BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 1
Januar 2024

Reformvorschläge für das Strafrecht und den Strafprozess angesichts der Digitalisierung

Vorschläge der Bundesrechtsanwaltskammer erarbeitet vom Ausschuss Strafprozessrecht

Mitglieder des Ausschusses Strafprozessrecht:

Rechtsanwalt Dr. Matthias Dann
Rechtsanwalt Prof. Dr. Michael Gubitz
Rechtsanwältin Dr. Vera Hofmann
Rechtsanwalt Prof. Dr. Christoph Knauer, Vorsitzender
Rechtsanwalt Dr. jur. Andreas Minkoff
Rechtsanwalt Maximilian Müller, LL.M.
Rechtsanwalt Jürgen Pauly
Rechtsanwältin Anette Scharfenberg
Rechtsanwältin Dr. Alexandra Schmitz
Rechtsanwältin Stefanie Schott
Rechtsanwalt Prof. Dr. Gerson Trüg

Rechtsanwältin Leonora Holling, Schatzmeisterin Bundesrechtsanwaltskammer
Rechtsanwältin Eva Melina Buchmann, Bundesrechtsanwaltskammer

Verteiler: Bundesministerium der Justiz
Bundesministeriums des Innern, für Bau und Heimat
Ausschuss für Recht- und Verbraucherschutz des Deutschen Bundestages
Ausschuss für Inneres und Heimat des Deutschen Bundestag
Fraktionsvorsitzende der CDU/CSU, SPD, BÜNDNIS 90/DIE GRÜNEN, DIE LINKE
Rechtspolitischen Sprecher der Fraktionen CDU/CSU, SPD, BÜNDNIS 90/DIE GRÜNEN, DIE LINKE
Arbeitskreise Recht der Bundestagsfraktionen
Landesjustizminister/Justizsenatoren der Länder
Innenministerien und Senatsverwaltungen für Inneres der Länder
Bundesgerichtshof
Rechtsanwaltskammern
Bundesverband der Freien Berufe
Bundesnotarkammer
Bundessteuerberaterkammer
Patentanwaltskammer
Deutscher Anwaltverein
Deutscher Juristinnenbund
Deutscher Notarverein
Deutscher Richterbund
Neue Richtervereinigung e.V.
Deutscher Steuerberaterverband e. V.
Wirtschaftsprüferkammer
Institut der Wirtschaftsprüfer in Deutschland e.V.
Bund Deutscher Kriminalbeamter
Verbraucherzentrale Bundesverband e.V.
Deutscher Juristentag e.V.
Redaktionen der NJW, NStZ, NZWiSt, Beck Verlag, ZAP, AnwBl, DRiZ, FamRZ, FAZ, Süddeutsche Zeitung, Die Welt, taz, Handelsblatt, dpa, Spiegel, Focus, Deubner Verlag Online Recht, LTO, Beck aktuell, Jurion, Juris Nachrichten, Juve, LexisNexis Rechtsnews, Otto Schmidt Verlag, Kriminalpolitische Zeitschrift, Strafverteidiger Forum, Zeitschrift HRR Strafrecht

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten[1] gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Inhaltsverzeichnis

[1] Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die im Folgenden gewählte männliche Form schließt alle Geschlechter gleichberechtigt ein.

I. Zielrichtung der Reform und Voraussetzungen

Ein zukunftssicherer Rechtsstaat ist ein digitaler Rechtsstaat.[2] Daher begrüßt die BRAK die Diskussionen zur Digitalisierung der Justiz und die Bereitschaft aller Beteiligten, die in Deutschland bereits umgesetzten Digitalisierungsschritte weiter voranzutreiben. Das mit der Digitalisierung verbundene Potential muss dafür genutzt werden, den Zugang zum Recht für alle gleichermaßen zu sichern und zu stärken.[3] Bereits jetzt stellen sich praktische Herausforderungen, da Informationen vermehrt und teilweise nur noch digital verfügbar sind und nicht nur die zu verarbeitenden Datenmengen, sondern auch die technischen Möglichkeiten exponentiell zugenommen haben.

Trotz einiger punktueller Anpassungen wird die StPO den veränderten Rahmenbedingungen derzeit noch nicht annähernd gerecht.[4] Es bestehen gesetzliche Unsicherheiten im Umgang mit Daten, die etwa die Akteneinsicht und die Datensicherheit und -vollständigkeit betreffen. Gleichzeitig bleiben Potentiale ungenutzt – nicht nur, aber gerade bei dem Einsatz von Audio- und Videotechnik. Zudem ist die Dauer erstinstanzlicher Strafverfahren vor den Landgerichten im vergangenen Jahr nach Daten des Statistischen Bundesamtes auf einen neuen Höchstwert von durchschnittlich 8,2 Monaten gestiegen[5] – wofür neben fehlendem Personal der Anstieg der Datenmengen als Grund angegeben wird.[6] Dies ist insbesondere im Hinblick auf das aus dem Rechtsstaatsprinzip abgeleitete Beschleunigungsgebot[7] kritisch zu sehen. Es muss eine Strategie erarbeitet werden, die einen effektiven, aber auch verantwortungsbewussten Umgang mit technischen Möglichkeiten und Datenmengen sicherstellt, dabei aber auch einen effektiven Grundrechtsschutz garantiert.

Dennoch ist Digitalisierung insbesondere im Strafverfahren dort mit Vorsicht zu begegnen, wo die Persönlichkeit und der persönliche Eindruck der Verfahrensbeteiligten regelmäßig sehr viel mehr Gewicht haben als etwa im Zivilprozess. Daher sind die Verfahrensgrundsätze des Strafprozesses auch bei Reformbemühungen zwingend zu beachten. Insbesondere die Grundsätze der Mündlichkeit, der Öffentlichkeit und der Unmittelbarkeit stehen mit der fortschreitenden Digitalisierung in einem Spannungsverhältnis.[8] Es verbietet sich aufgrund des Unmittelbarkeitsgrundsatzes insbesondere, eine strafrechtliche Hauptverhandlung rein digital durchzuführen.[9] Auch darf eine Videoaufzeichnung nicht dazu führen, dass bei dauerhaftem Ausfall eines Mitglieds des Gerichts die Hauptverhandlung unter Benennung eines neuen Richters oder Schöffen fortgesetzt wird, welcher sich lediglich die Aufzeichnungen der vorangegangenen Sitzungstage ansieht.[10] Die Digitalisierung des Strafverfahrens und eine entsprechende Änderung der StPO finden damit ihre Grenze in den verfassungs- und strafrechtlichen Verfahrensgrundsätzen.

Sämtlichen technischen Möglichkeiten im Strafverfahren ist abseits der Frage ihrer rechtlichen Zulässigkeit gemein, dass ihre praktische Umsetzung im Hinblick auf den Gleichheitsgrundsatz, das Gebot der Waffengleichheit und den Beschleunigungsgrundsatz nur bei der Verwendung möglichst effizienter und miteinander kompatibler Technologien und der Durchführung entsprechender Schulungen für sämtliche Nutzer verfahrenssicher erscheint. Um die Vorteile digitaler Technologien tatsächlich nutzbar zu machen, bedarf es einer leistungsfähigen, flächendeckenden digitalen Infrastruktur.[11] Zudem muss gewährleistet sein, dass alle Bürgerinnen und Bürger digitale Angebote der Justiz IT-sicher und datenschutzkonform nutzen können. Gleichzeitig müssen digitale Lösungen auch unmittelbar durch die Anwaltschaft für ihre Mandanten nutzbar sein.[12]

---

[2] BRAK-Stellungnahme Nr. 84/2020, 9 – Positionspapier „Rechtsstaat 2.1 – krisensicher durch die Epidemie und in die Zukunft“.
[3] Presseerklärung Nr. 12 der BRAK vom 27.09.2021: Digitalpakt, Zugang zum Recht und RVG-Anpassung.
[4] Knauer, BRAK-Mitt. 2022, 244.
[5] Statistisches Bundesamt, Fachserie 10, Reihe 2.3, 2021, S. 78.
[6] *Rebehn*, Neue Stellen, bessere Besoldung und mehr Tempo bei der Digitalisierung, DRiZ 2022, 286.
[7] BGH, Urt. v. 24.09.1974 – 1 StR 365/74; BGHSt 26, 1, 4; BVerfG, Beschl. v. 06.06.2001 - 2 BvR 828/01, NStZ 2001, 502 mwN.
[8] Knauer, BRAK-Mitt. 2022, 244.
[9] Knauer, BRAK-Mitt. 2022, 244; vgl. hierzu: BRAK-Stellungnahme Nr. 56/2020, 5 – Positionspapier „Rechtsstaat 2.0 – stark & zukunftssicher. Nur ein transparenter Rechtsstaat ist ein starker Rechtsstaat“: *„[...] das Gericht [muss im Strafverfahren] aufgrund seines persönlichen Eindrucks von Angeklagten, Zeugen und zentralen Beweismitteln in der Hauptverhandlung entscheiden [...].“*
[10] Vgl. *Bartl* StV 2018, 678, 684; a.A. *Wehowsky* StV 2018, 685, 688 ff.
[11] BRAK-Stellungnahme Nr. 60/2021, S. 1 f.
[12] BRAK-Stellungnahme Nr. 60/2021, S. 1 f.

Die fortschreitende Digitalisierung führte bereits zu der Normierung der elektronischen Aktenführung im Strafverfahren; diese ist ab dem 01.01.2026 auch in der Strafjustiz obligatorisch. Im Folgenden werden damit einhergehende Herausforderungen dargelegt und konkrete an eine elektronische Aktenführung zu stellende Maßstäbe bestimmt. So muss insbesondere eine einheitliche und vollständige Aktenführung, aus welcher sich Ermittlungs- und Verfahrensablauf in nachvollziehbarer Weise ergeben, gewährleistet werden. Dazu gehört etwa die Möglichkeit der Nachverfolgung nachträglicher Änderungen und Entnahmen von Aktenbestandteilen. Um dem Beschleunigungsgebot gerecht werden zu können, ist es nach Auffassung der BRAK unerlässlich, die vorstehend aufgeführten Bedingungen, welche durchaus als Grundvoraussetzungen für eine effektive elektronische Aktenführung bezeichnet werden können, durch eine entsprechende technische Umsetzung zu erfüllen. Damit auch eine praktische Umsetzung der elektronischen Aktenführung sichergestellt werden kann, ist der Gesetzgeber in der Pflicht, an die elektronische Aktenführung angepasste Regelungen bezüglich der Aktenüberlassung an Mandanten sowie einen Straftatbestand für die Weitergabe von Aktenbestandteilen an Unbefugte zu schaffen. (Hierzu unter **II.)**

Aufgrund der vorerst weiteren Verwendung von Akten in Papierform erscheint es ferner zwingend notwendig, eine Anpassung der Dokumentenpauschale der Nr. 7000 VV RVG vorzunehmen. Nach der derzeitigen Fassung ist lediglich das Fertigen von Kopien und Ausdrucken von Verfahrensakten (in Papierform) abrechnungsfähig. Die Anfertigung von Scans findet hierbei keinerlei Berücksichtigung. Insbesondere angesichts der fortschreitenden Digitalisierung erscheint eine solche Divergenz nicht weiter hinnehmbar, sodass hierzu nachfolgend eine entsprechende Neufassung der Nr. 7000 VV RVG vorgeschlagen wird. (Hierzu unter **II.3.**)

Zudem tritt die BRAK für eine Anpassung des § 110 StPO an die technische Entwicklung ein. Diese ist mittlerweile nahezu fast ausschließlich von Kommunikation per E-Mail und Messengerdiensten und der Datenarchivierung und daher von einem Rückgang der Informationserfassung und -übermittlung in Papierform geprägt. Das hat nicht nur zu einem exponentiellen Anstieg der Kommunikation an sich - und daher auch der verfügbaren Daten geführt – sondern – auch dazu, dass regelmäßig digitale Speichermedien und Kommunikationssysteme im Fokus strafprozessualer Datenerhebungsmaßnahmen stehen.[13] Da die derzeitige Praxis von erheblichen Rechtsunsicherheiten und auch unterschiedlichen Handhabungsweisen geprägt ist, müssen die Regelungen für die Durchsicht vom Gesetzgeber neu austariert werden – im Interesse aller am Strafverfahren Beteiligten. Insofern wird im Rahmen dieser Stellungnahme eine Neufassung des § 110 StPO vorgeschlagen, durch deren Ergänzungen insbesondere der Schutz beschlagnahmefreier Daten wie beispielsweise Verteidigungsunterlagen sowie die Wahrung des Verhältnismäßigkeitsgrundsatzes gestärkt werden sollen. (Hierzu unter **III.1.a.**)

Im Hinblick auf die Hauptverhandlung spricht sich die BRAK, wie in Stellungnahme Nr. 8 aus 2023,[14] Stellungnahme Nr. 23 aus 2023,[15] und Stellungnahme Nr. 63 aus 2023[16] ausgeführt, ausdrücklich für die Einführung einer umfassenden und zeitgemäßen digitalen Dokumentation der Hauptverhandlung in Strafsachen aus.[17] Insbesondere sollten die technischen Möglichkeiten der Videokonferenztechnik auch in der Hauptverhandlung verstärkt genutzt werden.[18] Dabei werden aber auch die rechtlichen Grenzen eines solchen Einsatzes deutlich. Gerade die Grundsätze der Mündlichkeit, der Öffentlichkeit und der Unmittelbarkeit stehen mit der fortschreitenden Digitalisierung in einem Spannungsverhältnis.[19]

[13] Vgl. *Wackernagel/Graßie* NStZ 2021, 12.
[14] Vgl. BRAK-Stellungnahme Nr. 8/2023, S. 3 ff.
[15] Vgl. BRAK-Stellungnahme Nr. 23/2023.
[16] Vgl. BRAK-Stellungnahme Nr. 63/2023.
[17] Zum aktuellen Stand des parlamentarischen Verfahrens: https://www.brak.de/newsroom/newsletter/nachrichten-aus-berlin/nachrichten-aus-berlin-2023/ausgabe-25-2023-v-14122023/dokumentation-im-strafprozess-brak-protestiert-gegen-angekuendigte-laender-blockade-im-bundesrat/ und https://www.brak.de/newsroom/news/digitalisierung-der-justiz-dokumentation-strafgerichtliche-hauptverhandlung-und-128a-zpo-im-bundesrat/
[18] Vgl. BRAK-Stellungnahme Nr. 63/2023.
[19] Knauer, BRAK-Mitt. 2022, 244.

II. Elektronische Aktenführung

Aufgrund des stetigen Fortschritts der Digitalisierung wurde durch das Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs vom 05.07.2017[20] die Möglichkeit der elektronischen Aktenführung normiert. Seither findet sie ihre gesetzliche Grundlage für das Strafverfahren in §§ 32 bis 32f StPO. Bisher müssen seit dem 01.01.2022 gemäß § 32d S. 2 StPO die Berufung und ihre Begründung, die Revision, ihre Begründung und die Gegenerklärung sowie die Privatklage und die Anschlusserklärung bei der Nebenklage als elektronisches Dokument per beA übermittelt werden, allerdings bleibt die flächendeckende Einführung der elektronischen Akte in der gesamten Strafjustiz bis zum 31.12.2025 fakultativ und wird erst ab dem 01.01.2026 obligatorisch.[21] Bis dahin sind wesentliche Fragen bezüglich der Anforderungen an die elektronische Aktenführung und Akteneinsicht zu klären.

Auf Grundlage der Verordnungsermächtigungen in § 32 Abs. 2 und 3, § 32b Abs. 5 und § 32f Abs. 6 StPO wurden bereits sowohl seitens der Bundes- als auch der Landesregierungen diverse Verordnungen erlassen. Auf Bundesebene wurden insoweit für das Strafverfahren in der Bundesstrafaktenführungsverordnung (BStrafAktFV)[22], der Strafaktenübermittlungsverordnung (StrafAktÜbV)[23] und der Strafakteneinsichtsverordnung (StrafAktEinV)[24] Regelungen geschaffen. Seitens der Landesregierungen wurden ebenfalls entsprechende Verordnungen erlassen, welche sich jedoch nur teilweise auf die elektronische Aktenführung im Strafverfahren erstrecken. So beschränken sich die Vorschriften der Länder oftmals auf zivilgerichtliche, familiengerichtliche und fachgerichtliche Verfahren. Soweit Regelungen zur elektronischen Aktenführung im Strafverfahren vorhanden sind, unterscheiden sich diese jedoch auch maßgeblich in ihrer Ausgestaltung, sodass die rechtlichen Vorgaben an die elektronische Aktenführung in Strafverfahren erheblich divergieren. Insofern sollten wesentliche Kriterien bundeseinheitlich geregelt werden, um tragfähige Grundsätze - insbesondere bezüglich Aktenwahrheit und -vollständigkeit - zu gewährleisten.

Dies ist auch vor dem Hintergrund zu sehen, dass über das Akteneinsichtsportal des Bundes und der Länder[25] Gerichte und Staatsanwaltschaften in Deutschland elektronische Akten für die Einsichtnahme online zum Abruf bereitstellen können. Das Akteneinsichtsportal wird in der Praxis bisher bedauerlicherweise nur vereinzelt genutzt. USB-Sticks und Papierakten werden vielfach eingesetzt.

1. Anlage, Erstellung und Führung von elektronischen Akten(bestandteilen)

Mit Blick auf die Anlage, Erstellung und Führung von elektronischen Akten(bestandteilen) haben die Länder hinsichtlich der technischen Rahmenbedingungen einschließlich der einzuhaltenden Anforderungen des Datenschutzes, der Datensicherheit und der Barrierefreiheit (vgl. § 32 Abs. 2 StPO) bereits sich in den Details teilweise deutlich unterscheidende Verordnungen erlassen.[26] Trotz Länder-Regelungen sollten wesentliche Grundsätze der Aktenführung zur Wahrung des Offizialprinzips, des Beschleunigungsgrundsatzes sowie der aus dem Rechtsstaatsprinzip abgeleiteten Grundsätze der

---

[20] BGBl. 2017 I, 2208.

[21] Vgl. Anders/Graalmann-Scheerer/Schady/*Mitterer*, Innovative Entwicklungen in den deutschen Staatsanwaltschaften, 2021, 353.

[22] Vgl. Verordnung über die technischen und organisatorischen Rahmenbedingungen für die elektronische Aktenführung im Strafverfahren (Bundesstrafaktenführungsverordnung - BStrafAktFV) v. 09.12.2019, (BGBl. I S. 2140), die allerdings nur für die Strafverfahrensakten des Bundesgerichtshofs bzw. des GBA beim Bundesgerichtshof sowie spezielle Verfahren der Finanzbehörden gilt (vgl. § 1).

[23] Verordnung über die Standards für die Übermittlung elektronischer Akten zwischen Strafverfolgungsbehörden und Gerichten im Strafverfahren (Strafaktenübermittlungsverordnung - StrafAktÜbV) v. 14.04.2020, BGBl. I S. 799.

[24] Vgl. Verordnung über die Standards für die Einsicht in elektronische Akten im Strafverfahren (Strafakteneinsichtsverordnung – StrafAktEinV) v. 24.02.2020, BGBl. 2020 I, 242.

[25] https://www.akteneinsichtsportal.de/web/guest/start

[26] Vgl. etwa Verordnung zur elektronischen Aktenführung bei den Gerichten und Staatsanwaltschaften im Land Berlin vom 04.05.2021; Bayerische Verordnung über den elektronischen Rechtsverkehr bei den ordentlichen Gerichten vom 15.12.2006, zuletzt geändert am 01.07.2023; Verordnung über die technischen und organisatorischen Rahmenbedingungen für die elektronische Aktenführung im Strafverfahren im Land Nordrhein-Westfalen (eAkten-Verordnung Strafverfahren – eAktVO Straf) vom 01.07.2023.

Aktenwahrheit und -vollständigkeit aufgrund des funktionalen Zusammenhangs mit §§ 32 ff. StPO in einem Bundesgesetz geregelt werden.

Die Staatsanwaltschaft ist bisher – und das muss sie weiterhin bleiben – aktenführende Behörde. Sie hat dafür Sorge zu tragen, dass die Verfahrensakten von Dritten nicht abgeändert werden. Jegliche Manipulationsmöglichkeiten müssen durch entsprechende technische Vorkehrungen ausgeschlossen sein. Insofern hält die BRAK die Beauftragung privater Unternehmen, welche etwa die Aktenstruktur bestimmen, für grundsätzlich unzulässig. Soweit dies in Einzelfällen aufgrund der notwendigen besonderen IT-forensischen Sachkunde zwingend erforderlich ist, ist zumindest ein bundeseinheitlicher enger rechtlicher Rahmen zu schaffen (hierzu unter III. 1. c. bb.).

Um dem Beschleunigungsgebot sowie dem aus dem Recht auf ein faires Verfahren abgeleiteten Prinzip der Waffengleichheit ausreichend Rechnung zu tragen, muss auch eine effektive und praktische Handhabung der elektronisch geführten Verfahrensakte gewährleistet sein. Diese setzt in inhaltlicher Hinsicht insbesondere eine Inhaltsübersicht sowie die Einheitlichkeit bei der Benennung einzelner Ordner, etwa Hauptbände, Beweismittelbände, Beschuldigtenbände, Zeugenbände, Durchsuchungsbände, Finanzermittlungen und andere Sonderbände mit Einzelfallbenennung (Oberbegriff für alle außer den Hauptbänden: „Sonderbände“) voraus. Mindestens die Hauptbände sind dabei streng chronologisch zu führen, so dass v.a. auch aus dem Hauptband der Gang der Ermittlungen nachvollziehbar ist. Die erforderliche Nachvollziehbarkeit bedeutet in jedem Falle, dass zusätzlich auch die Kommunikation einzelner Verfahrensbeteiligter mit der aktenführenden Stelle aufzunehmen ist und Vermerke darüber anzufertigen und einzufügen sind, welche Aktenbestandteile (nur) in Sonderbände aufgenommen wurden.

Alle Beweismittel, die ohne Erkenntnisverlust (digital) kopiert werden können, sind mindestens als Scans zur Akte zu nehmen und damit Aktenbestandteil. Bei der Fertigung von Kopien ist auf deren Qualität zu achten. So sollen z.B. farbige Darstellungen auch in der Kopie solche sein. Von Verkleinerungen etc. ist abzusehen.

> Vgl. § 32e Ab. 1 StPO: „Dokumente, die nicht der Form entsprechen, in der die Akte geführt wird (Ausgangsdokumente), sind in die entsprechende Form zu übertragen. Ausgangsdokumente, die als Beweismittel sichergestellt sind, können in die entsprechende Form übertragen werden.“
>
> Vgl. auch § 4 Abs. 2 S. 2 DokErstÜbV: „Ausgangsdokumente, die als Beweismittel sichergestellt sind, können in elektronische Dokumente übertragen oder von der elektronischen Übermittlung ausgenommen werden“ und § 4 Abs. 3 S. 1 DokErstÜbV: „Ausgangsdokumente, die nicht als Beweismittel sichergestellt sind, müssen während des laufenden Verfahrens im Anschluss an die Übermittlung mindestens sechs Monate lang gespeichert oder aufbewahrt werden.“
>
> Vgl. auch § 3 Abs. 3 S. 1 ElektAktFVO SH: „Beiakten, als Beweismittel eingereichte oder dienende Schriftstücke oder sonstige Unterlagen werden in die elektronische Form übertragen, wenn dies keinen unverhältnismäßigen Aufwand darstellt. Die Übertragung dient nicht der Ersetzung der Urschrift. § 97 der Grundbuchverfügung bleibt unberührt.“

Nach Anklageerhebung darf eine Veränderung oder Ergänzung der Akte nur noch durch das Gericht erfolgen. Zur Gewährleistung der Nachvollziehbarkeit ist auch hierfür für neu hinzukommende Aktenteile ein einheitliches System erforderlich. Das Akteneinsichtsrecht der Verteidigung kann ab diesem Zeitpunkt nicht mehr beschränkt, sondern muss vielmehr gestärkt werden – spätestens hier sollte die in der Praxis handhabbare „Live-Akte“ der Maßstab sein (hierzu unten II. 2. b)). Alternativ würde sich die Einführung eines einheitlichen Systems für neu hinzukommende Aktenbestandteile anbieten, z.B. durch inkrementelle Übersendung oder Beifügung eines Gesamtverzeichnisses.

Auf Basis der vorstehenden Ausführungen schlägt die BRAK folgende Erweiterung des § 32 StPO vor:

§ 32 **Elektronische Aktenführung; Verordnungsermächtigungen**	
geltende Fassung	**Neufassung**
(1) Die Akten können elektronisch geführt werden. Die Bundesregierung und die Landesregierungen bestimmen jeweils für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an die Akten elektronisch geführt werden. Sie können die Einführung der elektronischen Aktenführung dabei auf einzelne Gerichte oder Strafverfolgungsbehörden oder auf allgemein bestimmte Verfahren beschränken und bestimmen, dass Akten, die in Papierform angelegt wurden, auch nach Einführung der elektronischen Aktenführung in Papierform weitergeführt werden; wird von der Beschränkungsmöglichkeit Gebrauch gemacht, kann in der Rechtsverordnung bestimmt werden, dass durch Verwaltungsvorschrift, die öffentlich bekanntzumachen ist, geregelt wird, in welchen Verfahren die Akten elektronisch zu führen sind. Die Ermächtigung kann durch Rechtsverordnung auf die zuständigen Bundes- oder Landesministerien übertragen werden.	*(1) Die Akten können elektronisch geführt werden. Die Bundesregierung und die Landesregierungen bestimmen jeweils für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an die Akten elektronisch geführt werden. Sie können die Einführung der elektronischen Aktenführung dabei auf einzelne Gerichte oder Strafverfolgungsbehörden oder auf allgemein bestimmte Verfahren beschränken und bestimmen, dass Akten, die in Papierform angelegt wurden, auch nach Einführung der elektronischen Aktenführung in Papierform weitergeführt werden; wird von der Beschränkungsmöglichkeit Gebrauch gemacht, kann in der Rechtsverordnung bestimmt werden, dass durch Verwaltungsvorschrift, die öffentlich bekanntzumachen ist, geregelt wird, in welchen Verfahren die Akten elektronisch zu führen sind. Die Ermächtigung kann durch Rechtsverordnung auf die zuständigen Bundes- oder Landesministerien übertragen werden.* *(2) Vor Anklageerhebung obliegt die ordnungsgemäße Aktenführung den Strafverfolgungsbehörden. Sie müssen durch geeignete technische und organisatorische Maßnahmen sicherstellen, dass Dritte keine Veränderungen an der Akte vornehmen. Nach Anklageerhebung geht die Verantwortung zur Aktenführung auf das Gericht über.* *(3) Die Akten sind chronologisch zu führen. Bei der Anlage der Akte sollen neben der Hauptakte bereits die nach Art und Umfang des Verfahrens notwendigen Sonderbände namentlich definiert werden. Die Hauptakte muss insbesondere alle wesentlichen Ermittlungsmaßnahmen und Ermittlungsergebnisse beinhalten. Soweit ein Dokument nicht in die Hauptakte, sondern lediglich in die Sonderbände aufgenommen wird, ist dies in der Hauptakte zu vermerken.*

(2) Die Bundesregierung und die Landesregierungen bestimmen jeweils für ihren Bereich durch Rechtsverordnung die für die elektronische Aktenführung geltenden organisatorischen und dem Stand der Technik entsprechenden technischen Rahmenbedingungen einschließlich der einzuhaltenden Anforderungen des Datenschutzes, der Datensicherheit und der Barrierefreiheit. Sie können die Ermächtigung durch Rechtsverordnung auf die zuständigen Bundes- oder Landesministerien übertragen.	*(4) Die Bundesregierung und die Landesregierungen bestimmen jeweils für ihren Bereich durch Rechtsverordnung die für die elektronische Aktenführung geltenden organisatorischen und dem Stand der Technik entsprechenden technischen Rahmenbedingungen einschließlich der einzuhaltenden Anforderungen des Datenschutzes, der Datensicherheit und der Barrierefreiheit. Sie können die Ermächtigung durch Rechtsverordnung auf die zuständigen Bundes- oder Landesministerien übertragen.*
(3) Die Bundesregierung bestimmt durch Rechtsverordnung mit Zustimmung des Bundesrates die für die Übermittlung elektronischer Akten zwischen Strafverfolgungsbehörden und Gerichten geltenden Standards. Sie kann die Ermächtigung durch Rechtsverordnung ohne Zustimmung des Bundesrates auf die zuständigen Bundesministerien übertragen.	*(5) Die Bundesregierung bestimmt durch Rechtsverordnung mit Zustimmung des Bundesrates die für die Übermittlung elektronischer Akten zwischen Strafverfolgungsbehörden und Gerichten geltenden Standards. Sie kann die Ermächtigung durch Rechtsverordnung ohne Zustimmung des Bundesrates auf die zuständigen Bundesministerien übertragen.*

2. Einsicht in elektronisch geführte Strafakten

a) Bereitstellen der Akte

Die Einsicht in elektronisch geführte Strafakten soll sich in erster Linie nach § 32f StPO i. V. m. der Strafakteneinsichtsverordnung (StrafAktEinV) richten.[27] Diese sieht dabei verschiedene Übermittlungswege für die Gewährung der Einsicht in elektronische Strafakten vor. Grundsätzlich wird Akteneinsicht durch das Bereitstellen zum Abruf in einem Internetportal (§ 2 StrafAktEinV) oder die Übermittlung auf einem sicheren Übermittlungsweg i. S. des § 34a Abs. 4 StPO (§ 3 StrafAktEinV), § 32f Abs. 1 Satz 1 StPO gewährt. Die Einsichtnahme in den Diensträumen (§ 4 StrafAktEinV), das Ausdrucken (§ 5 StrafAktEinV) oder das Speichern auf einem physischen Datenträger (§ 6 StrafAktEinV) kommen nur auf besonderen Antrag hin in Betracht. Diese grundsätzliche Rangfolge ist notwendig, um dem Zweck der elektronischen Aktenführung gerecht zu werden.

Sofern die Bereitstellung über ein Internetportal erfolgt, muss neben ausreichenden datenschutzrechtlichen Sicherungsmaßnahmen gewährleistet sein, dass alle Prozessbeteiligten eine **Benachrichtigung** erhalten.[28] Dies sollte durch eine Ergänzung in § 2 StrafAktEinV klargestellt werden.

[27] Vgl. Verordnung über die Standards für die Einsicht in elektronische Akten im Strafverfahren (Strafakteneinsichtsverordnung – StrafAktEinV) v. 24.02.2020, BGBl. 2020 I, 242.

[28] Hierzu bereits BRAK-Stellungnahme Nr. 60/2021, S. 4.

§ 2 Bereitstellen des Inhalts zum Abruf	
geltende Fassung	**Neufassung**
(1) Für die Einsicht in elektronische Akten wird ihr Inhalt, soweit Einsicht gewährt werden soll, in Form des Repräsentats zum Abruf bereitgestellt. Auf dem Repräsentat ist der Name der Person, der Akteneinsicht gewährt wird, dauerhaft erkennbar anzubringen. Dem Repräsentat soll ein strukturierter maschinenlesbarer Datensatz beigefügt werden, der den nach § 8 Nummer 1 bekanntgemachten Definitions- oder Schemadateien entspricht.	*(1) Für die Einsicht in elektronische Akten wird ihr Inhalt, soweit Einsicht gewährt werden soll, in Form des Repräsentats zum Abruf bereitgestellt. Auf dem Repräsentat ist der Name der Person, der Akteneinsicht gewährt wird, dauerhaft erkennbar anzubringen. Dem Repräsentat soll ein strukturierter maschinenlesbarer Datensatz beigefügt werden, der den nach § 8 Nummer 1 bekanntgemachten Definitions- oder Schemadateien entspricht.*
(2) Die Bereitstellung erfolgt für 30 Tage. Die Person, der Akteneinsicht gewährt wird, ist auf die Bereitstellung, das Datum des Stands der elektronischen Akte sowie auf das Datum, an dem die Bereitstellung endet, hinzuweisen.	*(2) Die Bereitstellung erfolgt für 30 Tage. Die Person, der Akteneinsicht gewährt wird, ist auf die Bereitstellung, das Datum des Stands der elektronischen Akte sowie auf das Datum, an dem die Bereitstellung endet, hinzuweisen. Die Benachrichtigung soll über einen sicheren Übermittlungsweg nach § 32a Absatz 4 der Strafprozessordnung erfolgen.*
(3) Der Abruf ist über das Internet möglich. Die Internetseite wird in geeigneter Weise bekanntgemacht. Der Abruf darf nur erfolgen, wenn sich die Person, der Akteneinsicht gewährt wird, hinreichend sicher authentisiert hat. Der abzurufende Inhalt ist nach dem Stand der Technik verschlüsselt zu übertragen. Er soll auf dem System der Person, der Akteneinsicht gewährt wird, gespeichert werden können.	*(3) Der Abruf ist über das Internet möglich. Die Internetseite wird in geeigneter Weise bekanntgemacht. Der Abruf darf nur erfolgen, wenn sich die Person, der Akteneinsicht gewährt wird, hinreichend sicher authentisiert hat. Der abzurufende Inhalt ist nach dem Stand der Technik verschlüsselt zu übertragen. Er soll auf dem System der Person, der Akteneinsicht gewährt wird, gespeichert werden können.*
(4) Bei der Einrichtung der Internetseite für ein Akteneinsichtsportal sollen die Anforderungen an die Barrierefreiheit im Sinne der Barrierefreie-Informationstechnik-Verordnung vom 12. September 2011 (BGBl. I S. 1843), die zuletzt durch Artikel 1 der Verordnung vom 21. Mai 2019 (BGBl. I S. 738) geändert worden ist, in der jeweils geltenden Fassung beachtet werden.	*(4) Bei der Einrichtung der Internetseite für ein Akteneinsichtsportal sollen die Anforderungen an die Barrierefreiheit im Sinne der Barrierefreie-Informationstechnik-Verordnung vom 12. September 2011 (BGBl. I S. 1843), die zuletzt durch Artikel 1 der Verordnung vom 21. Mai 2019 (BGBl. I S. 738) geändert worden ist, in der jeweils geltenden Fassung beachtet werden.*

b) „Live-Akte“

Die Einführung einer sog. „**Live-Akte**“ ist sowohl hinsichtlich der Aktenführung als auch Akteneinsicht aus Sicht der BRAK die vorzugswürdigste Lösung. Live-Akte meint eine elektronisch geführte und in einem virtuellen Arbeitsraum hinterlegte Akte, auf die die Verfahrensbeteiligten grundsätzlich rund um die Uhr zugreifen können. Die Verfahrensbeteiligten können so z.B. schneller und eigenständig nachvollziehen, ob neue Aktenbestandteile hinzugekommen sind. Dabei wäre es praktikabel, wenn die Verfahrensbeteiligten bei dem Hinzukommen von Aktenbestandteilen eine Benachrichtigung erhalten, in der auch mitgeteilt wird, welche Aktenteile hinzugekommen sind.

Durch technische Vorkehrungen kann gewährleistet werden, dass es der Staatsanwaltschaft dabei möglich bleibt, bestimmte Seiten für bestimmte Prozessbeteiligte noch nicht freizugeben, sodass ermittlungstaktische Erwägungen nicht beeinträchtigt würden. Dies würde der beschränkten Akteneinsicht in die Papierakte gleichkommen und wäre aufgrund der Berücksichtigung bereits bei der Anlage der Akte mit weniger Aufwand verbunden als die nachträgliche Selektierung. Natürlich muss eine solche Beschränkung von der Staatsanwaltschaft, wie auch bisher, begründet und im Falle erneuter Akteneinsicht geprüft werden, ob die Seiten nunmehr freizugeben sind. So könnte im Übrigen auch der erforderlichen Begrenzung des Akteneinsichtsrechts Dritter (z.B. §§ 406e, 475 StPO) durch technische Vorkehrungen Rechnung getragen werden.

c) Akteneinsicht durch Mandanten

Hinsichtlich der Akteneinsicht und der Überlassung von Aktenbestandteilen an Mandanten gilt, dass für die in Haft befindlichen Mandanten von Seiten der Justizvollzugsanstalten die Möglichkeit geschaffen werden muss, die Akten im Haftraum digital lesen und für die eigenen Verteidigungszwecke bearbeiten zu können. Insoweit besteht in Verfahren mit umfangreichen Akten die Notwendigkeit der Zurverfügungstellung eines Laptops oder eines anderen geeigneten elektronischen Gerätes, mit dem die Akte sichtbar gemacht, bearbeitet und dauerhaft abgespeichert werden kann. Im Zusammenhang mit der Einführung des § 32f Abs. 1 S. 2 StPO hat der Gesetzgeber bereits klargestellt, dass die Verwendung von Kommunikationstechnik durch Gefangene in Justizvollzugsanstalten nicht mehr untersagt werden darf, sofern und soweit dies der Wahrnehmung des Akteneinsichtsrechts entgegensteht.[29] Ungeachtet dessen, ist die Rechtsprechung dazu immer noch uneinheitlich. Einzelne Gerichte lehnen die Nutzung eines Laptops durch Untersuchungsgefangene zur Gewährung von Akteneinsicht selbst bei extrem umfangreichen Akten weiterhin pauschal ab und verweisen stattdessen auf die Möglichkeit der Nutzung von sog. Anstaltsrechnern.[30] Dies ist jedoch keine akzeptable Alternative, da sie nur bei entsprechender Verfügbarkeit der wenigen Geräte in den oft sehr beschränkten Öffnungszeiten der Leseräume in den Haftanstalten verwendet werden können und damit auch kein Bearbeiten und Abspeichern der Akten möglich ist. Zu fordern ist daher die Klarstellung, dass für solche Fälle elektronische Geräte zur Nutzung im persönlichen Haftraum zur Verfügung zu stellen sind, wie dies heute bereits vielfach praktiziert wird.

d) Verbot der Verbreitung des Akteninhalts

Da sich bei der elektronischen Aktenführung ebenso wie bei weiteren möglichen Anpassungen des Prozessrechts wie etwa bei der Aufzeichnung der Hauptverhandlung auch die Möglichkeiten der Verbreitung des Akteninhalts zunehmen, erscheint die Schaffung eines entsprechenden Straftatbestandes angebracht. Insofern ist bereits in den vorliegenden Gesetzesentwürfen zur Aufzeichnung der

[29] Gesetzesbegründung zu § 32f Abs. 1 S. 2 StPO, BT-Drucks.1894/16, S. 56.
[30] So OLG Frankfurt am Main, Beschluss v. 27.10.2020 – 3 Ws 662/20 (nicht veröffentlicht).

Hauptverhandlung hinsichtlich der Verbreitung einer Bild-Ton-Aufzeichnung eine Erweiterung des § 353d StGB um eine entsprechende Nr. 4 vorgesehen.[31]

Die elektronische Aktenführung dient letztlich wie die digitale Aufzeichnung der Hauptverhandlung ausschließlich verfahrensbezogenen Zwecken.[32] So kommt im Falle von elektronischen Verfahrensakten dem Schutz der Persönlichkeitsrechte sowohl des Täters als auch des Opfers eine maßgebliche Bedeutung zu. Dies gilt insbesondere für die elektronischen Ermittlungsakten der Strafverfolgungsbehörden, deren Inhalt grundsätzlich – anders als die Inhalte der Hauptverhandlung – nicht vollumfänglich öffentlich sind, sondern allenfalls zum Gegenstand der öffentlichen Hauptverhandlung gemacht werden. Gleichermaßen wird beispielsweise durch die Kenntniserlangung eines Zeugen vom Akteninhalt dessen Unbefangenheit und damit auch die Wahrheitsfindung beeinträchtigt. Es erscheint daher notwendig, auch die Verbreitung von Akten(bestandteilen) - unabhängig von der bestehenden Regelung des § 353d Nr. 3 StGB - unter Strafe zu stellen.

Eine mögliche Regelung könnte wie folgt lauten:

§ 353d **Verbotene Mitteilungen über Gerichtsverhandlungen**	
geltende Fassung	**Neufassung**
Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer	*Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer*
1. entgegen einem gesetzlichen Verbot über eine Gerichtsverhandlung, bei der die Öffentlichkeit ausgeschlossen war, oder über den Inhalt eines die Sache betreffenden amtlichen Dokuments öffentlich eine Mitteilung macht,	*1. entgegen einem gesetzlichen Verbot über eine Gerichtsverhandlung, bei der die Öffentlichkeit ausgeschlossen war, oder über den Inhalt eines die Sache betreffenden amtlichen Dokuments öffentlich eine Mitteilung macht,*
2. entgegen einer vom Gericht auf Grund eines Gesetzes auferlegten Schweigepflicht Tatsachen unbefugt offenbart, die durch eine nichtöffentliche Gerichtsverhandlung oder durch ein die Sache betreffendes amtliches Dokument zu seiner Kenntnis gelangt sind, oder	*2. entgegen einer vom Gericht auf Grund eines Gesetzes auferlegten Schweigepflicht Tatsachen unbefugt offenbart, die durch eine nichtöffentliche Gerichtsverhandlung oder durch ein die Sache betreffendes amtliches Dokument zu seiner Kenntnis gelangt sind, oder*
3. die Anklageschrift oder andere amtliche Dokumente eines Strafverfahrens, eines Bußgeldverfahrens oder eines Disziplinarverfahrens, ganz oder in wesentlichen Teilen, im Wortlaut öffentlich mitteilt, bevor sie in öffentlicher Verhandlung erörtert worden sind oder das Verfahren abgeschlossen ist.	*3. die Anklageschrift oder andere amtliche Dokumente eines Strafverfahrens, eines Bußgeldverfahrens oder eines Disziplinarverfahrens, ganz oder in wesentlichen Teilen, im Wortlaut öffentlich mitteilt, bevor sie in öffentlicher Verhandlung erörtert worden sind oder das Verfahren abgeschlossen ist.* *[4. Neufassung i. S. d. RegE eines Hauptverhandlungsdokumentationsgesetzes – DokHVG]*

[31] Hierzu S. 27 f. Entwurf eines Gesetzes zur digitalen Dokumentation der strafgerichtlichen Hauptverhandlung (Hauptverhandlungsdokumentationsgesetz – DokHVG) und S. 70 f. Alternativ-Entwurf – Audiovisuelle Dokumentation der Hauptverhandlung (AE-ADH) des Arbeitskreises deutscher, österreichischer und schweizerischer Strafrechtslehrer.
[32] BRAK-Stellungnahme Nr. 8/2023, S. 9.

	5. elektronische Verfahrensakten der Strafverfolgungsbehörden oder Strafgerichte verbreitet, der Öffentlichkeit oder unbefugt Dritten zugänglich macht.

3. Überarbeitung der Gebührentatbestände

In wörtlicher Auslegung wird unter dem Wort „Kopie“ in Nr. 7000 VV RVG nur das Papierwerk subsumiert, nicht jedoch von Rechtsanwältinnen und Rechtsanwälten aus den Ermittlungsakten gefertigte Scans. Diese Scans werden seit 2013 je nach Bundesland und zuständigem Rechtspfleger i.d.R. nicht erstattet. Gegen diese Praxis erfolgte vielfältiger Widerspruch. Alle Forderungen, die Praxis bzw. den Gesetzeswortlaut zu ändern, blieben erfolglos. Im Rahmen des Kostenrechtsänderungsgesetzes 2021 wurde die explizite Einführung einer Dokumentenpauschale für das Einscannen von Papierakten abgelehnt. Nr. 7000 VV RVG blieb unverändert. Die bestehende Regelung und Praxis stellt eine unzulässige Beeinträchtigung der anwaltlichen Berufsausübung dar: Selbst wenn in Umfangsverfahren zunehmend die Akten in elektronischer Form vom Gericht zur Verfügung gestellt werden, so ist dies weiterhin die Ausnahme. Auch nach der Einführung der elektronischen Akte wird es eine Vielzahl von Altverfahren geben, die in Papierform begonnen haben und deshalb weiterhin in Papierform bestehen werden. Insbesondere komplizierte Verfahren haben eine Verfahrensdauer von mehreren Jahren.

Eine Anpassung des Nr. 7000 VV RVG gebietet auch der Klimaschutz. Aus Nachhaltigkeitsaspekten ist es unhaltbar, das Fertigen von Kopien zu fördern, indem das Fertigen von Scans benachteiligt wird. Der Gedanke, die natürlichen Ressourcen zu schonen, sollte auch im RVG Geltung entfalten.

Die Pauschale des Nr. 7000 VV RVG soll den Aufwand von Arbeitszeit und Material für die Erstellung von Dokumenten abdecken. Entgegen einer verbreiteten Ansicht führt das Anfertigen von Scans nicht zu einer (erheblichen) Kostenreduzierung in den Kanzleien. Der eingeschränkte Blick lediglich auf Papier, Toner, Aktenordner und Lagerraum[33] spiegelt die Realität nur unzureichend wider. Zu berücksichtigen sind die Anschaffung bzw. Haltung eines leistungsfähigen Scanners, die Abnutzungserscheinungen des Scanners sowie die kostenpflichtige Berechnung der einzelnen Scans durch die entsprechenden Leasingfirmen. Darüber hinaus entstehen erhebliche Kosten für Datenträger, Speicherplatz und für kostenintensive Textverarbeitungsprogramme, um die gescannte Akte vorhalten, lesen und bearbeiten zu können. Darüber hinaus ist der erhebliche Zeitaufwand beim Scannen zu berücksichtigen, der sich in keiner Weise vom Fertigen von Kopien unterscheidet, diesen in vielen Fällen sogar übersteigt.

Nr. 7000 VV RVG ist auch dahingehend zu konkretisieren, dass Ausdrucke von in elektronischer Form zur Verfügung gestellten Akten erstattungsfähig sind. Die gegenwärtige Regelung sieht vor, dass nur Auslagen erstattungsfähig sind, wenn sie zur sachgemäßen Durchführung der Angelegenheit erforderlich sind (§ 46 RVG). Auch Nr. 7000 VV RVG verweist darauf, dass die Erstattungsfähigkeit nur gegeben ist, wenn sie zur sachgemäßen Bearbeitung der Rechtssache geboten war. Die Erstattungsfähigkeit verlagert sich insoweit in die Diskussion darüber, ob die Ausdrucke notwendig waren. Konsens besteht jedoch dahingehend, dass der Anwalt einen gewissen, nicht zu engen, sondern eher großzügigen Ermessensspielraum hat, den er allerdings auch pflichtgemäß handhaben muss.[34] Die Verteidigung hat hier jedoch (im Gegensatz zu § 46 I RVG) die Darlegungs- und Beweislast. Zu betonen bleibt jedoch, dass es vielfältige Gründe geben kann, weshalb Ausdrucke aus der elektronischen Akte im Rahmen der Verteidigung erforderlich sein können.

Unter Berücksichtigung der vorstehenden Ausführungen wird die folgende Neufassung der Nr. 7000 VV RVG vorgeschlagen.

[33] Z.B. KG Berlin, Beschl. v. 28.08.2015 - 1 Ws 51/15 = NStZ-RR 2016, 63.
[34] Vgl. KG Berlin, Beschl. v. 28.08.2015 - 1 Ws 31/15 = JurBüro 2016, 135 m.w.N.

Nr. 7000 VV RVG Dokumentenpauschale	
geltende Fassung	**Neufassung**
Pauschale für die Herstellung und Überlassung von Dokumenten: *1. für Kopien und Ausdrucke* *a) aus Behörden- und Gerichtsakten, soweit deren Herstellung zur sachgemäßen Bearbeitung der Rechtssache geboten war,* *[…]* *für die ersten 50 abzurechnenden Seiten je Seite* 0,50 EUR *für jede weitere Seite* 0,15 EUR *für jede weitere Seite in Farbe* 0,30 EUR *[…]*	*Pauschale für die Herstellung und Überlassung von Dokumenten:* *1. für Kopien, Scans und Ausdrucke* *a) aus Behörden- und Gerichtsakten sowie elektronischen Akten, soweit deren Herstellung zur sachgemäßen Bearbeitung der Rechtssache geboten war,* *[…]* *für die ersten 50 abzurechnenden Seiten je Seite* 0,50 EUR *für jede weitere Seite* 0,15 EUR *für jede weitere Seite in Farbe* 0,30 EUR *[…]*

III. Besonderheiten in einzelnen Verfahrensabschnitten

1. Ermittlungsverfahren

a) Durchsicht von Papieren und elektronischen Speichermedien

Bezüglich der Durchsicht elektronisch gespeicherter Daten erscheint die derzeitige Fassung des § 110 StPO nicht mehr zeitgemäß. Die BRAK befürwortet eine Neufassung, die den mit der Digitalisierung einhergehenden technischen Herausforderungen ebenso gerecht wird, wie der in der Praxis um sich greifenden umfassenden und oftmals eben nicht beschränkten Durchsicht elektronischer Speichermedien.

aa) Dringendes Regelungsbedürfnis

§ 110 StPO dient der Trennung von nicht beweiserheblichen und beweiserheblichen Papieren als eine der Beschlagnahme vorgelagerte und mildere[35] Ermittlungsmaßnahme. Die derzeit geltenden Gesetzesvorgaben[36] sind im Hinblick auf die fortschreitende Digitalisierung nicht mehr zeitgemäß, weil u.a. § 110 StPO die ihm zugedachte Filterfunktion allenfalls eingeschränkt zu erfüllen vermag.[37] Der Zweck des § 110 StPO, durch die Vermeidung einer umfassenden, andauernden Beschlagnahme den Verhältnismäßigkeitsgrundsatz zu wahren,[38] kollidiert mit der Realität des massiven Eingriffscharakters, den

[35] Vgl. *Doege* NStZ 2022, 466, 467.
[36] Vgl. Begriff „Papier“ in § 110 StPO, der durch die Justizpraxis bereits ausgeweitet wurde.
[37] Vgl. *Peters* NZWiSt 2017, 465, 469.
[38] Vgl. nur BVerfG, Beschl. v. 12.04.2005 – 2 BvR 1027/02 = NJW 2005, 1917, 1921.

Maßnahmen nach § 110 StPO in der Praxis meist schon aufgrund der Menge der vermeintlich beweiserheblichen Daten etwa in Umfangsverfahren oftmals haben.[39] Es besteht daher ein dringendes Bedürfnis, die praktische Durchführung der Durchsicht gesetzlich zu regeln. Die mit einer vollständigen Spiegelung oder Mitnahme der Hardware verbundene Gefahr nicht nur für die Ermittlungsbehörden, sondern für alle Verfahrensbeteiligten, einerseits kaum bewältigbaren Datenmengen ausgesetzt zu sein, andererseits verfahrensfremde Zufallsfunde zu generieren, ist evident. Die als offene Ermittlungsmaßnahme ausgestaltete Durchsuchung wird durch die Durchsicht in den Räumen der Behörden faktisch mehr und mehr zu einer verdeckten Maßnahme. Dieser veränderten Ausgangslage muss im Hinblick auf den Verhältnismäßigkeitsgrundsatz mit einem angepassten regulatorischen Rahmen Rechnung getragen werden. Insofern wird eine Ergänzung der Regelung in § 110 Abs. 3 S. 3 StPO n.F. durch Aufnahme von Soll-Vorgaben angeregt. Die vorläufige Sicherstellung soll durch Erstellung von Kopien des Datenstammes unter Ausschöpfung der Möglichkeiten zur Beschränkung[40] erfolgen.

bb) Verfassungsrechtliche Grenzen der Durchsicht

Im Hinblick auf die Suche nach elektronischen Beweismitteln sollten §§ 105, 110 StPO angelehnt an die Rechtsprechung des Bundesverfassungsgerichts[41], wonach im Einzelnen Art und denkbarer Inhalt der Beweismittel, deren Sicherstellung die Durchsuchung dient, im Durchsuchungsbeschluss genannt werden müssen und hinsichtlich der Sicherung von Daten ergänzt werden. Hierbei sollte der Durchsuchungsbeschluss so weit wie möglich Vorgaben zum Inhalt sowie zur Art und Weise der Suche nach den Daten enthalten (z.B. zur Suche mittels konkreter Suchbegriffe, zur Durchsicht nur bestimmter Bereiche des Speichermediums). Weiter ist zu regeln, dass eine Mitnahme von Papieren oder eine vorläufige Sicherung von Daten nur dann erfolgen soll, wenn eine Durchsicht und Aussonderung vor Ort unmöglich ist.[42]

In § 110 StPO sollte zudem der Staatsanwaltschaft und ihren Ermittlungspersonen die Pflicht auferlegt werden, nach Möglichkeit die vorläufige Sicherstellung grundsätzlich auf Kopien der gegebenenfalls beweiserheblichen Papiere oder Datenbestände zu beschränken,[43] um den Eingriff in das Eigentum des Betroffenen (Art. 14 Abs. 1 GG) erheblich abzumildern.

In Bezug auf Datenbestände, die mithilfe eines IT-forensischen Datenauswertungssystems durchsucht werden sollen, muss eine vorläufige Sicherung auch dann auf eine Spiegelung beschränkt werden, wenn andernfalls eine Veränderung des Original-Datenbestands zu besorgen ist. Um sicherzustellen, dass Maßnahmen nach § 110 StPO im Hinblick auch auf das regelmäßig tangierte Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG)[44] ohne Kenntnisnahme des Inhalts erfolgen, schreibt die vorgeschlagene Neufassung des § 110 StPO vor, dass Papiere und Daten, unter Ausschöpfung aller verfügbaren technischen Möglichkeiten, nur soweit gesichtet werden sollen, wie dies zur Feststellung ihrer voraussichtlichen Beweiserheblichkeit erforderlich ist. Angesichts der staatsanwaltschaftlichen Praxis wird diese gesetzliche Klarstellung, in Verbindung mit einer entsprechenden Begründungspflicht, für notwendig erachtet. Zur Effektivierung des Verfahrens kann es sich anbieten, für die Verteidigung in geeigneten Fällen die Festlegung von Suchbegriffen einzubeziehen.

cc) Mehrstufiges Verfahren

Um zugleich eine effektive Strafverfolgung zu ermöglichen und im Hinblick auf die fortschreitende

[39] *Peters* NZWiSt 2017, 465, 469, vgl. auch *Wackernagel/Graßie* NStZ 2021, 12.
[40] Bspw. unter Ausschluss der Daten nichtbetroffener Personen, offenbar privilegierter Kommunikation i.S.d. § 97 StPO, irrelevanter Zeiträume.
[41] Vgl. etwa BVerfG, Beschl. v. 23.03.1994 – 2 BvR 396/94 = NJW 1994, 2079.
[42] Vom Bundesverfassungsgericht und Gesetzgeber bereits mehrfach festgelegt, vgl. BVerfG, Beschl. v. 12.04.2005 – 2 BvR 1027/02 = NJW 2005, 1917, 1921; BVerfG, Beschl. v. 16.06.2009 – 2 BvR 902/06 = NJW 2009, 2431, 2436 Rn. 87; BVerfG, Beschl. v. 15.08.2014 – 2 BvR 969/14 = NJW 2014, 3085, 3088 Rn. 44; BGH, Beschl. v. 05.08.2003 – StB 7/03 = NStZ 2003, 670 Rn. 7; BT-Drs. 19/27654, S. 74, vgl. auch *Cordes/Reichling* NStZ 2022, 712, 713.
[43] Vgl. etwa LG Lübeck, Beschl. v. 03.02.2022 - 75 Gs 56/21 = BeckRS 2022, 5388.
[44] BVerfG, Beschl. v. 12.04.2005 – 2 BvR 1027/02 = NJW 2005, 1917, 1918, 1922; BVerfG, Beschl. v. 16.06.2009 – 2 BvR 902/06 = NJW 2009, 2431 Rn. 50.

Digitalisierung dem Kernbereichsschutz des von der Durchsicht Betroffenen in angemessener Weise Rechnung zu tragen, sieht die vorgeschlagene Neufassung des § 110 StPO ein mehrstufiges Verfahren (angelehnt an § 98a Abs. 2, 3 StPO und § 100d StPO) vor.[45] Demnach ist bei Papieren oder Daten i.S.d. §§ 97, 148 StPO, die einem Beschlagnahmeverbot unterfallen, von einer Durchsicht abzusehen.

Eine vorläufige Sicherstellung bleibt auch in Bezug auf beschlagnahmefreie Unterlagen möglich, soweit eine Aussonderung der geschützten Papiere oder Daten am Ort nicht möglich ist. Den Strafverfolgungsbehörden soll weiterhin ermöglicht werden, eine Auswertung großer Datenmengen auch im Anschluss an eine Durchsuchung in anderen Räumen vorzunehmen. Für den Fall, dass unter Ausschöpfung aller verfügbaren technischen Möglichkeiten trotzdem eine Durchsicht erforderlich ist, wird vorgeschrieben, dass - soweit möglich - sicherzustellen ist, dass die geschützten Papiere oder Daten ihrem Inhalt nach nicht zur Kenntnis der Strafverfolgungsbehörden gelangen. Sie sind im Zuge der Durchsicht unverzüglich auszusondern und dem Inhaber auszuhändigen oder, soweit es sich um Kopien handelt, zu vernichten oder zu löschen.[46]

Ein Zugriff auf Daten in Clouds darf nur erfolgen, sofern auch die Zugangscodes über Beschlagnahme erlangt worden sind. Ein Zugriff bleibt den Ermittlungsbehörden bei im Ausland befindlichen Servern hingegen gänzlich verwehrt.

Aus Klarstellungsgründen wird in der vorgeschlagenen Neufassung die Dauer der nicht vor Ort der Durchsuchung erfolgten Durchsicht ausdrücklich geregelt, so dass mit der Durchsicht „unverzüglich“ begonnen werden muss und sie „zügig“[47] durchgeführt wird. Auch wenn sich der Umfang von Sichtungsmaßnahmen nicht vorab bestimmen lässt,[48] sollte eine Obergrenze für die Rückgabe von Geräten (in der Regel 4 Wochen ab dem Zeitpunkt der Mitnahme) festgelegt werden. Nur wenn eine Spiegelung innerhalb dieser Frist nicht möglich ist – was entsprechend zu begründen wäre – soll eine Verlängerung auf max. 3 Monate möglich sein.

dd) Hinzuziehung des Betroffenen oder eines Durchsuchungszeugen

Im Hinblick auf die derzeit[49] nicht ausdrücklich vorgesehene Hinzuziehung des Betroffenen oder eines Durchsuchungszeugen schlägt die BRAK vor, dass der Inhaber und, wenn er der Beschuldigte ist, auch sein Verteidiger von Ort und Zeit der Durchsicht zu benachrichtigen sind und ihnen die Anwesenheit zu gestatten ist. Konkret könnte die Aussonderung geschützter Verteidiger-Kommunikation in Anwesenheit des leitenden Ermittlungsbeamten, eines IT-Forensikers der zuständigen Ermittlungsbehörde und des Verteidigers durchgeführt werden, wobei Letzterer dem IT-Forensiker die von ihm benutzten Kommunikationsmedien und -adressen mitteilt. Identifizierung und Löschung der geschützten Kommunikation erfolgen dann durch den IT-Forensiker ohne den Ermittlungsbeamten, welchem anschließend ein um diese Kommunikation bereinigter Datenbestand für die Durchsicht nach § 110 StPO zur Verfügung gestellt wird. Diese Vorgänge sind zu dokumentieren. Ein solches Vorgehen ist auch dann noch geboten, wenn innerhalb von zwei Werktagen ab dem Tag der Sicherung von Daten im Zuge einer Durchsuchung angezeigt wird, dass der Datenbestand geschützte Kommunikation mit Berufsgeheimnisträgern enthält. Bis zu diesem Zeitpunkt sollte den Ermittlungsbehörden eine Durchsicht der gesicherten Daten gesetzlich untersagt sein.

Gegenüber Dritten, deren Daten und Korrespondenz gesichtet wird, stellt sich die Durchsicht regelmäßig als heimliche Maßnahme dar.[50] Da diesen gegenüber eine Benachrichtigungspflicht nicht praktisch

[45] Vgl. BVerfG, Beschl. v. 16.06.2009 – 2 BvR 902/06 = NJW 2009, 2431, 2437 Rn. 91 f.
[46] Vgl. hierzu BVerfG, Beschl. v. 16.06.2009 – 2 BvR 902/06 = NJW 2009, 2431, 2437 Rn. 90.
[47] *Cordes/Reichling* NStZ 2022, 712, 714.
[48] BGH, Beschl. v. 20.05.2021 – StB 21/21 = NStZ 2021, 623, 624.
[49] LG Braunschweig, Beschl. v. 12.04.2006 – 6 Qs 88/06 = BeckRS 2011, 9575; Da es sich bei den Unterlagen im Zeitpunkt der Durchsicht noch nicht um Beweisstücke handelt, greift auch das Besichtigungsrecht des § 147 Abs. 1 StPO nicht ein, vgl. BGH, Urt. v. 29.10.2021 – 5 StR 443/19 = NZWiSt 2022, 326; OLG Thüringen, Beschl. v. 20.11.2000 – 1 Ws 313/00 = NJW 2001, 1290; OLG Koblenz, Beschl. v. 30.03.2021 – 5 Ws 16/21 = NZWiSt 2021, 386, 389 f.
[50] *Peters* NZWiSt 2017, 465, 469, *Puschke/Singelnstein* NJW 2008, 113, 115; s. auch *Ladiges* GSZ 2021, 203, 207/208: Gefahr, dass sich die Durchsicht einer verdeckten Online-Durchsuchung annähert.

umsetzbar ist, wird ein Interessenausgleich angestrebt, indem Dritten, die ihre Betroffenheit bei den Strafverfolgungsbehörden glaubhaft machen, die Anwesenheit zu gestatten ist. Beim Einsatz IT-forensischer Datenauswertungssysteme ist der Anwältin bzw. dem Anwalt des Berechtigten Zugriff zu diesem System zu gewähren.[51] Dem erhöhten Aufwand bei der Verteidigung ist ggfs. durch Schaffung eines Gebührentatbestands und der Durchsicht umfangreicher Datenträger als ein Indiz für das Vorliegen eines Pflichtverteidigungstatbestandes Rechnung zu tragen.

ee) Dauer der Beschlagnahme und Anfertigung von Kopien

Um zu vermeiden, dass sichergestellte elektronische Speichermedien wochen-, teilweise monatelang ohne Bearbeitung bei den Ermittlungsbehörden liegen, wird eine Soll-Vorgabe in § 94 StPO angeregt, wonach nach der Beschlagnahme von Datenträgern und vor deren Verwendung unverzüglich die Erstellung einer nicht veränderbaren originalgetreuen Spiegelung (nur der möglicherweise beweiserheblichen) Daten unter Beachtung der Maßstäbe der IT-Forensik zu erfolgen hat.[52]

Auch eine Soll-Vorgabe in § 111n Abs. 1 StPO, wonach die Herausgabe von Datenträgern unverzüglich zu erfolgen hat, erscheint angezeigt.[53] Überdies wird die Schaffung einer ergänzenden Regelung angeraten, wonach beim Einbehalt von originalen Datenträgern unter Verweis auf Zwecke des Strafverfahrens i.S.d. § 111n Abs. 1 StPO die Anfertigung und Herausgabe von Kopien der Datenträger zu gewähren sind, soweit hierdurch der Untersuchungszweck nicht gefährdet wird. Zur (Folge-)Beschlagnahme zuvor gem. § 110 StPO vorläufig gesicherter und durchgesehener Daten soll zudem eine Pflicht zur Absonderung der beschlagnahmten Daten vom vorläufig gesicherten Datenstamm durch Kopie auf gesonderte Datenträger bestehen, um anschließend Vernichtung bzw. Rückgabe des zuvor vorläufig gesicherten Datenstamms zu ermöglichen.

ff) Nutzung IT-forensischer Datenauswertungssysteme

Aus der Zwecksetzung des § 110 StPO wie auch aus dem allgemeinen Grundsatz der Verhältnismäßigkeit folgt, dass die Strafverfolgungsbehörden verpflichtet sind, vorrangig eine Auswertung und Aussonderung nicht beweisrelevanter und geschützter Daten mithilfe eines IT-forensischen Datenauswertungssystems (z.B. Relativity, NUIX, ZyLAB) vorzunehmen.[54] Die Durchsicht einzelner Dateien durch die Ermittlungsbeamten darf nur soweit erfolgen, wie zu befürchten ist, dass beweiserhebliche Dateien übersehen werden.

Es soll dabei aber nach verbreiteter Auffassung keine strafprozessuale Verpflichtung bestehen, dem Betroffenen die bei einer Durchsicht verwendeten Suchkriterien mitzuteilen oder sie gar vorab mit ihm abzustimmen.[55] Wenn man jedoch darauf abstellt, dass es originäre Verantwortung der Ermittlungsbeamten ist, das Gebot der Verhältnismäßigkeit zu beachten, müssen der Verteidigung die Suchbegriffe zumindest mitgeteilt werden. Damit ist die Möglichkeit zu verbinden, vor Beginn einer Durchsicht gerichtliche Entscheidung zu beantragen, um eine rechtsstaatlich gebotene und frühzeitig Kontrolle zu ermöglichen. Unabhängig davon kann es unter Beschleunigungsgesichtspunkten sinnvoll sein, Suchbegriffe mit der Verteidigung abzustimmen.

Eine Pflicht zur Nutzung von Forensik-Programmen bei der Durchsuchung von Daten besteht auch, sofern andernfalls die Durchsicht der Daten unverhältnismäßig lange dauern würde. Es besteht mithin eine staatliche Verpflichtung, die Ermittlungsbehörden mit dem Stand der Technik entsprechenden IT-forensischen Datenauswertungssystemen sowie hierin geschultem Personal auszurüsten.[56] Auf dieser

[51] Alle gängigen IT-Forensiksysteme ermöglichen die Einräumung von Remote- Zugriffsprofilen, die einen in der Zukunft möglicherweise bestehenden Live-Zugriff der Verteidigung auf elektronische Ermittlungsakten flankieren könnten; alternativ könnte die Einrichtung eines Nutzerprofils zur Nutzung/Einsichtnahme in den Räumen der Behörden erfolgen.
[52] Vgl. S. 26 des Leitfadens IT-Forensik des Bundesamts für Sicherheit in der Informationstechnik.
[53] Ggf. richterliche Fristsetzungsbefugnisse, Begründungspflichten für Fristverlängerungsersuchen der StA.
[54] Vgl. dazu *Wackernagel/Graßie* NStZ 2021, 12, 15.
[55] *Wenzl* NStZ 2021, 395, 399; *Doege* NStZ 2022, 466, 471.
[56] Zu den Grenzen des Einsatzes externer IT-Forensiker *Wackernagel/Graßie* NStZ 2021, 12, 13 ff.

Grundlage schreibt die vorgeschlagene Neufassung des § 110 StPO vor, dass eine Durchsicht erst nach Ausschöpfung aller verfügbaren technischen Möglichkeiten zur Aussonderung von nicht beweiserheblichen oder geschützten Papieren oder Daten zulässig ist.

Eine **Dokumentationspflicht** der Ermittlungsbehörden betreffend die Parameter, die zur Festlegung des vorläufig zu sichernden Datenstammes geführt haben, und ein elektronisches Sicherungsverzeichnis soll im Nachhinein eine (gerichtliche) Überprüfung ermöglichen (§ 110 Abs. 4 S. 1 i.V.m. § 98 Abs. 2 S. 2 StPO).

gg) Regelungsvorschlag

Im Folgenden werden konkrete Ergänzungen des § 110 StPO zum Schutz beschlagnahmefreier Daten (insb. Verteidigungsunterlagen) und zur Wahrung des Verhältnismäßigkeitsgrundsatzes im Übrigen formuliert. Ein Anspruch auf Vollständigkeit wird hierbei jedoch nicht erhoben.

§ 110 Durchsicht von Papieren und elektronischen Speichermedien	
geltende Fassung	**Neufassung**
(1) Die Durchsicht der Papiere des von der Durchsuchung Betroffenen steht der Staatsanwaltschaft und auf deren Anordnung ihren Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) zu.	*(1) Die Durchsicht der Papiere des von der Durchsuchung Betroffenen steht der Staatsanwaltschaft und auf deren Anordnung ihren Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) zu.*
(2) Im Übrigen sind Beamte zur Durchsicht der aufgefundenen Papiere nur dann befugt, wenn der Inhaber die Durchsicht genehmigt. Andernfalls haben sie die Papiere, deren Durchsicht sie für geboten erachten, in einem Umschlag, der in Gegenwart des Inhabers mit dem Amtssiegel zu verschließen ist, an die Staatsanwaltschaft abzuliefern.	*(2) Im Übrigen sind Beamte zur Durchsicht der aufgefundenen Papiere nur dann befugt, wenn der Inhaber die Durchsicht genehmigt. Andernfalls haben sie die Papiere, deren Durchsicht sie für geboten erachten, in einem Umschlag, der in Gegenwart des Inhabers mit dem Amtssiegel zu verschließen ist, an die Staatsanwaltschaft abzuliefern.*
(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 befürchten ist. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden.	*(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 befürchten ist. Eine Durchsicht nach S. 2 setzt voraus, dass sich die Speichermedien oder die gespeicherten Daten im Inland befinden. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden.*
(4) Werden Papiere zur Durchsicht mitgenommen oder Daten vorläufig gesichert, gelten die §§ 95a und 98 Absatz 2 entsprechend.	*(4) Werden Papiere zur Durchsicht mitgenommen oder Daten vorläufig gesichert, gelten die §§ 95a und 98 Absatz 2 entsprechend. Eine Mitnahme oder vorläufige Sicherung darf nur erfolgen, soweit nicht in den Räumen der*

	Durchsuchung über eine Beschlagnahme nach § 94 entschieden werden kann. Zur Mitnahme oder vorläufigen Sicherung sollen Kopien gefertigt werden. Der Inhaber und, wenn er der Beschuldigte ist, auch sein Verteidiger, sind von Ort und Zeit der Durchsicht zu benachrichtigen. Ihnen ist die Anwesenheit während der Durchsicht zu gestatten. Satz 5 gilt auch für Dritte, deren schutzwürdige Interessen von der Durchsicht betroffen werden. Die Durchsicht erfolgt unverzüglich nach der Mitnahme oder vorläufigen Sicherung und ist auf einen angemessenen Zeitraum zu begrenzen. Die Rückgabe von Datenträgern des Beschuldigten oder Dritter soll schnellstmöglich, spätestes innerhalb von 4 Wochen ab dem Zeitpunkt der Mitnahme erfolgen; sie darf nur dann innerhalb eines Zeitraums von maximal 3 Monaten erfolgen, wenn eine Spiegelung nicht früher möglich ist. *(5) Papiere und Daten sind, unter Ausschöpfung aller verfügbaren technischen Möglichkeiten, nur soweit durchzusehen, wie dies zur Feststellung ihrer voraussichtlichen Beweiserheblichkeit erforderlich ist. Nicht beweiserhebliche Papiere und Daten sind auszusondern und dem Inhaber auszuhändigen oder, soweit es sich um Kopien handelt, zu vernichten oder zu löschen.* *(6) Suchkriterien, die für die Durchsicht von Datenbeständen verwendet werden sollen, sind dem Inhaber und, wenn er der Beschuldigte ist, auch seinem Verteidiger, mitzuteilen. Der von einer Durchsicht Betroffene kann innerhalb von 2 Wochen die gerichtliche Entscheidung der Festlegung der Suchkriterien beantragen. Die Zuständigkeit des Gerichts bestimmt sich nach § 162. Der Betroffene kann den Antrag auch bei dem Amtsgericht einreichen, in dessen Bezirk die Beschlagnahme stattgefunden hat; dieses leitet den Antrag dem zuständigen Gericht zu. Der Betroffene ist über seine Rechte zu belehren.* *(7) Von einer Durchsicht ist abzusehen, soweit erkennbar der Beschlagnahme nicht unterliegende Papiere oder Daten im Sinne der §§ 97, 148 StPO oder sonstige Erkenntnisse aus dem Kernbereich privater Lebensgestaltung betroffen sind. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder aus einem Verteidigungsverhältnis nach § 148 StPO, die durch eine Durchsicht gewonnen wurden, dürfen nicht verwertet werden. ₃Bei Zweifeln, ob Papiere oder Daten einem*

	Beschlagnahmeverbot unterliegen, ist eine Durchsicht in Anwesenheit des Ermittlungsrichters durchzuführen. *(8) Soweit unter Ausschöpfung aller verfügbaren technischen Möglichkeiten eine Durchsicht erforderlich ist, um beweiserhebliche Papiere oder Daten aufzufinden und der Beschlagnahme nicht unterliegende Dokumente im Sinne der §§ 97, 148 StPO und sonstige Erkenntnisse aus dem Kernbereich privater Lebensgestaltung auszusondern, soll sichergestellt werden, dass die geschützten Papiere oder Daten ihrem Inhalt nach nicht zur Kenntnis der Strafverfolgungsbehörden gelangen. Sie sind im Zuge der Durchsicht unverzüglich auszusondern und dem Inhaber auszuhändigen oder, soweit es sich um Kopien handelt, zu vernichten oder zu löschen. Eine Durchsicht ist unverzüglich zu unterbrechen, wenn sich während ihrer Durchführung tatsächliche Anhaltspunkte dafür ergeben, dass Daten betroffen sind, die dem Kernbereich privater Lebensgestaltung oder einem Verteidigungsverhältnis nach § 148 StPO zuzurechnen sind.* *(9) Bei jeder Durchsicht sind Maßnahmen nach den Absätzen 5 bis 8 zu dokumentieren.* *(10) Befindet das Speichermedium sich in einem anderen Staat, darf die Durchsicht ohne dessen Zustimmung nur erfolgen, soweit* *1. auf öffentlich zugängliche Daten zugegriffen wird, oder* *2. die Zustimmung des Dateninhabers/Datenberechtigten vorliegt.* *(11) Ist zum Zeitpunkt der Durchsicht nicht erkennbar, welcher Staat zustimmungsberechtigt ist, darf nur eine vorläufige Sicherung der Daten erfolgen. Verweigert der zu ersuchende Staat die Zustimmung, sind die Daten unverzüglich zu löschen.*

b) Datenlieferungsvereinbarungen

Es ist in der Praxis einiger Staatsanwaltschaften üblich geworden, die weitere Vollstreckung der Durchsuchung von digitalen Datenträgern dadurch abwenden zu lassen, dass sog. Datenlieferungsvereinbarungen zwischen dem Rechteinhaber an den Daten (zumeist das Unternehmen, daher ohnehin auch eine Frage der Abgrenzung von § 102 und § 103 StPO) und den Strafverfolgungsorganen geschlossen wird, die vorsieht, dass der Rechteinhaber selbst die vom Durchsuchungsbeschluss umfassten Daten zusammenstellt und zur Verfügung stellt. Die StPO enthält konkret dazu keine Regelungen, die

Normierung einer „Vereinbarung“ zwischen Strafverfolgungsbehörden und Beschuldigtem wäre ihr wohl auch wesensfremd.[57]

In der Rechtsprechung ist jedenfalls für die Durchsuchung nach § 103 StPO anerkannt, dass dem Betroffenen aus Verhältnismäßigkeitsgründen grundsätzlich eine Abwendungsbefugnis durch Herausgabe des Beweismittels eingeräumt werden soll.[58] Zudem soll das Herausgabeverlangen nach § 95 StPO gegenüber einer Durchsuchung bzw. Beschlagnahme die mildere Maßnahme darstellen.[59] Beides kommt jedoch nach derzeitiger Rechtslage nicht in Betracht, wenn der Ermittlungserfolg dadurch gefährdet werden würde.[60] Es ist mithin zu diskutieren, ob Regelungen gefunden werden können, die Voraussetzungen benennen, bei deren Vorliegen die Durchsicht der Daten durch freiwillige Herausgabe abgewendet werden kann. Es liegt nahe, hier dieselben Kriterien wie zur Präzisierung des Durchsuchungsbeschlusses (Begrenzung nach Zeiträumen, durch Suchbegriffe oder andere Kriterien, etwa beim Mailverkehr auf den Kontakt zu einzelnen anderen Postfächern) anzuwenden.

Außerdem kommt in Betracht, ein Recht auf freiwillige Zusammenstellung einzuräumen, das nur bei Vorliegen konkreter Ausschlusskriterien (z.B. besondere Eilbedürftigkeit, Verdunkelungsgefahr) beschränkt werden darf. Eine Gefährdung des Ermittlungserfolges ist ausgeschlossen, wenn die Durchsuchung und Sicherstellung der Daten durch Spiegelung stattgefunden hat. Die Spiegelung darf dann nur genutzt werden, wenn die Datenlieferungsvereinbarung nicht eingehalten wird. Es sollte dabei auch diskutiert werden, dies durch ein normiertes Verwertungsverbot abzusichern. Vorgeschlagen wird eine Ergänzung des § 103 StPO wie folgt:

§ 103 Durchsicht von Papieren und elektronischen Speichermedien	
geltende Fassung	**Neufassung**
(1) Bei anderen Personen sind Durchsuchungen nur zur Ergreifung des Beschuldigten oder zur Verfolgung von Spuren einer Straftat oder zur Beschlagnahme bestimmter Gegenstände und nur dann zulässig, wenn Tatsachen vorliegen, aus denen zu schließen ist, daß die gesuchte Person, Spur oder Sache sich in den zu durchsuchenden Räumen befindet. Zum Zwecke der Ergreifung eines Beschuldigten, der dringend verdächtig ist, eine Straftat nach § 89a oder § 89c Absatz 1 bis 4 des Strafgesetzbuchs oder nach § 129a, auch in Verbindung mit § 129b Abs. 1, des Strafgesetzbuches oder eine der in dieser Vorschrift bezeichneten Straftaten begangen zu haben, ist eine Durchsuchung von Wohnungen und anderen Räumen auch zulässig, wenn diese sich in einem Gebäude befinden, von dem auf Grund von Tatsachen anzunehmen ist, daß sich der Beschuldigte in ihm aufhält.	*(1) Bei anderen Personen sind Durchsuchungen nur zur Ergreifung des Beschuldigten oder zur Verfolgung von Spuren einer Straftat oder zur Beschlagnahme bestimmter Gegenstände und nur dann zulässig, wenn Tatsachen vorliegen, aus denen zu schließen ist, daß die gesuchte Person, Spur oder Sache sich in den zu durchsuchenden Räumen befindet. Zum Zwecke der Ergreifung eines Beschuldigten, der dringend verdächtig ist, eine Straftat nach § 89a oder § 89c Absatz 1 bis 4 des Strafgesetzbuchs oder nach § 129a, auch in Verbindung mit § 129b Abs. 1, des Strafgesetzbuches oder eine der in dieser Vorschrift bezeichneten Straftaten begangen zu haben, ist eine Durchsuchung von Wohnungen und anderen Räumen auch zulässig, wenn diese sich in einem Gebäude befinden, von dem auf Grund von Tatsachen anzunehmen ist, daß sich der Beschuldigte in ihm aufhält. Zum Zwecke der Beschlagnahme bestimmter Gegenstände ist eine Durchsuchung nur zulässig, wenn der Gewahrsamsinhaber die Gegenstände nicht gemäß § 95 herausgibt; es sei denn, der Ermittlungserfolg wird durch ein solches Herausgabeverlangen konkret gefährdet.*

[57] Vgl. *Schelzke* NZWiSt 2017, 142, 143.
[58] Vgl. BGH, Beschl. v. 28.06.2017 – 1 BGs 148/17 = NJW 2017, 2359 f.; BeckOK StPO/*Hegmann* § 103 Rn. 12; *Wenzl* NStZ 2021, 395.
[59] Vgl. BeckOK StPO/*Gerhold*, StPO § 95 Rn 8 mwN.
[60] BeckOK StPO/*Hegmann* § 103 Rn. 12; BeckOK StPO/*Gerhold*, StPO § 95 Rn 8.

(2) Die Beschränkungen des Absatzes 1 Satz 1 gelten nicht für Räume, in denen der Beschuldigte ergriffen worden ist oder die er während der Verfolgung betreten hat.	*Beweismittel, die unter Verletzung des Satzes 3 erhoben wurden, dürfen nicht verwertet werden.* *(2) Die Beschränkungen des Absatzes 1 Satz 1 gelten nicht für Räume, in denen der Beschuldigte ergriffen worden ist oder die er während der Verfolgung betreten hat.*

c) Neue Ermittlungsmethoden und Herausforderungen

aa) Künstliche Intelligenz (KI)

Für den Einsatz künstlicher Intelligenz gibt es in der StPO derzeit keine Rechtsgrundlage. Es ist aber damit zu rechnen, dass die Entwicklung auf den Einsatz von KI im Strafverfahren hinausläuft. Es existieren bereits diverse Forschungsprojekte und auf europäischer Ebene werden derzeit Vorgaben für den Einsatz von KI im Strafverfahren erarbeitet. Solange der Einsatz gesetzlich nicht erlaubt ist, erübrigen sich Regelungen dazu. Sollten zu einem späteren Zeitpunkt derartige Techniken zulässig werden, so wäre die Einführung von engen, verbindlichen Vorgaben z.B. für berücksichtigungsfähige Parameter und für die Dokumentation und Nachvollziehbarkeit der Prozesse zu fordern.

Im strafrechtlichen Ermittlungsverfahren hätte der Einsatz künstlicher Intelligenz i.R.d. IT-Forensik in Wirtschaftsstrafverfahren großes Potential zur Verfahrensbeschleunigung. Es werden oftmals enorme Datenmengen sichergestellt, die mittels KI-Systemen effizienter und damit zeit- und kostenschonender von den Strafverfolgungsbehörden strukturiert werden können. Dabei sind neben der Überprüfbarkeit und Transparenz des Einsatzes auch technische Aspekte wie die Datensicherheit und der Umgang mit potentiellen Hackerangriffen[61] zu bedenken.

Im Hinblick auf die Transparenz solcher Systeme muss beachtet werden, dass bei der Entwicklung durch private Anbieter, die Funktionsmechanismen als Betriebs- und Geschäftsgeheimnisse dem Schutzgehalt der Berufsfreiheit gemäß Art. 12 GG unterfallen. Dies hat zur Folge, dass die Unternehmen nicht gezwungen werden können, die Funktionsweise offen zu legen. Damit wäre das Programm nur eingeschränkt überprüfbar.

Programme für die Berechnung von Rückfallwahrscheinlichkeiten und Gefährdungsprognosen, wie sie etwa in den USA (beispielsweise COMPAS) eingesetzt werden, bergen hingegen das Risiko einer rechtsstaatswidrigen Diskriminierung. Die Datenbasis, aufgrund derer der Algorithmus seine Entscheidung berechnet, kann nicht nur ethnische Gruppen, sondern auch Geschlechter diskriminieren. Jedenfalls solange nicht sichergestellt ist, dass eine solche Diskriminierung durch menschliche Interventionen ausgeschlossen ist, ist der Einsatz nicht mit rechtsstaatlichen Prinzipien vereinbar.

Unabhängig davon dürfen Richter und Strafverfolgungsbehörden sich nicht einseitig auf die Ergebnisse der KI verlassen. Strafrechtliche Entscheidungen allein basierend auf Vorgaben selbstständig entscheidender KI-Systeme wären letztendlich eine reine Formalität.[62]

bb) Outsourcing staatlicher Ermittlungstätigkeit an Privatunternehmen

Mit Blick auf Verfahren mit besonders umfangreichen (potenziellen) Beweismittel in Form von Daten (z.B. Cum/Ex-Verfahren) werden unter anderem auch häufig private IT-Forensik-Anbieter mit der Sichtung und Vorsortierung der Daten beauftragt. Eine gesetzliche Grundlage gibt es dafür nicht. Insbesondere werden die privaten IT-Forensik-Anbieter nicht als Sachverständige tätig. Vielmehr handelt es sich dabei um originäre Ermittlungstätigkeit. Die Auslagerung an Privatunternehmen ist schon deshalb nicht hinnehmbar, weil bei privatwirtschaftlichen Untersuchungspersonen die wirtschaftliche Motivation für

[61] Guggenberger, NVwZ 2019, 844, 849.
[62] BRAK-Stellungnahme Nr. 52/2021.

eine möglichst große Ausweitung von Ermittlungen nicht ausgeschlossen werden kann, die Beurteilung von belastendem und entlastendem Beweismaterial in einem behördlichen Verfahren jedoch frei von einer entsprechenden Motivlage zu erfolgen hat. Es ist daher eine Klarstellung zu fordern, dass die Tätigkeit von Ermittlungspersonen vorgenommen werden muss. Dies gilt in Abgrenzung zur rein technischen IT-Forensik und der Prozessierung von Daten sowie dem Hosting jedenfalls für die Durchsicht und Auswertung von Daten.

cc) „IP-Tracking“ und „IP-Catching”

Weitere durch die Digitalisierung hervorgerufene und mit neuen Herausforderungen verbundene Ermittlungsmethoden stellen das sog. „IP-Tracking“ und „IP-Catching“ dar.

Beim sog. „IP-Catching“ nehmen die Ermittlungsbehörden eine Erhebung bzw. Protokollierung der IP-Adressen von Besuchern bestimmter Webseiten vor, wobei in diesen Fällen die Datenerhebung selbst regelmäßig vom Diensteanbieter durchgeführt wird.[63] Aufgrund der vielfältigen Erscheinungsformen[64] ist das Spektrum an Ansatzpunkten für die Ermittlungsbehörden entsprechend weit. Als Rechtsgrundlage für das „IP-Catching“ kommt eine differenzierte Anwendung[65] von § 100g StPO und § 100k StPO oder eine gesamtheitliche Anwendung von § 100g StPO[66] in Betracht. Dabei kommt es darauf an, ob der betroffene Dienstanbieter als Telekommunikationsdienst i.S.v. § 3 Nr. 61 TKG oder Telemediendienst § 1 Abs. 1 TMG i.V.m. § 2 Abs. 2 Nr. 1 TTDSG einzustufen ist. Die Abhängigkeit der einschlägigen Rechtsgrundlage von der Einordnung des Diensteanbieters erweist sich in der Praxis als problematisch, da es hierbei zu Abgrenzungsschwierigkeiten kommen kann. Die Schaffung einer gesamtheitlichen Rechtsgrundlage, beispielsweise unter Ergänzung des § 100g StPO, hätte den Vorteil, dass Rechtssicherheit hinsichtlich der Anforderungen an das “IP-Catching“ gewährleistet wäre.

Eine ähnliche Problematik hinsichtlich der einschlägigen Rechtsgrundlage stellt sich auch beim sog. „IP-Tracking“, bei dem den Behörden eine elektronische Kommunikationskennung der Zielperson bereits bekannt ist. Mit Hilfe dieser Kennung wird dann z.B. eine E-Mail mit Lesebestätigung oder nachzuladenden Bildern an die Zielperson versendet oder es werden Dateien mit Lesebestätigungsfunktion zum Download bereitgestellt. Sofern der Betroffene hiervon Gebrauch macht, wird bei diesem Vorgang auch die aktuelle IP-Adresse des verwendeten Geräts bzw. des Anschlusses mitübertragen.[67] Die auf diese Weise durch die Ermittlungsbehörde eigenständig erlangte IP-Adresse kann dann beispielsweise i.R.d. Bestandsdatenabfrage gem. § 100j Abs. 2 StPO zur Aufenthaltsermittlung verwendet werden.[68] Aufgrund des vielfältigen Einsatzes[69] bietet das „IP-Tracking“ den Ermittlungsbehörden eine weitreichende Zugriffsmöglichkeit, deren Rechtsgrundlage – es werden sowohl § 100g Abs. 1 StPO, § 100h Abs. 1 Nr. 2 StPO als auch §§ 161, 163 StPO diskutiert – umstritten bleibt. [70] Um für Zielpersonen und Ermittlungsbehörden Klarheit über die strafprozessualen Anforderungen einer „IP-Tracking“-Maßnahme zu schaffen, wäre eine klarstellende Verankerung im Rahmen des § 100g StPO durch den Gesetzgeber erstrebenswert.

dd) Im Internet ermittelnde Polizeibeamte

Die Digitalisierung hat zur Folge, dass polizeiliche Ermittlungen bereits seit einiger Zeit und weiterhin vermehrt auch über das Internet erfolgen.[71] Polizeibeamte werden hierbei regelmäßig nicht als verdeckter Ermittler, sondern „lediglich“ als noeP (nicht offen ermittelnder Polizeibeamter) einzustufen sein, weil

[63] MAH Strafverteidigung/*Grözinger*, § 50 Cybercrime und Datenkriminalität Rn. 314.
[64] Bspw. Ausgestaltung als Webseite, E-Mail-Dienstleister, Anonymisierungsdienst, Internet-Foren oder jede andere Internetdienstleistung denkbar, siehe MüKo StPO/*Rückert*, StPO § 100g Rn 127.
[65] MüKo StPO/*Rückert*, StPO § 100g Rn 128 mwN.
[66] so BeckOK StPO/*Bär,* StPO § 100g Rn. 26; Bär NZWiSt 2017, 81, 84; Bruns in KK-StPO § 100g Rn. 20.
[67] Krause NStZ 2016, 139; MüKo StPO/Rückert, StPO § 100g Rn 128 mwN.
[68] BeckOK StPO/*Bär*, StPO § 100g Rn. 26.
[69] BeckOK StPO/*Bär*, StPO § 100g Rn 24.
[70] Vgl. hierzu anschaulich MüKo StPO/Rückert, StPO § 100g Rn. 125.
[71] Bspw. Ermittlungen i.R.v. Kinderpornographie.

sie nicht unter einer (dauerhaften) Legende, sondern nur gelegentlich verdeckt ohne Offenlegung ihrer Funktion ermitteln.[72] § 110a StPO ist dagegen anwendbar, wenn das schutzwürdige Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners zur Datengewinnung ausgenutzt wird.[73] Zwar sind bei einem länger andauernden, verdeckten polizeilichen Auftreten im Internet die §§ 110a ff. StPO anzuwenden, allerdings wird Nutzern des Darknets aufgrund des Auftretens unter Pseudonymen nach vorherrschender Auffassung kein schutzwürdiges Vertrauen zugesprochen, sodass es bei den Anforderungen der §§ 161, 163 StPO verbliebe.[74] Im Hinblick auf die vermehrten Ermittlungen im Darknet könnten strengere Anforderungen in Erwägung gezogen werden (hierzu auch III. 1. c.).

Die Nutzung von „echten" Accounts durch Ermittlungsbehörden ermöglicht eine neue Chance, in der digitalen Welt Fuß zu fassen, indem durch die Verwendung von bereits im Internet (insbesondere im Darknet) etablierten Profilen gegenüber anderen Nutzern ein Vertrauen geschaffen wurde.[75] Ein Ermittlungsaufwand, der beispielsweise durch das Einschleusen von noeP ins Darknet entsteht, unterbleibt folglich. Die Verwendung bereits existierender Profile gibt Ermittlungsbehörden zudem den Vorteil, dass sog. Keuschheitsproben für die Aufnahme ins Forum vermieden werden können, welche oftmals Ermittlungsbehörden vor Probleme stellen kann, weil die ermittelnden Beamten sich selbst nicht strafbar machen sollen.

Digitale Profile mit Persönlichkeitsbezug bergen aufgrund des gegenüber anderen Nutzern bestehenden Vertrauensschutzes die Gefahr eines Panoptikums, also einer uneingeschränkten staatlichen Überwachung, was mit rechtsstaatlichen Prinzipien unvereinbar ist. Dies macht die Schaffung gesetzlicher Regeln und Schranken aus anwaltlicher Perspektive notwendig.

Vorgeschlagen wird eine Regelung entsprechend der §§ 100a und 100b StPO, in der die Voraussetzungen einer solchen Maßnahme konkret festgeschrieben werden. Hierbei sollte ein Tatverdacht beschränkt auf schwere Straftaten entsprechend dem Katalog des § 100a Abs. 2 StPO sowie ein Richtervorbehalt entsprechend § 100e Abs. 1 StPO erforderlich sein. Auch wenn im Darknet kein Vertrauensschutz anerkannt wird, der verletzt werden kann, sollten die Regelungen zur Vermeidung einer ausufernden staatlichen Überwachung auch hierauf anwendbar sein.

2. Anklageerhebung und Zwischenverfahren

In der Anklageschrift muss die Staatsanwaltschaft gemäß § 200 Abs. 1 Satz 2 StPO auch die Beweismittel angeben, auf die sie den Tatverdacht stützt. Bei der Auswahl der Beweismittel sollen nur Beweismittel angegeben werden, die für die Aufklärung des Sachverhalts und die Beurteilung der Persönlichkeit des Angeschuldigten wesentlich sind (vgl. RiStBV 111 I). Hierdurch soll einerseits die Hauptverhandlung nicht überfrachtet werden[76] und andererseits die Prozessbeteiligten, insbesondere der Angeschuldigte und sein Verteidiger, in die Lage versetzt werden, den Anklagevorwurf nachzuvollziehen und sich hiergegen zu verteidigen. Urkunden und Augenscheinsobjekte sollten dabei möglichst konkret mit Fundstelle in der Akte bezeichnet werden.

Hierbei ist die Praxis der Staatsanwaltschaften jedoch uneinheitlich. Teilweise ist zu beobachten, dass Beweismittel nicht konkret aufgelistet werden, sondern insbesondere im Falle von digitalen Daten auf ganze Datenträger Bezug genommen wird, die der Anklage beigefügt werden. Hierbei wird gerade kein konkretes, sondern eine Fülle lediglich potentiell relevanter Beweismittel bezeichnet. Durch ein solches Vorgehen bleibt offen, ob alle auf dem Datenträger befindlichen Daten tatsächlich für den Tatnachweis erforderlich sind. Dies überfrachtet die Hauptverhandlung mit oftmals umfangreichen Datenmengen und

[72] Vgl. hierzu BVerfGE 120, 274; Meyer-Goßner/Schmitt/*Köhler*, StPO § 110a Rn. 4 mwN.
[73] BVerfG NJW 2008, 822 Rn. 310; MüKoStPO/*Hauschild*, StPO § 110a Rn. 22; Meyer-Goßner/Schmitt/*Köhler*, StPO § 110a Rn. 4 mwN.
[74] MüKoStPO/*Hauschild*, StPO § 110a Rn. 22; Krause NJW 2018, 678; Hauck in Löwe/Rosenberg Rn. 26b; kritisch Eschelbach in Satzger/Schluckebier/Widmaier StPO Rn. 10.
[75] Müller/Schlothauer/Knauer/Grözinger, MAH Strafverteidigung, 3. Aufl. 2022, § 50 Rn. 245.
[76] Vgl. *Meyer-Goßner/Schmitt*, 64. Auflage, StPO, § 200 Rn. 16; KK-StPO/*Schneider*, 9. Aufl. 2023, StPO § 200 Rn. 26.

schränkt die Verteidigungsmöglichkeiten erheblich ein. Durch eine Klarstellung im Gesetz könnte dies vermieden und Einheitlichkeit hergestellt werden. Zudem wird eine gegebenenfalls folgende Erörterung des Verfahrensstands gemäß § 202a StPO und auch die Hauptverhandlung selbst erleichtert und beschleunigt.

Daher schlägt die BRAK die folgende Ergänzung des § 200 StPO vor:

§ 200 Inhalt der Anklageschrift	
geltende Fassung	**Neufassung**
(1) Die Anklageschrift hat den Angeschuldigten, die Tat, die ihm zur Last gelegt wird, Zeit und Ort ihrer Begehung, die gesetzlichen Merkmale der Straftat und die anzuwendenden Strafvorschriften zu bezeichnen (Anklagesatz). In ihr sind ferner die Beweismittel, das Gericht, vor dem die Hauptverhandlung stattfinden soll, und der Verteidiger anzugeben. Bei der Benennung von Zeugen ist nicht deren vollständige Anschrift, sondern nur deren Wohn- oder Aufenthaltsort anzugeben. In den Fällen des § 68 Absatz 1 Satz 3, Absatz 2 Satz 1 genügt die Angabe des Namens des Zeugen. Wird ein Zeuge benannt, dessen Identität ganz oder teilweise nicht offenbart werden soll, so ist dies anzugeben; für die Geheimhaltung des Wohn- oder Aufenthaltsortes des Zeugen gilt dies entsprechend. *(2) In der Anklageschrift wird auch das wesentliche Ergebnis der Ermittlungen dargestellt. Davon kann abgesehen werden, wenn Anklage beim Strafrichter erhoben wird.*	*(1) Die Anklageschrift hat den Angeschuldigten, die Tat, die ihm zur Last gelegt wird, Zeit und Ort ihrer Begehung, die gesetzlichen Merkmale der Straftat und die anzuwendenden Strafvorschriften zu bezeichnen (Anklagesatz). In ihr sind ferner die Beweismittel, das Gericht, vor dem die Hauptverhandlung stattfinden soll, und der Verteidiger anzugeben. Bei der Benennung von Zeugen ist nicht deren vollständige Anschrift, sondern nur deren Wohn- oder Aufenthaltsort anzugeben. In den Fällen des § 68 Absatz 1 Satz 3, Absatz 2 Satz 1 genügt die Angabe des Namens des Zeugen. Wird ein Zeuge benannt, dessen Identität ganz oder teilweise nicht offenbart werden soll, so ist dies anzugeben; für die Geheimhaltung des Wohn- oder Aufenthaltsortes des Zeugen gilt dies entsprechend. Wird im Beweismittelverzeichnis der Anklage auf einen Datenträger verwiesen, dürfen sich nur die für die Hauptverhandlung relevanten und in der Anklage konkret bezeichneten Beweismittel hierauf befinden.* *(2) In der Anklageschrift wird auch das wesentliche Ergebnis der Ermittlungen dargestellt. Davon kann abgesehen werden, wenn Anklage beim Strafrichter erhoben wird.*

3. Hauptverhandlung

a) Dokumentation der Hauptverhandlung

Im Hinblick auf die Hauptverhandlung begrüßt es die BRAK[77] ausdrücklich, dass nunmehr eine umfassende und zeitgemäße Dokumentation der Hauptverhandlung in Strafsachen eingeführt werden soll.[78] Mit einer Aufzeichnung des Verfahrens, wie sie die Gesetzesentwürfe vorsehen, soll nunmehr die Lücke der fehlenden inhaltlichen Dokumentation der erstinstanzlichen Verfahren vor dem Landgericht und dem Oberlandesgericht geschlossen werden. Hierdurch kann insbesondere die Transparenz, Wahrheitsfindung und Rechtskontrolle gestärkt werden. Dies erscheint vor allem bei (Zeugen)Aussagen von maßgeblicher Bedeutung, da hierbei eine für die Verfahrensbeteiligten verbindliche Dokumentation erfolgt.[79] Diese zuverlässige Dokumentation bildet wiederum auch eine zuverlässige Grundlage für das Urteil selbst.

b) Videoverhandlung

Eine Videoverhandlung im Strafverfahren, wie bereits jetzt im Zivilverfahren möglich[80], wird hingegen abgelehnt.[81] Wie eingangs erwähnt[82], würde es dem Grundsatz der Unmittelbarkeit zuwiderlaufen, wenn dem Gericht zu Lasten des Angeklagten die Möglichkeit des Verschaffens eines persönlichen Eindrucks verwehrt wird. Auch aufgrund der Grundsätze der Mündlichkeit und der Öffentlichkeit ist die persönliche Anwesenheit des Angeklagten als Zentralfigur der Hauptverhandlung absolut zwingend und muss dies auch bleiben.

c) Strafvollstreckungsverfahren

Im Strafvollstreckungsverfahren ist der Einsatz von Videokonferenztechnik hingegen zu begrüßen, sofern es den befassten Richtern möglich bleibt, einen unmittelbaren persönlichen Eindruck von dem Verurteilten zu erhalten.[83] Insofern ist etwa die Anhörung eines Sachverständigen mittels Einsatzes von Videokonferenztechnik denkbar, da hierbei der unmittelbare persönliche Eindruck des Gerichts nicht in gleicher Weise bedeutsam ist, wie bei dem Verurteilten selbst.

d) Erhebung und Einführung digitaler Beweismittel

Eine weitere Herausforderung im Hinblick auf die Digitalisierung und Modernisierung der Hauptverhandlung liegt in der Frage, ob und wie digitale Beweismittel erhoben bzw. eingeführt werden können. Die Menge digitaler Daten nimmt stetig zu, weshalb sie auch immer häufiger als Beweismittel im Strafverfahren Verwendung finden. Gleichzeitig werden hierdurch zunehmend persönlichkeitsrelevante Informationen gewonnen, sodass zwangsläufig Beeinträchtigungen des Allgemeinen Persönlichkeitsrechts

---

[77] Vgl. BRAK-Stellungnahme Nr. 08/2023 und 23/2023.

[78] Entwurf eines Gesetzes zur digitalen Dokumentation der strafgerichtlichen Hauptverhandlung (Hauptverhandlungsdokumentationsgesetz – DokHVG), BT-Drs. 20/8096. Zum aktuellen Stand des parlamentarischen Verfahrens: https://www.brak.de/newsroom/newsletter/nachrichten-aus-berlin/nachrichten-aus-berlin-2023/ausgabe-25-2023-v-14122023/dokumentation-im-strafprozess-brak-protestiert-gegen-angekuendigte-laender-blockade-im-bundesrat/ und https://www.brak.de/newsroom/news/digitalisierung-der-justiz-dokumentation-strafgerichtliche-hauptverhandlung-und-128a-zpo-im-bundesrat/

[79] BRAK-Stellungnahme Nr. 08/2023, S. 3.

[80] Vgl. § 128a ZPO; hierzu allgemein van Hattem/Bafteh, MMR 2023, 100.

[81] Vgl. bereits BRAK-Stellungnahme Nr. 70/2020.

[82] Vgl. hierzu A.

[83] BRAK StN Nr. 70/2020.

aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zu besorgen sind.[84] Da digitale Daten als Zahlenfolgen selbst keine körperliche Form aufweisen und für ihre Erfassung eine Umwandlung in eine wahrnehmbare Form erforderlich ist[85], muss bereits bei der Erhebung der Daten, zumeist im Ermittlungsverfahren, die Gefahr einer Kontaminierung der Daten, eine darauf basierende Unsicherheit hinsichtlich der Authentizität und damit einhergehenden Beeinträchtigung des Beweiswertes vermieden werden.[86] In der Hauptverhandlung werden elektronische Dokumente regelmäßig als Urkunden[87] oder Augenschein[88] in die Hauptverhandlung eingeführt. Die Authentizität solcher elektronischer Beweismittel wird in der Praxis in aller Regel nicht hinterfragt. Insbesondere aufgrund der zu erwartenden zunehmenden Nutzung von KI und damit zunehmenden Manipulationsmöglichkeiten wird eine kritischere Haltung aller Beteiligten angezeigt sein. Wesentlich sind insbesondere die lückenlose Nachvollziehbarkeit der Herkunft und Gewinnung der Beweismittel sowie angemessene Beweisverwertungsverbote.

4. Revision

Die Existenz einer vollständigen Aufzeichnung der Hauptverhandlung könnte zu einer Reihe für das Revisionsrecht neuer Fragestellungen führen.[89] Das folgt schon daraus, dass die Überprüfung von Verfahrensverstößen in der Revisionsinstanz bislang durch das Verbot der Rekonstruktion des Inhalts der tatrichterlichen Beweisaufnahme[90] begrenzt war aufgrund des Dokumentationsdefizits der Beweisaufnahme und der damit verbundenen Nachweisschwierigkeiten. Dieser Grund würde mit der Existenz der gesetzlich vorgesehenen Aufzeichnung entfallen.[91]

Durch die Bild-Ton-Aufzeichnung würde namentlich ein Beweismittel geschaffen, das geeignet ist, dem Revisionsgericht den Inhalt der tatgerichtlichen Beweisaufnahme ebenso zuverlässig zu vermitteln, wie dies z.B. bei Urkunden der Fall ist.[92] Auch wenn der Aufzeichnung nach dem Referentenentwurf „kein Protokollcharakter“ zukommen soll[93], darf und sollte sie im Revisionsverfahren daher nicht unberücksichtigt bleiben.[94]

IV. Ausblick

Die Digitalisierung und die damit verbundene Notwendigkeit zur Anpassung von strafprozessualen Vorschriften zeigt sich in allen (möglichen) Verfahrenssituationen und Stadien des Strafverfahrens. Sie hat die praktische Anwendbarkeit der StPO an mancherlei Stelle überholt, so dass ein Tätigwerden des Gesetzgebers erforderlich ist. Die Anpassung des Strafverfahrensrechts an die Digitalisierung darf nicht eindimensional bleiben; sie bedeutet nicht nur eine „Vereinfachung“ von Verfahrensschritten, vielmehr müssen die Rechte der Betroffenen gewahrt bleiben, gerade weil diese durch die fortschreitende Digitalisierung und die erweiterten technischen Möglichkeiten oftmals noch intensiver berührt werden.

Hinzu kommt, dass die mit der Digitalisierung einhergehenden Chancen und Gefahren sich nicht auf das deutsche Bundesgebiet beschränken. So geht die Thematik auch mit Fragen der Verwertung von im Ausland erhobenen Daten einher[95] - wie damit umzugehen ist, ist bisher nicht geklärt, wird aber in

---

[84] Fährmann MMR 2020, 228.
[85] Fährmann MMR 2020, 228.
[86] Vgl. Müller NZWiSt 2020, 96, 100.
[87] KK-StPO/Krehl, 9. Aufl. 2023, StPO § 244 Rn. 21.
[88] MüKo StPO/Trüg/Habetha, 1. Aufl. 2016, StPO § 244 Rn. 127.
[89] Hierzu BRAK-Stellungnahme Nr. 08/2023, 23/2023 und 63/2023.
[90] Nicht gesetzlich geregelt, da von der Rechtsprechung entwickelt und somit keine gesetzliche Neuregelung zur Aufhebung erforderlich, vgl. BRAK-Stellungnahme Nr. 8/2023, S. 10.
[91] Hierzu BRA*K*-Stellungnahme Nr. 8/2023 und 23/2023.
[92] BRAK-Stellungnahme Nr. 08/2023, S. 11.
[93] Hierzu S. 12. Entwurf eines Gesetzes zur digitalen Dokumentation der strafgerichtlichen Hauptverhandlung (Hauptverhandlungsdokumentationsgesetz – DokHVG).
[94] Vgl. hierzu schon *Schmitt* NStZ 2019, 1, 8; *Bartel* StV 2018, 678, 682; BRAK-Stellungnahme Nr. 08/2023, S. 11.
[95] Dies spielt beispielsweise in Encro-Chat oder Anom-Fällen eine Rolle.

Zukunft an Bedeutung gewinnen. Dieser Problemkreis wird nicht nur strafprozessuale Fragen aufwerfen, sondern auch die Thematik betreffen, wie die nationalen Strafverfolgungsorgane verschiedener Staaten untereinander agieren. Die Anpassung der durch die StPO vorgegebenen Standards im Umgang mit der Digitalisierung stellt eine wichtige, interdisziplinär wie international geprägte Aufgabe eines bereits begonnenen, aber noch lange nicht abgeschlossenen neuen Zeitalters dar, die eine ständige kritische Überprüfung erforderlich macht.

- - -