Leseprobe zu

Kohlmann
Steuerstrafrecht Kommentar

ISBN 978-3-504-25950-1
3 Bände, Ordner Leinen, 145x205

149,00 € inkl. MwSt. (Grundwerk mit Fortsetzungsbezug für mindestens 2 Jahre)

Die zu erwartenden Unterlagen sind so genau wie möglich zu bezeichnen. Beispielsweise bietet es sich an, die aufzufindenden Beweismittel in einem Kontext mit den beteiligten Beschuldigten/Unternehmen/Stpfl. zu stellen.[1]

„Die Durchsuchungsanordnung gegen einen Nichtverdächtigen setzt daher voraus, daß hinreichend individualisierte Beweismittel gesucht werden (BVerfG v. 4.3.1981 – 2 BvR 195/81, NJW 1981, 971; BGH v. 15.10.1999 – StB 9/99, BGHR StPO § 103 Gegenstände 1 und BGH v. 13.1.1989 – StB 1/89, BGHR StPO § 103 Tatsachen 1). Diese müssen, da die Durchsuchung ausdrücklich nur zur Beschlagnahme bestimmter Gegenstände zulässig ist, im Durchsuchungsbeschluß so weit konkretisiert werden, daß weder bei dem Betroffenen noch bei dem die Durchsuchung vollziehenden Beamten Zweifel über die zu suchenden und zu beschlagnahmenden Gegenstände entstehen können (vgl. für die Beschlagnahmeanordnung Rudolphi in SK-StPO 10. Lfg. – April 1994 – § 98 Rz. 17 m.w.Nachw.). Dazu ist es zwar nicht notwendig, daß sie in allen Einzelheiten beschrieben werden. Erforderlich ist es jedoch, daß sie zumindest ihrer Gattung nach bestimmt sind"

204 Diese Grundsätze gelten auch für die **Durchsuchung der Unternehmens-IT**. Der eingriffsintensive Zugriff auf Datenträger – insb. von Rechtsanwälten und Steuerberatern als Berufsgeheimnisträgern – bedarf im jeweiligen Einzelfall in besonderer Weise einer regulierenden Beschränkung.[2] Eine gesonderte Feststellung, dass auch die IT durchsucht werden kann, ist nicht zwingend erforderlich; eine Klarstellung jedoch sinnvoll. Zur Auffindung von Daten, die auf dem Server des Unternehmens vermutet werden, ist regelmäßig eine „virtuelle" Durchsuchung vonnöten. Eine vorherige Einschränkung mittels Suchbegriffen[3] ist jedoch die Regel. Zweifel an der Rechtmäßigkeit der Durchsuchung können dann bestehen, wenn die Beweismittel und die Schlagwortliste[4] nicht entsprechend aufeinander abgestimmt sind. Die im Durchsuchungsbeschluss aufgeführten Schlagworte müssen sich einem der im Durchsuchungsbeschluss als Beweismittel genannten Gegenstände zuordnen lassen. Es genügt jedoch, wenn sich eine Verknüpfung aus dem Zusammenhang und den weiteren Umständen herleiten lässt. Ein gewisser Handlungsspielraum ist den Ermittlern vor Ort einzuräumen.

205 Das aufgefundene Dokument wird im Wege der **„Datenbeschlagnahme"** des Dokuments mittels **Sicherung auf einem Speichermedium** beschlagnahmt. Wurde das zu suchenden Dokument aufgefunden, etwa eine als Beratervertrag getarnte Schmiergeldvereinbarung oder sonstige Abdeckrechnungen, Scheinrechnungen[5], ist die Durchsuchung abzubrechen. Das Ziel der Durchsuchung wurde insoweit erreicht.

1 BGH v. 21.11.2001 – StB 20/01, NStZ 2002, 215 (216).
2 LG Itzehoe v. 12.1.2015 – 2 Qs 162-164/14, juris.
3 Zur Funktion und Reichweite der Schlagwortsuche vgl. *Hiéramente*, wistra 2016, 432 (435).
4 Zur Möglichkeit des Einforderns einer abgestimmten Schlagwortliste vgl. *Heuel/Beyer*, AO-StB 2011, 245 (246); LG Itzehoe v. 12.1.2015 – 2 Qs 162-164/14, juris.
5 Dazu auch *Ebner*, PStR 2019, 195.

In jedem Fall bietet es sich an, die IT-Durchsuchung **durch IT-Experten des Unternehmens zu begleiten** und den **Datenzugriff** zu **dokumentieren**. Ein unzulässiger Zugriff kann ggf. bei § 98 Abs. 2 Satz 2 StPO analog nachträglich gerügt werden. Aus unternehmerischer Sicht bietet es sich an, die IT-Infrastruktur im Unternehmen dementsprechend anzupassen. Relevante Daten sollten sich zeitnah lokalisieren lassen, um die komplette Spiegelung und die Mitnahme zur Durchsicht zu verhindern. Von daher bietet es sich an, eine kunden- oder mandanten- oder projektbezogene Verzeichnisstruktur anzulegen und Vorgänge klar voneinander abzugrenzen. 206

g) EDV-Anlagen/E-Mail-Postfächer

Siehe § 385 Rz. 257. Die Sicherung und Beschlagnahme von EDV-Anlagen, elektronischen Speichermedien[1], E-Mail-Postfächern[2] ist mittlerweile **problemlos möglich**.[3] Wenngleich den Beschuldigten keine Verpflichtung zur Mitwirkung trifft, kann die Herausgabe von Passwörtern, Keys oder Dongles zur Abwendung einer Beschlagnahme oder Versiegelung sämtlicher Räumlichkeiten angezeigt sein. Der wirtschaftliche Betrieb kann so aufrechterhalten werden. Dritte sind entsprechend dem Rechtsgedanken aus § 95 StPO zur Mitwirkung verpflichtet (etwa der Systemadministrator). 207

In der Regel verfügen die Ermittlungsbehörden über ausreichende Speichermedien. Was die Speicherung von E-Mail-Postfächern betrifft (Outlook etc.), hat sich in der Praxis bewährt, lediglich die **konkret von dem Beschluss erfasste Kommunikation** zu sichern[4], etwa indem vorher ein entsprechender Ordner unter Outlook angelegt wird, die mittels Suchfunktion zusammenge- 208

1 Vgl. hierzu BVerfG v. 12.4.2005 – 2 BvR 1027/02, wistra 2005, 295 = CR 2005, 777 = BRAK 2005, 186 (dazu im Eilverfahren BVerfG v. 17.7.2002 – 2 BvR 1027/02 m. Anm. *Burhoff*, PStR 2002, 191); BGH v. 5.8.2003 – 2 BJs 11/03 – 5 StB 7/03, wistra 2003, 432 m. Anm. *Burhoff*, PStR 2003, 268; OLG Jena v. 20.11.2000 – 1 Ws 313/00, wistra 2001, 73 (76); *Spatscheck*/*Spatscheck*, PStR 2000, 188; *Braun*, PStR 2012, 856.

2 Vgl. BVerfG v. 16.6.2009 – 2 BvR 902/06, BVerfGE 124, 43 = NJW 2009, 2431; BVerfG v. 2.3.2006 – 2 BvR 2099/04, BVerfGE 115, 166 = wistra 2006, 217 = EWiR 2006, 305 (*Hülsdunk*); BVerfG v. 29.6.2006 – 2 BvR 902/06, PStR 2006, 220 = CR 2007, 383; BGH v. 31.7.1995 – 1 BGs 625/95 (2 BJs 94/94-6), NJW 1997, 1934 = CR 1996, 488; LG Mannheim v. 30.11.2001 – 22 KLs 628 Js 15705/500, StV 2002, 242; LG Hanau v. 23.9.1999 – 3 Qs 149/99, NJW 1999, 3647; *Dübbers*, StV 2000, 355; *Bär*, CR 1995, 489 (490).

3 Grundlegend und umfassend BVerfG v. 16.6.2009 – 2 BvR 902/06, NJW 2009, 2431; *Köhler* in Meyer-Goßner/Schmitt[65], § 94 StPO Rz. 16a, 19a; hierzu auch *Gotzens* in FS Streck, 2011, S. 519 (525); zum Ganzen auch *Hauschild* in MünchKomm, § 94 StPO Rz. 21; ausf. und nach Fallgruppen unterscheidend *Zerbes*/*El-Ghazi*, NStZ 2015, 425 = CR 2009, 584 m. Anm. *Brunst*.

4 Zum Übermaßverbot vgl. *Hauschild* in MünchKomm, § 94 StPO Rz. 32.

stellten E-Mails dort hinein kopiert werden und dieser Ordner dann exportiert wird. Die Sicherung von Smartphones, Blackberry etc. wird **bei Dritten** (z.B. bei Beratern) nur in Ausnahmefällen in Betracht kommen, da zumeist ein Abgleich mit dem Netzwerkrechner stattfindet. Andernfalls sollte auf eine zeitnahe „Spiegelung" bestanden werden. Die vorherige Einrichtung einer Rufumleitung kann zweckdienlich sein.

209 Bei **E-Mails** sind zudem **unterschiedliche Phasen** zu unterscheiden: die der Absendung, die der Lagerung im Postfach, die des Abrufens und die der abgerufenen Nachricht. Eingriffe in der ersten und dritten Phase bedürfen eines Beschlusses nach § 100a StPO.[1] End- oder zwischengespeicherte E-Mails können nach § 94 StPO beschlagnahmt werden.

210 Im Hinblick auf EDV-Anlagen und elektronisch geführte Akten steuerlicher Berater hat sich **in der Praxis bewährt**, entsprechend den höchstrichterlichen Vorgaben lediglich das **betreffende Mandantenverzeichnis** und die **dazugehörige elektronische Akte** zu sichern.[2] Schon aus Verhältnismäßigkeitsgründen ist die Suche hierauf zu beschränken, wenngleich eine grobe Durchsicht angezeigt sein kann. Die „gezielte Suche nach Zufallsfunden" (§ 108 StPO) ist freilich unzulässig. Bereits der Durchsuchungsbeschluss sollte zeitlich und sachlich bzw. inhaltlich umgrenzt sein.[3] Eine unbeschränkte Beschlagnahme ist auch bei Durchsuchungen beim Beschuldigten nur ausnahmsweise zulässig.[4] Die Beschlagnahme sämtlicher gespeicherten Daten ist allenfalls dann verhältnismäßig, wenn konkrete Anhaltspunkte dafür vorliegen, dass der gesamte Datenbestand, auf den zugegriffen werden soll, für das Verfahren potentiell beweiserheblich ist.

211 Die **Durchsicht** eines elektronischen Speichermediums (Server, Intranet, Cloud[5] etc.) bei dem von der Durchsuchung Betroffenen darf gem. § 110 Abs. 3 StPO auch auf hiervon **räumlich getrennte Speichermedien**, soweit auf sie von dem Speichermedium aus zugegriffen werden kann (auch durch Verwendung von Passwörtern), erstreckt werden, wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden; § 98 Abs. 2 StPO gilt entsprechend. Unzulässig ist trotz der Regelung des § 110 Abs. 3 StPO wegen Verstoßes gegen das **Territorialitätsprinzip** ein Online-Zugriff auf im Aus-

1 Zum Ganzen BVerfG v. 16.6.2009 – 2 BvR 902/06, NJW 2009, 2431 = CR 2009, 584 m. Anm. *Brunst*; *Köhler* in Meyer-Goßner/Schmitt[65], § 100a StPO Rz. 6b, § 94 StPO Rz. 16a.

2 Vgl. auch BVerfG v. 12.4.2005 – 2 BvR 1027/02, NJW 2005, 1917; BVerfG v. 17.7.2002 – 2 BvR 1027/02, wistra 2002, 378 = CR 2005, 777 = BRAK 2005, 186; BVerfG v. 28.4. 2003 – 2 BvR 358/03, NJW 2003, 2669.

3 *Köhler* in Meyer-Goßner/Schmitt[65], § 94 StPO Rz. 19a.

4 Vgl. auch BGH v. 24.11.2009 – StB 48/09 (a), NJW 2010, 1297 = wistra 2010, 230.

5 Eingehend *Zerbes/El-Ghazi*, NStZ 2015, 425 (431).

land befindliche Daten (sog. **„Transborder Searches"**), etwa solche auf ausländischen Servern.[1] Allein zur Abwendung eines Beweismittelverlusts kommt eine Sicherung in Betracht. In diesem Fall ist der Rechtshilfeweg zu beschreiten. Ein Verstoß kann unter Umständen zu einem Beweisverwertungsverbot führen, wenn der Verstoß sich als willkürlich oder absichtlich darstellt.[2]

h) Nachträgliche Datensicherung mittels Cloud Analyzer

212 Unzulässig ist indes nach hier vertretener Ansicht die zunächst vorläufige Sicherung elektronischer Speichermedien und der spätere Abruf der Daten, etwa mittels sog. Cloud Analyzer, bei denen dann mittels vorhandener Zugangsdaten des Betroffenen **im Nachgang sämtliche Daten aus sozialen Medien/Plattformen heruntergeladen** werden (eBay, Facebook, Instagram, LinkedIn usw.). Es fehlt an einer entsprechenden Rechtsgrundlage.[3]

213 § 110 Abs. 3 Satz 1 StPO erlaubt nach Ansicht des LG Koblenz den **offenen Zugriff** auf räumlich getrennte Speichermedien.[4] Die in den Accounts des Beschuldigten bei eBay, Facebook und Google gespeicherten Daten seien unmittelbar über die im durchsuchten Mobiltelefon des Beschuldigten gespeicherten Nutzerdaten zugänglich. Der Umstand, dass die Accounts passwortgesichert waren, stünde, da die jeweiligen Zugangsdaten den Ermittlungsbehörden über die im Rahmen der Durchsuchung erlangten Informationen bekannt waren, dem Zugang nicht entgegen.[5]

214 Eine **Online-Sichtung** nach § 110 Abs. 3 StPO sei dabei **abzugrenzen** von einem Zugriff auf fremde Computersysteme im Rahmen der **(verdeckten) Online-Durchsuchung** durch heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und Speichermedien ausgelesen werden können.[6]

Eine Online-Sichtung werde aber noch nicht dadurch zu einer (verdeckten) Online-Durchsuchung, wenn sie gegenüber dem Gewahrsamsinhaber der online zugänglichen Daten, also aus Sicht des Dritten (vorliegend eBay, Face-

1 Zum Ganzen bereits *Gercke*, StraFo 2009, 271.

2 BVerfG v. 16.3.2006 – 2 BvR 954/02, NJW 2006, 2684; BVerfG v. 12.4.2005 – 2 BvR 1027/02, NJW 2005, 1917, 1923 = CR 2005, 777 = BRAK 2005, 186 = wistra 2005, 295; *Köhler* in Meyer-Goßner/Schmitt[65], § 110 StPO Rz. 7a ff.

3 Vgl. insb. die Anm. von *Hiéramente/Basar*, jurisPR-StrafR 6/2022 Anm. 1; a.A. LG Koblenz v. 24.8.2021 – 4 Qs 59/21, juris.

4 LG Koblenz v. 24.8.2021 – 4 Qs 59/21, juris.

5 LG Koblenz v. 24.8.2021 – 4 Qs 59/21, juris unter Verweis auf: *Blechschmitt*, Strafverfolgung im digitalen Zeitalter, MMR 2018, 361 (363); *Hauschild* in MünchKomm, § 110 StPO Rz. 16.

6 LG Koblenz v. 24.8.2021 – 4 Qs 59/21, juris unter Verweis auf *Hauschild* in MünchKomm, § 110 StPO Rz. 16.

book und Google) heimlich erfolgt, solange dieser Zugriff auf Grund der Konfiguration des Computersystems des Betroffenen technisch möglich ist.[1] Bei dem Abruf der Daten der verschiedenen Accounts des Beschuldigten handele es sich um eine Online-Sichtung nach § 110 Abs. 3 StPO und nicht um eine verdeckte Infiltration eines informatorischen Systems des Beschuldigten.

215 Der Zugriff auf die (wohl) **im Ausland gespeicherten Daten** ist nach Ansicht des LG Koblenz auch ohne Rechtshilfeersuchen zulässig gewesen.

Der Streitstand ist hier indes uneinig. Teilweise wird vertreten, ein Rechtshilfeersuchen sei nur erforderlich, wenn die Daten zugangsgeschützt sind.[2] Teilweise wird ein Rechtshilfeersuchen dann nicht für erforderlich gehalten, wenn nicht bekannt ist, in welchem Ausland die Daten gespeichert werden,[3] bzw. wenn nicht klar ist, ob die Daten überhaupt im Ausland gespeichert sind und ein Zugriff auf die Daten vom Computer des Beschuldigten (bzw. mit dessen Zugangsdaten) aus möglich ist.[4]

Gegen das Erfordernis eines Rechtshilfeersuchens spricht nach Ansicht des LG Koblenz, dass der Staat, an den ein derartiges Ersuchen zu richten wäre, entweder nicht feststellbar ist oder sich durch eine Neuordnung des Speicherplatzes (durch den Dritten, nicht den Beschuldigten) jederzeit ändern könnte. Zudem entspreche es dem Geschäftsmodell der Drittanbieter, dass über eigene Serverkapazitäten hinaus erhebliche Serverleistungen „fremd" eingekauft werden, so dass der Standort der tatsächlich genutzten Server nicht mit denen der Drittanbieter übereinstimmen muss.

216 Entgegen dem LG Koblenz ist ein über die unmittelbare Sicherung vor Ort hinausgehender Zugriff indes nach der überwiegenden Literatur völkerrechtswidrig. Eine entsprechende Rechtsgrundlage fehlt de lege lata.[5]

Dies ergibt sich bereits aus der Gesetzesbegründung, auf die auch das LG Koblenz Bezug nimmt. Dort heißt es[6]:

---

1 LG Koblenz v. 24.8.2021 – 4 Qs 59/21, juris unter Verweis auf *Hauschild* in MünchKomm, § 110 StPO Rz. 16.

2 So *Hegmann* in BeckOK, § 110 StPO Rz. 16; *Hauschild* in MünchKomm, § 110 StPO Rz. 18; *Köhler* in Meyer-Goßner/Schmitt[65], § 110 StPO Rz. 7a.

3 *Hegmann* in BeckOK, § 110 StPO Rz. 16.

4 Vgl. *Köhler* in Meyer-Goßner/Schmitt[65], § 110 StPO Rz. 7b.

5 *Hauschild* in MünchKomm, § 110 StPO Rz. 16; *Gercke* in Borges/Meents, Cloud Computing, § 20 Strafrechtliche und strafprozessuale Aspekte von Cloud Computing und Cloud Storage, Rz. 40; *Bruns* in KK[8], § 110 StPO Rz. 80; *Köhler* in Meyer-Goßner/Schmitt[65], § 110 StPO Rz. 7a; *Bär* in Wabnitz/Janovsky/Schmitt[5], 28. Kap. Rz. 27; *Kempf/Schilling/Oesterle* in MAH Verteidigung in Wirtschafts- und Steuerstrafsachen[3], § 10 Rz. 99; *Grözinger* in MAH Strafverteidigung[3], § 50 Rz. 234; *Brodowski/Eisenmenger*, ZD 2014, 119 (122); *Hiéramente/Basar*, jurisPR-StrafR 6/2022 Anm. 1.

6 BT-Drucks. 16/5846, 27.

„Artikel 19 Abs. 2 des Übereinkommens verpflichtet die Vertragsparteien daher auch, die erforderlichen gesetzgeberischen Maßnahmen zu treffen, um sicherzustellen, dass ihre Behörden eine Durchsuchung oder einen ähnlichen Zugriff schnell auf ein weiteres Computersystem ausdehnen können, wenn sie ein bestimmtes Computersystem oder einen Teil davon durchsuchen oder in ähnlicher Weise darauf Zugriff nehmen und Grund zu der Annahme haben, dass die gesuchten Daten in einem anderen Computersystem oder einem Teil davon in ihrem Hoheitsgebiet gespeichert sind, und diese Daten von dem ersten System aus rechtmäßig zugänglich oder verfügbar sind."

Zudem war der **Durchsuchungsbeschluss mit der Vollstreckung verbraucht**.[1] Selbst wenn im Falle einer Mitnahme zur Durchsicht die Durchsuchung bis zum Ende der Durchsicht noch nicht als abgeschlossen gilt, bezieht diese sich nur auf Daten, die im Rahmen der Durchsuchung vorläufig unmittelbar (vor Ort) sichergestellt worden sind. 217

Greifen Ermittlungsbehörden nach Abschluss der räumlichen Durchsuchung erneut auf Nutzerkonten des Durchsuchungsbetroffenen **im Internet zu**, ermöglicht dieser Zugriff jedoch nicht nur die Sichtung der Daten, die Gegenstand der durchgeführten Durchsuchung waren, sondern auch die Sichtung von Daten, die erst nach Abschluss der Durchsuchungsmaßnahme entstanden sind.[2] Für letztere Daten besteht kein Durchsuchungsbeschluss. Auch für eine wiederholte (heimliche) Beschlagnahme der Daten (vgl. § 95a StPO) ist kein Raum, da ansonsten die (strengeren) Vorgaben des § 100a StPO umgangen werden könnten.[3] Ein verdeckter Zugriff auf die Nachrichten im Herrschaftsbereich des Social-Media-Anbieters ist nur nach § 100a StPO möglich. Wollen die Ermittlungsbehörden Zugriff auf Clouddaten nehmen, hat dies offen und im Zeitpunkt der Durchsuchung zu erfolgen. 218

In **praktischer Hinsicht** bietet es sich an, für den Fall der Durchsuchung den **Serververtrag parat** zu halten zum Nachweis, wo die Daten belegen sind. Sind die Daten im Ausland belegen oder der Speicherort unbekannt, sollten die Ermittlungsbehörden hierauf ausdrücklich und nachweislich hingewiesen werden. 219

Verwertungsverbote[4] (Rz. 1064 f.) können sich zunächst aus der **Missachtung der Souveränität fremder Staaten** ergeben, etwa bei eigenmächtigen grenzüberschreitenden Handlungen ohne Rechtshilfeersuchen oder bei einer bewussten Missachtung der inhaltlichen Reichweite des Ersuchens.[5] Aus einem bloßen **Verstoß gegen das Territorialprinzip** kann ein Beweisverwer- 220

1 *Köhler* in Meyer-Goßner/Schmitt[65], § 105 StPO Rz. 14.
2 *Hiéramente/Basar*, jurisPR-StrafR 6/2022 Anm. 1.
3 *Hiéramente/Basar*, jurisPR-StrafR 6/2022 Anm. 1 unter Verweis auf *Brodowski/Eisenmenger*, ZD 2014, 119 (124).
4 Zum Ganzen *Peters* in Schaumburg/Peters, Internationales Steuerstrafrecht[2], Rz. 6.250 ff.
5 BGH v. 21.11.2012 – 1 StR 310/12, ZWH 2013, 250 = wistra 2013, 282, unter Verweis auf *Ambos*, Beweisverwertungsverbote, 2010, 81; *Gless*, Beweisrechtsgrundsätze einer grenzüberschreitenden Strafverfolgung, 2006, 141 ff.; *Gless*, JR 2008, 317 (323 ff.).

tungsverbot zugunsten des Beschuldigten indes nicht hergeleitet werden. Sein Rechtskreis ist insofern nicht betroffen. Etwas anderes kann jedoch gelten, wenn der Rechtshilfeweg willkürlich und absichtlich umgangen wird und die völkerrechtliche Norm individualschützenden Charakter entfaltet.[1] Beweisverwertungsverbote im Zusammenhang mit Beweisrechtshilfe können sich auch aus der inländischen Rechtsordnung des ersuchenden Staates[2] oder aus völkerrechtlichen Grundsätzen ergeben,[3] etwa bei unzulässigen Eingriffen in das Souveränitätsrecht eines anderen Staates, z.B. bei bewusster Umgehung der Rechtshilfe.[4] Hinzu kommt, dass es häufig zu verzeichnen ist, dass in der Praxis im Nachgang kein Rechtshilfeersuchen gestellt wird bzw. sich um eine entsprechende Legitimation der Daten bemüht wird.

i) Geltungsdauer der Durchsuchungsanordnung

221 Richterliche Beschlüsse haben eine **Gültigkeitsdauer** von höchstens **sechs Monaten** (so auch Nr. 60 Abs. 10 AStBV (St) 2022; s. AStBV Rz. 60); danach ist von einer veränderten Sachlage und damit einer überholten Durchsuchungsanordnung auszugehen.[5] (Entsprechendes gilt für Beschlagnahmebeschlüsse.[6]) Es bedarf dann einer erneuten richterlichen Prüfung und Durchsuchungsanordnung. Die zur Begründung herangezogenen Beweismittel und Erkenntnisse sollen allerdings älter als sechs Monate sein können[7].

222 Die Anordnung einer **Dauerdurchsuchung** oder von **Mehrfachdurchsuchungen**, um nicht (nur) Beweismittel aufzufinden, sondern z.B. durch die Beobachtung des Kassenbetriebs oder Vernehmungen von Mitarbeitern die

1 BVerfG v. 16.3.2006 – 2 BvR 954/02, NJW 2006, 2684 (2686); BVerfG v. 12.4.2005 – 2 BvR 1027/02, NJW 2005, 1917 (1923) = CR 2005, 777 = BRAK 2005, 186 = wistra 2005, 295; BVerfG v. 22.3.1983 – 2 BvR 475/78, BVerfGE 63, 343; VerfGH Rheinland-Pfalz v. 24.2.2014 – VGH B 26/13, NJW 2014, 1434.

2 Zu Verstößen gegen § 136a StPO bei im Ausland vernommenen Zeugen vgl. *Nagler*, StV 2013, 324 (327).

3 BGH v. 21.11.2012 – 1 StR 310/12, juris, unter Verweis auf *Ambos*, Beweisverwertungsverbote, 2010, 81; *Gless*, Beweisrechtsgrundsätze einer grenzüberschreitenden Strafverfolgung, 2006, 141 ff.; *Gless*, JR 2008, 317 (323 ff.); *Bülte*, ZWH 2013, 265 = wistra 2013, 282.

4 BGH v. 8.4.1987 – 3 StR 11/87, BGHSt 34, 334 (343 f.) = wistra 1987, 259.

5 BVerfG v. 27.5.1997 – 2 BvR 1992/92, wistra 1997, 223 (226); diese Größenordnung erlaubt aber ein Überschreiten um wenige Tage: LG Zweibrücken v. 23.9.2002 – Qs 103/02, NJW 2003, 156; für eine Verwirkung LG Berlin v. 24.9.2002 – 508 Qs 115/02, NStZ 2004, 102.

6 LG Neuruppin v. 11.7.1997 – 14 Qs 59 Js 315/96, NStZ 1997, 563 (564).

7 BVerfG v. 15.12.2004 – 2 BvR 1873/04, BVerfGK 4, 303, abrufbar unter www.bundesverfassungsgericht.de, gegen LG Berlin v. 24.9.2002 – 508 Qs 115/02, NStZ 2004, 102; BVerfG v. 25.7.2017 – 2 BvR 1287/17, 1 BvR 1583/17, StV 2017, 705.