CHRISTIAN RÜHS

Durchsicht informationstechnischer Systeme

Veröffentlichungen zum Verfahrensrecht 187

Mohr Siebeck

Veröffentlichungen zum Verfahrensrecht

Band 187

herausgegeben von

Rolf Stürner

Christian Rühs

Durchsicht informations-technischer Systeme

§ 110 Abs. 3 StPO im Lichte des IT-Grundrechts

Mohr Siebeck

Christian Rühs, geboren 1991; Studium der Rechtswissenschaft an der Ruhr-Universität Bochum; Wissenschaftlicher Mitarbeiter am Lehrstuhl für Strafrecht, Strafprozessrecht und Internationales Strafrecht der Ruhr-Universität Bochum; 2021 Promotion; Rechtsreferendar am Landgericht Bochum.
orcid.org/0000-0001-9296-6926

ISBN 978-3-16-161315-9 / eISBN 978-3-16-161316-6
DOI 10.1628/978-3-16-161316-6

ISSN 0722-7574 / eISSN 2568-7255 (Veröffentlichungen zum Verfahrensrecht)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über *http://dnb.dnb.de* abrufbar.

Das Buch wurde von Gulde Druck in Tübingen auf alterungsbeständiges Werkdruckpapier gedruckt und von der Buchbinderei Nädele in Nehren gebunden.

Printed in Germany.

Vorwort

Die vorliegende Monographie ist der im Wesentlichen unveränderte Text, der im Sommersemester 2021 von der Juristischen Fakultät der Ruhr-Universität Bochum als Dissertation angenommen wurde. Die wichtigsten Entwicklungen in Gesetzgebung, Rechtsprechung und Literatur konnten vor Veröffentlichung noch bis einschließlich November 2021 berücksichtigt werden. Das betrifft insbesondere das „Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften" vom 25. Juni 2021, durch das unter anderem § 110 Abs. 3 StPO reformiert wurde.

Für das Gelingen meiner Promotion habe ich an erster Stelle Frau Prof. Dr. Sabine Swoboda zu danken. Sie hat mir nicht nur als Doktormutter, sondern auch in ihrer Eigenschaft als meine Chefin Zeit und Gelegenheit zur Promotion gegeben. Dass sie sich sogar in den Weihnachtsferien ausführlich mit meiner Dissertation befasste, dürfte Zeugnis genug dafür sein, mit wie viel Einsatzbereitschaft sie das Promotionsvorhaben von Anfang bis Ende betreut hat.

Dank gebührt auch Herrn Prof. Dr. Jörg Ennuschat. Er hat als Professor für Öffentliches Recht die Zweitbegutachtung dieser – im Kern strafprozessrechtswissenschaftlichen – Dissertation übernommen und konnte mir auf diesem Wege wertvolle Hinweise insbesondere zu den verfassungsrechtlichen Aspekten meiner Arbeit geben.

Aus dem außeruniversitären Umfeld habe ich natürlich vor allem meinen Eltern zu danken: Studium, Promotion und vieles andere in meinem Leben wäre ohne ihre Unterstützung nicht möglich gewesen.

Ich danke außerdem allen anderen, die mich während meines Studiums und meiner langen Promotionsphase unterstützt haben, sei es aus dem Familien-, Freundes- oder Kollegenkreis, sei es fachbezogen oder in privaten Angelegenheiten, sei es direkt oder indirekt, mittelbar oder unmittelbar, wissentlich oder unwissentlich.

Bochum, im November 2021 Christian Rühs

Inhaltsverzeichnis

Einleitung

A. Einführung

Die vorliegende Arbeit untersucht die strafverfahrensrechtlichen Vorschriften zur Durchsicht aus § 110 Abs. 1 und Abs. 3 StPO darauf, inwieweit sie in ihrer jetzigen Gestalt geeignete Rechtsgrundlagen für die Durchsicht informationstechnischer Systeme sind. § 110 Abs. 1 StPO ermächtigt die Strafverfolgungsbehörden im Rahmen einer strafprozessualen Durchsuchung allgemein zur Durchsicht von „Papieren", gemäß § 110 Abs. 3 S. 1 StPO ist auch die Durchsicht von „elektronischen Speichermedien" zulässig, worunter lokale informationstechnische Systeme wie PCs, Laptops und Smartphones bzw. deren Datenträger und die in ihnen gespeicherten elektronischen Daten fallen. § 110 Abs. 3 S. 2 StPO erweitert diese Befugnis speziell auf „räumlich getrennte Speichermedien", also auf externe informationstechnische Systeme wie zum Beispiel über das Internet angeschlossene Fileserver und Cloud-Speicher.

Die Untersuchung konzentriert sich vorrangig auf die Frage, ob § 110 Abs. 3 StPO die massiven Grundrechtseingriffe, die mit einer Durchsicht informationstechnischer Systeme einhergehen, hinreichend einhegen und begrenzen. Im Vordergrund steht dabei die Auswertung der verfassungsgerichtlichen Rechtsprechung zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht). In den einzelnen Untersuchungsschritten werden die verfassungsrechtlichen, aber auch einfachrechtlichen und ermittlungspraktischen Probleme der Durchsicht informationstechnischer Systeme herausgearbeitet. Hieraus werden Erkenntnisse zum gesetzlichen Reformbedarf der Rechtsgrundlagen zur Durchsicht informationstechnischer Systeme gewonnen.

I. Die konkreten Fragestellungen dieser Arbeit

1. Übergeordnete Fragestellungen

Das oben geschilderte Untersuchungsinteresse lässt sich durch die folgenden Fragestellungen weiter präzisieren:

1. Sind die Durchsuchungsvorschriften der §§ 102 ff. StPO, zu denen die Vorschriften zur Durchsicht gemäß § 110 StPO in systematischer Hinsicht

gehören, angesichts ihres Zuschnitts auf Gegebenheiten des physisch-realen Raums in der Lage, den neuartigen Formen der elektronischen Datenspeicherung und Datenverarbeitung im virtuellen Raum angemessen zu begegnen? Sind sie in der Lage, die dadurch bedingten neuartigen Ermittlungsmethoden hinreichend einzuhegen und zu begrenzen?

2. Wie wirkt sich die jüngere verfassungsgerichtliche Rechtsprechung zu modernen technikgestützten Maßnahmen wie der Online-Durchsuchung auf die vergleichbare Maßnahme der Durchsicht informationstechnischer Systeme gemäß § 110 Abs. 3 StPO aus? Sind auch Maßnahmen auf Grundlage des § 110 Abs. 3 StPO an den diesbezüglichen Vorgaben des Bundesverfassungsgerichts zu messen? Wenn ja, genügt § 110 Abs. 3 StPO diesen Vorgaben? Und inwieweit ist die Durchsicht informationstechnischer Systeme, insbesondere nach § 110 Abs. 3 S. 2 StPO, mit einer Online-Durchsuchung im Sinne des § 100b StPO vergleichbar?

3. Inwieweit müssen die Vorschriften zur Durchsicht nach § 110 StPO reformiert und ergänzt werden, damit die Durchsicht informationstechnischer Systeme auf taugliche, d. h. insbesondere verfassungskonforme Rechtsgrundlagen gestützt werden kann?

2. Einzelfragen im Überblick

Aus den oben geschilderten übergeordneten Fragestellungen leiten sich unter anderem folgende Einzelfragen ab, die im Laufe der folgenden Untersuchung aufgeworfen und nach Möglichkeit beantwortet werden sollen:

1. Erlaubt § 110 Abs. 3 S. 2 StPO auch den heimlichen Zugriff auf informationstechnische Systeme Dritter? Werden dadurch die in § 100b StPO für heimliche Online-Durchsuchungen normierten Hürden umgangen?

2. Schützt das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht) auch vor offen durchgeführten Durchsichten informationstechnischer Systeme, greift also eine Durchsicht informationstechnischer Systeme gemäß § 110 Abs. 3 StPO in das IT-Grundrecht ein?

3. Wie tiefgreifend sind die Grundrechtseingriffe bei einer Durchsicht informationstechnischer Systeme? Nach welchen Kriterien ist die Eingriffsintensität einer Durchsicht informationstechnischer Systeme im Einzelfall zu bewerten?

4. Kann eine Durchsicht informationstechnischer Systeme in ihrer praktischen Durchführung überhaupt zuverlässig auf verfahrensrelevante Daten begrenzt werden? Können und müssen Strafverfolgungsbehöden Alternativen zur Komplettdurchsicht eines informationstechnischen Systems ergreifen?

5. Inwieweit läuft eine Durchsicht informationstechnischer Systeme Gefahr, den unantastbaren Kernbereich der privaten Lebensgestaltung zu be-

rühren und damit die Menschenwürde aus Art. 1 Abs. 1 GG zu verletzen? Bedarf es für Maßnahmen nach § 110 Abs. 3 StPO eines eigenen gesetzlichen Kernbereichsschutzkonzepts? Können oder müssen die Schutzvorschriften aus § 100d Abs. 1 bis Abs. 3 StPO de lege ferenda oder sogar bereits de lege lata auf die Durchsicht informationstechnischer Systeme übertragen werden?

6. Kommt es bei einer (Komplett-)Durchsicht eines informationstechnischen Systems in vielen Fällen nicht zwangsläufig zur Bildung eines vollständigen Persönlichkeitsprofils des Systeminhabers, mit der Folge einer Verletzung der Menschenwürde aus Art. 1 Abs. 1 GG?

7. Kann vermieden werden, dass die Durchsicht eines informationstechnischen Systems und aller in ihm gespeicherten Daten zu einer unzulässigen systematischen Suche nach Zufallsfunden (*fishing expedition*) gerät?

8. Auf welche Speichermedien darf über § 110 Abs. 3 S. 2 StPO zugegriffen werden? Zählen dazu auch E-Mail-Konten? Wie sind hierbei Eingriffe in nach Art. 10 GG geschützte Kommunikationsdaten einerseits von Eingriffen in nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG geschützte nicht kommunikationsbezogene Datenbestände andererseits zu unterscheiden? In welchem Verhältnis stehen hierbei Fernmeldegeheimnis und IT-Grundrecht?

9. Dürfen Strafverfolgungsbehörden bei einem Zugriff gemäß § 110 Abs. 3 S. 2 StPO auch Hacking-Software zur Überwindung von Passwortsperren einsetzen?

10. Ermächtigt § 110 Abs. 3 S. 2 StPO zu Zugriffen auf im Ausland gespeicherte Daten (*transborder searches*)?

11. Werden bei einem Zugriff über § 110 Abs. 3 S. 2 StPO die Grundrechte unbeteiligter Dritte, insbesondere von Mitinhabern externer informationstechnischer Systeme, hinreichend geschützt?

12. Unter Berücksichtigung der obenstehenden Fragen: Inwiefern unterscheidet sich die Durchsicht externer informationstechnischer Systeme gemäß § 110 Abs. 3 S. 2 StPO in ihren Eingriffswirkungen überhaupt von einer Online-Durchsuchung im Sinne des § 100b StPO? Können oder müssen die in § 100b StPO normierten rechtlichen Hürden de lege ferenda oder sogar bereits de lege lata auf Maßnahmen nach § 110 Abs. 3 S. 2 StPO übertragen werden?

3. Nicht beantwortete Fragen / Grenzen der Untersuchung

Nicht alle der oben vorgestellten Fragen können in dieser Arbeit erschöpfend beantwortet werden. Manche Fragen und Probleme werden hier zudem gar nicht untersucht.

Insbesondere liefert die vorliegende Arbeit keine umfassende Untersuchung zur Frage, ob die Strafprozessordnung insgesamt in ihrer jetzigen Form dazu geeignet ist, den Umgang mit elektronisch gespeicherten Daten

im Ermittlungsverfahren hinreichend und in angemessener Weise zu regeln. Der Fokus der Untersuchung liegt auf der Durchsicht informationstechnischer Systeme gemäß § 110 Abs. 3 StPO. Überlegungen zur Reform anderer Rechtsgrundlagen oder gar einer Gesamtreform der StPO finden in der vorliegenden Arbeit nicht statt.[1]

Verfassungsrechtliche Fragen zum Umgang mit elektronisch gespeicherten Daten werden ebenfalls nur in Bezug zu § 110 Abs. 1 und Abs. 3 StPO behandelt. Die vorliegende Arbeit bezieht das einschlägige Verfassungsrecht zwar notwendigerweise in die Untersuchung ein und behandelt Inhalt und Grenzen des IT-Grundrechts, des Rechts auf informationelle Selbstbestimmung, des Fernmeldegeheimnisses und anderer Grundrechte und bearbeitet auch grundrechtsübergreifende Themen wie den Schutz des Kernbereichs privater Lebensgestaltung; dies aber nur so weit, wie es für den Untersuchungsgegenstand relevant ist. Eine umfassende Untersuchung zu den genannten Grundrechten oder zu anderen verfassungsrechtlichen Fragen leistet diese Arbeit nicht. Trotz starker verfassungsrechtlicher Bezüge ist die vorliegende Arbeit eine strafprozessrechtswissenschaftliche Untersuchung.

Auch Fragen des ermittlungspraktischen und technischen Umgangs mit elektronisch gespeicherten Daten werden hier nur so weit aufgeworfen und beantwortet, wie sie zur Untersuchung der Vorschriften zur Durchsicht informationstechnischer Systeme gemäß § 110 Abs. 3 StPO relevant sind. Erkenntnisse und Problemlagen aus dem Gebiet der IT-Forensik werden hier nur zur Illustration von Rechtsproblemen dargestellt. Eine vertiefte Auseinandersetzung mit Methoden der IT-Forensik ist damit nicht Bestandteil der vorliegenden rechtswissenschaftlichen Arbeit.

II. Methodik der Untersuchung

Ausgangspunkt der Untersuchung sind § 110 Abs. 1 und Abs. 3 StPO, also Vorschriften aus dem Strafprozessrecht. Neben allgemeiner Literatur zum strafrechtlichen Ermittlungsverfahren (z. B. zu den §§ 94 ff. und §§ 102 ff. StPO) wertet diese Arbeit vorrangig Literatur zu den technik- und datengestützten Zwangseingriffen der Strafprozessordnung aus. Literatur zu speziellen Ermittlungsmaßnahmen wie insbesondere der Online-Durchsuchung wird hierbei ebenso herangezogen wie überblicksmäßige Literatur zum Umgang mit elektronisch gespeicherten Daten im Ermittlungsverfahren. Auch die einschlägige strafgerichtliche Rechtsprechung wird ebenso wie die Rechtsprechung des Bundesverfassungsgerichts ausgewertet, soweit sie Zugriffe

[1] Ausführlich zum Reformbedarf *Sieber*, Gutachten zum 69. Deutschen Juristentag, C 9 ff. mit einzelnen Vorschlägen auf S. C 155 f.; vgl. auch den Überblick bei *Vogel*, ZIS 2012, 480 ff.

auf elektronisch gespeicherte Daten im Ermittlungsverfahren betrifft. Die Untersuchung blickt auch über die Normen der StPO hinaus und bezieht die Convention on Cybercrime als maßgeblichen völkerrechtlichen Vertrag zum Umgang der Strafverfolgungsbehörden mit elektronisch gespeicherten Daten ein, insbesondere hinsichtlich § 110 Abs. 3 S. 2 StPO.

Zur Klärung der verfassungsrechtlichen Fragen wertet diese Arbeit vorrangig die Rechtsprechung des Bundesverfassungsgerichts aus, insbesondere die Urteile zur Online-Durchsuchung[2] und zum Bundeskriminalamtsgesetz[3], aber auch die Entscheidungen zur Beschlagnahme von Daten aus lokalen Datenträgern[4] und von E-Mails aus einem E-Mail-Konto[5]. Zentral ist hierbei die Übertragung der in diesen Entscheidungen getroffenen Aussagen auf die Durchsicht informationstechnischer Systeme gemäß § 110 Abs. 3 StPO. Hinzu tritt die Auswertung verfassungsrechtlicher Literatur, insbesondere zu Grundrechtsfragen, aber auch zu grundrechtsübergreifenden Themen wie z. B. dem Schutz des Kernbereichs privater Lebensgestaltung.

Die Durchsicht informationstechnischer Systeme ist eine technikgestützte Ermittlungsmaßnahme. Folglich werden zur Illustration und Klärung der Rechtsfragen immer auch technische Sachverhalte dargestellt. Zur Erklärung der technischen Vorgänge wird ergänzend auf entsprechende Literatur aus dem Bereich der IT-Forensik zurückgegriffen.

B. Staatlicher Zugriff auf elektronisch gespeicherte Daten vor dem Hintergrund zweier Grundsatzurteile des BVerfG

Bereits 1983 erkannte das *BVerfG* in seinem Urteil zur Volkszählung[6], dass staatliche Sammlungen von personenbezogenen Daten die freie Entfaltung der Persönlichkeit hemmen und gefährden können. In Reaktion auf die gestiegene Bedeutung der elektronischen Datenverarbeitung sowohl für die Staatsverwaltung als auch für die gesamte Gesellschaft formulierte das *BVerfG* das Recht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG. Hiermit wollte das *BVerfG* auf grundrechtlicher Ebene den „Gefahren der automatischen Datenverarbeitung“[7] begegnen, die nach Auffassung des Gerichts daraus resultierten, dass „personenbezogene Daten […] technisch ge-

---

[2] BVerfGE 120, 274 („Online-Durchsuchung“).
[3] BVerfGE 141, 220 („Bundeskriminalamtsgesetz“).
[4] BVerfGE 113, 29 („Anwaltsdaten“).
[5] BVerfGE 124, 43 („E-Mail-Beschluss“).
[6] BVerfGE 65, 1.
[7] BVerfGE 65, 1 (46).

sehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entferungen in Sekundenschnelle abrufbar“[8] seien. Bei Formulierung des Rechts auf informationelle Selbstbestimmung hatte das *BVerfG* aber noch nicht so moderne Technologien wie das Cloud Computing[9] im Blick. Anlass zur Entwicklung des informationellen Selbstbestimmungsrechts war vielmehr eine geplante Volkszählung, bei der die Bürger mittels Erhebungsbögen in Papierform dazu aufgefordert waren, einzelne statistisch verwertbare Daten über ihr Leben preiszugeben, z. B. zu Alter, Familienstand und Wohnverhältnissen, Ausbildung und Berufstätigkeit oder auch Staatsangehörigkeit und Religionszugehörigkeit.[10] Die hierbei erhobenen Daten waren in ihrer Vielfalt und Menge vergleichsweise überschaubar und auf bestimmte Themengebiete begrenzt. Zudem behielt jeder einzelne Bürger bei der Befragung zumindest teilweise die faktische Kontrolle darüber, welche Daten erhoben werden: Die Bürger waren zwar rechtlich zur wahrheitsgemäßen Auskunft über die eigenen Lebensdaten verpflichtet, faktisch aber konnten sie bei der Befragung Informationen zurückhalten oder schlicht lügen.

Aus heutiger Sicht wirkt die damals geplante Volkszählung samt anschließender staatlicher Datenverarbeitung, die das *BVerfG* zur Formulierung eines Grundsatzurteils veranlasste, vergleichsweise harmlos. Inzwischen hat sich nicht nur die Menge der durch den Staat potentiell nutzbaren Daten drastisch vergrößert, sondern auch ihre Qualität und ihre Aussagekraft. Während sich das *BVerfG* im Volkszählungsurteil vorrangig um den Schutz personenbezogener Daten sorgte, die einzeln und begrenzt beim Bürger abgefragt wurden, stehen den Behörden heutzutage umfangreiche Datenbestände zur Verfügung, die nicht aus einzelnen Befragungen stammen, sondern von den Bürgern selbst im Alltag massenweise produziert und bevorratet werden. Mit der weiten Verbreitung von Computern, Laptops und Smartphones im privaten Lebensbereich, dem nicht mehr hinwegzudenkenden und geradezu allgegenwärtigen Internet[11] und der fortschreitenden Vernetzung und Speicherung von Daten in einer Vielzahl von informationstechnischen Systemen spiegelt sich potentiell der gesamte Alltag des Bürgers auch in elektronischen Daten wider. Das private und soziale Leben wird längst

---

[8] BVerfGE 65, 1 (42).

[9] „Cloud Computing“ bezeichnet die Speicherung von Daten oder die Nutzung von Diensten über das Internet oder andere Netzwerke, wobei die tatsächliche physische Hardware auf der ganzen Welt verteilt sein kann und durch Vernetzung dem Nutzer flexibel und virtuell als Einheit zur Verfügung gestellt wird. Dazu noch ausführlich unter Kap. 3 A.I.2.a) dieser Arbeit.

[10] Siehe zum damaligen Volkszählungsgesetz BVerfGE 65, 1 (4 ff.).

[11] Im Jahr 2019 waren 91 % aller deutschen Haushalte mit einem Internetanschluss samt passendem Gerät (Computer, auch Smartphone) ausgestattet; siehe *Statistisches Bundesamt*, Fachserie 15, Reihe 4, IKT 2019, Tabelle H1, S. 9.

nicht mehr nur im physisch-realen Raum, sondern auch im „virtuellen Raum“[12] gelebt und hinterlässt entsprechende Datenspuren. Diese vom Bürger selbst und geradezu beiläufig auf ihren technischen Geräten und Speichern im Netz erzeugten Daten dienen einerseits der eigenen Persönlichkeitsentfaltung und -darstellung.[13] Andererseits sind sie auch für den Staat interessant, insbesondere für die Sicherheits- und Strafverfolgungsbehörden, welche diese Datenbestände zur Aufklärung von Straftaten und gleichermaßen zur Ausforschung der Bürger benutzen können. Die vom Bürger selbst auf seinen Computersystemen angehäuften Datensammlungen können somit auch zur Gefahr für die ungehemmte Persönlichkeitsentfaltung werden.[14] Ein einziger Zugriff auf den Datenbestand eines privat genutzten Computers kann umfassende und tiefgreifende Einblicke in die Privatsphäre des Bürgers liefern, ohne dass dieser dabei noch zuverlässig steuern und kontrollieren könnte, welche einzelnen Daten zur Kenntnis der Strafverfolgungsbehörden gelangen.[15] Der Nutzer kann in diesem Augenblick keine einzelnen Daten mehr zurückhalten, und er hat auch keine Möglichkeit zur Lüge mehr. Die staatlichen Behörden müssen den Bürger hierbei nicht mehr nach bestimmten Informationen ausfragen. Vielmehr erzeugt der Bürger durch die alltägliche Nutzung der modernen Informationstechnik einen Datenpool, den die Behörden bei Gelegenheit nur noch abzuschöpfen brauchen.[16] Der Staat hat damit potentiell Zugriff auf das in elektronischer Form „ausgelagerte Gehirn“[17] des Bürgers. Unter diesen gewandelten Voraussetzungen und um diesen neuartigen Gefährdungen für die Privatsphäre des Einzelnen zu begegnen, schuf das *BVerfG* im Jahr 2008 in seinem Urteil zur Online-Durchsuchung eine weitere Ausprägung des allgemeinen Persönlichkeitsrechts: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (auch IT-Grundrecht genannt).[18] Das *BVerfG* sah hierbei die Notwendigkeit, den Bürger nicht nur vor einzelnen Erhebungen personenbezogener Daten aus beliebigen Quellen zu schützen, sondern

---

[12] Zu diesem Begriff s. noch Kapitel 1 dieser Arbeit.

[13] BVerfGE 120, 274 (304).

[14] BVerfGE 120, 274 (305 f.).

[15] BVerfGE 120, 274 (313).

[16] Vgl. BVerfGE 120, 274 (313); *Basar*, FS Wessing 2015, 635 (639 – Fn. 22); *Hauser*, IT-Grundrecht, 2015, S. 69.

[17] So formuliert von *Burkhard Hirsch*, s. Der Spiegel 6/2007, S. 18, abrufbar unter http://magazin.spiegel.de/EpubDelivery/spiegel/pdf/50424594 [zuletzt abgerufen am 04.11.2021]. Zuweilen wird dieser Ausspruch auch *Winfried Hassemer* zugeschrieben, siehe *Prantl*, Süddeutsche.de vom 22. Juni 2017, abrufbar unter http://www.sueddeutsche.de/digital/ueberwachung-der-staatstrojaner-ist-ein-einbruch-ins-grundgesetz-1.3555917 [zuletzt abgerufen am 04.11.2021]; *Hoffmann-Riem*, JZ 2008, 1009 (1012 – Fn. 22) zitiert *Hassemer* dagegen mit dem Ausspruch: „Der Computer ist ein ausgelagerter Teil des Körpers.“

[18] BVerfGE 120, 274.

auch und gerade die vom Bürger genutzten Computer und Datenspeicher als persönliche virtuelle Schutzräume anzuerkennen.[19]

Allein anhand der beiden maßgeblichen Grundsatzurteile des *BVerfG* zum grundrechtlichen Datenschutz lässt sich einerseits der technische und gesellschaftliche Fortschritt bei der elektronischen Datenverarbeitung und -nutzung erkennen. Andererseits illustrieren die Urteile die damals wie heute bestehende Notwendigkeit, auf diese technischen Möglichkeiten auch in rechtlicher Hinsicht zu reagieren. Diese Notwendigkeit lässt sich dabei zum einen aus grundrechtlicher Perspektive, also aus Perspektive des Bürgers formulieren: Da immer mehr Menschen immer mehr Daten mit Persönlichkeitsbezug mittels elektronischer Geräte erzeugen, verbreiten, speichern, vernetzen und nutzen, muss die Privatsphäre dieser Nutzer rechtlichen Schutz vor den daraus entstehenden Gefährdungen genießen. Zum anderen lässt sich die Notwendigkeit, auf technische Entwicklungen mit Mitteln des Rechts zu reagieren, aus Perspektive der Sicherheits- und Strafverfolgungsbehörden und damit aus der Perspektive des Polizeirechts im weitesten Sinne sowie des Strafprozessrechts bestimmen: Gerade weil immer mehr Menschen weite Teile ihres Lebens in den sogenannten virtuellen Raum verlagern und dort elektronische Daten ablegen, die Auskunft über Lebensverhältnisse und Persönlichkeit geben, besteht bei polizeirechtlichen wie strafprozessualen Ermittlungen das Bedürfnis, auf eben diese elektronischen Daten zuzugreifen[20] – was aus Perspektive des Bürgers wiederum als neuartige Gefährdung seiner Privatsphäre beschrieben werden kann, der mittels angepasstem Grundrechtsschutz begegnet werden muss.

C. § 110 Abs. 3 StPO als Reaktion auf neue Formen der EDV

Will man dem Bedürfnis nachkommen, den neuartigen Formen der elektronischen Datenspeicherung und Datenverarbeitung mit ebenso neuartigen Ermittlungsmethoden zu begegnen, so ist dies – zumindest in rechtlicher Hinsicht – mit passenden Rechtsgrundlagen zu tun.[21] Im Strafprozessrecht

---

[19] Vgl. nur BVerfGE 120, 274 (312 f.).

[20] *Bäcker*, Kriminalpräventionsrecht, 2015, S. 64 ff.; *Bär*, Zugriff auf Computerdaten, 1992, S. 1 ff., 455; *Beulke/Meininghaus*, FS Widmaier 2008, 63; *Denkowski*, Kriminalistik 2007, 177, 180; *Hiéramente/Pfister*, StV 2017, 477 f.; *Hofmann*, NStZ 2005, 121; *Korge*, Beschlagnahme elektronisch gespeicherter Daten, 2009, S. 1 f.; *Vogel*, ZIS 2012, 480 (481 f.).

[21] Damit ist nicht gemeint, dass einem solchen Bedürfnis auch immer entsprochen werden muss oder sollte, was zum Beispiel *Beulke/Meininghaus*, FS Widmaier 2008, 63 (71 f.) vor allem bezüglich heimlicher Online-Durchsuchungen treffend in Frage stellen und schließlich verneinen.

sind dies vor allem die Eingriffsgrundlagen zu Eingriffen in die persönliche Sphäre des Beschuldigten während des Ermittlungsverfahrens. Dazu gehören auch die Vorschriften über Durchsuchungen (§§ 102 ff. StPO) sowie über Sicherstellung und Beschlagnahme (§§ 94 ff. StPO). Diese Vorschriften aber sind seit der Urfassung der Strafprozessordnung aus dem Jahre 1877 weitgehend unverändert und somit auch weitgehend unbeeindruckt von den modernen Entwicklungen der Informationstechnik geblieben.[22] Bisher wurde zumeist versucht, neu aufkommende technologiegestützte Ermittlungsmethoden unter bereits bestehende Eingriffsnormen zu subsumieren.[23] Das ist zum Beispiel lange Zeit hinsichtlich des Zugriffs auf elektronisch gespeicherte Daten so geschehen. Allein aufgrund ihres Alters sind die §§ 94 ff. StPO sowie die §§ 102 ff. StPO vom Gesetzgeber nicht auf Anwendungsfälle wie das Sichten und Kopieren von elektronischen Daten einer Festplatte oder das Herunterladen von Dateien von einem Internetserver zugeschnitten,[24] mag es mit § 110 Abs. 3 S. 1 und S. 2 StPO mittlerweile auch ausdrückliche Rechtsgrundlagen zur Sichtung elektronischer Speichermedien geben, die aber weiterhin nur in das überkommene und ansonsten weitgehend unveränderte Regelungsgefüge der Durchsuchungs- und Beschlagnahmevorschriften eingefügt worden sind. Die Rechtsprechung wandte die §§ 94 ff. und § 102 ff. StPO schon früher – teils mit Billigung, teils mit Kritik aus dem rechtswissenschaftlichen Schrifttum – in ihrer unveränderten Gestalt an, um Zugriffe der Ermittler auf elektronisch gespeicherte Daten zu legitimieren.[25] Ein weitergehendes, noch nicht lange zurückliegendes Beispiel dafür ist eine Entscheidung des *BVerfG*, nach der die §§ 94 ff. StPO taugliche Rechtsgrundlage zum Kopieren von E-Mails von einem Internetserver sein sollen.[26] Das aber ist eine Ermittlungsmethode, die 1877 bei Verkündung der StPO[27] höchstwahrscheinlich nicht einmal in der Fantasie des Gesetzgebers Platz hatte, geschweige denn bei den Beratungen zur damaligen Gesetzgebung berücksichtigt wurde.

---

[22] BVerfGE 113, 29; zu dieser Einschätzung schon *Bär*, Zugriff auf Computerdaten, 1992, S. 3; *ders.*, in: Wabnitz/Janovsky (Hrsg.), Handbuch Wirtschafts- und Steuerstrafrecht, Kap. 28 Rn. 6; *Kudlich*, JA 2000, 227 (228) und *Matzky*, Zugriff auf EDV im Strafprozeß, 1999, S. 3; aus neuerer Zeit *Ludewig*, KriPoZ 2019, 293 (296); *Schilling/Rudolph/Kuntze*, HRRS 2013, 207 (209); *Zerbes/El-Ghazi*, NStZ 2015, 425; *Zimmermann*, JA 2014, 321.

[23] Vgl. zu diesem Vorgehen – auch aus kritischer Sicht – *Bär*, Zugriff auf Computerdaten, 1992, S. 51 ff., 455 ff. und passim; kritisch auch *Roggan*, NJW 2015, 1995 ff.; *Valerius*, Ermittlungen der Strafverfolgungsbehörden, 2004, 26 f.

[24] BVerfGE 113, 29 (32); vgl. dazu auch *Matzky*, Zugriff auf EDV im Strafprozeß, 1999, S. 3 f.; *Roggan*, NJW 2015, 1995 (1996 f.); *Vogel*, ZIS 2012, 480 (482); *von zur Mühlen*, Zugriffe auf elektronische Kommunikation, 2019, S. 427.

[25] Vgl. nur BGH StV 1988, 90; BGH NJW 1997, 1934.

[26] BVerfGE 124, 43 (sog. E-Mail-Beschluss).

[27] RGBl. 1877, S. 253.

Der Rechtsanwender ist allerdings nicht in jedem Fall moderner Ermittlungsmethoden auf die Auslegung bereits bestehender Rechtsgrundlagen verwiesen. Für bestimmte moderne, technikgestützte Ermittlungsmaßnahmen hat der Gesetzgeber im Laufe der Jahre eigene, neue Eingriffsgrundlagen geschaffen. Eine davon ist § 110 Abs. 3 StPO:

§ 110 StPO: Durchsicht von Papieren und elektronischen Speichermedien
[…]
(3) Nach Maßgabe der Absätze 1 und 2 ist auch die Durchsicht von elektronischen Speichermedien bei dem von der Durchsuchung Betroffenen zulässig. Diese Durchsicht darf auch auf hiervon räumlich getrennte Speichermedien erstreckt werden, soweit auf sie von dem elektronischen Speichermedium aus zugegriffen werden kann, wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden.
[…]

§ 110 Abs. 3 StPO wurde zuletzt durch das Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften vom 25. Juni 2021 geändert.[28] § 110 Abs. 3 StPO wurde hierbei in die Sätze 1, 2 und 3 aufgeteilt. Satz 1 regelt die allgemeine Befugnis zur Durchsicht (lokaler) elektronischer Speichermedien erstmals ausdrücklich. Satz 2 enthält nun die Befugnis zur Durchsicht räumlich getrennter Speichermedien, die bereits vorher im ursprünglichen § 110 Abs. 3 S. 1 StPO a. F. aus dem Jahr 2008 enthalten war:

§ 110 StPO a. F. (2008)
[…]
(3) Die Durchsicht eines elektronischen Speichermediums bei dem von der Durchsuchung Betroffenen darf auch auf hiervon räumlich getrennte Speichermedien, soweit auf sie von dem Speichermedium aus zugegriffen werden kann, erstreckt werden, wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden; § 98 Abs. 2 gilt entsprechend.

§ 110 Abs. 3 StPO a. F. wurde zum Jahr 2008 im Zuge des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ neu in die StPO eingefügt.[29] Dies diente auch der Umsetzung des von Deutschland ratifizierten Übereinkommens über Computerkriminalität des Europarats („Convention on Cybercrime“, „Cybercrime Convention“)[30], namentlich der Umsetzung dessen Art. 19 Abs. 2.[31] In systematischer Hinsicht ist die

[28] BGBl. 2021 I, S. 2099 ff.
[29] BGBl. 2007 I, S. 3198 ff.
[30] In deutscher Übersetzung abrufbar unter http://conventions.coe.int/Treaty/GER/Treaties/Html/185.htm [zuletzt abgerufen am 04.11.2021].
[31] Art. 19 Abs. 2 des Übereinkommens über Computerkriminalität lautet in deutscher Sprache: „Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass ihre Behörden, wenn sie ein bestimmtes Computer-

Sachregister