1717 Durchsuchung, Durchsicht von Papieren

Das Wichtigste in Kürze:

1. Die „Durchsicht von Papieren" ist noch Teil der Durchsuchung.
2. Zu den „Papieren" i.S.d. § 110 zählt alles, was wegen seines Gedankeninhalts Bedeutung hat.
3. Die Durchsicht der Papiere ist das Mittel, um die als Beweisgegenstände in Betracht kommenden Papiere oberflächlich inhaltlich darauf zu prüfen, ob eine richterliche Beschlagnahme zu beantragen oder die Rückgabe notwendig ist.
4. Die Durchsicht kann unmittelbar im Anschluss an die Durchsuchung „vor Ort", aber auch später an einem anderen Ort stattfinden.
5. Nach § 110 Abs. 1 ist für die Durchsicht der Papiere die StA bzw. der Richter zuständig.
6. Der Beschuldigte/Betroffene ist von der Durchsicht zumindest zu unterrichten. Dem Verteidiger dürfte ein Teilnahmerecht zustehen.
7. In § 110 Abs. 3 ist durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung v. 21.11.2007 die sog. Online-Sichtung eingeführt worden.
8. Das im Bereich der Durchsicht von Papieren zulässige Rechtsmittel ist i.d.R. der Antrag nach § 98 Abs. 2 S. 2.

1718 **Literaturhinweise:** **Artkämper**, Die „Durchsicht von Papieren" nach § 110 StPO, StRR 2007, 12; **Bär**, Der Zugriff auf Computerdaten im Strafverfahren, 1992; *ders.*, Durchsuchungen im EDV-Bereich, CR 1995, Teil I: CR 1995, 158; Teil II: CR 1995, 227; *ders.*, Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen – Gesetzliche Neuregelungen zum 1.1.2008, MMR 2008, 215; *ders.*, Transnationaler Zugriff auf Computerdaten, ZIS 2011, 53; **Bäumerich**, Verschlüsselte Smartphones als Herausforderung für die Strafverfolgung Neue Technologien, alte Befugnisse, NJW 2017, 2718; **Basar**, Anforderungen an die digitale Beweissicherung im Strafprozessrecht und in internen Untersuchungen, in: Festschrift für *Wessing*, 2015, S. 635; **Beyer**, Durchsicht von Papieren nach § 110 StPO, AO-StB 2009, 147, **Braun**, Die Durchsicht elektronischer Speichermedien: Zugriff auf Speichermedien andernorts zulässig, PStR 2012, 86; **Brodowski/Eisenmenger**, Zugriff auf Cloud-Speicher und Internetdienste durch Ermittlungsbehörden, ZD 2014, 119; **Burhoff**, Die Durchsicht von Papieren nach dem JuMoG, PStR 2005, 7; *ders.*, Beschlagnahme von Emails, StRR 2009, 331; **Cornelius**, Cloud Computing für Berufsgeheimnisträger, StV 2016, 380; **Dauster**, Betroffenheit in der Vertraulichkeitssphäre, polizeiliche „venia legendi" aufgrund richterlicher Beschlagnahmeanordnung und die Restriktionen des § 110 StPO, StraFo 1999, 186; **Gaede**, Der grundrechtliche Schutz gespeicherter E-Mails beim Provider und ihre weltweite strafprozessuale Überwachung, StV 2009, 96; **Gercke**, Zur Zulässigkeit sog. Transborder Searches – Der strafprozessuale Zugriff auf im Ausland gespeicherte Daten, StraFo 2009, 271; **Graulich**, Die Sicherstellung von während einer Durchsuchung aufgefundenen Gegenständen – Beispiel Steuerstrafverfahren, wistra 2009, 299; **Herrmann/Soine**, Durchsuchung persönlicher Datenspeicher und Grundrechtsschutz, NJW 2011, 2922; **Hiéramente**, Durchsuchung und „Durchsicht" der Unternehmens-IT – Betrachtungen zu §§ 103, 110 StPO, wistra 2016, 432; **Hiéramente/Fenina**, Telekommunikationsüberwachung und Cloud Computing Der § 100a-Beschluss als Nimbus der Legalität?, StraFo 2015 365; **Hirtz/Sommer**, 1. Justizmodernisierungsgesetz, 2004; **Hoffmann/Wißmann**, Zur zulässigen Dauer von Durchsuchungsmaßnahmen, NStZ 1998, 443; **Hornung**, Rechtswidrigkeit heimlicher Computerausforschung, CR 2007, CR 2007, 144; **Jahn/Kudlich**, Die strafprozessuale Zulässigkeit der Online-Durchsuchung, JR 2007, 57; **Kasiske**, Neues zur Beschlagnahme von E-Mails beim Provider, StraFo 2010, 228; **Kemper**, Das Beschlagnahmeverzeichnis nach § 109 StPO in Wirtschafts- und Steuerstrafverfahren, wistra 2008, 96; *ders.*, Die „Mitnahme zur Durchsicht" – Ein vom Gesetz nicht vorgesehenes Instrument zur Sicherstellung von Beweismitteln? – zugleich Replik auf *Graulich* wistra 2009, 299 –, wistra 2010, 295; **Knauer/Wolf**, Zivilprozessuale und strafprozessuale Änderungen durch das Erste Justizmodernisierungsgesetz – Teil 2: Änderungen der StPO, NJW 2004, 2932; **Knierim**, Fallrepetitorium zur Wohnraumüberwachung und anderen verdeckten Eingriffen nach neuem Recht, StV 2009, 206; **König**, Das Erste Gesetz zur Modernisierung der Justiz – Synoptische Darstellung und Kommentierung, auf www.strafverteidiger-berlin.de; **Krause**, Sicherung von ausländischen E-Mail-Postfächern durch heimliches Einloggen – innovativ oder unzulässig?, Krim 2014, 213; **Kronisch**, Zur zeitlichen Geltung von Durchsuchungs- und Beschlagnahmebeschlüssen, AnwBl 1988, 617; **Laurinat/Stalberg**, Durchsuchung: Durchsicht von Daten und Durchsuchung bei Dritten, PStR 2012, 283; **Mahnkopf/Funk**, Zur Frage des Anwesenheitsrechts von Sachverständigen bei strafprozessualen Durchsuchungsmaßnahmen im Zusammenhang mit ärztlichen Abrechnungsbetrügereien, NStZ 2001, 519; **R. Michalke**, Durchsuchung und Beschlagnahme – Verfassungsrecht im Alltag, StraFo 2014, 89; **Mildeberger/Riveiro**, Zur Durchsicht von Papieren, StraFo 2004, 43; **Niemeyer**, Step-by-step: Durchsuchung von Computern, Smartphones und sonstigen Datenspeichern CB 2013, 133; **Obenhaus**, Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft

NJW 2010, 651; **Park**, Der Anwendungsbereich des § 110 StPO bei Durchsuchungen in Wirtschafts- und Steuerstrafsachen, wistra 2000, 453; **Peters**, Anwesenheitsrecht bei der Durchsicht von Papieren im Rahmen von Durchsuchungen, NZWiSt 2017, 465; **Rolletschke**, Die Hinzuziehung eines Betriebsprüfer bei einer Durchsuchungsmaßnahem der Steuerfahndung, DStZ 1999, 444; **Schelzke**, Die iCloud als Gefahr für den Rechtsanwalt? HRRS 2013, 86; *dies*., Der „Vereinbarung" anlässlich einer Durchsuchung, NZWiSt 2017, 142; **Schilling/Rudolph/Kuntze**, Sicherstellung elektronischer Daten und „selektive Datenlöschung, HRRS 2013, 207; **Schlegel**, „Online-Durchsuchung light" – Die Änderung des § 110 StPO durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung, HRRS 2008, 23; **Sommer**, Moderne Strafverteidigung – Strafprozessuale Änderungen des Justizmodernisierungsgesetzes, StraFo 2004, 295; **Wicker**, Durchsuchung in der Cloud, MMR 2013, 765; **Winterhoff**, Kanzleidurchsuchungen im Lichte von Grund- und Menschenrechten, AnwBl. 2011, 789; **Zerbes/El-Ghazi**, Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung, NStZ 2015, 425; **Zimmermann**, Der strafprozessuale Zugriff auf E-Mails, JA 2014, 321; s.a. die Hinw. bei → *Beschlagnahme, Durchführung*, Rdn 930, bei → *Durchsuchung, Allgemeines*, Rdn 1555, bei → *Durchsuchung, Beweisverwertungsverbote*, Rdn 1685, und bei → *Online-Durchsuchung*, Rdn 2948.

1. Haben die Durchsuchungsbeamten bei einer Durchsuchung Papiere mitgenommen, ist für die Verteidigung die dann nach der eigentlichen Durchsuchungsmaßnahme stattfindende Durchsicht dieser Papiere und ggf. sog. räumlich getrennter Speichermedien von besonderer Bedeutung (§ 110). Diese „Durchsicht" ist **noch Teil** der **Durchsuchung** (vgl. u.a. BGH NStZ 2002, 215; 2003, 670 m.w.N.; NStZ-RR 2010, 67 [Ci/Zi]; OLG Bremen wistra 1999, 75), was für die Frage der Rechtsmittel von Bedeutung ist (→ *Durchsuchung, Rechtsmittel*, Rdn 1771). Im Zusammenhang mit einer Durchsicht muss der Verteidiger auf Folgendes **achten** (s.a. *Dahs*, Rn 384; *Wehnert* StraFo 1996, 78; *Park*, Rn 228 ff.; zu § 110 Abs. 3 s. eingehend *Schlegel* HRRS 2008, 23; *Bär* ZIS 2011, 53): **1719**

- **Zweck** des § 110 ist in erster Linie der **Schutz** der **Persönlichkeitssphäre** des von einer Durchsuchung Betroffenen (eingehend *Park* wistra 2000, 453). Das ist bei der Auslegung und Anwendung der Vorschrift zu beachten (vgl. krit. zur Erweiterung der Vorschrift durch das 1. JuMoG *Knauer/Wolf* NJW 2004, 2937; *König*, S. 8; *Sommer* AnwBl 2004, 507 = StraFo 2004, 295; krit. zur Erweiterung des § 110 durch das TKÜErwG v. 21.12.2007 *Schlegel* HRRS 2008, 25). In dem Zusammenhang hat– wenn es um die „Online-Durchsicht" geht – die Entscheidung des BVerfG v. 16.6.2009 (NJW 2009, 2431) Bedeutung. **1720**
- Insbesondere muss auch bei der Durchsicht noch immer der allgemeine **Verhältnismäßigkeitsgrundsatz** beachtet werden. Die Durchsicht muss nicht zwingend alle vorhandenen Papiere erfassen (SK-*Wohlers*, § 110 Rn 20), und sie ist zu beenden, wenn erkennbar wird, dass sie zu keinem Ergebnis führen wird (BGH CR 1999, 292, für Durchsicht eines Datenträgers; s.a. BVerfG, a.a.O.).
- § 110 ist durch das TKÜErwG v. 21.12.2007 geändert worden. Der neue Abs. 3 lässt danach eine sog. **Online-Sichtung** zu. Die damit zusammenhängenden Fragen sind dargestellt bei den Rdn 1735 ff.

☝ Nach **§ 160a** sind Zwangsmaßnahmen wie Durchsuchungen und damit auch die Durchsichten i.S.d. § 110 bei bestimmten **Berufsgeheimnisträgern** und deren Gehilfen unzulässig, wenn sie dem Ziel dienen, Gegenstände aufzufinden, auf die sich das Zeugnisverweigerungsrecht bezieht, bzw. unterliegen diese Maßnahmen einer besonderen Verhältnismäßigkeitsprüfung (→ *Beweiserhebungs-/Beweisverwertungsverbot für Berufsgeheimnisträger*, Rdn 1124). Das gilt auch für elektronische Datenbestände. Das BVerfG (s. ausdrücklich NJW 2005, 1917) fordert hier eine **automatisierte Suche**. Die Entscheidung ist zwar zur Durchsuchung einer Anwaltskanzlei ergangen, man wird ihre Grundsätze aber allgemein anwenden können/müssen (s. dazu BVerfG NJW 2009, 2431, in dem auf die Grundsätze von NJW 2005, 1917 verwiesen wird).

2. Erfasst werden von **§ 110 Abs. 1** nach h.M. **Papiere**, die bei einer Durchsuchung gefunden worden sind, nicht bei einer anderen Gelegenheit (*Meyer-Goßner/Schmitt*, § 110 Rn 1 m.w.N. auch zur a.A.; zum Begriff der „Papiere" eingehend *Artkämper* StRR 2008, 12, 13; *Park* wistra 2000, 455; *ders.*, Rn 222 ff.; *Schlegel* HRRS 2008, 24). **Entsprechend** anzuwenden ist § 110 auf Papiere, die nicht bei einer Durchsuchung, sondern bei **anderer Gelegenheit** in den Gewahrsam der Behörde gelangt sind (*Meyer-Goßner/Schmitt*, § 110 Rn 1; *Park* wistra 2000, 455 m.w.N.). **1721**

☝ **Grds**. ist Voraussetzung für die Anwendung des § 110 die Möglichkeit des **körperlichen** Zugriffs auf den Durchsuchungsgegenstand (BVerfG NJW 2006, 976, 981). Diese Voraussetzung ist für die Durchsicht von Speichermedien durch § 110 Abs. 3 allerdings aufgehoben worden (vgl. dazu Rdn 1735).

1722 Zu den „**Papieren**" i.S.d. § 110 zählt alles (s.a. *Peters* NZWiSt 2017, 465),

- was wegen seines Gedankeninhalts Bedeutung hat. I.d.R. wird es auf Papier geschrieben sein, also z.B. private und geschäftliche **Schriftstücke**, wie Briefe, Tagebücher, Bilanzen, Buchungsunterlagen, Werk- und Lagezeichnungen oder Skizzen (BGH NStZ 2003, 670).
- Zu den Papieren gehören aber auch Unterlagen, bei denen statt Papier ein **anderes Material** oder **System** verwendet worden ist (BGH, a.a.O.), wie z.B.
  - **Disketten** und die zum Lesen und Verarbeiten notwendigen **Zentralcomputereinheiten, EDV-Anlage** sowie auch ein **Notebook** mit den darauf gespeicherten EDV-Daten (BVerfG NJW 2002, 1410; 2005, 1917; BGHSt 45, 37; BGH NStZ 2003, 670; JR 2007, 78; LG Köln NStZ 1995, 54 [zur Durchsuchung einer EDV-Anlage]; *Meyer-Goßner/Schmitt*, § 110 Rn 1; *Schlegel* HRRS 2008, 23, 25, der darauf hinweist, dass durch die Einfügung des Abs. 3 daran kein Zweifel mehr besteht; *Hiéramente* wistra 2016, 432; *Zerbes/El-Ghazi* NStZ 2015, 425; zum sog. Cloud Computing *Obenhaus* NJW 2010, 651; *Braun* PStR 2012, 86, 89; *Cornelius* StV 2016, 380),
  - nach Abs. 3 auch Daten auf **räumlich getrennten Speichermedien** (sog. elektronische Netzwerkressourcen; *Schlegel* HRRS 2008, 23, 25; *Hiéramente*, *Zerbes/El-Ghazi*, jew. a.a.O.; zur Cloud *Schelzke* HRRS 2013, 86; *Brodowski/Eisenmenger* ZD 2014, 119; vgl. dazu inzidenter auch BVerfG NJW 2009, 2431, zur Beschlagnahme von E-Mails, die auf dem Mailserver des Providers gespeichert sind),
  - **Farbbänder** einer Schreibmaschine (LG Berlin StV 1987, 97),
  - **Tonträger**, **Filme**, **Lochkarten** oder **Magnetbänder** für Datenverarbeitungsanlagen (KK-*Bruns*, § 110 Rn 2; *Rengier* NStZ 1981, 376; zu den Sonderproblemen im EDV-Bereich s. den umfangreichen Aufsatz von *Bär* CR 1995, 158 ff., 227 ff., zum Kreis der Beweismittel insbesondere 159 ff.),
- **nicht** jedoch zur **Vorlage** bei Behörden **bestimmte Urkunden**, wie z.B. Führerscheine oder Personalausweise (vgl. *Meyer-Goßner/Schmitt*, § 110 Rn 1).

1723 **3.** Die Durchsicht der Papiere ist das Mittel, um die als Beweisgegenstände in Betracht kommenden Papiere oberflächlich inhaltlich darauf zu **prüfen**, ob eine richterliche **Beschlagnahme** zu **beantragen** oder die Rückgabe notwendig ist. Nach § 97 **beschlagnahmefreie Papiere** (→ *Beschlagnahme, Beschlagnahmeverbote*, Rdn 863) sind sofort herauszugeben (vgl. dazu BVerfG NJW 1990, 563 f.; 2002, 1410), und zwar ungelesen. Bei auf einem Computer gespeicherten Daten besteht die Herausgabe darin, dass von den herauszugebenden Daten Kopien für den Beschuldigten gefertigt und die Daten anschließend auf der Festplatte gelöscht werden (BVerfG, a.a.O.; zur „Online-Sichtung" s. Rdn 1753 ff.).

1724 **Handakten** dürfen allerdings daraufhin **durchgeblättert** werden, ob in ihnen ggf. „getarnt" Beweismaterial aufbewahrt wird (OLG Hamm NStE Nr. 3 zu § 103 StPO). Allein die Erklärung des Beschuldigten und/oder des Verteidigers macht Unterlagen auch nicht zu Verteidigungsunterlagen (LG Oldenburg PStR 2002, 95). Ist nicht sofort feststellbar, ob die Unterlagen beschlagnahmefrei sind, können sie zur Durchsicht vorläufig sichergestellt werden (BVerfG NJW 2005, 1917; 2009, 2431 für E-Mails). Die Papiere dürfen dann zum Zweck der Durchsicht mitgenommen und an die StA abgeliefert werden. Die durchsuchenden Beamten müssen i.Ü. so verfahren, wenn sie zur Durchsicht nicht befugt sind (OLG Bremen wistra 1999, 75 f.; s. Rdn 1728).

1725 **4.** Die Durchsicht kann **unmittelbar** im Anschluss an die Durchsuchung „**vor Ort**", aber **auch später** an einem anderen Ort stattfinden (s. zur dann erforderlichen Siegelung und zum Teilnahmerecht des Verteidigers u. Rdn 1732). Hat sie bereits unmittelbar „vor Ort" stattgefunden und haben die dazu befugten

Durchsuchungsbeamten entschieden, welche Unterlagen „mitgenommen" werden, liegt bereits eine Beschlagnahme vor, die Durchsuchung ist beendet und eine spätere, nochmalige Durchsicht ist nicht mehr „Durchsicht" i.S.v. § 110, sondern **Auswertung** der Unterlagen (OLG Bremen wistra 1999, 75).

Erfolgt die **Durchsicht** der Papiere am **Durchsuchungsort**, kann sofort über die **Beschlagnahme** entschieden werden. Werden die Papiere von einem vorliegenden, allerdings nicht konkret gefassten Beschlagnahmebeschluss nicht erfasst, müssen sie dem Richter zur Beschlagnahme vorgelegt werden. Der StA kann die Beschlagnahme nicht wegen „Gefahr im Verzug" selbst vornehmen, da die Voraussetzungen insoweit nicht vorliegen, die Papiere sind sichergestellt (*Park* wistra 2000, 456). **1726**

Anderenfalls können/müssen die Papiere **mitgenommen** werden. Diese Mitnahme zur Durchsicht ist noch keine Beschlagnahme (*Park*, a.a.O., m.w.N.; zur Durchsicht von Behördenakten OLG Jena NJW 2001, 1290; zu „Sicherstellung" auch *Graulich* wistra 2009, 299), sodass ein Beschlagnahmeverzeichnis (§ 109) noch nicht angelegt werden muss. Die Papiere sind zur Mitnahme in einem verschlossenen **Umschlag** zu **versiegeln** (§ 110 Abs. 2 S. 2; vgl. auch dazu *Park* wistra 2000, 456). Nach § 110 Abs. 3 Hs. 1 a.F. war dem Inhaber der Papiere oder dessen Vertreter „die Beidrückung eines Siegels gestattet". Diese Möglichkeit ist durch das 1. JuMoG gestrichen worden, weil sie in der Praxis – so der Rechtsausschuss des Bundestages – nur geringe Bedeutung gehabt habe (BT-Drucks 15/3482, S. 58; zur Siegelung s.a. *Meyer-Goßner/Schmitt*, § 110 Rn 5). **1727**

5.a) Nach § 110 Abs. 1 ist für die Durchsicht der Papiere die **StA** bzw. der **Richter** zuständig (vgl. dazu auch OLG Jena NJW 2001, 1290). Nach Auffassung des AG Hanau (NJW 1989, 1493; s.a. KK-*Bruns*, § 97 Rn 25) sind bei der Durchsuchung einer Anwaltskanzlei schriftliche Mitteilungen zwischen Verteidiger und Beschuldigtem von der StA ohne eigene Durchsicht dem zuständigen Richter zur Prüfung eines Beschlagnahmeverbots vorzulegen (→ *Beschlagnahme, Beschlagnahme der Handakten des Verteidigers*, Rdn 848; → *Beschlagnahme, Beschlagnahmeverbote*, Rdn 868). Die StA kann zur Durchsicht einen **SV hinzuziehen**, allerdings muss sie zunächst selbst oder durch → *Ermittlungspersonen der Staatsanwaltschaft*, Rdn 2105, zumindest eine Sichtung vornehmen, um die Notwendigkeit einer sachverständigen Begutachtung beurteilen zu können (LG Kiel NJW 2006, 3224; zur unzulässigen, weil „unverhältnismäßigen" Zuziehung eines Durchsuchungszeugen aus dem „Lager" der Anzeigeerstatterin s. LG Berlin wistra 2012, 410). Unzulässig ist es daher, wenn z.B. ein SV bei der Durchsuchung vor Ort selbstständig einen Rechner überprüft, alle für die weitere Untersuchung erforderlichen Feststellungen trifft und den weiteren Gang der Untersuchung bestimmt (LG Kiel, a.a.O.). Im **Steuerstrafverfahren** hat nach § 404 S. 2 AO die Steuerfahndung das Recht, Papiere und Schriftstücke sofort durchzusehen (s.a. *Streck* StV 1984, 348 ff.; *Mildenberger/Riveiro* StraFo 2004, 43, 45; → *Steuerstrafverfahren, Besonderheiten*, Rdn 3847 ff.). Die Steuerfahnder dürfen aber bei einer Durchsuchung nicht hinzugezogen werden, damit sie als SV „getarnt" Anhaltspunkte für Straftaten ermitteln können, um dann die entsprechenden Unterlagen gem. § 108 zu beschlagnahmen (LG Stuttgart NStZ-RR 1998, 55; → *Durchsuchung, Beweisverwertungsverbote*, Rdn 1712; zur Durchsicht in Steuerstrafverfahren eingehend *Park* wistra 2000, 454; zur Hinzuziehung eines Betriebsprüfers s. *Rolletschke* DStZ 1999, 444). **1728**

☝ Das **BVerfG** hat in Fortführung seiner Grundsatzentscheidung (in NJW 2005, 1917) in seinem Beschluss v. 5.7.2005 (NJW 2005, 3414) noch einmal ausdrücklich darauf hingewiesen, dass auch bei der Durchsicht zu berücksichtigen sei, dass die Gewinnung **überschießender** und **vertraulicher**, für das Verfahren aber bedeutungsloser **Informationen** im Rahmen des Vertretbaren **vermieden** werden müsse, was vor allem bei der beabsichtigten Beschlagnahme von Kanzleidaten eines Rechtsanwalts gelte; → *Beschlagnahme, Beschlagnahme der Handakten bzw. von Computerdateien des Verteidigers/Rechtsanwalts*, Rdn 863; vgl. noch BVerfG, Beschl. v. 17.11.2007 – 2 BvR 518/07, wonach bei einem ggf. bestehenden verfassungsrechtlichen BVV [Tagebuch] „größtmögliche Zurückhaltung zu wahren ist" und auch NJW 2009, 2431, für die Sichtung von Emails; zum Testament s. LG Koblenz NJW 2010, 2227).

1729 **b)aa)** Bis zu den Änderungen durch das 1. JuMoG im Jahr 2004 durften die sog. Hilfsbeamten der StA die Durchsicht von Papieren nicht durchführen. Durch das 1. JuMoG ist § 110 Abs. 1 dahin ergänzt worden, dass die Durchsicht von Papieren jetzt **auch** ohne Zustimmung des von der Durchsicht Betroffenen auf die → ***Ermittlungspersonen*** der ***Staatsanwaltschaft***, Rdn 2105, übertragen werden kann. Erforderlich ist nur eine **Anordnung** der **StA**, die telefonisch und auch vorab erteilt werden kann (BR-Drucks 378/03, S. 55). Diese Änderung, die der bis dahin schon geltenden Rechtslage im Steuerstrafverfahren nach § 404 Satz 2 AO entsprach, hat der Gesetzgeber damit begründet, dass die StA Datenbestände auf Computern, die immer häufiger beschlagnahmt werden, aus technischen Gründen nicht ohne Weiteres sichten könne, dafür sei die Polizei besser ausgerüstet (BR-Drucks 378/03, S. 56). Zu Recht wird in der Lit. (zum 1. JuMoG) diese Neuregelung als **bedenklich** angesehen. Die Gefahr, dass die Persönlichkeitsrechte des Betroffenen noch weiter ausgehöhlt werden als das schon bis dahin der Fall war, darf nicht übersehen werden (*Knauer/Wolf* NJW 2004, 2937; *König*, S. 8; *Sommer* AnwBl 2004, 507 = StraFo 2004, 295). Auch werden die die Papiere durchsehenden Polizeibeamten als juristische Laien nicht immer in der Lage sein zu beurteilen, ob ggf. ein Beschlagnahmeverbot besteht. Zudem besteht die Gefahr, dass bei der Durchsicht gewonnene Erkenntnisse von den „Ermittlungspersonen" zu weiteren Ermittlungen genutzt werden.

☝ Der **Verteidiger** muss daher noch mehr als in der Vergangenheit **versuchen**, bei einer seinen Mandanten betreffenden Durchsuchung bzw. Durchsicht von Papieren **anwesend** zu **sein**, um darauf achten zu können, dass die sich aus § 97 ergebenden Beschlagnahmeverbote auch beachtet werden (→ *Durchsuchung, Anwesenheit des Verteidigers*, Rdn 1653 ff.; s.a. *Sommer*, a.a.O.; *Peters* NZWiSt 2017, 465). In dem Zusammenhang kann ggf. ein Hinweis auf den Beschl. v. des BVerfG v. 16.6.2009 (NJW 2009, 2431) hilfreich sein. Das BVerfG hat dort für die Sichtung von E-Mails darauf hingewiesen, dass es geboten sein kann, aus Gründen der Verhältnismäßigkeit den Inhaber der sichergestellten E-Mails in die Prüfung von deren Verfahrenserheblichkeit einzubeziehen. Dessen Anwesenheitsrecht sei zwar durch das 1. JuMoG aufgehoben worden, was eine Anwesenheit jedoch nicht ausschließe (vgl. a. *Hiéramente* wistra 2016, 432; *Zerbes/El-Ghazi* NStZ 2015, 425).

Der Verteidiger muss insbesondere auf den Durchsuchungsbeschluss und die konkret dort aufzuführenden Beweisgegenstände, nach denen gesucht werden soll, achten. Dem Durchsuchungsbeschluss kommt entscheidende Bedeutung zu. Er umgrenzt das Durchsuchungsziel und nennt den Zweck der Durchsuchung. Alles, was darüber hinausgeht, darf nicht gesucht und auch nicht durchgesehen werden. Jeder **Versuch**, dass „**gezielt**" **gesucht** wird, ist zu **unterbinden**.

1730 **bb)** I.Ü. ist es aber auch nach den Änderungen durch das 1. JuMoG bei der Regelung des § 110 Abs. 2 verblieben, dass „**andere Beamte**" zur Durchsicht der aufgefundenen Papiere nur mit **Genehmigung** des **Inhabers** befugt sind. Die Genehmigung des Vertreters reicht nach § 106 Abs. 1 S. 2 nicht aus.

☝ „Andere Beamte" sind all diejenigen, die **nicht „Ermittlungspersonen"** i.S.d. § 152 GVG sind (vgl. dazu → *Ermittlungspersonen der Staatsanwaltschaft*, Rdn 2105). Der Begriff des „Beamten" in § 110 Abs. 2 ist der weitere Begriff.

1731 Den „**anderen Beamten**" kann die **Durchsicht** auch **nicht übertragen** werden (*Meyer-Goßner/Schmitt*, § 110 Rn 3). Sie können allerdings zur Unterstützung herangezogen werden. Allerdings ist damit vorsichtig umzugehen. Der „andere Beamte" darf die Durchsicht auf keinen Fall eigenverantwortlich vornehmen, sondern darf nur unterstützen (zu allem krit. *Park* wistra 2000, 154; zur Zuziehung von SV vgl. LG Kiel NJW 2006, 3224). Das bedeutet, dass „andere Beamte" beweiserhebliche Papiere lediglich durch Grobsichtung nach äußeren Kriterien, z.B. Briefköpfe, „Betr." u.a., aussortieren dürfen (*Mildeberger/Riveiro* StraFo 2004, 43, 46; s.a. Rdn 1723). Die Lektüre der Beamten darf nicht über den Anlass der Durchsuchung hinausgehen (OLG Celle StV 1985, 137, 139; *Rengier* NStZ 1981, 376). Die Beschränkungen entfallen allerdings nach richterlicher Bestätigung der von der StA angeordneten Beschlagnahme (OLG Frankfurt am Main NStZ-RR 1997, 74).

☝ Das gilt **auch** für **Durchsuchungen** im **EDV-Bereich**. Es ist Polizeibeamten grds. verwehrt, vom Inhalt elektronisch gespeicherter Daten Kenntnis zu nehmen (*Park* wistra 2000, 455; vgl. zur Reichweite des § 110 im Einzelnen: *Bär*, S. 225 ff.; *Hiéramente* wistra 2016, 432; *Zerbes/El-Ghazi* NStZ 2015, 425; s. aber auch BVerfG NJW 2002, 1410 und BGH NJW 1995, 3397; zur Online-Sichtung s.u. Rdn 1735 ff.).

6.a) Nach § 110 Abs. 3 Hs. 2 a.F. war der **Inhaber** der Papiere (Beschuldigte) früher zur **Teilnahme** an der Entsiegelung der Papiere (→ *Durchsuchung, Anwesenheit des Verteidigers*, Rdn 1653) aufzufordern. Diese Verpflichtung besteht, nachdem durch das 1. JuMoG nicht nur Hs. 1 des § 110 Abs. 3 gestrichen worden ist, sondern der gesamte Abs. 3 a.F. entfallen ist, nun nicht mehr. Die Verpflichtung bestand i.Ü. früher auch dann, wenn die StA die Durchsicht der Papiere durchführte, ohne dass gesiegelt worden war und entsiegelt werden musste (*Meyer-Goßner*, [47. Aufl.], § 110 Rn 5). **1732**

Das **bedeutet** m.E. aber **nicht**, dass der Betroffene nun nicht mehr von der Durchsicht in Kenntnis zu setzen ist und **kein Teilnahmerecht** an der Durchsicht mehr hat (s.a. BVerfG NJW 2009, 2431 für das Anwesenheitsrecht). Der Betroffene hat, da die Durchsicht der Papiere noch zur Durchsuchung gehört (vgl. u.a. BGH NStZ 2003, 670), aus § 106 Abs. 1 ein (allgemeines) Anwesenheitsrecht. Das des Verteidigers leitet sich aus §§ 163a Abs. 3 S. 2, 168c Abs. 1 ab (so auch *Knauer/Wolf* NJW 2004, 2938; vgl. auch *R. Michalke* StraFo2014, 89, 91). Das hat zur Folge, dass Betroffener/Beschuldigter und Verteidiger in diesen Fällen nach wie vor vorher von der Durchsicht zu unterrichten sind, um ihre Anwesenheit sicherzustellen (so auch *Knauer/Wolf*, a.a.O.). Der Gesetzgeber dürfte diese Frage schlicht übersehen haben. **1733**

☝ Der Verteidiger sollte daher nach wie vor auf die **Teilnahme** des Beschuldigten an der Durchsicht **drängen** und versuchen, seine eigene Anwesenheit unter Hinweis auf §§ 163a Abs. 3 S. 2, 168c Abs. 1 durchzusetzen (so auch immer noch *Dahs*, Rn 384 [argumentum a maiore ad minus]). Will die StA die Mitwirkung/Teilnahme unter Hinweis auf eine dadurch ggf. eintretende Zeitverzögerung verhindern, muss der Verteidiger darauf hinweisen, dass die Teilnahme nach altem Recht nur dann verweigert werden konnte, wenn sie so viel Zeit erforderte, dass der Untersuchungszweck gefährdet oder das Verfahren über Gebühr verzögert würde oder sonstige Schwierigkeiten, z.B. Störungen (§ 164), zu erwarten sind. Das wird i.d.R. nicht der Fall sein. Es empfiehlt sich zudem ein Hinweis auf die Rspr. des **BVerfG**. Dies hat in NJW 2005, 1917, 1922 und in NJW 2009, 2431, 2437 die Hinzuziehung des Inhabers (im Einzelfall) für **geboten** angesehen (s.a. *Meyer-Goßner/Schmitt*, § 110 Rn 5).

b) Die **Teilnahme** an der Durchsicht der Papiere hat für den Verteidiger den **Vorteil**, dass er auf diesem Weg erfährt, worauf es den Ermittlungsbehörden ankommt. Häufig hat er bis zu diesem Zeitpunkt noch keine AE gehabt, weil ihm diese unter Hinweis auf § 147 Abs. 2 verweigert worden ist (→ *Akteneinsicht, Beschränkung*, Rdn 290). Damit ist hier meist die erste Gelegenheit gegeben, Genaueres über den gegenüber dem Mandanten erhobenen Vorwurf zu erfahren. Auch ist der Verteidiger, wenn er an der Durchsicht der Papiere teilnimmt, in der Lage, schon früh das den Mandanten ggf. belastende Material kennen zu lernen. Er selbst kann entlastendes Material in den Vordergrund rücken bzw. versuchen, dieses zu erlangen, um es in das Verfahren einzuführen (s. *Dahs*, a.a.O., a.E.; zu allem auch *Park* wistra 2000, 457). **1734**

7.a) In § 110 Abs. 3 ist durch das TKÜErwG v. 21.12.2007 zum 1.1.2008 die sog. **Online-Sichtung** eingeführt worden (vgl. dazu eingehend die hervorragende Darstellung von *Schlegel* HRRS 2008, 23 ff.; *Meyer-Goßner/Schmitt*, § 110 Rn 6; *Bär* 2011, 53; *Schelzke* HRRS 2013, 80; *R. Michalke* StraFo2014, 89, 91 f.; *Peters* NZWiSt 2017, 465; zur Netzwerkdurchsicht (auch) *Knierim* StV 2009, 206, 211; [zur Durchsicht der Unternehmens-IT] *Hiéramente* wistra 2016, 432; *Zerbes/El-Ghazi* NStZ 2015, 425). Diese Regelung war erforderlich, da umstr. war, ob die Beschlagnahmeregelungen der §§ 94 ff. auch auf Fälle anwendbar sind, in denen die Daten lediglich von vorhandenen Datenträgern im Durchsuchungsobjekt bzw. aus dort zugänglichen Netzwerken auf Datenträger der Strafverfolger kopiert wurden. Elektronische Daten sind als solche keine körperlichen Gegenstände und können damit für sich gesehen kein taugliches **1735**

Objekt einer Sicherstellung/Beschlagnahme nach den §§ 94 ff. sein (vgl. dazu *Schlegel* HRRS 2008, 24, 24). Das gilt aber nicht nur für die Beschlagnahme, sondern auch für die ihr i.d.R. vorgelagerte Durchsuchung und die noch dazu gehörende „Durchsicht der Papiere" (vgl. dazu BGH NStZ 2003, 670). Insoweit war zudem **problematisch**, ob **Papier** i.S.d. § 110 (s. dazu o. Rdn 1721) auch die über einen Computer im Durchsuchungsobjekt zugänglichen, rein **elektronischen Netzwerkressourcen** sein können und ob darauf zugegriffen werden durfte (zu allem *Schlegel*, a.a.O.; *Bär* CR 1995, 227, 228 f.) Für diese Problematik enthält § 110 Abs. 3 nun eine ausdrückliche Regelung (vgl. zur Anwendung der §§ 94 ff. auf die Beschlagnahme von auf dem Mailserver des Providers gespeicherten E-Mails auch BVerfG NJW 2009, 2431). Im Einzelnen gilt:

1736 **b)** Nach § 110 Abs. 3 darf die **Durchsicht** eines elektronischen Speichermediums bei dem von der Durchsuchung Betroffenen auf hiervon **räumlich getrennte Speichermedien** erstreckt werden, soweit auf sie von dem Speichermedium aus zugegriffen werden kann, falls andernfalls der Verlust der gesuchten Daten zu besorgen ist.

1737 § 110 Abs. 3 erlaubt aber **nur** die **offene Durchsicht** von Daten, die sich auf externen Speichermedien, also auf einem Server im Intra- oder Internet, befinden. Sie erlaubt **nicht** den **heimlichen Zugriff** auf Computersysteme i.S.d. → *Online-Durchsuchung*, Rdn 2947 (*Meyer-Goßner/Schmitt*, § 110 Rn 6; *Schlegel* HRRS 2008, 23, 26; *Bär* MMR 2008, 215, 221; *R. Michalke* StraFo2014, 89, 91; *Hiéramente* wistra 2016, 432; *Zerbes/El-Ghazi* NStZ 2015, 425; BT-Drucks 16/6979, S. 66; zum Cloud Computing *Obenhaus* NJW 2010, 651 ff.; *Schelzke* HRRS 2013, 86; *Brodowski/Eisenmenger* ZD 2014, 119; *Braun* PStR 2012, 86, 89; *Cornelius* StV 2016, 380; vgl. aber LG Mannheim StV 2011, 352, wonach die Gewährung eines „Gastzugangs" durch den Provider zum E-Mail-Account des Beschuldigten zulässig sein soll und es sich bei gewonnenen Erkenntnissen um Zufallsfunde handeln soll). Dies ergibt sich (auch) daraus, dass sich Abs. 3 auf den „von der Durchsuchung Betroffenen" bezieht. Das setzt aber eine Durchsuchung i.S.d. §§ 102 ff. voraus (*Schlegel*, a.a.O.). Das BVerfG geht auch nur für den Fall der „offenen Durchsicht" davon aus, dass dann besondere Eingriffsvoraussetzungen für die Beschlagnahme von E-Mails nicht vorliegen müssen (NJW 2009, 2431; → *Beschlagnahme, Allgemeines*, Rdn 815).

☝ § 110 Abs. 3 lässt sich auch **nicht** ein **allgemeiner Grundsatz** entnehmen, wonach **alle Daten**, die über das System des von der Durchsicht Betroffenen abgerufen werden können, ggf. auch **unmittelbar** bei Dritten **durchgesehen** werden dürfen (*Schlegel* HRRS 2008, 23, 29). Eine solche Sicht hätte weitreichende Folgen, da dafür dann ggf. nur die Voraussetzungen der §§ 102, 103 und nicht die des § 100a zu beachten wären. Sie verbietet sich schon deshalb, weil § 110 Abs. 3 nur eine erleichterte Zugriffsmöglichkeit auf die externen Speichermedien schaffen will, auf die anderenfalls nur mit einem besonderen Durchsuchungsbeschluss zugegriffen werden könnte (zu allem auch *Obenhaus*, a.a.O.; *Schelzke* HRRS 2013, 86).

1738 **c)aa)** Die „Durchsicht" i.S.d. § 110 Abs. 3 hat ebenso wie die nach Abs. 1 den **Zweck**, nach einer inhaltlichen Kenntnisnahme zu entscheiden, ob aufgefundene Papiere = Daten (zum Begriff s. oben Rdn 1722) als Beweismittel in Betracht kommen. Das bedeutet, dass auf den „Speichermedien" sowohl der Inhalt der jeweiligen Ablageordner (directories) als auch der Inhalt der jeweiligen Dateien (files) zur Kenntnis genommen werden darf (*Schlegel* HRRS 2008, 23 26; s.a. wohl BVerfG NJW 2009, 2431). Zugegriffen werden darf auf alle Dateien, welche über das entsprechende Gerät erreichbar sind (*Schlegel* HRRS 2008, 23, 27; *Hiéramente* wistra 2016, 432; *Zerbes/El-Ghazi* NStZ 2015, 425; *Meyer-Goßner/Schmitt*, § 110 Rn 6).

☝ Es ist aber der **Verhältnismäßigkeitsgrundsatz** zu beachten und die Durchsuchung eines Datenbestandes so zu **beschränken**, dass ggf. nicht über das erforderliche Maß hinaus auf nicht verfahrensrelevante Daten Dritter zugegriffen wird (vgl. dazu LG Itzehoe StraFo 2015, 243 für die Durchsuchung/Durchsicht bei einem Steuerberater; s.a. *Hiéramente* wistra 2016, 432 für die Durchsuchung einer Unternehmens-IT). Die notwendige Begrenzung der Maßnahme hat auch nicht erst durch die mit

der Durchsicht betrauten Ermittlungspersonen, sondern bereits durch den Richter zu erfolgen, der über die Zulässigkeit der Maßnahme zu entscheiden und diese zugleich beschränkend zu regulieren hat (LG Itzehoe, a.a.O.; → *Durchsuchung, Anordnung, Verhältnismäßigkeit*, Rdn 1630).

bb) Der **Zugriff** auf die sich auf einem anderen System befindlichen Daten ist nur zulässig, soweit von dem System des von der Durchsuchung Betroffenen aus auf diese zugegriffen werden kann. Das bedeutet, dass allein aufgrund der vorgefundenen **aktuellen Konfiguration**, eine Erweiterung der Durchsicht auf andere, daran über ein Netzwerk angeschlossene, unabhängige Computersysteme ausgedehnt werden kann (*Schlegel* HRRS 2008, 23, 28, für E-Mail-Programm, in dem die Passwörter gespeichert sind). 1739

☝ Nach *Schlegel* (a.a.O.) und *Zerbes/El-Ghazi* (NStZ 2015, 425, 429) ist es auch zulässig, ein beim Betroffenen aufgefundenes **Passwort** einzugeben, da damit lediglich Informationen aus der Durchsicht aller beim Betroffenen vorhandenen „Papiere" verknüpft werden (so auch *Meyer-Goßner/Schmitt*, § 110 Rn 6; ähnlich *Bär* ZIS 2011, 53, 54). Dem wird man aber entgegenhalten können, dass das an sich mehr ist, als die aktuelle Konfiguration des Systems erlaubt.

Ist den Ermittlungsbehörden das **Passwort nicht bekannt,** gilt: Der Beschuldigte ist nicht herausgabe-/angabepflichtig; insoweit steht der nemo-tenetur-Grundsatz entgegen (*Meyer-Goßner/Schmitt*, § 95 Rn 32). M.E. muss er, wenn ein Herausgabeverlangen an ihn gestellt wird, nach § 136 **belehrt** werden (s.a. AG Tiergarten StraF0 2018, 67). Entsprechendes gilt für einen Betroffenen, der zur Zeugnisverweigerung berechtigt ist. Auch er kann die Herausgabe/Angabe von Passwörtern verweigern und ggf. ist ebenfalls zu belehren (s. auch *Obenhaus* NJW 2010, 651, 652 f.). Nichtbeschuldigte müssen die Passwörter herausgeben (*Meyer-Goßner/Schmitt*, a.a.O.; *Zimmermann* JA 2014, 321 f.). 1740

☝ Wird **nicht belehrt**, wird man die Frage eines **BVV** diskutieren müssen für die Erkenntnisse, die aufgrund des Zugriffs auf das System erlangt worden sind (bejaht von AG Tiergarten, a.a.O.). Insoweit gelten die allgemeinen Regeln (→ *Beweisverwertungsverbote, Allgemeines*, Rdn 1156 ff.). Geht es um das Entschlüsseln von durch **biometrische Merkmale** (Fingerabdruck; Iris) verschlüsselte Geräte, wie z.B. ein Smartphone, können ggf. Maßnahmen nach § 81b in Betracht kommen (vgl. dazu eingehend *Bäumerich* NJW 2017, 2718; → *Erkennungsdienstliche Behandlung des Beschuldigten*, Rdn 2071).

cc) Der Zugriff darf von einem Speichermedium auf ein anderes „**räumlich getrenntes Speichermedium**" erfolgen (**Cloud Computing**; *Meyer-Goßner/Schmitt*, § 110 Rn 7b; KK-*Bruns*, § 110 Rn 8a; *R. Michalke* StraFo2014, 89, 91 f.; *Hiéramente/Fenina* StraFo 2015, 365 ff.; zur Durchsuchung in der Cloud *Wicker* MMR 2013, 765; *Brodowski/Eisenmenger* ZD 2014, 119; *Cornelius* StV 2016, 380). Diese Formulierung geht zurück auf Art. 19 Abs. 2 des Übereinkommens über Computerkriminalität v. 23.11.2001 (abrufbar in deutscher Übersetzung unter http://conventions.coe.int/Treaty/GER/Treaties/Html/185.htm), der von einem „anderen System" spricht. „Räumlich getrenntes" Speichermedium ist daher so zu verstehen, dass davon alle Speichermedien erfasst sind, die nicht unmittelbar an das zu durchsuchende Speichermedium angeschlossen sind, d.h. ein anderes System darstellen und die sich zumindest nicht im gleichen Raum befinden (*Schlegel* HRRS 2008, 23, 27). 1741

☝ Dabei kommt es, was auch dem Sinn und Zweck der Regelung des § 110 Abs. 3 widersprechen würde, nicht darauf an, ob sich diese Systeme im gleichen **Durchsuchungsobjekt** befinden oder nicht.

Befinden sich die Daten, auf die zugegriffen werden soll, im **Ausland** ist zu unterscheiden: Auf öffentlich zugängliche Daten darf zugegriffen werden, nicht öffentlich zugängliche Daten dürfen mit Zustimmung des Berechtigten gesichert werden (Art. 32 Cybercrime-Convention). Andernfalls bedarf es grds. eines förmlichen Rechtshilfeersuchens (Art. 31 Cybercrime-Convention). Um den Beweisverlust zu vermei- 1742

den, wird aber meist die umgehende Sicherung der Daten im Wege der vorläufigen Rechtshilfe erfolgen (Art. 29 Cybercrime-Konvention, in dringenden Fällen per Fax- oder E-Mail-Abfrage gemäß Art. 25 Abs. 2 Cybercrime-Konvention) (zu allem *Meyer-Goßner/Schmitt*, § 110 Rn 7b f. m.w.N.).

1743 **d) § 110 Abs. 3 erweitert** die auf „Papiere" i.e.S. und damit auf körperliche Gegenstände bezogene **Regelung** des **Abs. 1** (vgl. Rdn 1721). Nach Abs. 1 müssen sich die Daten, die durchgesehen werden, nämlich auf bzw. im eigentlichen Durchsuchungsobjekt befinden, also körperlich – zumindest über das Speichermedium – greifbar sein. Abs. 3 lässt hingegen auch die Durchsicht von **Speichermedien** nach verfahrensrelevantem Material zu, welche vom durchzusehenden Medium **lediglich** auf **elektronischem Wege erreicht** werden können. Das sind also z.B. Netzwerke. Unter „Speichermedium, von dem zugegriffen wird," ist ebenso wie das Speichermedium, auf das zugegriffen wird, ein Computersystem zu verstehen, mit programmierbarem System mit Eingabe-, Ausgabe- und Speichermöglichkeiten (*Schlegel* HRRS 2008, 23, 27 m.w.N.; zum Begriff a. *Hiéramente/Fenina* StraFo 2015, 365 ff.). Daher fällt auch das sog. Cloud Computing unter die Vorschrift, da dies nur eine besondere Form der Speicherung auf einem externen Speicher darstellt (vgl. *Obenhaus* NJW 2010, 651; *Braun* PStR 2012, 86, 89; *Wicker* MMR 2013, 765; *Brodowski/Eisenmenger* ZD 2014, 119; *Cornelius* StV 2016, 380).

☝ **Andere Speichermedien** wie DVD, USB-Speichersticks oder Festplatten scheiden aus dem Anwendungsbereich des Abs. 3 aus. Sie unterfallen, da sie körperlich greifbar sind, § 110 Abs. 1.

1744 **e) Voraussetzung** für die Durchsicht ist, dass ohne sie der **Verlust beweiserheblicher Daten** zu **befürchten** ist. *Meyer-Goßner/Schmitt* (§ 110 Rn 6) geht davon aus, dass das immer dann der Fall ist, wenn noch vor einer körperlichen Sicherstellung des externen Speichermediums die Löschung der Dateien zu erwarten ist. Damit erhält die Vorschrift zwar einen weiten Anwendungsbereich, dies ist aber im Hinblick darauf, dass das externe Speichermedium z.B. auch im Ausland stehen kann, hinnehmbar. Ein Zugriff wird daher dort i.d.R. kaum möglich sein, sodass eine körperliche Sicherstellung ausscheidet. Zudem hat hier ja auch schon eine Prüfung der Anordnungsvoraussetzungen für die Durchsuchungsmaßnahme stattgefunden (zur Annahme von „Gefahr im Verzug" bei Durchsuchung und Beschlagnahme, wenn die Maßnahmen auf Dateien zielen, s. BayVGH PStR 2005, 278; vgl. dazu jetzt aber BGH StRR 2008, 460).

☝ Darüber hinaus ist auch bei der Durchsicht nach Abs. 3 der (allgemeine) **Verhältnismäßigkeitsgrundsatz** zu beachten (vgl. auch o. Rdn 1719; *Schlegel* HRRS 2008, 23, 28; zur Beachtung bei Durchsuchung einer Rechtsanwaltskanzlei LG Bonn, Beschl. v. 10.1.2011 – 27 Qs 33/10). Die Durchsicht ist zu beenden, wenn erkennbar wird, dass sie zu keinem Ergebnis führen wird (BVerfG NJW 2009, 2431; BGH CR 1999, 292). Sie hat von vornherein zu unterbleiben, wenn aufgrund der zu untersuchenden Straftat sicher ist, dass eine Durchsuchung des Computersystems des Beschuldigten keine Ergebnisse bringen wird (BVerfG NJW 2007, 1444) oder, wenn festgestellt wird, dass sich auf dem Mailserver des Providers überhaupt keine verfahrenserheblichen E-Mails befinden (BVerfG NJW 2009, 2431).

1745 **f)** Eine Regelung, wem die **Befugnis** zur Online-Durchsicht zusteht, enthält Abs. 3 nicht. Damit gelten die **allgemeinen Regeln** (s.a. *Schlegel* HRRS 2008, 23, 26 f.; *Meyer-Goßner/Schmitt*, § 110 Rn 7; vgl. dazu o. Rdn 1728 f.) mit der Folge, dass grds. nur Richter oder StA zur Durchsicht befugt sind. Die Durchsicht kann aber auf → *Ermittlungspersonen der Staatsanwaltschaft*, Rdn 2105, übertragen werden. Die bei Rdn 1728 dargestellt Einschränkungen für die Hinzuziehung von Hilfspersonen gelten ebenfalls entsprechend.

☝ **Andere Personen** bedürfen für die Online-Sichtung der **Genehmigung** nach § 110 Abs. 2 S. 1; vgl. o. Rdn 1730). Fehlt diese, dürfen sie eine inhaltliche Sichtung der Dateien nicht vornehmen (*Schlegel* HRRS 2008, 23, 26). Sie dürfen sich aber eine Dateiübersicht anzeigen lassen.

g)aa) Daten, die für die **Untersuchung von Bedeutung** sein können, dürfen nach Abs. 3 S. 2 auch aus einem Netzwerk gesichert werden. Diese Formulierung entspricht der Regelung in § 94 (→ *Beschlagnahme, Voraussetzungen*, Rdn 1010). Die dazu vorliegende Rspr. und Lit. ist daher entsprechend anzuwenden. Ausreichend ist also, dass die zu sichernde Datei zu Förderung des Verfahrens beitragen kann (vgl. *Meyer-Goßner/Schmitt*, § 94 Rn 6). Noch weiter kann die Vorschrift allerdings nicht verstanden werden. Zutreffend weist *Schlegel* (HRRS 2008, 23, 28) darauf hin, dass die Anforderungen an die potenzielle Beweisbedeutung deshalb nicht noch weiter reduziert werden können, weil es bei § 94 um die Beschlagnahme eines als schon „Beweismittel" erkannten Gegenstandes geht, während es bei § 110 Abs. 3 darum geht festzustellen, ob die Dateien/Daten überhaupt einen Inhalt mit Beweisbedeutung haben (vgl. auch *Schilling/Rudolph/Kuntze* HRRS 2013, 207). 1746

Die Sicherung erfolgt durch **Speicherung** auf Datenträger der Strafverfolgungsbehörde (*Meyer-Goßner/Schmitt*, § 110 Rn 7; vgl. *Schilling/Rudolph/Kuntze* HRRS 2013, 207). Fraglich ist, wie mit ausländischen Speichermedien zu verfahren ist, insbesondere, ob zu ihrer Sicherung die Zustimmung des fremden Staates oder des Berechtigten notwendig ist. Diese dürfte erforderlich sein. Eine wegen der i.d.R. vorliegenden Eilbedürftigkeit vorläufige Sicherung wird von der h.M. als unzulässig angesehen können (so auch *Meyer-Goßner/Schmitt*, a.a.O.; *Bär* MMR 2008, 215, 221 m.w.N.; vgl. auch *Obenhaus* NJW 2010, 651, 654). I.Ü. gelten die Regelungen des Übereinkommens über Computerkriminalität v. 23.11.2001 (s.o.). 1747

☝ Das **BVerfG** (NJW 2009, 2431) wendet auf den offenen Zugriff auf auf dem Mailserver des Providers gespeicherte **E-Mails** die §§ 94 ff. an. Nach Auffassung des BGH (NJW 2009, 1827) sind die Vorschriften über die → *Postbeschlagnahme*; Rdn 3540, gem. den §§ 94, 98, 99 anzuwenden, während das LG Hamburg der Auffassung ist, dass der Zugriff der Strafverfolgungsbehörden auf E-Mails, die in serverbasierten Postfächern (Accounts) von E-Mail-Providern (zwischen-)gespeichert sind, nur nach Maßgabe der §§ 100a, 100b, also nach den Vorschriften über die Telefonüberwachung (LG Hamburg StV 2009, 70), erfolgen darf (→ *Telefonüberwachung, Allgemeines*, Rdn 3919; dazu auch *Gaede* StV 2009, 96; abl. BVerfG und BGH, jeweils a.a.O.). Befinden sich die **Mailserver** im **Ausland**, können die Ermittlungsbehörden darauf nicht von sich aus Zugriff nehmen (LG Hamburg, a.a.O.; vgl. dazu auch *Gercke* StraFo 2009, 271, auch zur Frage eines BVV; *Hermann/Soiné* NJW 2011, 2922; a.A. *Braun* PStR 2012, 86, 88).

bb) Diese Sicherung/Speicherung ist noch keine Beschlagnahme der Daten, sodass noch kein **Beschlagnahmeverzeichnis** (§ 109) angelegt werden muss (vgl. dazu, insbesondere auch im Hinblick auf die Durchsuchung einer EDV-Anlage, *Kemper* wistra 2008, 96, 98 f.). 1748

cc) Für die **Sicherstellung** von E-Mails sind die Vorgaben des BVerfG zu beachten (vgl. dazu NJW 2009, 2431 und → *Beschlagnahme, Durchführung*, Rdn 937 ff.; zur Beachtung des Verhältnismäßigkeitsgrundsatzes bei der Durchsicht von Emails einer Rechtsanwaltskanzlei LG Bonn, Beschl. v. 10.1.2011 – 27 Qs 33/10): 1749

- Es ist darauf zu achten, dass **keine überschießenden**, für das Verfahren bedeutungslose Daten gewonnen werden.
- Der vorhandene E-Mail-Bestand muss darauf **überprüft** werden, ob eine Sicherstellung aller gespeicherten E-Mails erforderlich ist, oder ob die **Beschränkung** auf die potenziell beweiserheblichen E-Mails **ausreicht** (vgl. z.B. LG Itzehoe StraFo 2015, 243).
- Kann eine Unterscheidung der E-Mails nach ihrer Beweiserheblichkeit vorgenommen werden, ist die Möglichkeit einer **Trennung** von den restlichen E-Mails zu prüfen. Von Bedeutung ist hierbei aber die Möglichkeit der Auswertung der Struktur eines gespeicherten E-Mail-Bestands.
- Schließlich ist auf den Schutz des sog. „**Kernbereichs** der privaten Lebensgestaltung" besondere Rücksicht zu nehmen (vgl. zum Begriff → *Maßnahmen ohne Wissen des Betroffenen, Akustische Wohnraumüberwachung*, Rdn 2790).
- Ggf. kann es geboten sein, den **Inhaber** der E-Mails ist bei der Sichtung **einzubeziehen**.

1750 **8.** Wegen **Rechtsmittel** im Fall der Durchsicht von Papieren ist (allgemein) Folgendes zu beachten (s. dazu auch *Park* wistra 2001, 457 f.; *Artkämper* StRR 2007, 12, 14):

a) Die Mitnahme von Papieren, um diese durchzusehen, ist noch keine Beschlagnahme (BGH NStZ 2003, 670), sodass ein Antrag auf gerichtliche Entscheidung nach § 98 Abs. 2 S. 2 unmittelbar nicht zulässig ist (*Meyer-Goßner/Schmitt*, § 110 Rn 10 m.w.N.). In Betracht kommt aber eine **entsprechende Anwendung** von **§ 98 Abs. 2 S. 2**, da die vorläufige amtliche Verwahrung der Sachen zur Durchführung der Durchsicht eine der Beschlagnahme vergleichbare Beschwer darstellt, die von derjenigen aufgrund der Durchsuchung zu unterscheiden ist (BVerfG NJW 2002, 1410; NStZ-RR 2002, 144; BGHSt 45, 37; LG Frankfurt am Main NJW 1997, 1170; LG Koblenz WM 1998, 2290, 2291; zu den Rechtsmitteln auch *Graulich* wistra 2009, 299, 301; eingehend Burhoff/Kotz/*Hunsmann*, RM, Teil B Rn 144 ff.; → *Durchsuchung, Rechtsmittel*, Rdn 1765). Nachfolgend ist dann das Rechtsmittel der → *Beschwerde*, Rdn 1054, gegeben (BVerfG, a.a.O.). Geltend gemacht werden kann z.B., dass die Sicherstellung über die thematisch begrenzte Zielvorgabe des Durchsuchungsbeschlusses, der nur bestimmte Datensätze betraf, hinausgeht (BVerfG NJW 2009, 2518). Nach LG Oldenburg (PStR 2002, 95) soll der von der Durchsuchung Betroffene während der Durchsuchung keinen Anspruch auf Prüfung der Beschlagnahmefreiheit von Unterlagen durch den Richter haben (s. aber *Burkhard* PStR 2001, 159).

☝ Das gilt jedoch dann **nicht** mehr, wenn – nach zunächst nur vorläufiger Sicherstellung – inzwischen die richterliche **Beschlagnahme** der bei der Durchsuchung sichergestellten Papiere beantragt worden ist (BGH NJW 1995, 3397). Dann muss (direkt) gegen die Beschlagnahmeanordnung vorgegangen werden (BGH, a.a.O.).

Entsprechendes gilt, wenn die Durchsuchungsbeamten bereits „vor Ort" entschieden haben, welche Papiere/Daten beschlagnahmt und deshalb mitgenommen werden sollen. Eine spätere Durchsicht ist dann „**Auswertung**" der Unterlagen (OLG Bremen wistra 1999, 76).

1751 **b)** Während der noch **(länger) andauernden Durchsicht** kann grds. auch gegen die **Zulässigkeit** der Fortdauer der **Durchsuchung**, etwa wenn die Behörden nicht zügig arbeiten, vorgegangen werden, und zwar entsprechend § 98 Abs. 2 S. 2 (so BVerfG NJW 2002, 1410 unter Hinw. auf BGHSt 45, 37; LG Frankfurt am Main, a.a.O.). Allerdings gilt die Rspr. des BVerfG zur zeitlichen Geltung von Durchsuchungsbeschlüssen (vgl. BVerfG NJW 1997, 2165) nicht (mehr) für die Phase der Durchsicht von Unterlagen (BVerfG NJW 2002, 1410; a.A. *Hoffmann/Wißmann* NStZ 1998, 443; → *Beschlagnahme, Beweisverwertungsverbote*, Rdn 921). Ein Überschreiten der zulässigen zeitlichen Dauer der Durchsuchungsmaßnahme kann der Verteidiger erfolgreich also nur rügen, wenn nach allgemeinen **Verhältnismäßigkeitsgesichtspunkten** die Durchsicht der Unterlagen unzumutbar lange (an-)dauert (so wohl BVerfG, a.a.O.; LG Mühlhausen StraFo 2003, 237; LG Ravensburg NStZ-RR 2014, 348 [neun Monate bei Beschlagnahme nicht zu lang]). Allerdings kann er in der Phase der Durchsuchung ggf. (auch) geltend machen, dass eine neue Beweislage eingetreten und dadurch der → ***Anfangsverdacht***, Rdn 543, **entfallen** ist, wodurch die Durchsuchungsmaßnahme unzulässig wird (LG Leipzig StraFo 2008, 294). Bei der **Bestimmung** der **zulässigen Dauer** sind der Umfang des Materials und ggf. der Umstand zu berücksichtigen, dass z.B. die Daten auf einer Festplatte gespeichert sind, die mit einem der StA unbekannten, noch zu entschlüsselnden Kennwort gesichert ist.

☝ Auch hier bietet es sich m.E. an, die zu § 121 entwickelten **Grundsätze** entsprechend heranzuziehen (→ **Haftprüfung** *durch das Oberlandesgericht*, Rdn 2335 ff.; s.a. *Artkämper* StRR 2007, 12, 14). Auf der Grundlage hat das LG Köln (StV 2002, 413) eine sieben Monate, das LG Dresden (NStZ 2003, 567) eine drei Monate, das LG Limburg (StraFo 2006, 195) eine acht Monate dauernde Durchsicht von Papieren als unverhältnismäßig angesehen (vgl. auch LG Kiel StraFo 2004, 93, wonach die neun Monate andauernde Beschlagnahme eines Computers bei nur geringem Tatverdacht als unverhältnismäßig anzusehen ist; a.A. LG Ravensburg NStZ-RR 2014, 348 [neun Monate nicht zu lang bei Beschlagnahme]).

Die Durchsicht hat **zügig** zu erfolgen (LG Mühlhausen, a.a.O.; *Artkämper*, a.a.O.; wohl auch *Meyer-Goßner/Schmitt*, § 110 Rn 2), damit die Papieren **möglichst schnell** zurückgegeben werden können (zum Rückgabeort *Graulich* wistra 2009, 302 [wie bei der Beschlagnahme; → *Beendigung/Herausgabe der beschlagnahmten Sache*, Rdn 840]). Das gilt vor allem bei der Durchsicht einer EDV-Anlage (vgl. dazu Rdn 1721). Hier ist eine schnelle Spiegelung der Daten möglich (AG Karlsruhe StraFo 2007, 152). Die Herausgabe kann auch nicht etwa mit Begründung verweigert/heraus gezögert werden, dass keine passenden Festplatten vorhanden seien und erst – für ca. 200,00 € – beschafft werden müssten (AG Karlsruhe, a.a.O.). 1752

☝ Soll die Frage der **Rechtsmitteleinlegung** in **Ruhe** nach Abschluss der Durchsuchung **entschieden** werden, empfiehlt es sich, um nicht „prozessuale Überholung" eintreten zu lassen, auf der Versiegelung der Unterlagen zu **bestehen**, da die Durchsuchung erst nach Durchsicht der Papiere abgeschlossen ist (*Wehnert* StraFo 1996, 79). Außerdem wird damit auch deutlich nach außen **dokumentiert**, dass die Durchsuchung **beendet** und damit die ihr zugrundeliegende Durchsuchungsanordnung verbraucht ist.

c) Die vorstehenden Regeln gelten für den von der Durchsuchung Betroffenen grds. auch bei einer **Online-Sichtung** nach § 110 Abs. 3. 1753

Sind Daten gesichert worden (§ 110 Abs. 3 S. 2 Hs. 2, kann nach dem Verweis im Hs. 2 der **Inhaber** des **externen Speichermediums** den Antrag nach § 98 Abs. 3 S. 2 Hs. 2 stellen (*Meyer-Goßner/Schmitt*, § 110 Rn 11; eingehend Burhoff/Kotz/*Hunsmann*, RM, Teil B Rn 152 ff.; → *Beschlagnahme, Bestätigung nichtrichterlicher Anordnungen*, Rdn 901). Darüber ist er nach § 98 Abs. 2 S. 6 zu belehren. I.Ü. hat der Verweis auf § 98 Abs. 2 zur Folge, dass der die Durchsicht durchführende Beamte binnen drei Tagen die gerichtliche Bestätigung der Sicherung der vorgefundenen Daten beantragen muss. Zuständig zur Entscheidung ist nach § 162, solange die öffentliche Klage noch nicht erhoben ist, das Gericht am Sitz der StA. Ist öffentliche Klage erhoben, entscheidet das damit befasste Gericht. 1754

Siehe auch: → *Durchsuchung, Allgemeines*, Rdn 1554, m.w.N.; → *Durchsuchung, Beweisverwertungsverbote*, Rdn 1684.

Durchsuchung, Rechtmäßigkeits-Checkliste 1755

Literaturhinweise: S.a. die Hinw. bei → *Beschlagnahme, Allgemeines*, Rdn 816, bei → *Beschlagnahme, Beschlagnahmeverbote*, Rdn 869, bei → *Durchsuchung, Allgemeines*, Rdn 1555, und bei den jeweils dort genannten weiteren Stichworten. 1756

1. Die Tätigkeit des Verteidigers für den Beschuldigten beschränkt sich bei der Durchsuchung im Wesentlichen auf die **nachträgliche Kontrolle** der Rechtmäßigkeit (→ *Durchsuchung, Allgemeines*, Rdn 1554). Diese Kontrolle setzt die Kenntnis der wesentlichen Rechtsfragen/-probleme voraus. Dazu soll die nachfolgende Rechtmäßigkeits-Checkliste Hilfestellung leisten (wegen der weiteren Einzelh. verweise ich auf die Komm. bei *Meyer-Goßner/Schmitt*, §§ 102 ff.; KK-*Bruns*, §§ 102 ff.; LR-*Tsambikakis*, §§ 102 ff.; *Park*, Rn 29 ff. sowie auf die angeführten weiterführenden Stichworte). 1757

2. Die Rechtmäßigkeitskontrolle erfordert zunächst, dass der Verteidiger klärt, wer die Durchsuchungsmaßnahme **angeordnet** hat: 1758

- Das kann der **Richter**, der **StA** oder eine von den → ***Ermittlungspersonen** der Staatsanwaltschaft*, Rdn 2105 sein.
- Hat der **StA** oder eine der **Ermittlungspersonen** die Durchsuchung angeordnet, müssen die besonderen Voraussetzungen für die Anordnung durch diese, nämlich „**Gefahr** im **Verzug**" vorliegen (vgl. zu allem → *Durchsuchung*, *Anordnung, Verfahren/Gefahr im Verzug*, Rdn 1615 ff.).
- Soll der Beschuldigte sich ggf. **freiwillig** mit der Durchsuchung einverstanden erklärt haben, ist zu prüfen, ob die insoweit erforderlichen Voraussetzungen vorliegen (vgl. dazu → *Durchsuchung, Anordnung, Allgemeines*, Rdn 1569 f.).