrag zur Problematik der Gefahr der Bildung von Persönlichkeitsprofilen, die es im Folgenden im Rahmen des Schutzes des Kernbereichs privater Lebensgestaltung zu berücksichtigen gilt.

316 *Schmitt*, in: Meyer-Goßner/Schmitt, § 100b, Rn. 6.

d) Zwischenergebnis

Im Ergebnis lässt sich festhalten, dass durch die Online-Durchsuchung eine erhebliche Datenmenge auf unterschiedliche Art und Weise gesammelt werden kann. Diese ist potenziell in der Lage, ein ausdrucksstarkes Bild über die Persönlichkeit der betroffenen Person zu erstellen. Zum einen können sich auf einem IT-Gerät Daten befinden, die ein Äquivalent zu jenen Daten darstellen, die auch bei einer klassischen Durchsuchung gefunden worden wären. Des Weiteren ist es aber auch möglich, durch eine Live-Überwachung diese Daten mittels eines Prozesses des Profilings als Profiling-Daten zu verwerten. Diese Datenerhebung kann durch verschiedene, mitverwirklichte Ermittlungsmaßnahmen geschehen, die durch die passive Kenntnisnahme von Peripheriegeräten ermöglicht wird. Einer Online-Durchsuchung liegt jedoch immer der Gedanke einer Überwachung zugrunde. Ihr kommt es somit nicht auf das Auffinden eines einzelnen Datums an, sondern, wie es auch schon die Gesetzesbegründung beschreibt, auf die Überwachung des Nutzungsverhaltens und die Aufzeichnung gespeicherter Inhalte.[317] Damit handelt es sich bei der Online-Durchsuchung nicht um eine herkömmliche Durchsuchung, die offen und punktuell stattfindet, sondern um eine Überwachungsmaßnahme. Bei einer solchen Überwachung mittels der Online-Durchsuchung ist eine optische Überwachung der Wohnung aufgrund von Art. 13 Abs. 3 GG stets ausgeschlossen. Grundsätzlich können durch die Online-Durchsuchung aber auch Anteile einer akustischen Wohnraumüberwachung mitverwirklicht werden. Im Ergebnis führt dies dazu, dass es sich bei der Online-Durchsuchung um eine eingriffsintensive Ermittlungsmaßnahme handelt, auch weil eine erhöhte Gefahr der Bildung von Persönlichkeitsprofilen besteht, was auch auf den Schutz des Kernbereichs der privaten Lebensgestaltung durchschlägt und hier zu berücksichtigen ist.

3. Verdachtsgrad

Als nächstes Tatbestandsmerkmal braucht es für die Durchführung der Online-Durchsuchung einen Verdacht. In § 100b Abs. 1 Nr. 1 StPO heißt es, dass eine Online-Durchsuchung durchgeführt werden darf, „(…) wenn *bestimmte Tatsachen den Verdacht* begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete besonders schwere Straftat begangen oder in den Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat, (…)“. Dabei geht die wohl herrschende Meinung davon aus, dass es aufgrund der Heimlichkeit der Maßnahme eines Tatverdachts bedarf, der über den reinen Anfangsverdacht hinausgeht. Eines hinreichenden oder sogar

317 BT-Drucks., 18/12785, S. 54.

dringenden Tatverdachts bedürfe es aber nicht.[318] Dieser sogenannte qualifizierte Tatverdacht fordert konkrete und bereits in gewissem Umfang verdichtete Umstände, die eine ausreichende Tatsachengrundlage für den Verdacht einer Katalogtat begründen.[319] Dabei hat das Bundesverfassungsgericht für die akustische Wohnraumüberwachung entschieden, dass bei einem solchen Tatverdacht bereits Erkenntnisse vorliegen müssen, die eine erhöhte Wahrscheinlichkeit für die Begehung einer besonders schweren Katalogtat aufweisen.[320]

Andere gehen noch weiter und sehen die Notwendigkeit einer verfassungskonformen, restriktiven Auslegung, welche einen *dringenden Tatverdacht* fordere.[321] Dies wird mit der Eingriffsintensität und der Nähe zum Kernbereich der privaten Lebensgestaltung begründet.[322]

Zwar ist die Online-Durchsuchung eine der beziehungsweise oftmals auch die intensivste(-n) Ermittlungsmaßnahme(-n) in der StPO und hat eine große Nähe zum Kernbereich der privaten Lebensgestaltung, dies gilt aber auch für die akustische Wohnraumüberwachung. Der Wortlaut „bestimmte Tatsachen" findet sich auch bei jener Ermittlungsmaßnahme und ist bereits vor der Reformierung der StPO Teil dieser gewesen. Auch an dieser Stelle ging man von der Voraussetzung eines qualifizierten Tatverdachts aus. Der Wortlaut zeigt somit eindeutig, dass der Gesetzgeber einen qualifizierten Tatverdacht schaffen wollte. Dies ist auch mit der Verfassung vereinbar. Denkbar ist es zwar, für eine solch intensive Maßnahme wie die Online-Durchsuchung mit der Begründung der Verhältnismäßigkeit den höchstmöglichen Verdachtsgrad zu fordern; dies verkennt allerdings den Sinn und Zweck des Tatverdachts. Der dringende Tatverdacht findet sich unter anderem als Voraussetzung der Untersuchungshaft gem. § 112 Abs. 1 S. 1 StPO. Dieser fordert die hohe Wahrscheinlichkeit, dass die verdächtige Person die Straftat begangen hat. Weniger hohe Anforderungen hat der hinreichende Tatverdacht, den es für die Anklageerhebung gem. § 170 Abs. 1 StPO braucht und der eine Wahrscheinlichkeit fordert, dass die verdächtige Person die strafbare Handlung begangen hat und verurteilt wird.

---

318 *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 77; *Graf*, in: BeckOK StPO, § 100b, Rn. 12; *Schmitt*, in: Meyer-Goßner/Schmitt, § 100b, Rn. 4.

319 *Schmitt*, in: Meyer-Goßner/Schmitt, § 100b, Rn. 4.

320 BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 351 = NJW 2004, 999.

321 *Knierim/Oehmichen*, Quellen TKÜ und Online-Durchsuchung, in: Gesamtes Strafrecht aktuell, 378; *Großmann*, GA 2018, 439, 452.

322 *Knierim/Oehmichen*, Quellen TKÜ und Online-Durchsuchung, in: Gesamtes Strafrecht aktuell, 378; *Großmann*, GA 2018, 439, 452.

Für die Durchführung von Ermittlungsmaßnahmen reicht zumeist ein Anfangsverdacht oder aber der hier in Frage stehende qualifizierte Tatverdacht aus. Denn Ermittlungsmaßnahmen haben grundsätzlich das Ziel, den Anfangsverdacht zu untermauern, und stehen am Anfang eines Ermittlungsverfahrens, um Erkenntnisse zu sammeln, die dann einen hinreichenden oder dringenden Tatverdacht begründen.[323] Dabei stellt der qualifizierte Tatverdacht schon ein deutliches Mehr zum Anfangsverdacht dar. Somit wird bereits eine erhöhte Anforderung an den Tatverdacht geschaffen und der Grundsatz der Verhältnismäßigkeit eingehalten.

Es ist nicht ersichtlich, dass die Voraussetzung eines qualifizierten Tatverdachts nicht mit der Verfassung vereinbar ist. Nichtdestotrotz muss auf die Besonderheiten der Online-Durchsuchung, die insbesondere in der enormen Eingriffstiefe liegen, Rücksicht genommen werden, sodass Vermutungen oder allgemeine Erfahrungssätze nicht ausreichen. Es bedarf vielmehr konkreter und bereits in gewissem Umfang verdichteter Umstände, die eine ausreichende Tatsachengrundlage für den Verdacht einer Katalogtat begründen.[324] Mit dieser Einordnung ist den verfassungsrechtlichen Anforderungen, zumindest auf Ebene des Tatverdachts, ausreichend Rechnung getragen.

4. Katalogtat

Nach § 100b Abs. 1 Nr. 1 StPO muss der Verdacht einer „*besonders schweren Straftat*“ gegeben sein, um eine Online-Durchsuchung vornehmen zu können. Eine Konkretisierung erhält der Begriff dann in Abs. 2 der Norm. Der dort genannte Katalog (Nrn. 1–7 mit weiteren Aufgliederungen) entspricht dem der akustischen Wohnraumüberwachung aus § 100c Abs. 2 StPO a. F.[325] Außerdem enthält die neue Fassung der akustischen Wohnraumüberwachung in § 100c Abs. 1 Nr. 2 StPO einen Verweis auf diesen Straftatenkatalog. Dieser durchaus weitreichende Katalog an Straftaten ist bereits im Gesetzgebungsverfahren auf erhebliche Kritik[326] gestoßen, die auch nach Inkrafttreten des Gesetzes anhält.[327] Insbesondere habe man sich hier die

---

323 A. A.: *Großmann*, GA 2018, 439, 453.

324 Vgl.: *Schmitt*, in: Meyer-Goßner/Schmitt, § 100b, Rn. 4; *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 78.

325 BT-Drucks., 18/12785, S. 55.

326 *Bundesbeauftragte für Datenschutz und Informationsfreiheit Voßhoff*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 2 ff.; *Deutscher Anwaltsverein durch den Ausschuss Strafrecht*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 6, 7; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 12 ff.

327 *Singelnstein*, verfassungsblog 2017, Hacken zur Strafverfolgung? Gefahren und Grenzen der strafprozessualen Online-Durchsuchung; online abzurufen über https://verfassungsblog.de/hacken-zur-strafverfolgung-gefahren-und-grenzen-der-

Übertragung vom präventiven in den repressiven Bereich zu leicht gemacht.[328] Im Bereich der Strafverfolgung gehe es nicht um die Gefahrenabwehr, sondern um die Durchsetzung des staatlichen Strafanspruchs. Dieser müsse von vergleichbarer Wertigkeit sein wie die Abwehr einer drohenden Gefahr der vom Bundesverfassungsgericht genannten Rechtsgüter.[329] So muss zunächst konstatiert werden, dass die StPO immer dann als Ermächtigung herangezogen wird, wenn bereits eine Straftat begangen worden ist und somit eine Rechtsgutsverletzung bereits stattgefunden hat und nicht mehr abgewendet werden kann. Für die verfassungsrechtliche Rechtfertigung bedeutet dies, dass der Eingriff in die Rechtsgüter der betroffenen Person nicht mehr mit einer Gefahr für ein anderes Rechtsgut, sondern lediglich mit der Durchsetzung des staatlichen Strafanspruches und damit der Funktionsfähigkeit der Strafrechtspflege abgewogen werden kann. Dem wohnt die Frage inne, ob eine Maßnahme dann noch angemessen und demnach verhältnismäßig ist. Von Seiten des BKA in Gestalt des damaligen Vizepräsidenten *Henzler* wird dieser Frage entgegengehalten, dass das Urteil von 2008 deutlich gemacht habe,[330] dass die Online-Durchsuchung zur Verfolgung schwerer Straftaten denkbar sei.[331] Außerdem habe das Bundesverfassungsgericht die Wertigkeit der akustischen Wohnraumüberwachung und der Online-Durchsuchung auf eine Stufe gestellt, sodass eine Übertragung des Straftatenkatalogs die logische Konsequenz sei.[332] Dieser Diskussion liegt somit die Frage zugrunde, ob bereits die Funktionsfähigkeit der Strafrechtspflege einen heimlichen Eingriff in das IT-Grundrecht rechtfertigen kann.

---

strafprozessualen-online-durchsuchung/ (zugegriffen am 12.11.2020); *Blechschmitt*, StraFo 2017, 361, 364; *Singelnstein/Derin*, NJW 2017, 2646, 2647; *Freiling/Safferling/Rückert*, JR 2018, 9, 21; *Gercke*, in: Heidelberger Kommentar, § 100b, Rn. 7; *Hauck*, in: Löwe-Rosenberg, § 100a, Rn. 86.

328 *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 11; *Roggan*, StV 2017, 821, 827; anderer Ansicht und hierauf eingehend: *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 88.

329 *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 11; *Roggan*, StV 2017, 821, 827; anderer Ansicht und hierauf eingehend: *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 88.

330 Feststellung, dass Online-Durchsuchung auch zu repressiven Zwecken denkbar: BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 315 = NJW 2008, 822.

331 *Vizepräsident des Bundeskriminalamts Henzler*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 2.

332 *Vizepräsident des Bundeskriminalamts Henzler*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 2; *Huber*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 3, 4; nicht zuletzt argumentiert so auch der Gesetzgeber in: BT-Drucks., 18/12785, S. 55; *Sinn*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 10, 11.

Nach Ansicht des Bundesverfassungsgerichts ist es denkbar, dass Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme bei heimlichen Maßnahmen wie der Online-Durchsuchung gerechtfertigt sind, wenn die aus dem Eingriff resultierenden Daten nach strengen Maßstäben erhoben werden.[333] Diese strengen Maßstäbe könnten durch das Vorliegen einer erhöhten Eingriffsschwelle wie eines qualifizierten Tatverdachts[334] oder der Verfolgung von besonders gravierenden Straftaten erfüllt sein.[335] Im Fall der präventiven Online-Durchsuchung heißt dieser strenge Maßstab, dass eine drohende konkrete Gefahr für ein überragend wichtiges Rechtsgut bestehen muss.[336]

a) Die Funktionsfähigkeit der Strafrechtspflege als Rechtsgut von Verfassungsrang

Die Funktionsfähigkeit der Strafrechtspflege als solche liegt nach Ansicht des Bundesverfassungsgerichts im öffentlichen Interesse an einer möglichst vollständigen Wahrheitsermittlung und der Aufklärung schwerer Straftaten.[337] Dies sei ein wesentlicher Auftrag des Gemeinwesens, denn ohne eine funktionstüchtige Rechtspflege könne der Gerechtigkeit nicht zum Durchbruch verholfen werden. Das Grundgesetz messe dem Erfordernis der Funktionsfähigkeit der Rechtspflege eine besondere Bedeutung bei.[338]

Dem liege der Gedanke zugrunde, dass ein Rechtsstaat nur funktionieren könne, wenn er in der Lage sei, die eigenen Sanktionsnormen durch Ermittlungen, Gerichtsverfahren und Bestrafung durchzusetzen. Es sei demnach die Pflicht eines Staates gegenüber seinen Bürger*innen, die Sicherheit und das Vertrauen in die eigene Funktionsfähigkeit zu schützen.[339] Daher ergebe sich das Rechtsgut der Funktionsfähigkeit der Strafrechtspflege aus dem Rechtsstaatsprinzip.[340] Die Literatur schließt sich der Ansicht des Bundesverfas-

---

[333] BVerfG 24.04.2013 – 1 BvR 1215/07, BVerfGE 133, 277, 373 = NJW 2013, 1499; BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 304 f. = NJW 2016, 1781.

[334] Siehe hierzu: B. I. 3.

[335] BVerfG 24.04.2013 – 1 BvR 1215/07, BVerfGE 133, 277, 373 = NJW 2013, 1499.

[336] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 305 = NJW 2016, 1781.

[337] BVerfG 31.01.1973 – 2 BvR 454/71, BVerfGE 34, 238, 248 f. = NJW 1973, 891.

[338] BVerfG 31.01.1973 – 2 BvR 454/71, BVerfGE 34, 238, 249 = NJW 1973, 891.

[339] BVerfG 20.10.1977 – 2 BvR 631/77, BVerfGE 46, 214, 222f. = NJW 1977, 2355.

[340] BVerfG 08.10.1974 – 2 BvR 747/73, BVerfGE 38, 105, 116 = NJW 1975, 103.

sungsgerichts an und geht davon aus, dass die Funktionsfähigkeit der Strafrechtspflege ein Ausfluss des rechtsstaatlich gesicherten Justizgewährungsanspruchs sei.[341]

Landau geht an dieser Stelle noch weiter und sieht die Funktionsfähigkeit der Strafrechtspflege nicht nur als einen Ausfluss des Rechtsstaatsprinzips an, sondern sieht in ihr auch die Ausübung des Gewaltmonopols des Staates als solchem, die es zur Existenz eines demokratischen Rechtsstaates brauche.[342] Teil der Funktionsfähigkeit der Strafrechtspflege sei aber auch, ein ausgeglichenes Verfahren durchzuführen und nicht die Strafverfolgung um jeden Preis durchzusetzen.[343] *Landau* zustimmend ist somit festzustellen, dass die Funktionsfähigkeit der Strafrechtspflege kein reines „Gegeninteresse" zu den Grundrechten und bloßes Abwägungskriterium darstellt, sondern eine eigenständige Pflicht des Staates.[344] Damit hat die Funktionsfähigkeit der Strafrechtspflege, die sich aus dem Rechtsstaatsprinzip ergibt, als solche eben durch diese Entwicklung aus dem Rechtsstaatsprinzip Verfassungsrang. Die Übertragung von heimlichen Ermittlungsmaßnahmen aus dem präventiven in den repressiven Bereich fordert keine Vergleichbarkeit bezogen auf die Rechtsgüter, die bei der gleichen Ermittlungsmaßnahme präventiv geschützt werden sollen,[345] sondern es muss vielmehr die Frage gestellt werden, ab wann die Funktionsfähigkeit der Strafrechtspflege als Ausfluss des Rechtsstaatsprinzips nicht mehr gewährleistet werden kann.[346] Dies lässt sich allerdings nicht anhand einer klaren Grenze bestimmen, sondern es muss bei der Erfüllung dieser Pflicht auch Raum für die Einschätzungsprärogative des Gesetzgebers bleiben. In diesem Zusammenhang gilt es insbesondere zu berücksichtigen, durch welche weniger schwerwiegenden Ermittlungsmaßnahmen die Funktionsfähigkeit der Strafrechtspflege ebenfalls gesichert werden kann. Aus diesem Gedanken resultiert, dass auch die Subsidiaritätsklausel ein bedeutendes Gewicht bei der Rechtfertigung eines repressiven Eingriffs hat. Dieser Aspekt wird in der späteren Bearbeitung noch Berücksichtigung finden.

Das bedeutet zunächst zusammenfassend, dass die Funktionsfähigkeit der Strafrechtspflege durchaus Verfassungsrang hat, aus dem sich eine Rechtfertigung eines heimlichen Eingriffs in das IT-Grundrecht ergeben kann, da sie ähnlich ins Gewicht fallen kann wie eine drohende konkrete Gefahr als Ein-

---

341 *Jarass*, in: Jarass/Pieroth Kommentar zum GG, Art. 20, Rn. 142; *Grzeszick*, in: Herzog/Scholz/Klein, Art. 20, Rn. 143; *Rieß*, StraFo 2000, 364, 366.

342 *Landau*, NStZ 2007, 121, 127.

343 *Landau*, NStZ 2007, 121, 129.

344 *Landau*, NStZ 2007, 121, 128.

345 *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 10.

346 So auch: *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 88.

griffsschwelle im präventiven Bereich. Dabei gefährdet nicht jeder nicht durchgesetzte Strafanspruch des Staates diese Funktionsfähigkeit der Strafrechtspflege. Vielmehr fordert das Rechtsstaatsprinzip auch ein faires Verfahren. Aus diesem Grund müssen insbesondere zwei Faktoren für die Erfüllung der Angemessenheit berücksichtigt werden. Zum einen kann ein Eingriff in das IT-Grundrecht nicht bei allen Straftaten mit der Funktionsfähigkeit der Strafrechtspflege gerechtfertigt sein und auch an die Subsidiaritätsklausel sind hohe Anforderungen zu stellen.

b) Besondere Schwere der Straftat

Zunächst ist zu berücksichtigen, dass das Bundesverfassungsgericht festgestellt hat, dass es bei heimlichen Überwachungsmaßnahmen, die der Strafverfolgung dienen, für ihre Zulässigkeit auf das Gewicht der verfolgten Straftat ankommt.[347] Dem ist zuzustimmen, denn die Funktionsfähigkeit der Strafrechtspflege beinhaltet, wie zuvor dargestellt, keine Strafaufklärung um jeden Preis. Nur bei besonders schweren Straftaten besteht eine Pflicht des Staates gegenüber seinen Bürger*innen, den Strafanspruch durchzusetzen. Dennoch kommt dem Gesetzgeber ein Gestaltungsspielraum zu, wenn es darum geht festzulegen, welche Straftaten er als besonders durchsetzungswürdig ansieht. Damit kann keine klare Grenze gezogen werden, wann eine Straftat als besonders schwer einzustufen ist. Welche Straftaten als besonders schwer und damit für die Funktionsfähigkeit der Strafrechtspflege und die Durchsetzung des Strafanspruchs notwendig anzusehen sind, kann durch Zuhilfenahme verschiedener Faktoren bestimmt werden. Denn je größer das durch den*die Täter*in verwirklichte Unrecht ist, umso größer ist auch die Pflicht des Staates zur Aufklärung ebendieser Straftat. Diese Unrechtswertigkeit kann durch die Wertigkeit des zu schützenden Rechtsguts bestimmt werden. Allerdings muss am Ende dem Gesetzgeber eine Einschätzungsmöglichkeit bleiben. Diese Einschätzung hat der Gesetzgeber mit dem Straftatenkatalog in § 100b Abs. 2 StPO vorgenommen. Es gilt nun zu untersuchen, ob die Online-Durchsuchung bei allen dort genannten Straftaten durch die Funktionsfähigkeit der Strafrechtspflege als Staatspflicht gerechtfertigt werden kann.

Denn in dem Straftatenkatalog des § 100b Abs. 2 StPO finden sich solche, die wohl nicht mehr als besonders durchsetzungswürdig anzusehen und damit nicht als besonders schwere Straftaten einzustufen sind. Damit wären diese nicht mehr mit der Funktionsfähigkeit der Strafrechtspflege zu rechtfertigen.

---

[347] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 270 = NJW 2016, 1781.

aa) Überragend wichtige Rechtsgüter im Strafprozessrecht

Nach der Rechtsprechung des Bundesverfassungsgerichts sind, um dem Verhältnismäßigkeitsgrundsatz bei einer Ermächtigung zum heimlichen Zugriff auf ein informationstechnisches System zu genügen, besondere Anforderungen an den Eingriffsanlass zu stellen.[348] Dies kann die Gefahrenprävention sein, wenn eine konkrete Gefahr für ein überragend wichtiges Rechtsgut gegeben ist.[349] Dabei sind als überragend wichtige Rechtsgüter zunächst Leib, Leben und Freiheit einer Person zu nennen. Weiterhin zählen Rechtsgüter der Allgemeinheit zu den überragend wichtigen Rechtsgütern, deren Bedrohung die Grundlage oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.[350] Dies gilt es nun, in den repressiven Bereich zu übertragen. Wie oben bereits dargestellt, ist im repressiven Bereich eine Rechtfertigung eines solchen Eingriffs lediglich durch die Funktionsfähigkeit der Strafrechtspflege möglich. Eine repressive Online-Durchsuchung kann nicht mit der Funktionsfähigkeit der Strafrechtspflege gerechtfertigt werden, wenn schon die Abwehr einer konkreten Gefahr für diese Rechtsgüter eine Online-Durchsuchung nicht rechtfertigen kann.[351] Die Aufklärung von Straftaten, die nicht überragend wichtige Rechtsgüter zum Gegenstand haben, kann nicht höher wiegen als der präventive Schutz jener Rechtsgüter. Konkret bedeutet dies, dass jene Straftaten, die sich im Katalog befinden und keine Verletzung eines überragend wichtigen Rechtsguts ahnden, eine Online-Durchsuchung nicht rechtfertigen können.

Dies ist insbesondere bei den folgenden Straftaten problematisch.

(1) Betreiben krimineller Handelsplattformen

2021 fand in § 100b Abs. 2 Nr. 1 lit. b StPO der umstrittene neugeschaffen Straftatbestand des Betreibens krimineller Handelsplattformen im Internet gem. § 127 StGB Eingang in den Straftatenkatalog. Unter Strafe gestellt wird hier das Betreiben einer Handelsplattform im Internet, deren Zweck es ist, rechtswidrige Taten zu ermöglichen oder zu fördern. Eine Festlegung der

348 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 328 = NJW 2008, 822.

349 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 328 = NJW 2008, 822.

350 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 328 = NJW 2008, 822.

351 *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 86; *Kruse/Grzesiek*, KritV 2017, 331, 347; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, 12; *Roggan*, StV 2017, 821, 827.

Taten, die § 127 StGB umfasst, erfolgt seinerseits durch einen Straftatenkatalog.

Schutzgut des § 127 StGB ist die Sicherheit und Ordnung, die mittels einer Vorverlagerung der Strafbarkeit anschließende Straftaten verhindern soll. Hier handelt es sich, ähnlich wie bei der Bildung der kriminellen Vereinigung, um eine Verschachtelung der Straftaten. Da eine Online-Durchsuchung schon aus präventiven Gründen nur durchgeführt werden darf, wenn eine Gefahr für ein überragend wichtiges Rechtsgut besteht, darf auch im repressiven Bereich nichts anderes gelten. Da § 127 Abs. 1 Nr. 1 und 2 StGB nicht alleine überragend wichtige Rechtsgutsverletzungen beinhaltet, darf insoweit auch keine Online-Durchsuchung durchgeführt werden. Nach § 127 Abs. 1 StGB kann bereits die Förderung oder Ermöglichung jedes Verbrechens durch das Betreiben einer kriminellen Handelsplattform eine Strafbarkeit begründen. Damit wird die Ermächtigung in erheblicher Art und Weise ausgedehnt.

Dies kann, unabhängig von der Frage nach der Sinnhaftigkeit der Norm als solcher, nicht überzeugen. Eine Online-Durchsuchung zu diesem Zwecke, sei es aufgrund der Begehung im Internet auch noch so sinnvoll, kann nicht mit der Funktionsfähigkeit der Strafrechtpflege gerechtfertigt werden.

(2) Bildung einer kriminellen Vereinigung

Gem. § 100b Abs. 2 Nr. 1 lit. c StPO kann der Einsatz einer Online-Durchsuchung mit der Aufklärung einer Straftat der Bildung einer kriminellen Vereinigung (§ 129 Abs. 1 i. V. m. Abs. 5 S. 3 StGB) und der Bildung einer terroristischen Vereinigung (§ 129a Abs. 1, 2, 4, 5 S. 1 Alt. 1 StGB) gerechtfertigt werden. Nach Ansicht des Bundesgerichtshofs kann sie als Katalogtat nur herangezogen werden, wenn die geplante oder begangene Straftat der Mitglieder eine erhebliche Gefahr für die öffentliche Sicherheit bedeutet.[352] Grundsätzlich sollen durch die Straftatbestände die Rechtgüter der öffentlichen Sicherheit und Ordnung einschließlich des öffentlichen Friedens geschützt werden.[353] Somit handelt es sich bei den Rechtsgütern um solche der Allgemeinheit. Problematisch ist jedoch, ob diese Rechtsgüter auch die Existenz der Menschen berühren. Die Gefahren, die von kriminellen Vereinigungen ausgehen, liegen insbesondere in ihrer Eigendynamik.[354] Dabei handelt es sich um eine Straftat, die vorverlagerten Rechtsschutz gewährleisten

352 BGH 31.05.2016 – 3 StR 86/16 = StV 2018, 95.

353 *Schäfer*, in: MüKO, § 129, Rn. 1.

354 *Sternberg-Lieben/Schittenhelm*, in: Schönke/Schröder, § 129, Rn. 1; *Heintschel-Heinegg*, in: BeckOK StGB, § 129, 1.

soll.[355] Eine Online-Durchsuchung darf somit nur dann gem. § 100b Abs. 2 Nr. 1 lit. c StPO durchgeführt werden, wenn die in Rede stehende kriminelle Vereinigung eine Gefahr für überragend wichtige Rechtsgüter darstellt. Eine Umgehung der Vorgaben des Bundesverfassungsgerichts darf an dieser Stelle nicht erfolgen.

(3) Geld- und Wertzeichenfälschung

§ 100b Abs. 2 Nr. 1 lit. d StPO beinhaltet die Geld- und Wertzeichenfälschung. Der Strafrahmen der hier genannten Straftaten beläuft sich von nicht unter einem Jahr bis zu einem Jahr und bis zu zehn Jahren. Damit hat der Gesetzgeber bereits im Strafrahmen eine Erheblichkeit der Straftat festgestellt. Schutzgut dieser Straftaten ist die Sicherheit und Zuverlässigkeit des Verkehrs mit Geld, Wertpapieren und -zeichen.[356] Dabei handelt es sich zwar um ein Rechtsgut der Allgemeinheit und der Schaden, der durch eine solche Straftat angerichtet werden kann, kann immens sein. Dennoch ist die Durchsetzung dieses Strafanspruchs nicht von überragend wichtiger Bedeutung. Dies ist nicht zuletzt deswegen anzunehmen, weil der Schaden primär ein finanzieller ist und nicht die Existenz der Menschen oder den Bestand des Staates berührt. Aus diesem Grund sind die in lit. d genannten Delikte nicht als besonders schwere Straftaten einzustufen, die eine Aufklärung mittels Online-Durchsuchung, begründet mit der Funktionsfähigkeit der Strafrechtspflege, rechtfertigen können.[357]

(4) Verbreitung, Erwerb und Besitz von kinderpornografischen Inhalten

Außerdem wird die Verbreitung, der Erwerb und Besitz kinderpornografischer Schriften gem. § 184b Abs.1 S. 1 und Abs. 2 StGB als eine taugliche Straftat zur Rechtfertigung der repressiven Online-Durchsuchung benannt. Hier beträgt die angedrohte Strafe bis zu zehn Jahre beziehungsweise nicht unter zwei Jahren und befindet sich, allein aufgrund des Strafrahmens, auch im Bereich der erheblichen Strafen. Schutzgut ist der Schutz von Kindern.[358] Grundsätzlich ist hierin zunächst keines der vom Bundesverfassungsgericht als überragend wichtiges Rechtsgut eingestuften Güter zu erkennen. Allerdings darf nicht unberücksichtigt bleiben, dass durch die Verbreitung und

355 *Heintschel-Heinegg*, in: BeckOK StGB, § 129, 1.

356 *Erb*, in: MüKO, § 146, Rn. 1.

357 *Deutscher Anwaltsverein durch den Ausschuss Strafrecht*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 14; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 13; *Großmann*, GA 2018, 439, 451.

358 *Fischer*, in: Fischer, § 184b, Rn. 2.

Betrachtung pornographischer Abbildungen, die ohne die Einwilligung der betroffenen Personen passieren, die Persönlichkeitsrechte und die Menschenwürde der Kinder erheblich beeinträchtigt werden.[359] § 184b Abs. 2 StGB stellt durch die Tatbestandsmerkmale der Gewerbsmäßigkeit und der fortgesetzten Begehung als ein Mitglied einer Bande die auf Dauer angelegten Persönlichkeitsrechts- und Menschenwürdeverletzungen der betroffenen Kinder unter Strafe. Die Vorbeugung der Verbreitung solch erheblicher Persönlichkeitsrechtsverletzungen von Kindern stellt ein überragend wichtiges Rechtsgut dar, welches eine Online-Durchsuchung rechtfertigen kann.

(5) Bandendiebstahl und schwerer Bandendiebstahl

Der Bandendiebstahl und der schwere Bandendiebstahl können nach dem aktuellen Straftatenkatalog ebenfalls Anlass für eine Online-Durchsuchung sein. Der angedrohte Strafrahmen sieht an dieser Stelle sechs Monate bis zehn Jahre und ein Jahr bis zehn Jahre vor. Geschützt werden soll das Eigentum.[360] Dies kann als Rechtsgut zur Begründung einer besonders schweren Straftat nicht genügen.[361] An dieser Stelle wäre eine Online-Durchsuchung schon nicht zu präventiven Zwecken, also zur Verhinderung der Rechtsgutsverletzung, zulässig. Der Verhinderung einer Rechtsgutsverletzung kommt ein höherer Stellenwert zu als ihrer Aufklärung. In Abwägung ist somit die präventive Verhinderung höher zu werten. Bereits zur Verhinderung einer solchen Straftat kann eine Online-Durchsuchung nicht gerechtfertigt werden, dann ist dies auch denklogisch nicht zu ihrer Aufklärung denkbar. Aus diesem Grund kann erst recht nicht die Durchsetzung des Strafanspruchs wegen der Verletzung eines solchen Rechtsguts eine Online-Durchsuchung rechtfertigen. Eine Qualifikation des Diebstahls kann somit keinen heimlichen Eingriff in das IT-Grundrecht rechtfertigen und ist als nicht verfassungsmäßig einzustufen.

(6) Raub und räuberische Erpressung

Weiterhin finden sich der schwere Raub und der Raub mit Todesfolge im Straftatenkatalog des § 100b Abs. 2 Nr. 1 StPO wieder. Diese beiden Delikte sind aufgrund ihres Strafrahmens zunächst als erheblich einzustufen. Zu dem

359 *Siebert*, JZ 2009, 653, 655; *Popp*, ZIS 2011, 193, 202.

360 *Schmitz*, in: MüKO, § 242, Rn. 4.

361 *Roggan*, StV 2017, 821, 827; *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 85; *Deutscher Anwaltsverein durch den Ausschuss Strafrecht*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 14; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 13.

Schutzgut des Eigentums tritt im Rahmen des Raubes noch die persönliche Freiheit in Form der freien Willensbetätigung und -entschließung hinzu.[362] Wie bereits zuvor dargestellt, reicht das Eigentum als alleiniges Schutzgut für die Rechtfertigung eines heimlichen Eingriffs in das IT-Grundrecht nicht aus. Nun tritt beim Raub aber die Willensbetätigung und -entschließung als weiteres Rechtsgut hinzu. Aus diesem Grund ist das verwirklichte Unrecht als höher einzustufen. Ob das Unrecht an dieser Stelle für eine besonders schwere Straftat ausreicht, ist noch von der Einschätzungsprärogative des Gesetzgebers mitumfasst und damit als für mit der Verfassung vereinbar anzusehen.

Weiterhin werden die räuberische Erpressung und der besonders schwere Fall einer Erpressung im Straftatenkatalog genannt. Die Strafe der räuberischen Erpressung entspricht der des Raubes, dessen Strafrahmen sich nicht unter einem Jahr bewegt. Warum der Raub in seiner Gestalt des Grunddeliktes nicht mit aufgenommen wurde, die räuberische Erpressung aber ihren Eingang in den Straftatenkatalog gefunden hat, ist unklar, stellt aber letztlich eine vertretbare Wertung des Gesetzgebers dar. Ferner ist an dieser Stelle neben dem Rechtsgut Vermögen die Freiheit zur Willensbetätigung und -entschließung geschützt.[363] Aus diesem Grund gilt das zuvor Gesagte zum schweren Raub und Raub mit Todesfolge und die Aufnahme dieser Straftaten in den Straftatenkatalog ist als verfassungsgemäß anzusehen.

(7) Gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei

Ebenfalls kritisch zu sehen ist die Aufnahme der gewerbsmäßigen Hehlerei, der Bandenhehlerei und der gewerbsmäßigen Bandenhehlerei in den Straftatenkatalog. Hier bewegt sich der Strafrahmen in dem Bereich der anderen zuvor besprochenen Straftaten. Allerdings ist bei diesen Straftaten das geschützte Rechtsgut das Vermögen.[364] Das Rechtsgut Vermögen reicht, ähnlich wie das Rechtsgut Eigentum, als einziges Rechtsgut nicht aus, um einen heimlichen Eingriff in das IT-Grundrecht zu rechtfertigen. Der entstandene Schaden ist hier ebenfalls rein finanzieller Natur und ist somit letztlich nicht mit der Funktionsfähigkeit der Strafrechtpflege aufzuwiegen. Die Online-Durchsuchung wäre zur Abwendung einer Gefahr für das besagte Rechtsgut nicht mit der Verfassung vereinbar. Damit ist die Aufnahme dieser

362 BGH 18.04.2002 – 3 StR 52/02, Rn. 16 = NJW 2002, 2043.
363 BGH 20.04.1995 – 4 StR 27/95, BGHSt 41, 123, 125 = NJW 1995, 2799.
364 BGH 29.11.1977 – 1 StR 582/77 = NJW 1978, 710.

Straftaten in den Straftatenkatalog des § 100b Abs. 2 StPO mangels Verhältnismäßigkeit nicht mit der Verfassung vereinbar.[365]

(8) Besonders schwerer Fall der Geldwäsche, Verschleierung unrechtmäßig erlangter Vermögenswerte

Zudem hat der besonders schwere Fall der Geldwäsche und der Verschleierung unrechtmäßig erlangter Vermögenswerte Eingang in den Straftatenkatalog gefunden und ermöglicht eine Online-Durchsuchung. Hier handelt es sich lediglich um ein Vergehen. Geschützt wird die inländische Rechtspflege in ihrer Aufgabe, Wirkungen einer Vortat zu beseitigen,[366] und zusätzlich die durch die Vortat geschützten Rechtsgüter.[367] Auch hierbei handelt es sich nicht um überragend wichtige Rechtsgüter, die eine Online-Durchsuchung im präventiven Bereich rechtfertigen könnten. Zwar ist die inländische Rechtspflege ein Rechtsgut der Allgemeinheit und ihre Verletzung kann in Ausnahmefällen und bei einem erheblichen Ausmaß den Bestand des Staates berühren, allerdings wird sie bei dem Straftatbestand der Geldwäsche und der Verschleierung erlangter Vermögenswerte lediglich in ihrer Aufgabe, die Wirkung von Vortaten zu beseitigen, geschützt. Die Nichtwahrnehmung dieser Aufgabe im Einzelfall ist nicht in der Lage, die Existenz des Staates in Frage zu stellen. Somit kann auch der besonders schwere Fall der Geldwäsche und die Verschleierung unrechtmäßig erlangter Vermögenswerte eine Online-Durchsuchung nicht rechtfertigen.[368]

(9) Computerbetrug

Ebenfalls mit der Erweiterung des Straftatenkatalogs ist in § 100d Abs. 2 Nr. 1 lit. n StPO der Computerbetrug gem. § 263a Abs. 2 in Verbindung mit § 263 Abs. 5 StGB in den Straftatenkatalog hinzugekommen. Hiernach macht sich die Person strafbar, die einen Computerbetrug als Mitglied einer Bande gewerbsmäßig begeht. Dabei ist das Rechtsgut des § 263a StGB das Vermögen.[369] Auch zum Schutz dieses Rechtsgutes könnte schon keine präventive

365 *Deutscher Anwaltsverein durch den Ausschuss Strafrecht*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 14; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 13; *Großmann*, GA 2018, 439, 451.

366 OLG Karlsruhe 20.01.2005 – 3 Ws 108/04 = NJW 2005, 767.

367 BGH 06.06.2018 – 2 ARS 163/18, 2 AR 106/18 = NJW 2018, 2742.

368 *Großmann*, GA 2018, 439, 451; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 13.

369 *Hefendehl/Noll*, in: MüKO § 263a Rn. 1.

Online-Durchsuchung stattfinden, sodass auch hier eine repressive Online-Durchsuchung nicht gerechtfertigt werden kann.

(10) Besonders schwerer Fall der Bestechlichkeit

Gem. § 100b Abs 2 Nr. 1 lit. o StPO hat der besonders schwere Fall der Bestechlichkeit und der Bestechung Eingang in den Straftatenkatalog gefunden. Die §§ 331 ff. StGB schützen die Lauterkeit des öffentlichen Dienstes[370] sowie die Unbefangenheit der Amtsträger*innen und damit auch die sachliche Richtigkeit von Entscheidungen.[371] Des Weiteren wird vertreten, dass die Funktionsfähigkeit des Staatsapparates geschützt werden soll.[372] Unabhängig davon, welcher konkreten Ansicht über die Rechtsgüter der §§ 331 ff. StGB gefolgt wird, ist hier in jedem Fall ein Rechtsgut der Allgemeinheit betroffen, welches in Ausnahmefällen dazu geeignet sein kann, den Bestand des Staates zu berühren. Nur im Rahmen eines solchen Ausnahmefalles ist die Rechtfertigung einer repressiven Online-Durchsuchung unter Einhaltung weiterer Verhältnismäßigkeitsgesichtspunkte denkbar. Dann darf eine Online-Durchsuchung durchgeführt werden. Diese Straftat kann im Straftatenkatalog des § 100b StPO verbleiben.

(11) Straftatbestände aus dem Asyl- und Aufenthaltsgesetz

Ebenfalls als problematisch angesehen werden die Straftaten aus dem Asylgesetz (Nr. 2) und dem Aufenthaltsgesetz (Nr. 3). Die Aufnahme der hier genannten Delikte müsse zu einer Verfassungswidrigkeit führen.[373] Dem ist insoweit zuzustimmen, soweit nicht die Rechtsgüter Leib und Leben betroffen sind. Schutzgut der Straftaten aus dem Asylgesetz ist die Gesetzmäßigkeit der Verwaltung.[374] Die Durchsetzungsfähigkeit von Verwaltungsentscheidungen kann letztlich kein so hohes Schutzgut darstellen, dass ein so immenser Eingriff wie die Online-Durchsuchung gerechtfertigt werden kann. Schutzgut des Aufenthaltsgesetzes ist zum einen zwar die Durchsetzung von verwaltungsrechtlichen Entscheidungen, zum anderen sind es aber auch die

370 *Korte*, in: MüKO, § 331, Rn. 4; *Heintschel-Heinegg*, in: BeckOK StGB, § 331, Rn. 4.

371 *Korte*, in: MüKO, § 331, Rn. 4; *Heine/Eisele*, in: Schönke/Schröder, § 331, Rn. 7; *Heintschel-Heinegg*, in: BeckOK StGB, § 331, Rn. 4.

372 *Heine/Eisele*, in: Schönke/Schröder, § 331, Rn. 7.

373 *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 13; *Deutscher Anwaltsverein durch den Ausschuss Strafrecht*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 14.

374 *Schmidt-Sommerfeld*, in: MüKO, § 84 AsylG, Rn. 1.

Individualrechtsgüter wie Leib und Leben von Ausländer*innen.[375] Letzteres stellt ein überragend wichtiges Rechtsgut dar. Hier wäre auch eine präventive Online-Durchsuchung denkbar. Die Durchsetzungsfähigkeit von Verwaltungsentscheidungen stellt hingegen kein Rechtsgut dar, welches den Bestand des Staates berührt. Damit darf bei einem Verdacht der in § 100b Abs. 2 Nr. 2 StPO genannten Straftaten keine Online-Durchsuchung durchgeführt werden. Anderes muss hingegen bei Nr. 3 gelten, hier ist bei einer Straftat nach § 97 AufenthG eine Online-Durchsuchung möglich, da auch das Rechtsgut Leben geschützt wird.

(12) Straftatbestände aus dem Betäubungsmittelgesetz

Daneben sind die Straftaten aus dem Betäubungsmittelgesetz problematisch. Rechtsgut der Betäubungsmittelstrafbarkeit ist die Gesundheit der Bevölkerung und des Einzelnen sowie das Ziel, Jugendliche vor der Abhängigkeit zu bewahren.[376] Das Rechtsgut der Gesundheit der Bevölkerung und des Einzelnen ist tendenziell als hohes Rechtsgut einzustufen. Jedoch stellt es kein überragend wichtiges Rechtsgut dar. Die Gesundheit der Bevölkerung wird hier nur mittelbar gewährleistet. Aus diesem Grund ist eine Online-Durchsuchung, die der Aufklärung einer Straftat dient, die in § 100b Abs. 2 Nr. 5 StPO genannt wird, als verfassungswidrig anzusehen.[377]

(13) Straftatbestände aus dem Gesetz über die Kontrolle von Kriegswaffen

Gem. § 100b Abs. 2 Nr. 6 lit. a, b StPO ist zur Verfolgung von Straftaten aus dem Gesetz über die Kontrolle von Kriegswaffen eine Online-Durchsuchung vorgesehen. Ziel des Gesetzes ist die Verhinderung der Beteiligung von Deutschen an der Errichtung und Herstellung von Atomwaffen.[378] Der Schutzzweck der Vorschrift ergibt sich aus dem Verfassungsauftrag aus Art. 26 Abs. 2 GG. Das KrWaffG dient damit in erster Linie der Friedenssicherung und Kriegsverhinderung.[379] Außerdem dient das Kriegswaffenkontrollgesetz dem Schutz der inneren Sicherheit.[380] Diese Rechtsgüter sind solche der Allgemeinheit und eine Verletzung dieser Rechtsgüter kann den Bestand des Staates berühren. Aus diesem Grund ist es denkbar, dass die

375 *Gericke*, in: MüKO, § 97 AufenthG, Rn. 2.
376 BVerfG 09.03.1994 – 2 BvL 43/92, BVerfGE 90, 145, 174 = NJW 1994, 1577.
377 A.A.: *Großmann*, GA 2018, 439, 451.
378 BT-Drucks., 11/4609, 6, 7.
379 *Heinrich*, in: MüKO, Vorbemerkung zu § 1 KrWaffG, Rn. 3.
380 BT-Drucks., 8/1614, S. 1.

Aufklärung solcher Straftaten eine Online-Durchsuchung rechtfertigen können. Diese Straftaten können im Katalog des § 100b Abs. 2 StPO verbleiben.

(14) Straftatbestände aus dem Waffengesetz

Ebenfalls zu berücksichtigen sind die Straftaten aus dem Waffengesetz. Das Waffengesetz hat sicherheitsrechtliche Interessen zum Gegenstand.[381] Dieses Rechtsgut reicht zur Rechtfertigung eines intensiven Eingriffs wie dem der Online-Durchsuchung nicht aus. Die durchaus erhebliche Gefahr, die von Waffen grundsätzlich ausgeht, namentlich die Verletzung von Leib und Leben von Menschen, ist durch andere Straftatbestände ausreichend geschützt, sodass es auf einen mittelbaren Gesundheitsschutz nicht ankommen kann. Bestraft wird durch das Waffengesetz das verwaltungsrechtliche Zuwiderhandeln. Dies genügt zur Rechtfertigung nicht, sodass auch die Nr. 7 als verfassungswidrig anzusehen ist.

bb) Weitere Straftaten

Alle weiteren Straftaten des Straftatenkatalogs haben eindeutig ein überragend wichtiges Rechtsgut zum Gegenstand, sodass auch eine präventive Online-Durchsuchung gerechtfertigt wäre. Aus diesem Grund können sie grundsätzlich im Straftatenkatalog verbleiben. Allerdings müssen zur konkreten Durchführung einer Online-Durchsuchung weitere Verhältnismäßigkeitsgesichtspunkte berücksichtigt werden.

c) Zwischenergebnis

Damit ist der Straftatenkatalog des § 100 Abs. 2 StPO zumindest in Bezug auf die Online-Durchsuchung teilweise nicht mit der Verfassung vereinbar. Zu berücksichtigen ist, dass das Bundesverfassungsgericht die Online-Durchsuchung nicht mit der akustischen Wohnraumüberwachung auf eine Stufe gestellt hat, sondern lediglich hervorhebt, dass eine Vergleichbarkeit der beiden Ermittlungsmaßnahmen besteht,[382] wobei dies bezweifelt werden darf. Eine einfache Übertragung auf die Rechtsgüter des Strafrechts kann allerdings nicht erfolgen. Der überwiegenden Meinung, dass der Katalog der Anlasstaten zu weitreichend ist,[383] kann zugestimmt werden. Eine Übertra-

381 *Heinrich*, in: MüKO, § 1 WaffG, Rn. 2.

382 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 269, 274, 307, 312, 329 = NJW 2016, 1781.

383 *Singelnstein*, verfassungsblog 2017, Hacken zur Strafverfolgung? Gefahren und Grenzen der strafprozessualen Online-Durchsuchung; online abzurufen über

gung des Straftatenkatalogs von der akustischen Wohnraumüberwachung auf die Online-Durchsuchung, so wie es der Gesetzgeber getan hat und wie es *Henzler* als denklogisch betrachtet,[384] kann nicht überzeugen. Es ist bereits fraglich, ob die reine Feststellung der generellen Vergleichbarkeit dazu führt, dass der gesamte Straftatenkatalog sich von der akustischen Wohnraumüberwachung auf die Online-Durchsuchung übertragen lässt. Warum sollten sich bei unterschiedlichen Ermächtigungsgrundlagen, die unterschiedliche Beweise hervorbringen und im Einzelfall eine unterschiedliche Effektivität aufweisen, nicht auch unterschiedliche Wertungen für einzelne Straftaten ergeben? Wenn auch bei der akustischen Wohnraumüberwachung eine besonders schwere Straftat zur Rechtfertigung gefordert wird, sollte darüber nachgedacht werden, ob es auch hier einer Anpassung bedarf. Aufgrund einer pauschalen Übertragung kann dies aber nicht geschehen. Im Übrigen muss berücksichtigt werden, dass mit der Online-Durchsuchung eine gewichtigere Menge an Daten erlangt werden kann als bei der akustischen Wohnraumüberwachung, sodass der Eingriff intensiver ist und andere Voraussetzungen an die Rechtfertigung zu stellen sind. Allein die Tatsache, dass die Online-Durchsuchung in das IT-Grundrecht eingreift und nicht, wie die akustische Wohnraumüberwachung, in Art. 13 GG, zeigt, dass die Vergleichbarkeit und eine Übertragungsmöglichkeit nur an der Oberfläche kratzt und eine zu pauschale Lösung darstellt.

Darüber zeigen die neusten Erweiterungen des Straftatenkatalog aus dem Jahr 2021, wie das Hinzufügen von § 127 StGB und dem Computerbetrug gem. § 263a StGB, dass der Gesetzgeber die Online-Durchsuchung insbesondere von Praktikabilitätsgesichtspunkten abhängig macht. Dies ist zwar grundsätzlich verständlich, bei einem solchen erheblichen Grundrechteingriff wie der Online-Durchsuchung kann dies aber nicht der Leitgedanke sein. Bereits seit Inkrafttreten der Norm 2017 ist es zu erheblichen Ergänzungen gekommen, ohne das auch im Rahmen des Grundrechtschutzes nachjustiert wurde.

---

https://verfassungsblog.de/hacken-zur-strafverfolgung-gefahren-und-grenzen-der-strafprozessualen-online-durchsuchung/ (zugegriffen am 12.11.2020); *Blechschmitt*, StraFo 2017, 361, 364; *Singelnstein/Derin*, NJW 2017, 2646, 2647; *Freiling/Safferling/Rückert*, JR 2018, 9, 21; *Gercke*, in: Heidelberger Kommentar, § 100b, Rn. 7; *Hauck*, in: Löwe-Rosenberg, § 100a, Rn. 86.

[384] *Vizepräsident des Bundeskriminalamts Henzler*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 2; *Huber*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 3, 4; nicht zuletzt argumentiert so auch der Gesetzgeber in: BT-Drucks., 18/12785, S. 55; *Sinn*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 10, 11.

Damit kann eine verfassungsgemäße Online-Durchsuchung nur bei dem Verdacht einer Straftat gem. § 100 Abs. 2 StPO

1. aus dem StGB:

a) nach den §§ 81, 82, §§ 94, 95 Abs. 3 und § 96 Abs. 1, jeweils auch in Verbindung mit § 97b, sowie nach den §§ 97a, 98 Abs. 1 S. 2, § 99 Abs. 2 und den §§ 100, 100a Abs. 4

b) entfällt

c) nach § 129a Abs. 4 S. 1 1. Alt, auch in Verbindung mit § 129b Abs. 1

d) entfällt

e) in den Fällen des § 176a Abs. 2 Nr. 2 oder Abs. 3

f) in den Fällen des § 184b Abs. 2

g) nach den §§ 211, 212

h) in den Fällen der §§ 234, 234a Abs. 1, 2, der §§ 239a, 239b, nach § 232a Abs. 3, 4, § 232b Abs. 3 oder 4 i. V. m. § 232a Abs. 4 oder 5 2. Hs. und nach § 233a Abs. 3 oder 4 2. Hs. 1

i) *entfällt*

j) nach § 250 Abs. 1 oder Abs. 2, 251

k) nach § 255, 253 unter den in § 253 Abs. 4 S. 2 genannten Voraussetzungen

l) *entfällt*

m) *entfällt*

n) *entfällt*

o) nach § 335 Abs. 1

2. aus dem Asylgesetz: entfällt

3. aus dem Aufenthaltsgesetz:

a) *entfällt*

b) nach § 97

4. aus dem Außenwirtschaftgesetz

5. *entfällt*

6. aus dem Gesetz über Kriegswaffen

a) eine Straftat nach § 19 Abs. 2oder § 20 aAbs. 1 jeweils auch in Verbindung mit § 21

b) nach § 22a Abs. 1 i. V. m. Abs. 2

7. aus dem Grundstoffüberwachungsgesetz

8. aus dem Neue-psychokatove-Stoffegesetz

9. aus dem Völkerstrafgesetzbuch:

a) nach § 6

b) nach § 7

c) nach den §§ 8 bis 12

d) nach § 13

10. *entfällt*

erfolgen. Eine Online-Durchsuchung aufgrund eines Verdachts einer anderen Straftat darf nicht durchgeführt werden.

5. Schwere der Tat auch im Einzelfall

Eine weitere Einschränkung kann diese korrigierte Aufzählung von Straftaten in § 100b Abs. 2 StPO dadurch erfahren, dass „die Tat auch *im Einzelfall besonders schwer*" wiegen muss (§ 100b Abs. 1 Nr. 2 StPO). Dies stellt eine Ausprägung des Verhältnismäßigkeitsgrundsatzes dar.[385] Weitere Ausführungen finden sich in der Gesetzesbegründung allerdings nicht.

Teilweise wird davon ausgegangen, dass dieser Ausdruck zu unbestimmt sei und es aus diesem Grund der Festlegung eines weiteren Tatbestandsmerkmals zur Bestimmung bedürfe. Dies könne die im Einzelfall zu erwartende Strafe sein.[386] Die Schwere im Einzelfall könne außerdem nach verschiedenen Kriterien wie der Art und Weise der Tatausführung, der Beteiligung weiterer Beschuldigter, der Verzahnung mit anderen Katalogtaten und den Folgen der Tat bestimmt werden.[387] Dabei wird im Umgang mit diesem Ausdruck der *Schwere auch im Einzelfall* auf das Kriterium des § 112 Abs. 2 Nr. 2 StPO verwiesen.[388] Hierbei geht es um die Frage nach der Fluchtgefahr der Betroffenen. Um dem Verhältnismäßigkeitsgrundsatz zu entsprechen, sollten mehrere Kriterien zu Rate gezogen werden, die ein möglichst großes Feld im Einzelfall abdecken. Berücksichtigt werden muss jedoch, dass die Online-Durchsuchung als Ermittlungsmaßnahme zumeist zu Beginn des Ermittlungsverfahrens durchgeführt wird und somit einige Kriterien zum Zeitpunkt der Anordnung einfacher zu prüfen sein werden als andere. Gerade die zu erwartende Strafe im Einzelfall wird wohl, wenn es um eine konkrete Vorhersage geht, von den Erkenntnissen der Online-Durchsuchung abhängen. Dennoch sollten auch diese Erwägungen im Rahmen der Beurteilung der Schwere im Einzelfall eine Rolle spielen – wie auch die anderen zuvor ge-

385 BT-Drucks., 18/12785, S. 55.

386 *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 80; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 14.

387 *Schmitt*, in: Meyer-Goßner/Schmitt, § 100b, Rn. 5.

388 *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 80; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 14.

nannten Kriterien. Dies insbesondere deswegen, weil sie zu einem frühen Zeitpunkt der Ermittlungsarbeit bereits bestimmbar sind. Aus diesem Grund sind im Sinne der Verhältnismäßigkeit zur Bestimmung der Schwere der Tat im Einzelfall folgende Kriterien zu berücksichtigen: Soweit möglich die im Einzelfall zu erwartende Strafe, die Art und Weise der Tatausführung, die Beteiligung anderer Personen, die Verzahnung mit anderen Katalogtaten und die Folgen der Tat. Dabei ist die Aufzählung der Kriterien nicht abschließend.

Wie oben bereits dargestellt, kann die strafprozessuale Online-Durchsuchung nur durch die Funktionsfähigkeit der Strafrechtspflege gerechtfertigt werden, was hohe Anforderungen an die Verhältnismäßigkeit stellt und bei jedem Schritt der Online-Durchsuchung zu berücksichtigen ist. Aus diesem Grund sind auch die genannten Kriterien im Einzelfall an diesen Grundsatz anzupassen und können, nach dem jeweiligen Stand der Ermittlung, eine unterschiedliche Wertung erhalten.

6. Subsidiaritätsklausel

Des Weiteren fordert § 100b Abs. 1 Nr. 3 StPO, dass die Online-Durchsuchung nur Anwendung finden soll, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes Beschuldigter auf andere Weise *wesentlich erschwert oder aussichtslos wäre*.

Aussichtslosigkeit ist gegeben, wenn andere Ermittlungsmaßnahmen nicht zur Verfügung stehen oder keine Erfolgsaussichten haben.[389] Eine „wesentliche Erschwernis“ ist gegeben, wenn andere Ermittlungsmaßnahmen zeitlich erheblich aufwendiger sind beziehungsweise zu schlechteren Ergebnissen führen.[390] Damit ist die Online-Durchsuchung die ultima ratio des Strafverfahrens,[391] da sie dann greift, wenn andere Ermittlungsmaßnahmen versagen.[392] Beispielsweise müsse im Sinne der Verhältnismäßigkeit vorher geprüft werden, ob eine offene Durchsuchung und Beschlagnahme in Betracht kommt.[393]

389 *Günther*, in: MüKO StPO, § 100c, Rn. 34.
390 *Graf*, in: BeckOK StPO, § 100b, Rn. 16.
391 *Schmitt*, in: Meyer-Goßner/Schmitt, § 100b, Rn. 6.
392 BT-Drucks., 18/12785, S. 55.
393 BT-Drucks., 18/12785, S. 55.

a) Das Verhältnis zur akustischen Wohnraumüberwachung

Schwieriger zu bewerten sein dürfte allerdings das Verhältnis zwischen Online-Durchsuchung und akustischer Wohnraumüberwachung. Geht man allein nach dem Wortlaut der Subsidiaritätsklauseln, so stellt man fest, dass der Gesetzgeber für die akustische Wohnraumüberwachung festgelegt hat, dass die Wohnraumüberwachung gem. § 100c Abs. 1 Nr. 4 StPO nur stattfinden darf, wenn eine Aufklärung „(…) auf andere Weise *unverhältnismäßig erschwert oder aussichtslos* wäre". In der Literatur wird davon ausgegangen, dass der Gesetzgeber mit dieser Subsidiaritätsklausel eine nochmals erhöhte Steigerung zum Ausdruck bringen wollte und damit bewusst eine Rangfolge festgelegt hat, die die akustische Wohnraumüberwachung als letztes Mittel kennzeichnet.[394] Eine solche Festlegung der Rangfolge wird dem Wortlaut der Subsidiaritätsklausel allerdings nicht gerecht, denn die Frage nach der Verhältnismäßigkeit stellt auf die Zweck-Mittel-Relation ab und ist aus diesem Grund ein relativer Begriff.[395] Denn hier soll die Klausel „*unverhältnismäßig erschwert*" einen Ermittlungsaufwand beschreiben, den es benötigt, wenn eine andere, mildere Ermittlungsmaßnahme greift.[396] „*Wesentlich erschwert*" ist eine andere Ermittlungsmaßnahme dann, wenn sie erheblich aufwendiger oder schlechter ist.[397] Bei den beiden Klauseln geht es demnach darum, den Ermittlungsaufwand im konkreten Einzelfall für andere Ermittlungsmaßnahmen zu bestimmen. Bei der Online-Durchsuchung muss der Ermittlungsaufwand für andere Maßnahmen wesentlich erschwert sein, für die akustische Wohnraumüberwachung muss dieser für andere Maßnahmen unverhältnismäßig erschwert sein. Bei der Online-Durchsuchung geht es um die faktische Festlegung der Erheblichkeit des Mehraufwandes, die sich nicht in absoluten Zahlen ausdrücken lässt,[398] bei der akustischen Wohnraumüberwachung geht es hingegen um eine Abwägung zwischen dem Mittel und dem Ziel der Maßnahme.[399] Deswegen liegt es nahe, dass „unverhältnismäßig erschwert" mal eine größere und mal eine kleinere Erschwernis im Verhältnis zu „wesentlich erschwert" darstellt.[400] Denn wie *Blozik* zutreffend darstellt, liegt eine unverhältnismäßige Erschwernis bei einem hohen Ziel später vor als bei einem wesentlichen Erschwernis. Bei einem niedrigen Ziel tritt die

394 *Hegmann*, in: BeckOK StPO, § 100c, Rn. 12; *Blozik*, Subsidiaritätsklauseln im Strafverfahren, S. 151.

395 Vgl.: *Blozik*, Subsidiaritätsklauseln im Strafverfahren, S. 152.

396 *Günther*, in: MüKO StPO, § 100c, Rn. 34.

397 *Graf*, in: BeckOK StPO, § 100b, Rn. 16.

398 *Blozik*, Subsidiaritätsklauseln im Strafverfahren, S. 152.

399 *Blozik*, Subsidiaritätsklauseln im Strafverfahren, S. 152.

400 *Blozik*, Subsidiaritätsklauseln im Strafverfahren, S. 152.

unverhältnismäßige Erschwernis hingegen früher ein.[401] Das Ziel der Ermittlungsmaßnahme der Online-Durchsuchung ist gem. § 100b Abs. 1 Nr. 3 StPO die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes der beschuldigten Person bei besonders schweren Straftaten, die auch im Einzelfall besonders schwer wiegen. Das gleiche Ziel hat auch die akustische Wohnraumüberwachung. Damit haben beide Ermittlungsmaßnahmen das höchste Ziel gemein, welches die StPO für Ermittlungsmaßnahmen kennt. Da beide Ermittlungsmaßnahmen ein gleich hohes Ziel und auch sonst dieselben Eingriffsvoraussetzungen haben, kommt es auf den konkreten Einzelfall an, wann das Mittel – die Ermittlungsmaßnahme der akustische Wohnraumüberwachung – schwerer wiegt als das Ermittlungsmittel Online-Durchsuchung. Denn die abstrakte Schwierigkeit zur Erreichung des Ziels ist mit der Festlegung des gleichen Ermittlungsziels zunächst gleich hoch. Der Ermittlungsaufwand, welcher betrieben werden muss, um dieses Ziel erreichen zu können, ist dann in einem nächsten Schritt im Einzelfall zu prüfen.

Damit kann die Subsidiaritätsklausel „wesentlich erschwert oder aussichtslos" der Online-Durchsuchung nicht abstrakt als höherrangig eingestuft werden als die Klausel „unverhältnismäßig erschwert oder aussichtslos", sondern es muss eine Abwägung im konkreten Einzelfall vorgenommen werden, wobei stets zu berücksichtigen ist, dass die Online-Durchsuchung zumeist die intensivere Maßnahme darstellt und deswegen die akustische Wohnraumüberwachung ihr gegenüber vorrangig anzuwenden ist.[402] Eine Ermittlungsmaßnahme kann demnach nicht allein aufgrund ihrer Subsidiaritätsklausel einem höheren Rang zugeordnet werden. Hierfür ist nicht nur die Intensität im konkreten Fall ausschlaggebend, sondern insbesondere die Zielsetzung der Maßnahme entscheidend.

b) Verfassungskonforme Auslegung der Subsidiaritätsklausel

Unklar ist, warum der Gesetzgeber überhaupt eine solche Unterscheidung innerhalb der Subsidiaritätsklauseln vorgenommen hat, wo doch stets die Vergleichbarkeit beider Maßnahmen sowohl durch den Gesetzgeber als auch durch die Rechtsprechung postuliert wurde.[403] Dem schließt sich die Frage an, ob die Online-Durchsuchung an dieser Stelle noch die Schranke des Art. 13 Abs. 3 GG einhält. Denn wie zuvor bereits dargestellt, greift die Online-Durchsuchung im Einzelfall mittels der passiven Kenntnisnahme von

401 *Blozik*, Subsidiaritätsklauseln im Strafverfahren, S. 152.

402 Vgl. zum Verhältnis akustische Wohnraumüberwachung und Online-Durchsuchung im Rahmen der Subsidiaritätsklauseln auch: *Großmann*, GA 2018, 439, 447 f.

403 BT-Drucks., 18/12785, S. 54, 55; BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 269, 274, 307, 312, 329 = NJW 2016, 1781.

Mikrofonaufnahmen in Art. 13 Abs. 1 GG ein. Dabei handelt es sich um eine strafprozessuale akustische Wohnraumüberwachung, deren Schranken sich aus Art. 13 Abs. 3 GG ergeben. Hier heißt es: „(…), wenn die Erforschung des Sachverhalts auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre". Diese, sich aus der Verfassung ergebende Subsidiaritätsklausel wurde so nicht im Gesetzeswortlaut der strafprozessualen Online-Durchsuchung umgesetzt. Aus diesem Grund ist der Gesetzestext an dieser Stelle verfassungskonform auszulegen. Wird eine Online-Durchsuchung durchgeführt, die in Art. 13 GG eingreift – was zumeist der Fall sein wird –, dann gilt auch hier die Subsidiaritätsklausel „unverhältnismäßig erschwert oder aussichtslos".

Ein Erklärungsversuch für diese unzureichende Schrankenregelung durch den Gesetzgeber könnte sein, dass es sich bei der Subsidiaritätsklausel der Online-Durchsuchung um einen redaktionellen Fehler des Gesetzgebers handelt. Für den redaktionellen Fehler spricht, dass auch in § 20k Abs. 1 S. 3 BKAG a. F. (heute § 49 Abs. 1 S. 3) die Subsidiaritätsklausel „aussichtlos oder wesentlich erschwert" genutzt wurde. Dieselbe Klausel wurde auch für die Wohnraumüberwachung in § 20h Abs. 1 BKAG a. F. (heute: § 46 Abs. 1 BAKG) verwendet. Da, wie zuvor festgestellt, die Vorschrift der StPO aus dem Urteil des Bundesverfassungsgerichts aus dem Jahr 2016 entwickelt wurde, ist es denkbar, dass die nichtbeanstandete Festlegung der Subsidiaritätsklausel übernommen worden ist, ohne zu berücksichtigen, dass sich in der StPO eine vermeintlich strengere Klausel zur akustischen Wohnraumüberwachung findet. Auch der Umstand, dass das Gesetzgebungsverfahren für eine solch tief in Grundrechte eingreifende Ermittlungsmaßnahme relativ schnell stattgefunden hat, unterstützt diese These, da wohl wenig Zeit für eine genaue Aufarbeitung des Gesetzestextes geblieben ist.[404] Allerdings würde ein solcher redaktioneller Fehler nicht zu einer anderen Anwendung der Klausel führen, denn auch der Wortlaut gibt nicht zwingend ein Rangverhältnis vor, sondern fordert, dass immer im konkreten Einzelfall eine Abwägung erfolgen muss.

c) Zwischenergebnis

Somit müssen beide Ermittlungsmaßnahmen mit dem Ultima-ratio-Gedanken angewendet und im Einzelfall im Rahmen einer Prognose durch den*die Richter*in gegeneinander abgewogen werden.[405] Die Online-Durchsuchung ist demnach aufgrund ihrer Subsidiaritätsklausel nicht als rangniedriger einzustufen und stellt nicht immer das mildere Mittel im Vergleich zu einer

404 Vgl. hierzu: 3. Kapitel A. V. 1.

405 Genauer hierzu: *Park*, Durchsuchung und Beschlagnahme, Rn. 838.

akustischen Wohnraumüberwachung dar. Außerdem ist die Subsidiaritätsklausel verfassungskonform auszulegen, da sie den Schranken des Art. 13 Abs. 3 GG sonst nicht gerecht wird. Das Wort „wesentlich" muss durch „unverhältnismäßig" ersetzt werden, was aber im Ergebnis keine Auswirkung auf die Anwendung der Vorschriften hat, da ein Rangverhältnis als solches aus dem Wortlaut der Subsidiaritätsklauseln ohnehin nicht abgeleitet werden kann.

7. Verhältnismäßigkeit

Wie jede staatliche Maßnahme muss auch die Ermittlungsmaßnahme der Online-Durchsuchung, insbesondere aufgrund der Heimlichkeit der Maßnahme, verhältnismäßig sein. Dabei muss die Verhältnismäßigkeit innerhalb des gesamten Zeitrahmens gegeben sein, also ab Erlass des Anordnungsbeschlusses und bis zum Abschluss der Maßnahme.[406] In diesem Zusammenhang finden die allgemeinen Regeln der Verhältnismäßigkeit Anwendung.

Bei der Online-Durchsuchung im Speziellen ist die Verhältnismäßigkeit nicht mehr gegeben, wenn die Möglichkeit des Auffindens von relevanten Daten nicht mehr vorliegt.[407] Um die Angemessenheit der einzelnen Online-Durchsuchung bestimmen zu können, ist es wichtig, das verfolgte Beweisziel festzulegen, welches dann gegen die Schutzinteressen abgewogen werden muss. Zu diesen Schutzinteressen gehören Geheimhaltungs- und Vertraulichkeitsinteressen, die Integrität eines IT-Systems und die Rechtsgüter Dritter. Diesen hohen Schutzinteressen steht allein das staatliche Interesse an der Aufklärung einer besonders schweren Straftat gegenüber.[408] Außerdem sind in die Überlegungen zur Verhältnismäßigkeit die Tatsache der Heimlichkeit der Maßnahme, die konkrete Eingriffsintensität und der erhobene Datenumfang einzubeziehen.[409]

Auf die Verhältnismäßigkeit bei der Erhebung von kernbereichsrelevanten Daten sowie auf den Eingriff in Grundrechte und deren Rechtfertigung wird später in der Bearbeitung einzugehen sein.

II. § 100b Abs. 3 StPO – Betroffene*r einer Maßnahme

Eine Regelung zur Online-Durchsuchung gegen andere Personen findet sich in § 100b Abs. 3 StPO. Zunächst ist die Maßnahme gem. § 100b Abs. 3

406 *Graf*, in: BeckOK StPO, § 100b, Rn. 20.
407 *Graf*, in: BeckOK StPO, § 100b, Rn. 40.
408 *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 96.
409 *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 96.

S. 1 StPO nur gegen die beschuldigte Person zu richten. Dabei muss die betroffene Person selbst in Verdacht stehen, eine der in Abs. 2 genannten Straftaten verwirklicht zu haben.

Denkbar ist bei der Online-Durchsuchung aber nach S. 2, unabhängig von der in S. 3 genannten unvermeidbaren Betroffenheit, auch, dass in das informationstechnische System einer anderen Person eingegriffen wird, wenn die Voraussetzungen der Nrn. 1 und 2 gegeben sind. Hierfür bedarf es zweier Prognosen. Die eine muss ergeben, dass ein Fremdnutzungsverhalten vorliegt, und die zweite muss darlegen, dass die Überwachung des IT-Systems des*der Beschuldigten nicht ausreicht.[410] Um der Verfassung zu genügen, bedarf es eines Erst-Recht-Schlusses aus der Rechtsprechung des Bundesverfassungsgerichts zum alten BKAG, wenn sich die Maßnahme auf Nachrichtenmittler*innen erstreckt.[411] Hier hat das Gericht entschieden, dass in der Anordnung Anhaltspunkte dargelegt werden müssen, die zeigen, dass der*die Nachrichtenmittler*in in die Tatdurchführung eingebunden wurde und eine besondere Tat- oder Gefahrennähe aufweist.[412] Dies bedeutet, dass eine Anordnung der Online-Durchsuchung bei einer nicht beschuldigten Person nach den Voraussetzungen des Abs. 3 S. 2 Nr. 1 und 2 und im Rahmen einer verfassungskonformen Auslegung erfolgen darf. Diese verfassungskonforme Auslegung beinhaltet die Voraussetzungen der Tateingebundenheit und der Tatnähe.[413]

Nach Nr. 3 darf die Online-Durchsuchung auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

III. § 100b Abs. 4 i.V.m. § 100a Abs. 5, 6 StPO – technische Anforderungen

Nach § 100b Abs. 4 StPO sollen die Vorschriften des § 100a Abs. 5, 6 StPO, mit Ausnahme von Abs. 5 S. 1 Nr. 1 StPO, entsprechend angewendet werden. Diese Regelungen stellen eine Ausprägung des Verhältnismäßigkeitsgrundsatzes dar und sind dem § 49 Abs. 2 S. 1 Nrn. 1, 2 und S. 2 BKAG nachempfunden.[414] Hier ist der Wortlaut der Norm entsprechend dem BKAG gefasst worden. Diesen Wortlaut hatte der Eingriff in ein informationstechnisches System bereits in § 20k Abs. 2 und 4 BKAG a.F., worauf auch die

410 *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 114.

411 *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 115.

412 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 311 = NJW 2016, 1781.

413 Vgl.: *Hauck*, in: Löwe-Rosenberg, § 100b, Rn. 115.

414 BT-Drucks., 18/12785, S. 53.

Begründung zum neuen BKAG verweist.[415] Am Ende dieser Kette von Verweisungen in den Gesetzesbegründungen steht die Normierung der Online-Durchsuchung im BKAG aus dem Jahr 2008.[416] Diese muss zur Auslegung und zum Verständnis der StPO-Vorschrift herangezogen werden. Die Normierung aus dem BKAG wurde für mit der Verfassung vereinbar erklärt.[417]

Nach § 100a Abs. 5 S. 1 Nr. 2 StPO dürfen nur Änderungen an dem IT-System vorgenommen werden, wenn diese für die Datenerhebung unerlässlich sind. Dies umfasse nicht nur die Anwender-, sondern auch die Systemdateien, letztere bedarf es zur Funktion des IT-Systems.[418] Bereits im Gesetzgebungsverfahren wurde vom *CCC* gefordert, dass die Infiltrierung des IT-Systems nicht das allgemeine Sicherheitsniveau des Gerätes schwächen dürfe.[419] Eine solche Voraussetzung kann jedoch nicht in die Nr. 2 hineingelesen werden, auch wenn dies rechtspolitisch wünschenswert wäre.

1. Das Tatbestandsmerkmal der technischen Umsetzbarkeit

Außerdem müssen nach § 100a Abs. 5 S. 1 Nr. 3 StPO vorgenommene Veränderungen an dem IT-System bei Beendigung der Maßnahme, „soweit technisch möglich", rückgängig gemacht werden. Hierbei soll die verwendete Überwachungssoftware möglichst vollständig gelöscht und Veränderungen an den Systemdateien sollen rückgängig gemacht werden.[420] Dabei hat diese Rückgängigmachung automatisiert zu erfolgen.[421] Einziger Aspekt bei der Beurteilung ist somit die technische Realisierungsmöglichkeit. Der finanzielle oder zeitliche Aufwand einer solchen Realisierungsmöglichkeit muss daher von Grund auf unberücksichtigt bleiben.[422] Dem ist zuzustimmen, der Wortlaut der Vorschrift geht lediglich von der grundsätzlichen Möglichmachung einer solchen Rückgängigmachung aus. Aufgrund der Eingriffstiefe dürfen zeitliche und finanzielle Aspekte keine Rolle spielen, dies gebietet der Verhältnismäßigkeitsgrundsatz. Aus technischer Sicht ist bereits fraglich, ob eine solche „vollständige" Löschung überhaupt möglich ist.[423] Damit wird deutlich, dass es sich auch hier eher um eine „Placebo-Norm" handelt als um

415 BT-Drucks., 18/11163, S. 118.

416 Dabei handelt es sich um die Bundestagsdrucksache: BT-Drucks., 16/10121.

417 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 303, 306 = NJW 2016, 1781.

418 BT-Drucks., 16/10121, S. 29.

419 *Chaos Computer Club* et al., Stellungnahme zur Bundestagsdrucksache 18/11272, 16; dem sich anschließend: *Hauck*, in: Löwe-Rosenberg, § 100a, Rn. 156.

420 BT-Drucks., 16/10121, S. 29.

421 *Graf*, in: BeckOK StPO, § 100b, Rn. 28.

422 *Gercke*, in: Heidelberger Kommentar, § 100b, Rn. 41.

423 *Freiling/Safferling/Rückert*, JR 2018, 9, 19.

eine vollständig umsetzbare Regelung. Dennoch ist es dem Wortlaut nach zulässig „möglichst" eine Software einzusetzen, der es technisch nicht möglich ist, sich vollständig selbst zu löschen. Dies genügt dem Verhältnismäßigkeitsgrundsatz erst dann, wenn sich bei dem Vorhandensein verschiedener Softwares für jene entschieden wird, die diese Löschung bei Weiterentwicklung der Technik vollständig oder mit den heutigen technischen Gegebenheiten soweit möglich durchführt.

2. Schutz gegen unbefugte Dritte

Nach § 100a Abs. 5 S. 2 StPO sind die eingesetzten Mittel gegen eine unbefugte Nutzung Dritter zu schützen. In diesem Zusammenhang haben die Ermittlungsbehörden Sorge dafür zu tragen, dass die Software nicht durch Dritte zweckentfremdet wird. Dies soll dadurch gewährleistet werden, dass die Software von Unbefugten weder erkannt noch angesprochen werden kann.[424] Damit werden die Ermittlungsbehörden eine Art der Garantenstellung einnehmen müssen und ein Schadensersatzanspruch ist dann „(…) nicht sofort von der Hand zu weisen (…)", wenn es um Schäden geht, die durch einen möglichen Datenverlust entstehen.[425]

3. Schutz der kopierten Daten

§ 100a Abs. 5 S. 3 StPO sieht vor, dass die kopierten Daten „nach dem Stand der Technik" gegen Veränderungen, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen sind. Die Formulierung „nach dem Stand der Technik" bedeutet nach Ansicht des Gesetzgebers, „(…) dass sich das BKA der fortschrittlichsten technischen Verfahren bedienen muss, die nach Auffassung führender Fachleute aus Wissenschaft und Technik auf der Grundlage neuester wissenschaftlicher Erkenntnisse erforderlich sind".[426] Dies gelinge dadurch, dass die einschlägigen Aktivitäten auf den Gebieten von Wissenschaft und Technik umfassend und sorgfältig ausgewertet werden.[427] Diese Formulierung ist durch einen hohen Grad an Unbestimmtheit geprägt und ist abhängig von subjektiven Empfindungen der „Fachleute aus Wissenschaft und Technik". So ist allein, eine Auswahl dieser „Fachleute" zu treffen, ein Akt, der hohes Missbrauchspotenzial aufweist.[428]

---

424 BT-Drucks., 16/10121, S. 29.

425 *Graf*, in: BeckOK StPO, § 100b, Rn. 29.

426 BT-Drucks., 16/10121, S. 29.

427 BT-Drucks., 16/10121, S. 29.

428 Zur Missbrauchsanfälligkeit vergleiche auch: *Hauck*, in: Löwe-Rosenberg, § 100a, Rn. 149.

Es fehlt zudem eine Klarstellung, ob die Software von staatlicher Seite programmiert werden soll und, wenn nicht, wie der Ankauf von Softwares von Unternehmen reguliert werden kann. Daraus resultiert die Frage, ob es einer Zertifizierung von Softwares bedarf, die durch staatliche Stellen angekauft werden.[429] Der Verhältnismäßigkeitsgrundsatz gebietet es, eine irgendwie geartete Regulation der Softwares vorzunehmen.

§ 100a Abs. 6 StPO enthält dann in den Nrn. 1 bis 4 Protokollierungspflichten.

4. Zwischenfazit

Bei den genannten Vorgaben handelt es sich um nachvollziehbare, aber auch naive Voraussetzungen, deren praktische Umsetzbarkeit nicht zuletzt auch wegen ihrer Unbestimmtheit teilweise fraglich erscheint. Denn Formulierungen wie „soweit technisch möglich“ und „möglichst“ lassen doch einen erheblichen Interpretationsspielraum und machen eine Kontrolle der Software schwer. Dennoch bewegen sie sich wohl noch gerade am Rande der Verhältnismäßigkeit. Werden diese Vorgaben an die Spähsoftware nicht eingehalten, führt dies zur Unzulässigkeit der Maßnahme.[430]

IV. § 100e StPO – Verfahren im Vergleich zur akustischen Wohnraumüberwachung

Gem. § 100e Abs. 2 StPO darf die Maßnahme der Online-Durchsuchung auf Antrag der Staatsanwaltschaft durch die in § 74 Abs. 4 GVG genannte Kammer des Landgerichts angeordnet werden. Bei Gefahr in Verzug kann die Anordnung auch durch die*den Vorsitzende*n der Kammer erfolgen. Diese Anordnung muss dann innerhalb von drei Werktagen durch die Kammer bestätigt werden. Geschieht dies nicht, tritt die Anordnung der Maßnahme außer Kraft. Dabei darf die Anordnung auf höchstens einen Monat befristet werden. Danach ist eine Verlängerung um nicht mehr als einen Monat möglich. Wenn die Anordnung auf insgesamt sechs Monate verlängert worden ist, ist eine weitere Verlängerung nur durch das Oberlandesgericht denkbar. Beendet die Staatsanwaltschaft innerhalb der erwähnten drei Werktage die Maßnahme, ist eine Bestätigung durch die Kammer nicht notwendig und die bis zu diesem Zeitpunkt erlangten Erkenntnisse bleiben grundsätzlich verwertbar.[431]

---

429 *Roggan*, StV 2017, 821, 824; *Schmitt*, in: Meyer-Goßner/Schmitt, § 100a, 14k.

430 *Schmitt*, in: Meyer-Goßner/Schmitt, § 100a, 14i.

431 *Graf*, in: BeckOK StPO, § 100e, Rn. 18; *Hauck*, in: Löwe-Rosenberg, § 100e, Rn. 32.

Um bei diesem Vorgehen gegen eine Umgehung des Richtervorbehaltes zu argumentieren, könnte man auf die Rechtsprechung des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung zurückgreifen. Hier wurde argumentiert, dass eine solche Umgehung nicht stattfinde, weil der Erfolg einer Abhörmaßnahme innerhalb von drei Tagen nicht erwartet werden könne.[432]

Eine Übertragung dieser Argumentation ist wohl nicht möglich. Bereits eine einmalige „Spiegelung" der Daten des IT-Geräts kann einen Eingriff von erheblicher Intensität darstellen. Außerdem können 72 Stunden der Überwachung schon genügen, um einen erheblichen Datenbestand zu erheben und eine weitreichende Überwachung zu ermöglichen. Des Weiteren ist festzuhalten, dass eine absolute Höchstdauer der Maßnahme nicht vorgesehen ist, diese muss sich aber jederzeit an der Frage der Verhältnismäßigkeit messen lassen.[433] § 100e Abs. 2 S. 3 StPO wird somit dem Verhältnismäßigkeitsgrundsatz nicht gerecht und ist im mindesten in der Form verfassungskonform auszulegen, dass Erkenntnisse aus einer Online-Durchsuchung, die zunächst nur von dem*der Vorsitzenden angeordnet worden ist und über drei Tage hinweg angedauert hat, nicht verwertet werden dürfen, wenn diese nicht von der Kammer bestätigt wird. Auch hier ist ein Vergleich mit der akustischen Wohnraumüberwachung nicht gewinnbringend. Bereits bei einer kurzen Überwachung und einer einmaligen Spiegelung der Daten mittels der Online-Durchsuchung können erhebliche Datenmengen generiert werden, die weite Teile der Vergangenheit mitumfassen, während bei einer akustischen Wohnraumüberwachung lediglich das gesprochene Wort zum Zeitpunkt der Überwachung aufgezeichnet werden kann.

V. Weitere Verfahrensregelungen

Weiterhin legt § 100eAbs. 3 StPO fest, welche Daten in der Entscheidungsformel der Anordnung anzugeben sind.

Nach § 100e Abs. 4 StPO sind in der Begründung der Anordnung (dies gilt für die Ermittlungsmaßnahmen der §§ 100a – 100c StPO) die Voraussetzungen der jeweiligen Ermittlungsmaßnahme und ihre wesentlichen Abwägungsgesichtspunkte darzulegen. In diesem Zusammenhang muss berücksichtigt werden, dass Nr. 2 bei jeder Verlängerung eine erneute Erfolgsprognose fordert.[434]

---

[432] *Hauck*, in: Löwe-Rosenberg, § 100e, Rn. 32; mit Verweis auf BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279 = NJW 2004, 999.

[433] *Hauck*, in: Löwe-Rosenberg, § 100e, Rn. 36.

[434] *Schmitt*, in: Meyer-Goßner/Schmitt, § 100e, Rn. 8.

Dabei sind die aufgeführten Abwägungsgesichtspunkte nicht abschließend aufgezählt.[435]

§ 100e Abs. 5 StPO befasst sich sodann mit der Beendigung der Ermittlungsmaßnahme. Eine Beendigung soll erfolgen, wenn die Voraussetzungen der Anordnung nicht mehr gegeben sind. Das anordnende Gericht ist über die Ergebnisse der Maßnahme zu unterrichten. Im Falle der Online-Durchsuchung gilt eine solche Unterrichtungspflicht auch während des Verlaufes der Ermittlungsmaßnahme. Wenn die Voraussetzungen der jeweiligen Maßnahme nicht mehr gegeben sind, hat das Gericht den Abbruch der Maßnahme anzuordnen. Dies kann auch durch den*die Vorsitzende*n der Kammer erfolgen. Die Frist beginnt mit der Anordnung des Gerichts und nicht mit dem Beginn der Maßnahmen.[436] An eine Beendigung beziehungsweise einen Abbruch der Maßnahme ist insbesondere zu denken, wenn sie nicht mehr verhältnismäßig ist, also wenn die zu erwartenden Erkenntnisse nicht im Verhältnis zur Schwere des Eingriffs oder der Schuld des*der Beschuldigten stehen.[437]

§ 100e Abs. 6 StPO bestimmt nun, für welche anderen Zwecke die erlangten und verwertbaren personenbezogenen Daten verwendet werden dürfen und unter welchen Maßgaben dies geschehen soll.

Verstöße gegen diese Verfahrensvoraussetzungen können zu Beweisverwertungsverboten führen.[438] Eine solche Unverwertbarkeit muss aber in jedem Einzelfall für sich genommen festgestellt werden.[439]

All diese verfahrensrechtlichen Anforderungen gelten für die Online-Durchsuchung und die akustische Wohnraumüberwachung gleichermaßen. Hier macht der Gesetzgeber also erneut eine Vergleichbarkeit der beiden Maßnahmen aus und es fehlt weiterhin an einer klaren Abgrenzung dieser beiden Maßnahmen voneinander.

C. Zwischenergebnis

Im Ergebnis lässt sich sagen, dass sich der Ursprung des Wortes Online-Durchsuchung aus der Tatsache ergibt, dass sich die Online-Durchsuchung seit jeher an der „klassischen“ Durchsuchung messen lassen musste und zeitweise sogar unter diese subsumiert wurde. Die Darstellung des rechtlichen Rahmens verdeutlicht jedoch, dass sich zwischen diesen beiden Er-

435 *Gercke*, in: Heidelberger Kommentar, § 100e, Rn. 16.
436 *Schmitt*, in: Meyer-Goßner/Schmitt, § 100e, Rn. 8.
437 *Schmitt*, in: Meyer-Goßner/Schmitt, § 100e, Rn. 19.
438 *Hauck*, in: Löwe-Rosenberg, § 100e, 96, 101.
439 *Graf*, in: BeckOK StPO, § 100e, Rn. 44.

mittlungsmaßnahmen nur schwer Parallelen ziehen lassen. Vielmehr handelt es sich bei der Online-Durchsuchung um eine Maßnahme, die verschiedenste Maßnahmen mitverwirklichen und in sich vereinen kann. Dies birgt die Gefahr, dass eine erhebliche Menge an Daten aus verschiedensten Lebensbereichen erhoben werden kann, die dann die Grundlage eines Persönlichkeitsprofils bilden können.

Dies ist zum einen auf eine weite Definition des Begriffs des IT-Systems zurückzuführen. Denn dieser orientiert sich nicht allein an dem verfassungsrechtlichen Begriff aus dem IT-Grundrecht, sondern ist schon aufgrund des Verhältnismäßigkeitsprinzips für das Strafprozessrecht ein System, dass Daten verarbeitet, speichert oder erzeugt.

Zum anderen kommt dem Umgang mit Peripheriegeräten wesentliche Bedeutung zu, da durch sie ein erheblicher Teil an Daten mittels der Online-Durchsuchung generiert werden kann. Dabei ist die passive Erhebung von Daten mittels Peripheriegeräten grundsätzlich möglich, die Erhebung bei einer aktiven Aktivierung der Peripheriegeräte durch die Ermittlungsbehörden ist unzulässig. Lediglich bei einer Aktivierung durch den*die Nutzer*in selbst, dürfen diese Daten wahrgenommen werden. So kann eine Online-Durchsuchung bereits eine klassische Durchsuchung, eine akustische Wohnraumüberwachung, eine (Quellen-)TKÜ oder auch eine Observation in sich vereinen. Hier wird deutlich, wie schnell und einfach bei einer intensiven Nutzung des IT-Geräts durch die betroffene Person die Bildung von Persönlichkeitsprofilen ermöglicht wird. Die Möglichkeiten der Datengewinnung werden dabei nicht auf ein Äquivalent zur klassischen Durchsuchung begrenzt, sondern ergeben sich aus spezielleren Ermittlungsmaßnahmen wie der akustischen Wohnraumüberwachung – mittels der passiven Kenntnisnahme des Mikrofons –, der (Quellen-)TKÜ oder auch der Observation. Lediglich die passive Kenntnisnahme der Kamera innerhalb des Wohnraums der betroffenen Person ist im strafprozessualen Bereich als verfassungswidrig einzustufen.

Mit all diesen gewonnenen Daten ist es dann denkbar, in einem Prozess des Profilings, die Daten in einen Kontext zu setzen und damit Profiling-Daten zu erstellen, die eine Abbildung der Persönlichkeit der betroffenen Person ermöglichen, welche bereits als solche Kernbereichsrelevanz aufweisen kann.

Die Betrachtung der historischen Entwicklung der Online-Durchsuchung zeigt, dass sie seit ihrer Einführung Schwächen in Bezug auf den Schutz des Kernbereichs der privaten Lebensgestaltung aufweist, und bis heute ist unklar, ob der für die Online-Durchsuchung normierte Schutz diesbezüglich ausreicht. Dies herauszufinden, soll Aufgabe der weiteren Ausarbeitung sein.

Denn mit dem Fortschritt der Informationstechnik steigt die Gefahr zur Bildung von Persönlichkeits- und Kommunikationsprofilen. Die Ursache hierfür ist in dem Umfang der Daten zu sehen, die gebündelt erhoben werden können, indem ein IT-Gerät überwacht wird, das den*die Nutzer*in zu jedem Zeitpunkt seines*ihres Lebensalltags begleitet.

4. Kapitel

Kernbereichsschutz bei der Online-Durchsuchung de lege lata

Nachdem in den vorherigen Kapiteln dargelegt wurde, welche Anforderungen das Grundgesetz bzw. das Unionsrecht an die Online-Durchsuchung stellen, wird in diesem Kapitel dargestellt, inwieweit der deutsche Gesetzgeber diesen Anforderungen gerecht geworden ist.

Zunächst gilt es darzustellen, wie der Kernbereichsschutz der privaten Lebensgestaltung bei der strafprozessualen Online-Durchsuchung de lege lata ausgestaltet worden ist. Der Kernbereich der privaten Lebensgestaltung ist in der StPO in § 100d normiert. Dabei ist fraglich, ob sich ausreichende Sicherungen finden, um bereits auf der Erhebungsebene die Menge an Daten in einem Rahmen zu halten, der die Gefahr der Bildung von Persönlichkeitsprofilen verhindert. Die Notwendigkeit von Regelungen, die den Kernbereich privater Lebensgestaltung absichern, ergibt sich aus der zutreffenden ständigen Rechtsprechung des Bundesverfassungsgerichts.[1] Da es sich hier um einen erheblichen Grundrechtseingriff mit Bezug zur Menschenwürde handelt, ist es zwingend notwendig, das Verfahren zum Schutz des Kernbereichs normklar auch einfachgesetzlich zu normieren.

Wie diese Begrenzung nach aktueller Umsetzung des Kernbereichs in § 100d StPO funktioniert, sei zur Verdeutlichung in einem Beispiel zum Umgang mit Daten, die wohlmöglich Kernbereichsrelevanz i. S. d. § 100d StPO aufweisen, dargestellt:

B hat vermutlich mehrere kernbereichsrelevante Fotos von sich auf seinem IT-Gerät, und sein gesamtes Gerät wird über drei Monate hinweg Objekt einer Online-Durchsuchung. Dabei wird eine Datenmenge erhoben, die es ermöglicht, ein Persönlichkeitsprofil – nach der in Kapitel 1 erarbeiteten Definition – des B zu erstellen. Mit der jetzigen Normierung der Online-Durchsuchung gibt es folgende Optionen für die Ermittlungsbehörden, mit der Vermutung zur Kernbereichsrelevanz umzugehen:

1. Zunächst ist an eine Anwendung von § 100d Abs. 1 StPO zudenken. Die Fotos dürften dann nicht erhoben werden und die Online-Durchsuchung wäre

[1] Ständige Rechtsprechung mit weiteren Nachweisen: BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 277 = NJW 2016, 1781.

unzulässig, wenn ausschließlich diese Fotos erhoben werden sollten. Dies ist bei einer Online-Durchsuchung zumeist nicht der Fall. Es wurde auch hier über einen längeren Zeitraum hinweg eine Online-Durchsuchung durchgeführt. Es ist davon auszugehen, dass weitere Daten, über die kernbereichsrelevanten Fotos hinausgehend, erhoben worden sind, die für sich genommen keine Kernbereichsrelevanz aufweisen. Die durchgeführte Online-Durchsuchung wäre nicht mehr vom Anwendungsbereich des § 100d Abs. 1 StPO umfasst.

2. In einer zweiten Option stellt sich nach einer Sichtung und möglicherweise durch eine Entscheidung einer unabhängigen Stelle heraus, dass die Fotos gar nicht kernbereichsrelevant waren, weil sie beispielsweise einen unmittelbaren Straftatbezug aufweisen und damit verwertbar sind. Die Online-Durchsuchung wurde durchgeführt, die Daten dürften in einer Hauptverhandlung verwertet werden, aber die Gefahr der Bildung von Persönlichkeitsprofilen ist dennoch eingetreten.

3. Aber auch eine dritte Option ist denkbar: Die Fotos stellen sich als tatsächlich kernbereichsrelevant heraus, möglicherweise auch hier nach einer Sichtung durch eine unabhängige Stelle, und sind unverwertbar. Sie sind aber für den Nachweis der Tat nicht notwendig und damit ohne Grund erhoben worden.

Nichtsdestotrotz wurde in der gesamten Zeit der Online-Durchsuchung eine solche Menge Daten generiert – bei einer durchschnittlichen Smartphone-Nutzung von 3 bis 4 Stunden am Tag[2], über drei Monate hinweg, wären das ca. 306 Stunden Liveüberwachung erhoben worden, hinzukommen noch die sich bereits auf dem Gerät befindlichen Daten –, die wahrscheinlich ein Persönlichkeitsprofil ermöglicht hätten.

Dieses Beispiel zeigt, dass nach bisheriger Anwendung des § 100d StPO und weiterer Vorschriften zum Kernbereich privater Lebensgestaltung, eine ausreichende Begrenzung der Daten bei der Erhebung der Daten nicht erfolgt und die Gefahr der Bildung von Persönlichkeitsprofilen nicht verhindert wird. Die Problematik einer Rundumüberwachung mit der Bildung von Persönlichkeitsprofilen bleibt unberücksichtigt. Dieses Problem kann nur dann

---

[2] Eine Studie der Ruhr Universiät Bochum: Brailovskaia/Stirnberg/Rozgonjuk/Magraf/Elhai: From low sense of control to problematic smartphone use severity during Covid-19 outbreak: The mediating role of fear of missing out and the moderating role of repetitive negative thinking, abrufbar unter: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0261023 (zugegriffen am 02.08.2022); dieser Zeitraum wird darüberhinaus in mehreren Zeitungsartikeln für das Jahr 2021 genannt. U.a. in: https://www.heise.de/news/Datenanalyse-Deutsche-ueber-drei-Stunden-taeglich-am-Smartphone-6369952.html (zugegriffen am 30.06.2022); https://geek-magazin.com/statistik-bildschirmzeit/ (zugegriffen am 30.06.2022).

gelöst werden, wenn sich der Blick weg vom einzelnen Datum und hin zu der Gesamtbetrachtung aller Daten richtet und dem Kernbereich privater Lebensgestaltung zugeordnet wird.

A. Erhebungsebene

In einem ersten Schritt ist herauszufinden, ob diese zwingenden einfachgesetzlich umzusetzenden Vorschriften, die eine Begrenzung der Daten auf das Nötigste vorsehen, sodass die Gefahr der Bildung von Persönlichkeitsprofilen nicht entsteht, de lege lata in der StPO umgesetzt wurden.

I. § 100d Abs. 1 StPO – Erhebungsebene: keine Erhebung von allein kernbereichsrelevanten Daten

§ 100d Abs. 1 StPO sieht vor, dass eine Online-Durchsuchung nicht erfolgen darf, wenn *allein* Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung erlangt werden. Dies bedeutet im Umkehrschluss, dass, wenn durch die Maßnahme *auch* kernbereichsrelevante Daten erhoben werden, Abs. 1 keine Anwendung mehr findet.[3] § 100d Abs. 1 StPO normiert somit ein Erhebungsverbot[4] in der Form eines Beweisthemenverbots.[5]

Um festzustellen, ob *allein* kernbereichsrelevante Daten erhoben werden, muss eine Prognose der Kernbereichsrelevanz der Daten vorgenommen werden.[6] Eine solche Prognose kann vor allem auf der Art der Kommunikation basieren. So ist die Kernbereichsrelevanz insbesondere dann gegeben, wenn mit der Person, mit der der*die Betroffene kommuniziert, ein Vertrauensverhältnis besteht.[7] *Schmitt* geht davon aus, dass es für eine solche Prognose keine gesonderten vorausgehenden Ermittlungen bedarf.[8]

---

[3] Mit weiteren Nachweisen zu anderen Ansichten in der Literatur: *Hauck*, in: Löwe-Rosenberg, § 100d, Rn. 22.

[4] *Graf*, in: BeckOK StPO, § 100d, Rn. 9; *Schmitt*, in: Meyer-Goßner/Schmitt, § 100d, 5a: *Hauck*, in: Löwe-Rosenberg, § 100d, Rn. 22; *Großmann*, JA 2019, 241, 246; *Großmann*, GA 2018, 439, 442.

[5] *Großmann*, JA 2019, 241, 246.

[6] *Schmitt*, in: Meyer-Goßner/Schmitt, § 100d, 5a; BT-Drucks., 18/12785, S. 56.

[7] *Schmitt*, in: Meyer-Goßner/Schmitt, § 100d, 5a; BT-Drucks., 18/12785, S. 56.

[8] *Schmitt*, in: Meyer-Goßner/Schmitt, § 100d, 5a.

Kritiker*innen gehen davon aus, dass die Anwendung dieser Norm in der Praxis so gut wie nicht vorkommt[9] und diese aus diesem Grund als „Placebo-Regelung“ einzustufen ist.[10]

Dem ist im Hinblick auf die aktuelle Anwendung des Kernbereichsschutzes auf die Online-Durchsuchung zunächst zuzustimmen, denn in aller Regel wird es nicht vorkommen, dass durch eine Maßnahme, die so viele Daten hervorbringen kann wie die Online-Durchsuchung, allein solche Daten erhoben werden, die unter den heutigen Begriff des Kernbereichsschutzes zu subsumieren sind. Eine darüberhinausgehende Begrenzung der Daten auf Erhebungsebene erfolgt nicht.

II. § 100d Abs. 3 S. 1 StPO – Vermeidung der Erhebung von kernbereichsrelevanten Daten

§ 100d Abs. 3 S. 1 StPO bestimmt, dass technisch sicherzustellen ist, dass bei einer Online-Durchsuchung kernbereichsrelevante Daten nach Möglichkeit nicht zu erheben sind. Hier hat der Gesetzgeber versucht, das vom Bundesverfassungsgericht zur Sicherung des Kernbereichs der privaten Lebensgestaltung vorgegebene zweistufige Schutzkonzept umzusetzen.[11] In § 100d Abs. 3 S. 1 StPO ist verankert, dass, soweit möglich, technisch sicherzustellen ist, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Dabei fällt die Formulierung „soweit möglich, technisch sicherzustellen“ direkt ins Auge. Hierbei stellt sich insbesondere die Frage: Kann es technisch umgesetzt werden, dass kernbereichsrelevante Daten gar nicht erst erhoben werden?[12]

1. Durch Live-Überwachung

Für die technische Umsetzbarkeit dieser Vorgabe finden sich in der rechtswissenschaftlichen Literatur verschiedene Ansatzpunkte. Zum einen wäre es denkbar, bei einer „Live-Überwachung“ im Rahmen der Online-Durchsuchung auch zeitgleich eine menschliche Überwachung der Kernbereichsrelevanz durch Ermittlungspersonen durchführen zu lassen. Vergleichbar wäre diese Umsetzung auf Erhebungsebene mit den Vorgaben zum großen Lausch-

---

9 *Deutscher Anwaltsverein durch den Ausschuss Strafrecht*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 15; *Freiling/Safferling/Rückert*, JR 2018, 9, 14.

10 *Deutscher Anwaltsverein durch den Ausschuss Strafrecht*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 15; *Roggan*, StV 2017, 821, 828.

11 BT-Drucks., 18/12785, S. 56.

12 Vgl.: *Eschelbach*, in: SSW StPO, § 100d, Rn. 23.

angriff in § 100d Abs. 4 StPO.[13] Ein solches Vorgehen wäre zwar grundsätzlich denkbar, würde den Kernbereichsschutz aber nur bei einem Teilaspekt der Online-Durchsuchung absichern, denn die Live-Überwachung stellt zwar einen intensiven Eingriff dar, ist aber nur ein Teil der möglichen, zu erhebenden Daten. Außerdem wird es wohl letztlich aufgrund der enormen Datenmenge technisch schwer umsetzbar sein, eine solche „Live"-Überwachung einzusetzen beziehungsweise eine solche durch Ermittlungspersonen überhaupt vorzunehmen.[14] Des Weiteren ist dieser Auslegung des ersten Satzes entgegenzuhalten, dass er eben nicht so gefasst ist wie in Abs. 4, der die Besonderheiten des großen Lauschangriffs im Hinblick auf den Kernbereichsschutz regelt. Hier heißt es in S. 2: „Das Abhören und Aufzeichnen ist unverzüglich zu unterbrechen, wenn sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden." Im Unterschied zur akustischen Wohnraumüberwachung hat der Gesetzgeber bei der Online-Durchsuchung keine Unterbrechung der Überwachung vorgesehen. Dies ist als eine bewusste Entscheidung des Gesetzgebers verstehen, sodass ein solches Vorgehen bei der Online-Durchsuchung nicht angedacht ist.[15] Hierin wird regelmäßig ein nicht hinzunehmender Wertungswiderspruch zur akustischen Wohnraumüberwachung gesehen. Da die akustische Wohnraumüberwachung keine weniger intensive Maßnahme darstelle als die Online-Durchsuchung, sei die Unterbrechung der Maßnahme auf die Online-Durchsuchung zu übertragen.[16]

2. Durch die Verwendung von Suchbegriffen

Denkbar wäre es auch, solche Daten nicht zu erheben, die unter bestimmte Suchbegriffe fallen[17] oder einem bestimmten Dateityp (wie Bilder oder Videos) angehören.[18] Bei diesem Vorgehen deutet sich bereits die Ungeeignet-

---

[13] *Bruns*, in: KK, § 100d, Rn. 9; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 15; *Soiné*, NStZ 2018, 497, 503; *Freiling/Safferling/Rückert*, JR 2018, 9, 13; A.A. aufgrund eines anderen Charakters der Maßnahme: *Krauß*, Stellungnahme zur Ausschussdrucksache 18(6)334, S, 11.

[14] *Bundesbeauftragte für Datenschutz und Informationsfreiheit Voßhoff*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 9; *Großmann*, GA 2018, 439, 449.

[15] *Roggan*, StV 2017, 821, 828; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 15.

[16] *Roggan*, StV 2017, 821, 828; *Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 15; *Deutscher Anwaltsverein durch den Ausschuss Strafrecht*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 16; *Großmann*, GA 2018, 439, 449.

[17] *Bruns*, in: KK, § 100d, Rn. 9.

[18] *Freiling/Safferling/Rückert*, JR 2018, 9, 14.

heit an. So ließe sich eine Spähsoftware leicht durch die betroffene Person manipulieren und es würde letztlich einer effektiven Strafverfolgung gänzlich zuwiderlaufen. Regelmäßig werden die für das Strafverfahren relevanten Daten Bilder oder Videos sein. Auch eine Nichterhebung einer Datei, weil sie beispielsweise den Titel „Tagebuch" trägt, ist wenig sinnvoll und stellt eine nicht zu vertretende Willkür dar. Eine Grenzziehung ist hier kaum möglich. Insgesamt braucht es, um einen effektiven Schutzmechanismus für den Kernbereichsschutz auf Ebene der Erhebung zu ermöglichen, eine Analyse der Daten auf dem IT-System. Dies stellt einen komplexen normativen Abwägungsvorgang dar, den ein Computerprogramm nicht leisten kann.[19]

3. Durch Verbot der Nutzung von Peripheriegeräten

Möglich wäre es auch, eine Nutzung von Peripheriegeräten zum Schutz des Kernbereichs der privaten Lebensgestaltung von vornherein zu unterlassen.[20] Ein solches Vorgehen erscheint denkbar, löst das Problem aber nicht. Kernbereichsrelevante Daten entstammen nur zu geringen Anteilen der Nutzung von Peripheriegeräten. Außerdem hängt diese Forderung rechtlich im luftleeren Raum, denn weder der Wortlaut noch der Sinn und Zweck der Norm geben ein solches Vorgehen vor. Auch eine verfassungskonforme Auslegung in diese Richtung scheint aufgrund der geringen Anwendungsmöglichkeiten und der damit verbundenen geringen Effektivität wenig sinnvoll. Nach *Bruns* kommt es nicht *allein* auf die technische Umsetzbarkeit an, sondern der Wortlaut verlange eine eingeschränkte Kernbereichsprognose. Bereits bekannte Tatsachen, Wahrscheinlichkeiten und der mögliche Umfang eines Eingriffs in das Persönlichkeitsrecht müssen zur Grundlage dieser Prognose gemacht werden.[21]

III. Zwischenergebnis

Im Ergebnis lässt sich somit konstatieren, dass der Gesetzgeber durch die Umsetzung des zweistufigen Schutzkonzepts auf der Erhebungsebene Forderungen an die IT-Wissenschaft stellt, ohne dass aus technischer Sicht eine Sicherung möglich ist. Dies geht eindeutig zulasten des Kernbereichsschutzes. Außerdem zeigt dies, dass der Kernbereichsschutz der privaten Lebensgestaltung *so* für die Online-Durchsuchung nicht tragbar ist. Bereits nach der Entscheidung zum IT-Grundrecht 2008 war sich die Literatur einig, dass es einer Konkretisierung der Voraussetzung der Nichterhebung von kernbe-

19 *Freiling/Safferling/Rückert*, JR 2018, 9, 14.
20 *Bruns*, in: KK, § 100d, Rn. 9.
21 *Bruns*, in: KK, § 100d, Rn. 9.

reichsrelevanten Daten durch Bundes- und Landesgesetzgebung bedürfe, was eine enorme Aufgabe darstelle.[22] Diesen berechtigten Erwartungen ist der Gesetzgeber für die Strafprozessordnung nicht gerecht geworden. Schlussendlich ist ebenfalls zu erkennen, dass, wenn der Kernbereichsschutz von der Erhebungsebene auf die Verwertungsebene verschoben wird, dies eine Verringerung des Schutzniveaus darstellt. Sind Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung einmal erhoben, erhöht sich das Risiko der Weitergabe der Daten und dies geht mit einer Vertiefung des Grundrechtseingriffs einher.[23]

Zwar dürfen, abhängig von den technischen Möglichkeiten, kernbereichsrelevante Daten nicht erhoben werden (vgl. § 100d Abs. 3 S. 1 StPO), allerdings fehlt es an einer Vorgabe, dass eine Online-Durchsuchung abgebrochen wird, wenn kernbereichsrelevante Daten erhoben werden, die nicht mehr nur eine Verknüpfung zum Ermittlungsziel darstellen, und dass, wenn bei einer Live-Überwachung prognostiziert wird, dass sich in einem zeitlichen Zusammenhang kernbereichsrelevante Daten ergeben werden oder solche bereits erhoben werden, die Ermittlungsmaßnahme unterbrochen wird. Es fehlen somit jene Vorschriften zum Schutz des Kernbereichs der privaten Lebensgestaltung, die eine Unterbrechung der Maßnahme vorsehen, wie sie bei einer akustischen Wohnraumüberwachung bestehen. Insoweit können die Regelungen nicht überzeugen, und ohne diese Zusätze ist der Kernbereichsschutz nicht als angemessen anzusehen. Eine verfassungskonforme Auslegung kommt schon deswegen nicht in Betracht, weil der Gesetzgeber der Pflicht unterliegt, Vorschriften, die nötig sind, um den Kernbereich privater Lebensgestaltung zu schützen, explizit zu normieren.[24] Eine Online-Durchsuchung ohne entsprechende Vorkehrungen ist demnach als verfassungswidrig einzustufen.

Darüber hinaus erfolgt keine Begrenzung der Daten auf der Erhebungsebene. So bleiben zum einen der Anknüpfungspunkt der alleinigen Kernbereichsrelevanz, was nach aktueller Rechtsprechung nur bei punktuell kernbereichsrelevanten Daten der Fall ist, oder aber in Abhängigkeit von einer technischen Möglichkeit.

---

[22] *Erd*, KJ 2008, 118, 126; *Hornung*, CR 2008, 299, 304; *Böckenförde*, JZ 2008, 925.

[23] *Wolter*, in: GS Weßlau, 452.

[24] Ständige Rechtsprechung mit weiteren Nachweisen: BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 277 = NJW 2016, 1781.

B. Verwertungsebene

In einem nächsten Schritt ist herauszuarbeiten, inwieweit die Menge der erhobenen Daten eine Begrenzung auf Ebene der Verwertung erfährt.

I. § 100d Abs. 2 StPO – Verfahrensvorschriften

Neben den Vorschriften zur Erhebung von Daten ist darüber hinaus vorgesehen, dass Verfahrensvorschriften bestehen, die sicherstellen sollen, dass erhobene kernbereichsrelevante Daten in ihrer Intensität der Kernbereichsverletzung und ihren Auswirkungen auf die Persönlichkeit und Entfaltung des*der Betroffenen so gering wie möglich bleiben. Dies hat der Gesetzgeber durch die Löschungs- und Protokollierungspflichten in § 100d Abs. 2 StPO klargestellt. Er geht davon aus, dass diese Dokumentation der Löschung der entsprechenden Erkenntnisse in Form eines Löschungsprotokolls zu den Akten genommen wird, um die Beurteilung der Rechtmäßigkeit der Maßnahme durch das Gericht zu ermöglichen.[25] Im Übrigen gelten die Dokumentations- und Löschungspflichten des § 101 Abs. 8 StPO.[26]

Mehr als die unverzügliche Löschung von kernbereichsrelevanten Daten unmittelbar nach ihrer Wahrnehmung ist auf der Verwertungsebene nicht möglich. Die Erstellung eines Löschungsprotokolls ist ebenfalls plausibel und sichert den weiteren Verfahrensgang. Auf die Menge der Daten hat eine Protokollierung der Löschung jedoch keine Auswirkungen.

II. § 100d Abs. 2 S. 1 StPO – Absolutes Verwertungsverbot

Außerdem sieht der Gesetzgeber vor, dass die erhobenen Daten durchzusehen sind und kernbereichsrelevante Daten unverzüglich gelöscht werden und die Weitergabe oder Verwertung absolut ausgeschlossen werden muss. Nach § 100d Abs. 2 S. 1 StPO dürfen in einem nächsten Schritt Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung nicht verwertet werden. Erkenntnisse aus solchen Aufzeichnungen sind unverzüglich zu löschen. Diese Löschung ist dann zu dokumentieren.

Satz 1, der die Unverwertbarkeit normiert, beinhaltet ein Beweisverwertungsverbot für Daten, die den Kernbereich der privaten Lebensgestaltung berühren. Dieses Verwertungsverbot gilt absolut und verbietet jegliche Ver-

[25] BT-Drucks., 18/12785, S. 56.
[26] BT-Drucks., 18/12785, S. 56.

wendung der Daten.[27] Mitumfasst ist dabei auch eine mögliche Fern- und Drittwirkung des Beweises.[28] Auch das Bundesverfassungsgericht geht in seiner ständigen Rechtsprechung davon aus, dass kernbereichsrelevante Informationen weder im Hauptsacheverfahren verwertet werden dürfen noch Anknüpfungspunkt für weitere Ermittlungen darstellen können.[29]

Aus diesem Grund bestehen für kernbereichsrelevante Informationen gem. § 100d Abs. 2 S. 1 StPO ein absolutes Beweisverwertungsverbot.

III. § 100d Abs. 3 S. 2, 3 StPO – Entscheidung durch eine unabhängige Stelle

§ 100d Abs. 3 S. 2 StPO normiert, dass Daten mit Kernbereichsrelevanz nach ihrer Erhebung unverzüglich zu löschen sind oder von der Staatsanwaltschaft dem anordnenden Gericht zur Entscheidung über Verwertbarkeit und Löschung vorzulegen sind. Das Gericht stellt dabei die vom Bundesverfassungsgericht im Urteil zum BKAG[30] aus dem Jahr 2016 geforderte unabhängige Stelle dar.[31] Damit hat die Staatsanwaltschaft zunächst die Kompetenz der Entscheidung über die Kernbereichsrelevanz der Daten. Sollte die Staatsanwaltschaft die Möglichkeit der Kernbereichsrelevanz zwar erkannt, aber eine andere Bewertung vorgenommen haben, so ist dies dem Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen.[32]

1. Bindungswirkung und Gewaltenteilung

Durchaus als problematisch anzusehen ist allerdings der Wortlaut des § 100d Abs. 2 S. 2 StPO. Hier heißt es: „Erkenntnisse, (…), sind unverzüglich zu löschen oder von der Staatsanwaltschaft dem anzuordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen." *Hauck* erkennt in diesem Zusammenhang ein Problem mit dem Grundsatz der Gewaltenteilung. Denn durch diese Wahlmöglichkeit habe die Staatsanwaltschaft als Teil der Exekutive selbst die Wahl, sich der Gewalt

---

[27] *Hauck*, in: Löwe-Rosenberg, § 100d, Rn. 23; *Großmann*, JA 2019, 241, 246; *Bruns*, in: KK, § 100d, Rn. 7; *Schmitt*, in: Meyer-Goßner/Schmitt, § 100d, Rn. 6.

[28] *Eschelbach*, in: Satzger/Schluckebier/Widmaier, StPO Kommentar, § 100d, Rn. 18; *Bruns*, in: KK, § 100d, Rn. 7.

[29] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, 331 = NJW 2004, 999.

[30] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 307 = NJW 2016, 1781.

[31] BT-Drucks., 18/12785, S. 56.

[32] *Bruns*, in: KK, § 100d, 10.

der Judikative auszusetzen. Hier hätte der Gesetzgeber für klarere Verhältnisse sorgen müssen.[33] Dem ist nur insoweit zuzustimmen, als dass die Staatsanwaltschaft eine Wahlmöglichkeit hat, wenn sie die Kernbereichsrelevanz der Daten erkannt hat. Dann erst kann sie diese Daten entweder selbst löschen oder aber, wenn sie von einer Kernbereichsrelevanz nicht ausgeht, die Möglichkeit dieser aber erkannt hat, sie zur Entscheidung dem Gericht vorlegen. Ein Problem der Gewaltenteilung würde lediglich dann bestehen, wenn die Staatsanwaltschaft, als Exekutivgewalt, die Wahl hätte, bei der Erkennung der Möglichkeit der Kernbereichsrelevanz zu entscheiden, ob die Daten trotz der Möglichkeit der Kernbereichsrelevanz verwertet werden. Diese Entscheidung kann durch die Staatsanwaltschaft nicht getroffen werden. Wird die Möglichkeit der Kernbereichsrelevanz erkannt, so muss seitens der Staatsanwaltschaft gehandelt werden. Eine vergleichbare Vorschrift fand sich bisher auch in § 100c Abs. 5 S. 6 StPO a. F. und findet sich nun in § 100d Abs. 4 S. 4 StPO zur akustischen Wohnraumüberwachung. Auch hier hat die Staatsanwaltschaft lediglich im Zweifel über die Fortführung der Maßnahme eine gerichtliche Entscheidung herbeizuführen.

Im deutschen Strafprozessrecht ist dies, trotz der Heimlichkeit der Maßnahme, nicht als unzulässige Beschneidung von Beschuldigtenrechten anzusehen, da die Staatsanwaltschaft gem. § 160 Abs. 2 StPO und dem hieraus resultierenden Ermittlungsgrundsatz zu Gerechtigkeit und Objektivität verpflichtet ist und somit in alle Richtungen ermitteln muss, um dem Gebot des fairen Verfahrens gerecht zu werden.[34] Außerdem ist neben der Löschung eine Dokumentation notwendig, welche aber keinen Hinweis auf den Informationsgehalt der Daten haben darf. Die Dokumentation ist dann zu den Akten zu geben.[35] Damit ist die Staatsanwaltschaft als Teil der Exekutive zu keinem Zeitpunkt einer (nachträglichen) gerichtlichen Kontrolle entzogen. Somit ist dem Gewaltenteilungsprinzip Genüge getan. Sollte die Staatsanwaltschaft wider ihrer Rolle im Ermittlungsverfahren eine Entscheidung über die Kernbereichsrelevanz bewusst nicht herbeiführen, so wie *Hauck* es zu befürchten scheint, hat das Gericht in der Hauptsache weiterhin die Möglichkeit der Feststellung der Unverwertbarkeit der Daten. Der Staatsanwaltschaft wird somit in aller Regel, sähe man sie allein als Partei an, daran gelegen sein, gerichtsfest feststellen zulassen, dass die in Rede stehenden Daten verwertbar sind. So kann sie eine mögliche Anklage schon in einem frühen Stadium absichern, und weitere Ermittlungen wären nicht notwendig.

---

33 *Hauck*, in: Löwe-Rosenberg, § 100d, Rn. 36.

34 *Sackreuther*, in: BeckOK StPO, § 160, Rn. 13.

35 *Eschelbach*, in: Satzger/Schluckebier/Widmaier, StPO Kommentar, § 100d, Rn. 21; *Schmitt*, in: Meyer-Goßner/Schmitt, § 100d, Rn. 11; *Hauck*, in: Löwe-Rosenberg, § 100d, Rn. 35.

2. Umfang der Bindungswirkung

Die Bindungswirkung des § 100d Abs. 3 S. 3 StPO entfaltet sich nur im Ermittlungsverfahren. Das erkennende Gericht und das Rechtsmittelgericht sind von dieser aufgrund ihrer Unabhängigkeit frei. Eine Bindung für das gesamte Verfahren wäre aus diesem Grund nur denkbar, wenn die Verwertbarkeit verneint wurde.[36] Dem Wortlaut muss entnommen werden, dass sowohl eine bejahende als auch eine verneinende Entscheidung des Gerichts über die Verwertbarkeit für das erkennende und das Rechtsmittelgericht bindend ist. *Bruns* sieht hier eine durch den Gesetzgeber neu geschaffene Rechtslage, die dennoch zur Folge habe, dass positive Entscheidungen keine Bindungswirkung entfalten.[37] Eine solche neu geschaffene Rechtslage lässt sich an dieser Stelle nicht erkennen. Bereits in § 100c Abs. 7 S. 2 StPO fand sich das Wort „bindend" wieder und auch hier ging man davon aus, dass lediglich eine ablehnende Entscheidung des Gerichts über die Verwertbarkeit Bindungswirkung entfalten könne.[38] Damit ist der einhelligen Meinung zuzustimmen, dass sich die Bindungswirkung nur auf Entscheidungen bezieht, die eine Verwertbarkeit der Daten verneinen. Dann gilt dies aber auch für das gesamte folgende Verfahren.[39]

C. Zwischenresümee

Zusammenfassend lässt sich sagen, dass versucht worden ist, das zweistufige Schutzkonzept nach Maßgabe des Bundesverfassungsgerichts auch für die repressive Online-Durchsuchung umzusetzen.[40]

Problematisch an diesem Vorgehen ist insbesondere, dass Forderungen an die IT-Wissenschaft gestellt werden, die kaum bis gar nicht umzusetzen sind, was das Schutzniveau, welches ohnehin aufgrund der Verlagerung von der Erhebungs- auf die Verwertungsebene gesunken ist, noch stärker verringert. Damit stellt das zweistufige Schutzkonzept ein unausgegorenes Prinzip dar, welches, um dem Menschenwürdegehalt des Kernbereichsschutzes der privaten Lebensgestaltung gerecht werden zu können, einer Konkretisierung bedarf.

---

36 *Eschelbach*, in: SSW StPO, § 100d, Rn. 26.

37 *Bruns*, in: KK, § 100d, Rn. 16.

38 *Löffelmann*, ZIS 2006, 87, 98; *Graf*, in: BeckOK StPO, § 100d, Rn. 18.

39 Vgl.: *Graf*, in: BeckOK StPO, § 100d, Rn. 18; *Eschelbach*, in: SSW StPO, § 100d, Rn. 26; *Bruns*, in: KK, § 100d, Rn. 16.

40 BT-Drucks., 18/12785, S. 56.

Dabei enthält der Kernbereichsschutz bei der Online-Durchsuchung, wie er vom Bundesverfassungsgericht entwickelt und vom Gesetzgeber in § 100d Abs. 1, 2 und 3 StPO umgesetzt worden ist, an zwei Punkten wesentliche Probleme, die es zu berücksichtigen gilt. Zum einen fehlt es an einer Vorschrift, die die Unterbrechung der Maßnahme vorsieht, und zum anderen braucht es einen neuen Umgang mit der Gefahr der Bildung von Persönlichkeitsprofilen. Der kann nur gelingen, wenn auf der Erhebungsebene eine Beschränkung der Daten erfolgt. Diese ist vom Bundesverfassungsgericht in den Entscheidungen zur Online-Durchsuchung und zum Kernbereichsschutz nicht gefordert worden, sodass der Gesetzgeber, der sich mit mittels des Bundesverfassungsgerichts den verfassungsrechtlich möglichen Rahmen einer Online-Durchsuchung hat abstecken lassen, eine solche auch nicht geschaffen hat.

Diese – nach den in dieser Arbeit dargelegten Gründe unzureichend beschränkten – Erhebungsmöglichkeit eröffnet die Gefahr der Bildung von Persönlichkeitsprofilen und kann so weder in verfassungsrechtlicher noch in europarechtlicher Hinsicht überzeugen. Die Gefahr der Bildung von Persönlichkeitsprofilen steht in Abhängigkeit zu der Menge an Daten, die generiert werden. Die Gefahr verwirklicht sich nicht erst bei der Verwertung der Daten, dies mag bei punktuell kernbereichsrelevanten Daten anders sein, sondern bereits bei ihrer Erhebung. Aus diesem Grund sind zum Schutz des Kernbereichs privater Lebensgestaltung bereits Regelungen zu schaffen, die die Menge der erheblichen Daten begrenzt.

Die derzeit geltenden Regelungen zur Erhebungsebene sind nicht in der Lage, den Kernbereich privater Lebensgestaltung effektiv zu schützen.

5. Kapitel

Fazit: Unzureichende Regelungen zur Begrenzung der Datenmenge

Die Entwicklungen im Bereich des Internets und die neuen Gefahren, die mit der Digitalisierung insbesondere im Zusammenhang mit „Big Data" einhergehen, haben auch erhebliche Auswirkungen auf die Bildung von Persönlichkeitsprofilen. Vielen Menschen ist oftmals nicht bewusst, welche Auswirkungen die Kundgabe ihrer Daten für die Abbildung ihrer Persönlichkeit hat. So hat eine Studie[1] herausgefunden, dass es bereits mit der Auswertung von 65 Facebook-Likes (die Betätigung des „Gefällt mir"-Buttons bei der Social-Media-Plattform „Facebook") mittels eines Algorithmus möglich ist, die selbstbeurteilenden fünf Hauptfaktoren der Persönlichkeit eines Menschen mit der gleichen Präzision vorherzusagen, wie dies Freund*innen gelingt. Bei 125 Likes ist die Vorhersage vergleichbar mit der von Familienangehörigen und bereits 100 Likes reichen aus, um viele Persönlichkeitseigenschaften valide zu erfassen.[2] Hierfür müssen die Likes nur in einen Kontext zueinander gesetzt werden. Dies ist bei einer Online-Durchsuchung ebenfalls denkbar.

Dieses Beispiel zeigt, wie viele Rückschlüsse auf die Persönlichkeit eines Menschen in kürzester Zeit mittels Algorithmen bereits jetzt möglich sind.

Mit diesen neuen Gefahren und Herausforderungen muss sich spätestens mit der Einführung der Online-Durchsuchung in die StPO nun auch die Strafrechtswissenschaft auseinandersetzen. Denn tendenziell ist davon auszugehen, dass zukünftig immer mehr Ermittlungsarbeit im Internet und auf IT-Geräten erfolgen wird. Ein effektiver Grundrechtsschutz muss somit auch bei diesem Übertrag in die digitale Welt gelingen.

---

[1] *Youyou/Kosinski/Stillwell*, Proceedings of the National Academy of Sciences of the United States of America 2015, Computer-based personality judgments are more accurate than those made by humans; online abzurufen über https://www.pnas.org/content/pnas/112/4/1036.full.pdf (zugegriffen am 12.11.2020).

[2] *Youyou/Kosinski/Stillwell*, Proceedings of the National Academy of Sciences of the United States of America 2015, Computer-based personality judgments are more accurate than those made by humans; online abzurufen über https://www.pnas.org/content/pnas/112/4/1036.full.pdf (zugegriffen am 12.11.2020).

Dadurch, dass bei der Online-Durchsuchung eine so erhebliche Menge an Daten aus den verschiedensten Lebensbereichen erhoben werden kann, erhöht sich die Gefahr der Bildung von Persönlichkeitsprofilen im Einzelfall um ein Vielfaches. Diesem Problem ist mit den Grundsätzen zum Schutz des Kernbereichs der privaten Lebensgestaltung entgegenzuwirken.

Nachdem nunmehr im Kapitel zuvor dargestellt wurde welchen Anforderungen der Gesetzgeber beim Schutz des Kernbereichs privater Lebensgestaltung Rechnung getragen hat, geht es in diesem Kapitel darum, wie mit den nicht umgesetzten Anforderungen an die Gefahr der Bildung von Persönlichkeitsprofilen bei der Online-Durchsuchung umgegangen werden muss. Denn nach der aktuellen Anwendung des Rechts findet sich keine befriedigende Beschränkung der Daten auf der Erhebungsebene. Die Erhebung von Daten wird nicht auf das absolut Notwendige beschränkt, sodass die Gefahr der Bildung von Persönlichkeitsprofilen nicht effektiv verhindert wird.

Da die Gefahr der Bildung von Persönlichkeitsprofilen aus der Menge der erhobenen Daten resultiert, wird es in einem nächsten Schritt darum gehen, Voraussetzungen herauszuarbeiten, die verhindern, dass Daten willkürlich und für alle Lebensbereiche offen erhoben werden. Es muss eine Beschränkung der Menge und eine vorherige Festlegung der zu erhebenden Daten erfolgen.

Hierfür wird zunächst kurz auf den Gedanken des additiven Grundrechtseingriffs einzugehen sein, den das Bundesverfassungsgericht selbst im Zusammenhang mit der Online-Durchsuchung anführt. Dann werden eigene Ansätze entwickelt, dabei ist über eine verfassungskonforme beziehungsweise europarechtskonforme Auslegung sowie über eine neue eigenständige Verfahrensvorschrift nachzudenken.

A. Additiver Grundrechtseingriff

Bei der Konstruktion des additiven Grundrechtseingriffs geht es ebenfalls darum, die Menge der Daten, die erhoben werden dürfen, zu begrenzen. Auch hier erkennt das Bundesverfassungsgericht aufgrund der Menge der erhobenen Daten ein Gefährdungspotenzial, wenn es feststellt:

> „Beim Einsatz moderner, insbesondere dem Betroffenen verborgener Ermittlungsmethoden müssen die Sicherheitsbehörden mit Rücksicht auf das dem ‚additiven' Grundrechtseingriff innewohnenden Gefährdungspotenzial koordinierend darauf Bedacht nehmen, dass das Ausmaß der Überwachung insgesamt beschränkt bleibt."[3]

[3] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 280 = NJW 2016, 1781.

Grundsätzlich liegt somit diesem Ansatz der Gedanke einer Beschränkung der Menge der Daten, die erhoben werden dürfen, zugrunde. Bei dem additiven Grundrechtseingriff geht es um eine Situation, bei der verschiedene einzelne, für sich betrachtet geringfügige Eingriffe in geschützte Bereiche in ihrer Gesamtwirkung zu einer schwerwiegenden Beeinträchtigung führen, sodass das Maß der rechtsstaatlich hinnehmbaren Eingriffsintensität überschritten wird.[4]

Dies ist aber keine Frage des Schutzes des Kernbereichs privater Lebensgestaltung, sondern der grundsätzlichen durch die Maßnahme immer intensiver werdenden Grundrechtseingriffe und deren Verhältnismäßigkeit.[5] Im Übrigen geht es bei dem Gedanken des additiven Grundrechtseingriffs nach Ansicht des Bundesverfassungsgerichts[6] wohl darum, dass mehrere Überwachungsmaßnahmen miteinander kumulieren. Bei der Online-Durchsuchung ist hingegen bereits diese eine Ermittlungsmaßnahme in der Lage, eine solche Menge an Daten zu erheben, dass mit ihr die Gefahr der Bildung eines Persönlichkeitsprofils einhergeht.[7] Dabei darf nicht unberücksichtigt bleiben, dass durch die verschiedenen Ermittlungsmaßnahmen, die mitverwirklicht werden können, in verschiedenste Grundrechte eingegriffen wird, was auch Auswirkungen auf die Verhältnismäßigkeit der Maßnahme im konkreten Einzelfall hat.

Der Gedanke des additiven Grundrechtseingriffs kann Teil einer Prognose in Bezug auf den Schutz des Kernbereichs privater Lebensgestaltung werden, denn Grundrechten wohnt ein Teil der Menschenwürde inne, welcher bei Ermittlungsmaßnahmen in Form eines Eingriffs in den Kernbereich privater Lebensgestaltung berührt werden kann. Umso intensiver und zahlreicher in Grundrechte eingegriffen wird, desto höher ist auch die Wahrscheinlichkeit, dass der Kernbereich privater Lebensgestaltung betroffen ist. Wie bereits oben aufgezeigt, kann auch die Zusammenschau mehrerer zunächst punktuell nicht kernbereichsbetroffener Informationen bei der Gefahr der Bildung von Persönlichkeitsprofilen Kernbereichsrelevanz aufweisen. Besteht die Gefahr eines additiven Grundrechtseingriffs, kann dies auch regelmäßig ein Indikator für die Gefahr der Bildung von Persönlichkeitsprofilen sein.[8] Auch bei

---

[4] BVerfG 10.06.2009 – 1 BvR 706/08, 1 BvR 819/08, 1 BvR 832/08, 1 BvR 837/08, BVerfGE 123, 186, 265f. = NJW 2009, 2033.

[5] *Winkler*, JA 2014, 881, 884.

[6] So ist in dem folgenden Urteil die Rede von „verschiedene einzelne, für sich betrachtet geringfügige Eingriffe in grundrechtliche geschützte Bereiche“: BVerfG 10.06.2009 – 1 BvR 706/08, 1 BvR 819/08, 1 BvR 832/08, 1 BvR 837/08, BVerfGE 123, 186 = NJW 2009, 2033.

[7] Vgl.: *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung, S. 112.

[8] So auch: *Desoi*, Intelligente Videoüberwachung, S. 74.

dem Gedanken des additiven Grundrechtseingriffs besteht die erhöhte Gefahr darin, dass Daten mittels unterschiedlicher Ermittlungsmaßnahmen erhoben werden und so in verschiedene Lebensbereiche einer Person eingegriffen wird.

Dies stellt jedoch nur einen Teilaspekt der Gefahr der Bildung von Persönlichkeitsprofilen dar, denn hier geht es neben den verschiedenen Daten auch um die Menge der Daten und deren Zusammenschau. Damit ist die Gefahr der Bildung von Persönlichkeitsprofilen weitreichender als die des additiven Grundrechtseingriffs. Die Konstruktion des additiven Grundrechtseingriffs als solchem ist getrennt von der Gefahr der Bildung von Persönlichkeitsprofilen und dem Kernbereich privater Lebensgestaltung zu betrachten. Er spielt dann eine Rolle, wenn mehrere Ermittlungsmaßnahmen nebeneinander angeordnet werden, dies kann aber, wie oben bereits dargestellt, nicht durch eine Ermittlungsmaßnahme – namentlich die Online-Durchsuchung – geschehen. Die Gefahr bei der Online-Durchsuchung in Bezug auf die Bildung von Persönlichkeitsprofilen ist jedoch als weitreichender anzusehen. Der Gedanke des additiven Grundrechtseingriffs ist somit allein nicht in der Lage, die Menge der Daten bei der Online-Durchsuchung entgegen der Gefahr der Bildung von Persönlichkeitsprofilen effektiv zu begrenzen, da das Merkmal der „Höchstpersönlichkeit“ beim additiven Grundrechtseingriff nur eine untergeordnete Rolle spielt. Im Übrigen ist er jedoch bei der Verhältnismäßigkeitsprüfung einer Online-Durchsuchung im konkreten Einzelfall zu berücksichtigen, da bereits eine solche Maßnahme mehrere Ermittlungsmaßnahmen in sich vereinen kann, die in verschiedenste Grundrechte eingreifen.

B. Ebene des Kernbereichsschutzes

Da die Gefahr der Bildung von Persönlichkeitsprofilen dem Kernbereich privater Lebensgestaltung zuzuordnen ist, ist auch auf dieser Ebene eine Begrenzung der zu erhebenden Daten vorzunehmen. Letztlich kann die Eindämmung der Gefahr der Bildung von Persönlichkeitsprofilen nur über die Vorschriften zum Kernbereich privater Lebensgestaltung gem. § 100d StPO gelingen, indem das zweistufige Schutzkonzept des Bundesverfassungsgerichts erweitert und präzisiert wird.

Nach dem zuvor der unzureichende Schutz durch das zweistufige Schutzkonzept im Hinblick auf die Gefahr der Bildung von Persönlichkeitsprofilen dargestellt wurde, muss eine Erweiterung des Konzepts auch auf die Menge der Daten erfolgen. Dabei muss berücksichtigt werden, wie die Menge der Daten mittels des Schutzes des Kernbereichs privater Lebensgestaltung auf das Nötigste reduziert werden kann.

I. Verfassungs- und unionsrechtskonforme Auslegung des § 100d Abs. 1 StPO

Zur Bildung von Persönlichkeitsprofilen werden unterschiedlichste Daten aus verschiedenen Lebensbereichen so erhoben, dass diese eine Beschreibung der Person des*der Betroffenen mittels seiner*ihrer Eigenschaften zulassen. Dieses Persönlichkeitsprofil ist dem Kernbereich privater Lebensgestaltung zuzuordnen. Darauf ist § 100d Abs. 1, 3 StPO konsequent anzuwenden und entsprechend verfassungskonform beziehungsweise unionsrechtskonform auszulegen.

Eine verfassungskonforme Auslegung ist dann geboten „(…), wenn unter Berücksichtigung von Wortlaut, Entstehungsgeschichte und Gesamtzusammenhang und Zweck mehrere Deutungen möglich sind, von denen jedenfalls eine zu einem verfassungsgemäßen Ergebnis führt."[9]

Hier dargestellt wird nunmehr, wie eine verfassungskonforme beziehungsweise unionsrechtskonforme Auslegung der Vorschriften zum Kernbereich privater Lebensgestaltung auf der Erhebungsebene aussehen müsste.

§ 100d Abs. 1 StPO normiert, dass die Online-Durchsuchung unzulässig ist, wenn allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden. Vielfach wurde hier von einer „Placebo-Norm" gesprochen, die keine Anwendung finde.[10] Das Gegenteil ist allerdings der Fall, wenn bereits die Gefahr der Bildung von Persönlichkeitsprofilen dem Kernbereich privater Lebensgestaltung zugeordnet wird. Sie bildet für sich genommen das konstitutive Merkmal der Höchstpersönlichkeit. Besteht die Gefahr der Bildung von Persönlichkeitsprofilen, dann werden bei der Durchführung der Maßnahme schon durch diese Möglichkeit allein kernbereichsrelevante Daten erhoben, da jedes erhobene Datum – unabhängig von seiner punktuellen Kernbereichsrelevanz – in einer Gesamtschau Kernbereichsrelevanz aufweist. Somit findet § 100d Abs. 1 StPO bei einer konsequenten verfassungs- und europarechtskonformen Auslegung immer dann Anwendung, wenn eine erhebliche Datenmenge aus unterschiedlichen Lebensbereichen erhoben werden soll. Ein besonderes Augenmerk ist bei der Prognose auf die bereits im zweiten Kapitel genannten Profilingdaten[11] zu richten. Jene Daten können in einer Gesamtschau dazu führen, dass die Gefahr der Bildung von Persönlichkeitsprofilen erheblich steigt.

---

[9] Ständige Rechtsprechung des Bundesverfassungsgerichts s. u. hier: BVerfG, Beschl. 10.06.2009 – 1 BvR 825, 831/08, BVerfGE 124, 25, 39 = JuS 2009, 1037.

[10] *Deutscher Anwaltsverein durch den Ausschuss Strafrecht*, Stellungnahme zur Bundestagsdrucksache 18/11272, S. 15; *Roggan*, StV 2017, 821, 828.

[11] Siehe hierzu: 2. Kapitel B. I. 2. b).

Eine Online-Durchsuchung darf somit gem. § 100d Abs. 1 StPO nicht durchgeführt werden, wenn die Gefahr besteht, dass durch die konkrete Online-Durchsuchung aufgrund der Menge und der Art der zu erhebenden Daten ein Persönlichkeitsprofil gebildet werden kann. Dann stellt jedes Datum für sich genommen bereits eine Information mit Kernbereichsrelevanz dar. Für die Praxis bedeutet dies, dass sich die Online-Durchsuchung auf eine bestimmte Art der Daten beschränken muss, deren Umfang nicht die Gefahr der Bildung eines Persönlichkeitsprofils begründen kann. Es kommt demnach auf eine Prognose in Bezug auf die Gefahr der Bildung von Persönlichkeitsprofilen an, die sich aus der Art der zu erhebenden Daten ergibt.

Bereits jetzt wird davon ausgegangen, dass mittels einer Prognose festzustellen ist, ob *allein* kernbereichsrelevante Daten erhoben werden.[12] Eine solche Prognose könne vor allem auf der Art der Kommunikation basieren.[13] So sei die Kernbereichsrelevanz insbesondere dann gegeben, wenn mit der Person, mit der der*die Betroffene kommuniziert, ein Vertrauensverhältnis bestehe.[14] Dieser Ansatz kann überzeugen, wenn die punktuelle Kernbereichsrelevanz eines Datums festgestellt werden soll, greift bei der Prognose in Bezug auf die Gefahr der Bildung von Persönlichkeitsprofilen aber zu kurz. Für diese Prognose ist vielmehr zu berücksichtigen, ob die Daten aus verschiedenen Lebensbereichen stammen, in welchem Umfang die Erstellung von Profilingdaten ermöglicht wird und inwieweit die jeweilige Online-Durchsuchung speziellere Ermittlungsmaßnahmen in sich vereint, wobei diese Kriterien sich gegenseitig bedingen. Auch die Nutzung des IT-Geräts muss dabei berücksichtigt werden. Nutzt eine Person ihr IT-Gerät lediglich zur Telefonie, wird eine Prognose anders ausfallen als bei einer Person, die ihr IT-Gerät in allen Lebensbereichen, beruflich und privat, nutzt, sodass eine deutlich weitreichendere Verknüpfung möglich ist.

Das könnte in einem konkreten Fall bedeuten, dass zuvor festgelegt werden muss, ob beispielsweise lediglich die Kommunikation, über die Quellen-TKÜ hinausgehend auch einschließlich vergangener Chatverläufe, erhoben werden soll. Bei der Person, deren IT-Gerät Objekt einer Online-Durchsuchung ist, handelt es sich in diesem Beispielfall um eine Person, die vermutlich erhebliche Bereiche ihres Lebens über ihr IT-Gerät organisiert. Da die Beobachtung des Kommunikationsverhaltens bereits eine erhebliche Datenmenge darstellt, dürfen, um den Schutz des Kernbereichs zu wahren, lediglich wenige weitere Informationen erhoben werden.

---

12 *Schmitt*, in: Meyer-Goßner/Schmitt, § 100d, 5a; BT-Drucks., 18/12785, S. 56.
13 *Schmitt*, in: Meyer-Goßner/Schmitt, § 100d, 5a; BT-Drucks., 18/12785, S. 56.
14 *Schmitt*, in: Meyer-Goßner/Schmitt, § 100d, 5a; BT-Drucks., 18/12785, S. 56.

Lässt somit eine Prognose bereits im Vorfeld der Durchführung der Online-Durchsuchung darauf schließen, dass aufgrund der Menge und der Art der zu erhebenden Daten, die Gefahr der Bildung eines Persönlichkeitsprofils besteht, stellt dies einen Fall des § 100d Abs. 1 StPO dar und die Maßnahme darf nicht durchgeführt werden.

Dieses Vorgehen, also die Anwendung von § 100d Abs. 1 StPO auf die Gefahr der Bildung von Persönlichkeitsprofilen, würde zwar zu einem befriedigenden Ergebnis führen, findet seine Grenzen aber in dem gesetzgeberischen Willen.

Die Grenzen einer verfassungskonformen Auslegung liegen dort, wo die gefundene Auslegung klar dem gesetzgeberischen Willen widerspricht.[15] Der Gesetzgeber hat sich bei der Normierung der Online-Durchsuchung mehr als offensichtlich an der Rechtsprechung des Bundesverfassungsgerichts orientiert beziehungsweise hat die Norm anhand der Rechtsprechung des Bundesverfassungsgerichts entwickelt.

Wie die Darstellung der Entwicklung des zweistufigen Schutzkonzeptes gezeigt hat, fehlt es gänzlich an einer Begrenzung der Daten auf der Erhebungsebene. Mit § 100d Abs. 1 StPO wollte der Gesetzgeber die Erhebungsebene des vom Bundesverfassungsgericht entwickelten zweistufigen Konzepts normieren.[16] Die Annahme, dass auf dieser Ebene auch die Gefahr der Bildung von Persönlichkeitsprofilen fallen soll, widerspricht zwar nicht dem klar geäußerten Willen des Gesetzgebers. Da sich dieser allerdings an der Rechtsprechung des Bundesverfassungsgerichts orientiert hat und das Gericht – wie dargelegt – eine solche Begrenzung nicht vorsieht, ist eine verfassungskonforme Auslegung nicht zwingend ausgeschlossen, wohl aber sehr schwer zu begründen.

Darüber hinaus ist zu berücksichtigten, dass das Bundesverfassungsgericht in ständiger Rechtsprechung zum Schutz des Kernbereichs privater Lebensgestaltung einfachgesetzliche Vorschriften fordert, die im Verfahren diesen Schutz absichern.[17] Diese müssen dem Grundsatz der Bestimmtheit und Normklarheit genügen, sodass es unabhängig von der Möglichkeit einer verfassungs- beziehungsweise unionskonformen Auslegung rechtspolitisch wünschenswert wäre, bei Regelungen, die die Menschenwürde betreffen, klare und präzise Vorschriften in der StPO vorzufinden.

---

15 Ebenfalls ständige Rechtsprechung siehe u. a.: BVerfG Beschl. 14.10.2008 – 1 BvR 2310/06, BVerfGE 122, 39, 61 = NJW 2009, 209.

16 Vgl.: BT-Drucks., 18/12785, S. 55.

17 Ständige Rechtsprechung mit weiteren Nachweisen: BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 277 = NJW 2016, 1781.

Das Gleiche gilt für eine Ausweitung der Auslegung auch für § 100d Abs. 3 StPO. Wie oben dargestellt, betrifft diese Norm die technische Absicherung, dass kernbereichsrelevante Daten nicht erhoben werden. Nach einer Auslegung könnte die Anwendbarkeit des Absatzes insoweit erweitert werden, dass technisch sicherzustellen ist, dass nicht eine solche Menge an Daten generiert wird, dass die Gefahr der Bildung von Persönlichkeitsprofilen besteht.

II. § 47 Nr. 3 BDSG

Wie im Abschnitt zum Unionsrecht dargestellt, begrenzt auch § 47 Nr. 3 BDSG, als Umsetzung der DSRL-JI als einfaches Bundesgesetz, die Datenmenge. Hier wird der Grundsatz der Datenminimierung statuiert. Der Wortlaut der DSRL-JI wurde jedoch mit der Begründung, man wolle sich der deutschen Rechtssprache anpassen,[18] nicht umgesetzt. Insbesondere die die Datenmenge klar begrenzenden Begriffe „maßgeblich“ und „übermäßig“ finden sich im § 47 Nr. 3 BDSG nicht wieder.

Denkbar wäre, auch diese Vorschrift unionsrechts- und verfassungskonform auszulegen, sodass auch an dieser Stelle eine Begrenzung der Datenmenge nach den Anforderungen des Grundgesetzes und der Grundrechtecharta möglich wäre. Eine solche Auslegung muss sich jedoch den selben Problemen stellen, wie die der § 100d StPO auch, sodass dieser Lösungsweg ebenfalls als wenig praktikabel anzusehen ist und aus rechtspolitischer Perspektive nicht die gewünschte Rechtssicherheit bietet. Unklar ist darüber hinaus, in wieweit ein solcher Grundsatz direkte Anwendung findet oder es eine deutlichere und auf die einzelne Maßnahme zugeschnittene Vorschrift braucht.

III. Unterbrechung der Maßnahme

Ein weiteres Problem im Rahmen der Beschränkung der Erhebung von Daten stellt sich beim Fehlen einer Vorschrift zur Unterbrechung der Maßnahme.

Anders als für die akustische Wohnraumüberwachung in § 100d Abs. 4 StPO findet sich für die Online-Durchsuchung keine Vorgabe zur Unterbrechung. Dies ist absolut unverständlich, insbesondere weil die Gesetzesbegründung zur Online-Durchsuchung explizit von einem Zugriff ausgeht, der sich „über einen längeren Zeitraum erstreckt“ und nicht nur einmalig und

[18] BT-Drucks. 18/12144, S. 7.

punktuell stattfindet.[19] Bereits hier hätte wirksam die Erhebung der Menge der Daten reguliert werden können, selbstverständlich nur dann, wenn man die Gefahr der Bildung von Persönlichkeitsprofilen unter den genannten Voraussetzungen dem Kernbereich zuordnet.

Im Rahmen der Durchführung der Online-Durchsuchung ist es durchaus denkbar, dass sich viele Informationen, derer es für eine Prognose im Vorfeld der Ermittlungsmaßnahme bedürfte – wir befinden uns im Anwendungsbereich des § 100d Abs. 1 StPO – erst im Laufe der Überwachung ergeben. Darum ist es für die Verfassungsmäßigkeit der Online-Durchsuchung wichtig, dass sich dies einer Vorschrift zur Unterbrechung der Maßnahme wiederfindet, um auch hier das Maß auf das Nötigste zu reduzieren.

Das bedeutet für die Gefahr der Bildung von Persönlichkeitsprofilen Folgendes: Wenn deutlich wird, dass mit einer weiteren Erhebung der Daten aufgrund der Art und der Menge der bereits erhobenen Daten diese Gefahr besteht, die Online-Durchsuchung abgebrochen werden muss, um den Schutz des Kernbereichs privater Lebensgestaltung gewährleisten zu können.[20] Somit muss eine Prognose über die Verletzung des Kernbereichs zu jedem Zeitpunkt stattfinden und eine Absicherung dieses Vorgehens ebenfalls Berücksichtigung in § 100d StPO finden.

IV. Exkurs: Verwendung intelligenter Systeme in der Zukunft? Ergebnis und Ausblick

Denkbar wäre es, die Ebene der Auswertung der IT-Geräte bei der Online-Durchsuchung in Zukunft mittels intelligenter Systeme durchzuführen, wenn sich der technische Fortschritt in diese Richtung entwickeln sollte. Dann wäre technisch zwar nicht gewährleistet, dass gem. § 100d Abs. 3 S. 1 StPO kernbereichsrelevante Daten nicht erhoben werden, aber die erste Einschätzung der Kernbereichsrelevanz könnte mittels eines Systems und nicht durch Ermittlungspersonen durchgeführt werden. So könnte argumentiert werden, dass die Verwendung von intelligenten Systemen ein milderes Mittel darstellte, da hier die Daten allein durch das System, nicht aber durch eine Ermittlungsperson wahrgenommen würden.

Dem ist nicht zuzustimmen. Das Verbot der Bildung von Persönlichkeitsprofilen umfasst auch die Verwendung von intelligenten Systemen. Intelligente Systeme nehmen nicht nur eine große Menge an Daten auf, sondern

---

[19] BT-Drucks., 18/12785, S. 54.

[20] Zum Abbruch, sobald erkennbar wird, dass in den Kernbereich eingegriffen wird, auch: BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220, 279 = NJW 2016, 1781.

interpretieren diese auf ein bestimmtes Muster hin und können selbstständig auf dieses reagieren.[21] So sind intelligente Systeme in der Lage, anhand von Daten wie Bewegungsprofilen, Nutzungsverhalten et cetera Kategorien zu schaffen, die sich menschlichen Erfahrungswerten verschließen.[22] Hier kann das schaffende System sich selbst optimieren und neue Kategorien bilden.[23] Bei der Verwendung solcher Algorithmen besteht die Gefahr, dass die betroffene Person der Situation noch hilfloser gegenübersteht.[24]

Sollte die Technik in Zukunft so weit fortgeschritten sein, dass eine Einschätzung von kernbereichsrelevanten Daten aus ermittlungstaktischen Gründen erwünscht und allein durch intelligente Systeme möglich wäre, dürften diese nicht genutzt werden, wenn sie eine solche Menge an Daten generierten, sodass sie in der Lage wären, ein Persönlichkeitsprofil zu erstellen. Dies gilt insbesondere, weil die Gefahr der Bildung von Persönlichkeitsprofilen unabhängig von der Art der Auswertung, ob maschinell oder persönlich, nicht bestehen darf. Der Mensch darf erst recht nicht von der Maschine zum Objekt strafrechtlicher Ermittlungsarbeit gemacht werden, indem der Kernbereich privater Lebensgestaltung nicht ausreichend geschützt wird.

Bei der Verwendung von intelligenten Systemen wird die betroffene Person ebenfalls zum Objekt der Ermittlungsbehörden und ist ihnen hilflos ausgesetzt. Aus diesem Grund ist die Verwendung von intelligenten Systemen zur Auswertung der Kernbereichsrelevanz bei der Online-Durchsuchung wegen der erhöhten Gefahr der Erstellung von Persönlichkeitsprofilen unzulässig und mit dem Schutz des Kernbereichs unvereinbar. Es darf zu keinem Zeitpunkt die Gefahr der Bildung von Persönlichkeitsprofilen bestehen, unabhängig davon, ob die erste Einschätzung der Kernbereichsrelevanz durch die Ermittlungspersonen oder durch ein intelligentes System erfolgt. Auch hier findet § 100d Abs. 1 StPO Anwendung.

V. Die Rolle des § 100e Abs. 3 S. 2 Nrn. 3, 4 StPO

Denkbar wäre es, eine mögliche bereits bestehende Einschränkung der Menge der Daten, die der Gefahr der Bildung von Persönlichkeitsprofilen entgegenwirkt, in § 100e Abs. 3 S. 2 Nrn. 3 und 4 StPO zu sehen. Mit § 100e StPO hat der Gesetzgeber eine Norm geschaffen, nach der in der Entscheidungsformel unter anderem die Art, der Umfang, die Dauer und der

---

21 *Gleß/Weigend*, ZStW 2014, 561, 563; *Schantz/Wolff*, Das neue Datenschutzrecht, S. 228; *Stiemerling*, CR 2015, 762.

22 *Stiemerling*, CR 2015, 762, 764.

23 *Stiemerling*, CR 2015, 762, 764.

24 *Schantz/Wolff*, Das neue Datenschutzrecht, S. 229.

Endzeitpunkt der Maßnahme sowie die Art der durch die Maßnahme zu erhebenden Informationen und ihre Bedeutung für das Verfahren angegeben werden müssen. Aus ermittlungstaktischen Gründen wird zumeist ein Interesse daran bestehen, diese Erfordernisse möglichst allgemein und offen zu interpretieren.[25] Denkbar wäre es, bereits hierin eine gelungene Hürde gegen die Erhebung sämtlicher Daten und eine Einschränkung der Datenmenge zu sehen.

Grundsätzlich handelt es sich bei § 100e StPO zwar um eine gelungene Verfahrensvorschrift, sie macht jedoch keine inhaltlichen Vorgaben, sondern ist lediglich dazu geeignet, die Einhaltung der Vorschriften zum Kernbereich der privaten Lebensgestaltung zu gewährleisten. Diese Vorschrift ist weder in der Lage, dem Umfang der Daten selbst Grenzen zu setzen,[26] noch ermöglicht sie aus sich heraus einen gelungenen Schutz des Kernbereichs privater Lebensgestaltung. Sie stellt somit keine Absicherung des Kernbereichs dar.

Aus diesem Grund muss die Art der zu erhebenden Daten mit Blick auf die Gefahr der Bildung von Persönlichkeitsprofilen in der Entscheidungsformel gem. § 100e StPO genannt werden, um so die Prognose zum Schutz des Kernbereichs privater Lebensgestaltung plausibel machen zu können.

VI. Erweiterung der Vorschriften

Wie zuvor dargelegt wäre eine verfassungskonforme beziehungsweise europarechtskonforme Auslegung zwar denkbar, aber rechtspolitisch nicht zielführend und darüber hinaus nicht im Sinne der Normklarheit. Im Übrigen fehlte es dann weiterhin an einer Vorschrift zur Unterbrechung der Maßnahme.

Aus diesen Gründen sollte eine Begrenzung der Daten auf der Erhebungsebene normiert werden. Das zweistufige Schutzkonzept des Bundesverfassungsgerichts kann so nicht bestehen und ist mit europarechtlichen Vorgaben – Art. 7, 8 GRC – nicht vereinbar.

Anknüpfungspunkt für eine Erweiterung der Vorschriften, um der Gefahr der Bildung von Persönlichkeitsprofilen Rechnung zu tragen, ist der Kernbereich privater Lebensgestaltung. Geregelt werden muss eine Begrenzung der zu erhebenden Daten und die Unterbrechung der Maßnahme.

---

[25] *Schmitt*, in: Meyer-Goßner/Schmitt, § 100e, Rn. 13.

[26] Vgl. auch: *Großmann*, GA 2018, 439, 447.

1. Ergänzung des § 100d Abs. 1 StPO

Zunächst braucht es somit einen klarstellenden Satz in § 100d Abs. 1 StPO. Dieser muss das oben Gesagte, normieren nämlich, dass die Bildung von Persönlichkeitsprofilen dem Kernbereich privater Lebensgestaltung zu zuordnen ist und eine alleinige Kernbereichsrelevanz im Sinne des Satz eins besteht, wenn die Gefahr einer solchen gegeben ist.

Denkbar für einen Satz 2 des § 100d Abs. 1 StPO wäre folgende Formulierung:

> Dabei kann nicht nur dem einzelnen Datum Kernbereichsrelevanz zu kommen, sondern allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung werden auch dann erlangt, wenn die Gefahr der Bildung von Persönlichkeitsprofilen besteht. Erkenntnisse aus einer unzulässigen Online-Durchsuchung dürfen nicht verwertet werden. Die Sätze 2 und 3 des Absatz 2 gelten entsprechend.

Einer solchen Formulierung kommt zum einen zugute, dass sie klar benennt, dass die Gefahr der Bildung von Persönlichkeitsprofilen dem Kernbereich privater Lebensgestaltung zu zuordnen ist und dass eine Online-Durchsuchung unzulässig ist, wenn die Gefahr der Bildung von Persönlichkeitsprofilen besteht.

Aufgrund der Eingriffsintensität bei der unzulässigen Online-Durchsuchung sollte nicht nur auf der Erhebungsebene klargestellt werden, dass eine solche Maßnahme nicht hätte stattfinden dürfen, sondern es bedarf auch auf der Verwertungsebene eines expliziten absoluten Verwertungsverbots, um darzulegen, dass nicht nur die im Einzelfall punktuell kernbereichsrelevanten Daten nach § 100d Abs. 3 S. 1 StPO nicht verwertet werden dürfen. Die Löschungs- und Protokollierungspflichten des Absatz 2 müssen entsprechende Anwendung finden, um dem Schutz des Kernbereichs privater Lebensgestaltung Rechnung zu tragen.

Mit der vorgeschlagenen Klarstellung in Abs. 1 wäre dann auch mitgeregelt, dass technische Gewährleistung aus § 100d Abs. 3 StPO nicht nur das punktuelle kernbereichsrelevante Datum betrifft, sondern darüber hinaus auch die Gefahr der Bildung von Persönlichkeitsprofilen. Gemäß der Klarstellung ist somit technisch – nach Möglichkeit – sicherzustellen, dass die Gefahr der Bildung von Persönlichkeitsprofilen nicht besteht. So findet bereits eine Begrenzung der Daten auf der Erhebungsebene statt.

2. Normierung der Unterbrechung der Maßnahme

Darüber hinaus bedarf es der Normierung der Unterbrechung der Maßnahme. Eine solche kann an den Wortlaut für die Unterbrechung bei der

akustischen Wohnraumüberwachung in § 100d Abs. 4 S. 2 StPO angelehnt werden.

So könnte ein ergänzend einzufügender Abs. 2 des § 100d StPO wie folgt gefasst werden:

> Die Online-Durchsuchung ist unverzüglich zu unterbrechen, wenn sich während der Überwachung Anhaltspunkte dafür ergeben, dass Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Entsteht bei Durchführung der Maßnahme die Gefahr der Bildung von Persönlichkeitsprofilen, ist die Maßnahme zu beenden.

Aufgrund der Klarstellung in Abs. 1 bedarf es hier keiner erneuten Erläuterung, dass dem Kernbereich privater Lebensgestaltung auch die Gefahr der Bildung von Persönlichkeitsprofilen innerwohnt.

Außerdem kann durch einen zusätzlichen Satz klargestellt werden, dass auch die Fortführung der Online-Durchsuchung unzulässig ist, wenn sich während der Durchführung die Gefahr der Bildung von Persönlichkeitsprofilen ergibt. So findet eine Absicherung nicht nur vor Beginn der Maßnahme wie in § 100d Abs. 1 StPO, sondern auch während der Maßnahme statt.

Ergebnis und Ausblick

Die Online-Durchsuchung stellt den Schutz des Kernbereichs privater Lebensgestaltung aufgrund der dargestellten erheblich erhöhten Gefahr der Bildung von Persönlichkeitsprofilen im Vergleich zu anderen Ermittlungsmaßnahmen vor neue Herausforderungen. Diesen sind das Bundesverfassungsgericht und der Gesetzgeber, der die Arbeit in Bezug auf die Gewaltenteilung in fragwürdiger Art und Weise dem Bundesverfassungsgericht überlassen hat, nicht gerecht geworden.

Die besondere Herausforderung liegt dabei in der Ermöglichung einer Datenerhebung, der keine Grenzen gesetzt sind und nicht auf das Nötigste, wie vom Europäische Gerichtshof in eindeutiger Rechtsprechung gefordert, beschränkt wird.

Denn die besondere Gefahr der Bildung eines Persönlichkeitsprofils ergibt sich aus einer möglichen Gesamtschau der Daten. Die Online-Durchsuchung ist eine Ermittlungsmaßnahme, mit der so viele verschiedene Daten erhoben werden können wie bei keiner anderen. Im Ergebnis kann bei der Online-Durchsuchung eine solche Menge an Daten generiert werden, dass die Gesamtschau der punktuell nicht kernbereichsrelevanten Daten die Gefahr der Bildung von Persönlichkeitsprofilen begründet, sodass dann die Gesamtheit der Daten Kernbereichsrelevanz aufweist.

Um dieser Gefahr der Bildung von Persönlichkeitsprofilen als Teil des Kernbereichs privater Lebensgestaltung wirksam begegnen zu können, muss der Generierung von Daten auf Erhebungsebene Einhalt geboten werden. Unter rechtspolitischen Gesichtspunkten braucht es dafür eine Klarstellung in § 100d Abs. 1 StPO, dass auch der Gefahr der Bildung von Persönlichkeitsprofilen Kernbereichsrelevanz zu kommt. Wenn eine solche Gefahr bereits vor Beginn der Maßnahme besteht, ist ihre Durchführung unzulässig. Gleiches gilt dann, wenn sich während der Durchführung eine solche Gefahr herauskristallisiert. Darüber hinaus ist die Maßnahme zu unterbrechen, wenn eine Prognose ergibt, dass kernbereichsrelevante Daten erhoben werden könnten.

Diese drei wesentlichen Grundsätze finden sich bisher in dem Schutz des Kernbereichs privater Lebensgestaltung nicht wieder, sind aber essenziell zur Verhinderung der Bildung von Persönlichkeitsprofilen. Nur so kann den verfassungsrechtlichen und europarechtlichen Vorgaben Genüge getan werden.

Da in diesem Bereich mit weiteren Verfassungsbeschwerden und Entscheidungen des Europäischen Gerichtshofs zu rechnen ist, sollte der Gesetzgeber im eigenen Interesse selbstständig aktiv werden und entsprechender Absicherungen für die Menschenwürde schaffen.

Es ist zu erwarten, dass sich immer mehr Ermittlungsarbeit ins Internet und in Richtung der IT-Überwachung verlagern wird. Nicht zuletzt ist auch die Einführung der Online-Durchsuchung selbst der „fortschreitenden Entwicklung der Informationstechnik“ geschuldet.[1] Auch der Umgang mit der Überwachung von Smart-Home-Geräten wird immer mehr ins Blickfeld der Ermittlungsbehörden rücken.[2] Hier stellen sich, wie diese Ausarbeitung verdeutlicht, noch wesentliche Folgefragen.

Im Ergebnis zeigt diese Dissertation somit einen Lösungsweg auf, wie mit der Erhebung erheblicher Datenmengen auch in Zukunft umgegangen werden kann und muss. Der Gefahr der Bildung von Persönlichkeitsprofilen wird im Zuge der Digitalisierung immer größere Bedeutung zukommen, was nicht länger ignoriert werden darf.

[1] BT-Drucks., 18/12785, S. 46.

[2] *Blechschmitt*, MMR 2018, 361; BT-Drucks., 19/11133.

Literaturverzeichnis

Baldus, Manfred: Der Kernbereich privater Lebensgestaltung – absolut geschützt, aber abwägungsoffen, JZ 2008, S. 218–227.

Bär, Wolfgang: Der Zugriff auf Computerdaten im Strafverfahren, Köln 1992.

Bär, Wolfgang: BGH-Ermittlungsrichter: Online-Durchsuchung eines Computers. Anmerkung, MMR 2007, S. 239–242.

Barrot, Johannes M.: Der Kernbereich privater Lebensgestaltung. Zugleich ein Beitrag zum dogmatischen Verständnis des Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG, Baden-Baden 2012.

Becker, Jörg-Peter/*Erb*, Volker/*Esser*, Robert/*Graalmann-Scheerer*, Kirsten/*Hilger*, Hans/*Ignor*, Alexander: StPO, 27. Aufl., hrsg. von Löwe-Rosenberg, Berlin 2019 (zitiert: *Bearbeiter*, in: Löwe-Rosenberg).

Benda, Ernst: Privatsphäre und „Persönlichkeitsprofil". Ein Beitrag zur Datenschutzdiskussion, in: Gerhard Leibholz/Hans Faller/Paul Mikat (Hrsg.), Menschenwürde und freiheitliche Rechtsordnung. Festschrift für Willi Geiger zum 65. Geburtstag, Tübingen 1974, S. 23–44 (zitiert: *Benda*, in: FS Geiger).

Bernstorff, Jochen von: Der Streit um die Menschenwürde im Grund- und Menschenrechtsschutz: Eine Verteidigung des Absoluten als Grenze und Auftrag, JZ 2013, S. 905–915.

Beukelmann, Stephan: Die Online-Durchsuchung, StraFo 2008, S. 1–8.

Beulke, Werner/*Meinighaus*, Florian: Der Staatsanwalt als Datenreisender. Heimliche Online-Durchsuchung, Fernzugriff und Mailbox-Überwachung, in: Heinz Schoch/Helmut Satzger/Gerhard Schäfer et al. (Hrsg.), Festschrift für Gunter Widmaier, Strafverteidigung, Revision und die gesamten Strafrechtswissenschaften, Köln 2008, S. 63–80 (zitiert: *Beulke/Meinighaus*, in: FS Widmaier).

Blechschmitt, Lisa: Zur Einführung von Quellen-TKÜ und Online-Durchsuchung, StraFo 2017, S. 361–365.

Blechschmitt, Lisa: Strafverfolgung im digitalen Zeitalter. Auswirkungen des stetigen Datenaustauschs auf das strafrechtliche Ermittlungsverfahren, MMR 2018, S. 361–366.

Blozik, Michael: Subsidiaritätsklauseln im Strafverfahren, Göttingen 2012.

Böckenförde, Thomas: Auf dem Weg zur elektronischen Privatsphäre. Zugleich Besprechung von BVerfG, Urt. v. 27.02.2008 – „Online-Durchsuchung", JZ 2008, S. 925–939.

Bode, Thomas A.: Verdeckte strafprozessuale Ermittlungsmaßnahmen, Berlin/Heidelberg 2012.

Brailovskala, Julia/*Stirnberg*, Jan/*Rozgonjuk*, Dmitri/*Magrfrag*, Jürgen/*Elhai*, Jon D.: From low sense of control to problematic smartphone use severity during Covid-19 outbreak: The mediating role of fear of missing out and the moderating role of repetitive negative thinking, PLOS ONE, 22.12.2021, abrufbar unter: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0261023.

Buermeyer, Ulf: Die „Online Durchsuchung". Technischer Hintergrund des verdeckten hohelichen Zugriffs auf Computersysteme, HRRS 2007, S. 154–166.

Dammann, Ilmer: Der Kernbereich der privaten Lebensgestaltung. Zum Menschenwürde- und Wesensgehaltsschutz im Bereich der Freiheitsgrundrechte, Berlin 2011.

Desoi, Monika: Intelligente Videoüberwachung. Rechtliche Bewertung und rechtsgemäße Gestaltung, Wiesbaden 2018.

Di Fabio, Udo: Grundrechte als Werteordnung, JZ 2004, S. 1–8.

Dreier, Horst (Hrsg.): Grundgesetz Kommentar, 3. Aufl., hrsg. von Horst Dreier, Tübingen 2018 (zitiert: *Bearbeiter*, in: Grundgesetz Kommentar).

Dürig, Günter/*Herzog*, Roman/*Scholz*, Rupert: Grundgesetz Kommentar, 96. Aufl., München 2022 (zitiert: *Bearbeiter*, in: Dürig/Herzog/Scholz Kommentar),

Epping, Volker/*Hillgruber*, Christian (Hrsg.): BeckOK Grundgesetz, 45. Aufl., 2020 (zitiert: *Bearbeiter*, in: BeckOK GG).

Erd, Rainer: Bundesverfassungsgericht versus Politik. Eine kommentierende Dokumentation der jüngsten Entscheidung zu drei Sicherheitsgesetzen, KJ 2008, S. 118–133.

Erp, Volker/*Schäfer*, Jürgen: Kommentar zum StGB, 3. Aufl., hrsg. von Wolfgang Joecks/Lutz Meyer-Goßner/Bertram Schmitt, München 2020 (zitiert: *Bearbeiter*, in: MüKO).

Eser, Albin: Kommentar zum StGB, 30. Aufl., hrsg. von Adolf Schönke/Horst Schröder, München, 2019 (zitiert: *Bearbeiter*, in: Schönke/Schröder).

Fischer, Thomas (Hrsg.): Kommentar zum StGB, 68. Aufl., hrsg. von Thomas Fischer, München 2021 (zitiert: *Bearbeiter*, in: Fischer).

Freiling, Felix/*Safferling*, Christoph/*Rückert*, Christian: Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung. Rechtliche und technische Herausforderungen, JR 2018, S. 9–22.

Gazeas, Nikolaos: Verfassungsbeschwerde gegen die Regelungen der Strafprozessordnung zur Online-Durchsuchung und Quellen-Telekommunikationsüberwachung; online abzurufen über https://www.fdp.de/sites/default/files/uploads/2018/08/20/fdp-vfb-gazeas-zusammenfassung.pdf (zugegriffen am 19.9.2019).

Geis, Max-Emanuel: Der Kernbereich des Persönlichkeitsrechts – Ein Plädoyer für die „Sphärentheorie", JZ 1991, S. 112–117.

Gercke, Björn/*Julius*, Karl-Peter/*Temming*, Dieter/*Zöller*, Mark Alexander (Hrsg.): Kommentar Strafprozessordnung, 6. Aufl., Heidelberg 2019 (zitiert: *Bearbeiter*, in: Heidelberger Kommentar).

Gleß, Sabine/*Weigend*, Thomas: Intelligente Agenten und das Strafrecht, ZStW 2014, S. 561–591.

Graf, Jürgen: Internet: Straftaten und Strafverfolgung, DRiZ 1999, 281.

Graf, Jürgen (Hrsg.): StPO Kommentar, 39. Aufl., hrsg. von Jürgen Graf 2021 (zitiert: *Bearbeiter*, in: BeckOK StPO).

Großmann, Sven: Zur repressiven Online-Durchsuchung, GA 2018, S. 439–456.

Großmann, Sven: Telekommunikationsüberwachung und Online-Durchsuchung: Voraussetzungen und Beweisverwertungsverbote, JA 2019, S. 241–248.

Hain, Karl-E.: Konkretisierung der Menschenwürde durch Abwägung?, Der Staat 2006, S. 189–214.

Hannich, Rolf: Karlsruher Kommentar StPO, 8. Aufl., hrsg. von Rolf Hannich, München 2019 (zitiert: *Bearbeiter*, in: KK).

Hauck, Pierre: Heimliche Strafverfolgung und Schutz der Privatheit. Eine vergleichende und interdisziplinäre Analyse des deutschen und englischen Rechts unter Berücksichtigung der Strafverfolgung in der Europäischen Union und im Völkerstrafrecht, Tübingen 2014.

Heintschel-Heinegg, Bernd v. (Hrsg.), BeckOK zum StGB, 49. Aufl., München 2021 (zitiert: *Bearbeiter*, in: BeckOK StGB).

Herzog, Roman/*Scholz*, Rupert/*Klein*, Hans (Hrsg.): Grundgesetz Kommentar, München 2020 (zitiert: *Bearbeiter*, in: Herzog/Scholz/Klein).

Hoffmann-Riem, Wolfgang: Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, S. 1009–1022.

Hofmann, Manfred: Die Online-Durchsuchung – staatliches „Hacken" oder zulässige Ermittlungsmaßnahme, NStZ 2005, S. 121–125.

Hömig, Dieter: „Neues" Grundrecht, neue Fragen? Zum Urteil des BVerfG zur Online-Durchsuchung, JURA 2009, S. 207–213

Hong, Mathias: Der Menschenwürdegehalt der Grundrechte. Grundfragen, Entstehung und Rechtsprechung, Tübingen 2019.

Hornung, Gerrit: Ermächtigungsgrundlage für die „Online-Durchsuchung"? Verfassungsrechtliche Anforderungen an und Grenzen für den heimlichen Zugriff auf IT-Systeme im Ermittlungsverfahren, DuD 2007, S. 575–580.

Hornung, Gerrit: Ein neues Grundrecht. Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme", CR 2008, S. 299–306.

Jahn, Matthias/*Kudlich*, Hans: Die strafprozessuale Zulässigkeit der Online-Durchsuchung, JR 2007, S. 57–61.

Jarass, Hans: Charta der Grundrechte der Europäischen Union, 4. Aufl. München 2021.

Jarass, Hans/*Kment*, Martin: Kommentar zum GG, 16. Aufl., hrsg. von Hans Jarass/Bodo Pieroth, München 2020 (zitiert: *Bearbeiter*, in: Jarass/Pieroth Kommentar zum GG).

Johannes, Paul/*Weinhold*, Robert: Das neue Datenschutzrecht bei Polizei und Justiz, Baden-Baden 2018.

Knauer, Christoph/*Kudlich*, Hans/*Schneider*, Hartmut (Hrsg.): Münchener Kommentar zur StPO, München 2014 (zitiert: *Bearbeiter*, in: MüKO StPO).

Knierim, Thomas C./*Oehmichen*, Anna: Quellen TKÜ und Online-Durchsuchung, in: Thomas C. Knierim/Anna Oehmichen/Susanne Beck et al. (Hrsg.), Gesamtes Strafrecht aktuell, NomosPraxis, Baden-Baden 2018, S. 353–405 (zitiert: *Knierim/Oehmichen*, Quellen TKÜ und Online-Durchsuchung, in: Gesamtes Strafrecht aktuell).

Kruse, Björn/*Grzesiek*, Mathias: Die Online-Durchsuchung als „digitale Allzweckwaffe" – Zur Kritik an überbordenden Ermittlungsmethoden, KritV 2017, S. 331–350.

Kudlich, Hans: Unzulässigkeit einer Online-Durchsuchung, JA 2007, S. 391–394.

Kühling, Jürgen/*Buchner*, Benedikt (Hrsg.): Kommentar zur Datenschutz-Grundverordnung, und zum Bundesdatenschutzgesetz, München 2018 (zitiert: *Bearbeiter*, in: Kühling/Buchner, DSGVO/BDSG).

Kutscha, Martin: Verdeckte „Online-Durchsuchung" und die Unverletzlichkeit der Wohnung, NJW 2007, S. 1169–1172.

Lammer, Dirk: Verdeckte Ermittlungen im Strafprozeß. Zugleich eine Studie zum Menschenwürdegehalt der Grundrechte, Berlin 1992.

Landau, Herbert: Die Pflicht des Staates zum Erhalt einer funktionstüchtigen Strafrechtspflege, NStZ 2007, S. 121–129.

Lindemann, Michael: Der Schutz des „Kernbereichs privater Lebensgestaltung" im Strafverfahren, JR 2006, S. 191–198.

Lisken, Hans/*Denniger*, Erhard (Hrsg.): Handbuch des Polizeirechts, 7. Aufl. München 2021 (zitiert: *Bearbeiter*, in: Handbuch des Polizeirechts).

Löffelmann, Markus: Das Gesetz zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004 (akustische Wohnraumüberwachung), ZIS 2006, S. 87–98.

Löffelmann, Markus: Datenerhebung aus dem „Smart-Home" im Sicherheitsrecht, GSZ 2020, S. 244–250.

Lutz, Martin/*Jungholt*, Thorsten: Online-Razzia: Schäuble legt Entwurf vor, Welt Online 2007; online abzurufen über https://www.welt.de/wams_print/article1027727/Online-Razzia-Schaeuble-legt-Entwurf-vor.html (zugegriffen am 11.2.2019).

Mansdörfer, Marco: Sicherheit und Strafverfahren. Online-Ausspähen, genetische Sippenhaft und der Abbau richterlicher Störenfriede im Kontext einer strafverfassungsrechtlichen Abwägungstheorie, GSZ 2018, S. 45–84.

Meyer, Jürgen/*Bernsdorff*, Norbert (Hrsg.): Charta der Grundrechte der Europäischen Union. Kommentar, 4. Aufl., Baden-Baden 2014 (zitiert: *Bearbeiter*, in: NK Charta der Grundrechte der Europäischen Union).

Münch, Ingo/*Kunig*, Philip (Hrsg.): Grundgesetzkommentar, 6. Aufl., München 2012 (zitiert: *Bearbeiter*, in: Münch/Kunig).

Neyer, Franz J./*Asendorpf*, Jens: Psychologie der Persönlichkeit, 6. Aufl., Berlin 2018.

Paa, Bernhard: Der Zugriff der Strafverfolgungsbehörden auf das Private im Kampf gegen schwere Kriminalität, Hamburg 2013.

Park, Tido: Durchsuchung und Beschlagnahme, 4. Aufl., München 2018.

Pechstein. Matthias/*Nowak*, Carsten/*Häde*, Ulrich (Hrsg.): Frankfurter Kommentar zu EUV, GRC, und AEUV, 2017 (zitiert: *Bearbeiter*, in: Frankfurter Kommentar EUV GRC AEUV).

Popp, Andreas: Strafbarer Bezug von kinder- und jugendpornographischen „Schriften": Zeit für einen Paradigmenwechsel im Jugendstrafrecht, ZIS 2011, S. 193–204.

Rath, Christian: Online-Schnüffeln ohne Freibrief?, TAZ 2007; online abzurufen über https://www.taz.de/Archiv-Suche/!287008&s=Online-Durchsuchung&SuchRahmen=Print/ (zugegriffen am 22.8.2018).

Reichert, Johannes: Der Schutz des Kernbereichs privater Lebensgestaltung in den Polizeigesetzen des Bundes und der Länder, Tübingen 2015.

Rieß, Peter: Sicherung einer effektiven Strafrechtspflege – ein Verfassungsgebot?, StraFo 2000, 364 – 369.

Roggan, Fredrik: Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigten und die Allgemeinheit, StV 2017, S. 821–829.

Rosenbach, Marcel: Digitale Spaltung, Spiegel 2007; online abzurufen über http://www.spiegel.de/spiegel/print/d-52109100.html (zugegriffen am 22.8.2018).

Roth, Wolfgang: Gutachterliche Stellungnahme Drucks., 14/0645 des Landes Nordrhein-Westfalen.

Rottmeier, Christian: Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, Tübingen 2017.

Rux, Johannes: Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden – Rechtsfragen der „Online-Durchsuchung", JZ 2007, S. 285–295.

Sachs, Michael (Hrsg.): Kommentar zum Grundgesetz, 8. Aufl., München 2018 (zitiert: *Bearbeiter*, in: Sachs GG Kommentar).

Sachs, Michael/*Krings*, Thomas: Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme", JuS 2008, S. 481–486.

Satzger, Helmut/*Schluckebier*, Wilhelm/*Widmaier*, Gunter: StPO Kommentar Strafprozessordnung mit GVG und EMRK: Kommentar, 4. Aufl., Köln 2020 (zitiert: *Bearbeiter*, in: SSW StPO).

Schantz, Peter/*Wolff*, Heinrich Amadeus: Das neue Datenschutzrecht. Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, München 2017.

Schlegel, Stephan: Warum die Festplatte keine Wohnung ist – Art. 13 GG und die „Online-Durchsuchung", GA 2007, S. 648–663.

Schmitt, Bertram: Strafprozessordnung, Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen, 62. Aufl., hrsg. von Lutz Meyer-Goßner/Bertram Schmitt, München 2019 (zitiert: *Bearbeiter*, in: Lutz Meyer-Goßner/Bertram Schmitt).

Schmitt, Manfred/*Altstötter-Gleich*, Christine: Differentielle Psychologie und Persönlichkeitspsychologie kompakt, Grundlagen Psychologie, Weinheim 2010.

Schwabenbauer, Thomas: Heimliche Grundrechtseingriffe. Ein Beitrag zu den Möglichkeiten und Grenzen sicherheitsbehördlicher Ausforschung, Tübingen 2013.

Schwichtenberg, Simon: Die „kleine Schwester" der DSGVO: Die Richtlinie zur Datenverarbeitung bei Polizei und Justiz, DuD 2016, S. 605–609.

Siebert, Ulrich: Sperrverpflichtungen gegen Kinderpornografie im Internet, JZ 2009, S. 653–662.

Simitis, Spiros/*Hornung*, Gerrit/*Spieker*, Indra (Hrsg.): Kommentar zum Datenschutzrecht DSGVO mit BDSG, Baden-Baden 2019 (zitiert: *Bearbeiter*, in: NK zum Datenschutzrecht).

Singelnstein, Tobias: Hacken zur Strafverfolgung? Gefahren und Grenzen der strafprozessualen Online-Durchsuchung, verfassungsblog 2017; online abzurufen über https://verfassungsblog.de/hacken-zur-strafverfolgung-gefahren-und-grenzen-der-strafprozessualen-online-durchsuchung/ (zugegriffen am 12.11.2020).

Singelnstein, Tobias/*Derin*, Tobias: Das Gesetz zur effektiven und praxistauglichen Ausgestaltung des Strafverfahrens. Was aus der StPO-Reform geworden ist, NJW 2017, S. 2646–2652.

Soiné, Michael: Die strafprozessuale Online-Durchsuchung, NStZ 2018, S. 497–504.

Specht-Riemenschneider, Louisa/*Mantz*, Reto: Handbuch Europäisches und deutsches Datenschutzrecht, München, 2019.

Stachl, Clemens/*Au*, Quay/*Schoedel*, Ramona et al.: Predicting personality from patterns of behavior collected with smartphones, PNAS; online abzurufen über https://www.pnas.org/content/117/30/17680#ref-28 (zugegriffen am 14.4.2021).

Stark, Holger: Digitale Spionage, Spiegel 2009; online abzurufen über http://www.spiegel.de/spiegel/print/d-64497190.html (zugegriffen am 31.5.2021).

Stemmler, Gerhard/*Hagemann*, Dirk/*Amelang*, Manfred et al.: Differentielle Psychologie und Persönlichkeitsforschung, 8. Aufl., Stuttgart 2016.

Stiemerling, Oliver: „Künstliche Intelligenz" – Automatisierung geistiger Arbeit, Big Data und das Internet der Dinge, Eine technische Perspektive, CR 2015, S. 762–765.

Strate, Gerhard/*Ventzke*, Klaus-Ulrich: Beschwerdeschrift. Verfassungsbeschwerde 2018; online abzurufen über https://freiheitsrechte.org/home/wp-content/uploads/2018/08/GFF_Verfassungsbeschwerde_Staatstrojaner_anonym.pdf (zugegriffen am 19.2.2019).

Valerius, Brian: Ermittlungsmaßnahmen im Internet, JR 2007, S. 275–280.

Warntjen, Maximilian: Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung. Eine Konzeption im Anschluss an das Urt. des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung, BVerfGE 109, 279, Baden-Baden 2007.

Winkler, Daniela: Der „additive Grundrechtseingriff": Eine adäquate Beschreibung kumulierender Belastungen?, JA 2014, S. 881–887.

Wolter, Jürgen: Repressive und präventive Verwertung tagebuchartiger Aufzeichnungen, zugleich Besprechung der Tagebuch-Entscheidung des BVerfG, StV 1990, S. 175–180.

Wolter, Jürgen: Die neue Nachlässigkeit des BVerfG bei verdeckten Ermittlungseingriffen und die Funktionstüchtigkeit der Strafverfolgung, in: Felix Herzog/Reinhold Schlothauer/Wolfgang Wohlers (Hrsg.), GS Weßlau. Rechtsstaatlicher Strafprozess und Bürgerrechte, Berlin 2016, S. 445–461 (zitiert: *Wolter*, in: GS Weßlau).

Youyou, Wu/*Kosinski*, Michal/*Stillwell*, David: Computer-based personality judgments are more accurate than those made by humans, Proceedings of the National Academy of Sciences of the United States of America 2015; online abzurufen über https://www.pnas.org/content/pnas/112/4/1036.full.pdf (zugegriffen am 12.11. 2020).

Zerbes, Ingeborg/*El-Ghazi*, Mohamad: Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung, NStZ 2015, S. 425–433.

Stichwortverzeichnis