Aufsätze und Kurzbeiträge

Strafprozessrecht

Rechtsanwalt Dr. André-M. Szesny, LL.M., Düsseldorf*

Durchsicht von Daten gem. § 110 StPO

I. Einführung

In Zeiten der stark zunehmenden Digitalisierung steigt die Bedeutung von Daten immens. Sowohl im privaten wie im beruflichen Bereich wird die Papierkorrespondenz und -ablage durch elektronische Kommunikation und Datenverarbeitung maßgeblich ergänzt, teilweise sogar ersetzt. Die Digitalisierung interner Protokolle z. B. von Aufsichtsrats- oder Vorstandssitzungen,[1] die papierlose Buchführung gem. §§ 238 ff. HGB, das Digitalisieren steuerrelevanter Unterlagen, die Nutzung von Emails als Standardkommunikationsmittel und die Einführung digitaler Signaturen sind nur Beispiele der unzähligen Möglichkeiten der elektronischen Datenverarbeitung. Auch wenn das „papierlose Büro" in vielen Branchen noch Zukunftsmusik ist: Spätestens seit der Etablierung von Smartphones und Tablet PCs nimmt die Bedeutung der klassischen Papiernotiz ab. Hinzu kommt, dass auch das Internet nicht mehr lediglich zu Informations- und Abfragezwecken, sondern insbesondere durch Teilnahme in sozialen Netzwerken und Internetblogs aktiv als Kommunikations-, Austausch- und Werbeplattform genutzt wird. Nicht zuletzt führen Online-Banking, Online-Einkauf und die Nutzung von Suchmaschinen dazu, dass der Mensch nicht nur eine „Papierspur" seiner Lebensaktivitäten hinterlässt, sondern auch eine Datenspur. Diese ist im Rahmen von strafprozessualen Ermittlungen von nicht geringerem Interesse als körperliche Beweismittel. Insbesondere in Wirtschaftsstrafverfahren sind elektronisch gespeicherte Daten für die Beweisführung maßgeblich.

II. Anwendbarkeit der Vorschrift des § 110 StPO auf Daten

Entsprechend nimmt auch die Bedeutung der Durchsicht von Daten im Rahmen von Durchsuchungsmaßnahmen erheblich zu. Eine ausdrückliche Ermächtigung zur Datendurchsicht enthält die StPO zwar nicht. Es ist aber anerkannt, dass die Vorschrift über die Durchsicht von Papieren (§ 110 Abs. 1 StPO) nicht nur auf Papiere im Sinne des Wortlauts, sondern darüber hinaus auch auf Daten bzw. die sie verkörpernden elektronischen Speichermedien anwendbar ist,[2] insbesondere lokale Festplatten in Personalcomputern und mobile Speichermedien (z. B. DVDs, externe Festplatten, Speicherkarten in Mobiltelefonen oder Kameras, Speichersticks). Mit Blick auf die Anwendbarkeit der §§ 94, 98 StPO auf Daten[3] ist dies nur konsequent und nicht zu beanstanden. Auch § 110 Abs. 3 StPO spricht für eine Anwendung der gesamten Vorschrift auf Daten: Danach darf bei Gefahr des Beweismittelverlusts der Staatsanwalt auch vom Durchsuchungsort räumlich getrennte, über eine Netzwerkverbindung erreichbare Speichermedien durchsichten, womit vor allem der Speicherplatz auf einem Server im Intra- oder Internet erfasst wird.

Zweck der Durchsicht

Der Zweck der Durchsicht liegt in der Aussonderung verfahrensirrelevanter und beschlagnahmeunfähiger Unterlagen.[4] Staatsanwaltschaft und (auf deren Anordnung) ihre Ermittlungspersonen prüfen also im Wege der Durchsicht, welchen Unterlagen Beweisqualität zukommt und welche einem etwaigen Beschlagnahmeverbot (§§ 97, 148 StPO) unterliegen. Es

* Der Autor ist Rechtsanwalt und Salaried Partner am Düsseldorfer Standort von Heuking Kühn Lüer Wojtek. Er dankt Frau Rechtsreferendarin Katharina *Mellis* für die hilfreiche Unterstützung bei der Vorbereitung und Abfassung dieses Beitrages.

[1] So stellte die Beratungsgesellschaft *Edis-Bates Associates* bei einer Befragung von 150 an der Londoner Börse notierten Unternehmen fest, dass 40 Prozent von ihnen die Unterlagen für Verwaltungsratssitzungen auf elektronischen Weg versenden.

[2] *BVerfG* NJW 2005, 1917, 1920 unter Hinweis auf BR-Drucks. 378/03, S. 28; *BVerfG* NStZ 2002, 377 (Notebook); *BGH* StV 1988, 90; BGH NJW 1995, 3397; *BGH* CR 1999, 292; *BGH* NStZ 2003, 670; vgl. *Herrmann/Soine* NJW 2011, 2922; *Schäfer* in: Löwe-Rosenberg, StPO, 25. Aufl., 29. Lfg., § 110 Rn. 5; KK-StPO/*Nack*, § 110 Rn. 2.

[3] Vgl. *BVerfG* NJW 2005, 1917 ff.; *Park*, Durchsuchung und Beschlagnahme, 2. Aufl. 2009, Rn. 771; a. A. *Kemper* NStZ 2005, 538, 541.

[4] Vgl. *VerfGH Bayern* BeckRS 2011, 46287, III. 3; *Haffke* NJW 1974, 1983.

gehört inzwischen zum Standard, dass EDV-Experten der Landeskriminalämter bei Durchsuchungen eingesetzt werden, um den Zugriff auf elektronisch gespeicherte Beweismittel zu garantieren und die Durchsicht bzw. die spätere Sicherstellung der Daten zu ermöglichen.

Soweit sich die Durchsicht auf Daten bezieht, dient sie nicht nur der Verschlankung des Beweisumfangs und damit der Verfahrenseffizienz, sondern schützt den Betroffenen auch vor einer übermäßigen und auf Dauer angelegten Datenerhebung.[5] Die mit der Durchsuchung und Sicherstellung verbundene Intensität des Eingriffs in das Recht auf informationelle Selbstbestimmung und das Recht auf Gewährung der Integrität und Vertraulichkeit informationstechnischer Systeme soll auf diese Weise effektiv vermindert werden.[6]

Tendenz zur Mitnahme überschießender Datenbestände

Diese vom BVerfG hervorgehobene Schutzintention des § 110 StPO scheint in der Rechtstatsächlichkeit indes Praktikabilitätserwägungen gewichen zu sein.[7] Zu beobachten ist eine Tendenz der Ermittlungsbehörden, die Durchsicht von Daten nicht an Ort und Stelle der Durchsuchungsmaßnahme vorzunehmen, sondern bei der Staatsanwaltschaft bzw. den Ermittlungspersonen.[8] Hierzu wird im Regelfall das gesamte Speichermedium zur Durchsicht mitgenommen bzw. der darauf gespeicherte Datenbestand „gespiegelt", also „eins zu eins" auf ein von den Ermittlungsbeamten mitgebrachtes Speichermedium (regelmäßig ist dies eine externe Festplatte) übertragen: In der Praxis der Strafverfolgungsbehörden dominiert die Komplettsicherung von Speichermedien,[9] sofern sich auf dem Medium potentiell beweisrelevante Daten befinden. Dies führt zu einer Mitnahme beträchtlicher Datenmengen und insbesondere auch solcher Daten, die für das jeweilige Verfahren ohne Bedeutung sind, da sie keine Beweisrelevanz besitzen oder gar einem Beschlagnahmeverbot unterliegen. Mancherorts scheint es sogar innerbehördliche Anweisungen zu geben, schon „vorsichtshalber" den gesamten Datenbestand eines verdächtigten Mitarbeiters oder den Datenbestand eines Servers zu sichern, um ihn einer späteren – zeitlich „entspannteren" – Durchsicht zu unterziehen, um bloß nichts Verfahrensrelevantes „liegen zu lassen". Insoweit lässt sich eine Diskrepanz zwischen der Durchsicht von Papieren im engeren Sinne und der Durchsicht von Daten beobachten: Staatsanwälte und Ermittlungspersonen nehmen im Rahmen von Durchsuchungen regelmäßig noch jeden Papierordner in die Hand, blättern diesen zumindest durch und entscheiden dann über die Mitnahme desselben. Anderes ist in Bezug auf elektronisch gespeicherte Daten zu beobachten: Selbst wenn einzelne Dateiordner geöffnet und Dateien exemplarisch durchgesehen werden, folgt regelmäßig die Spiegelung des gesamten Festplatteninhalts – dies entweder vor Ort oder nach Mitnahme des Rechners des Betroffenen in der Dienststelle, etwa des Landeskriminalamtes.

Die Eigenheiten der elektronischen Datenverarbeitung lassen diese Praxis nur auf den ersten Blick als nachvollziehbar erscheinen. Heterogene und außen stehenden Personen undurchsichtige Ablagestrukturen auf Unternehmensservern und Mitarbeiterlaufwerken, uneinheitliche Dateinamen, nicht eindeutige Zugriffsbefugnisse und andere Intransparenzen machen es den Ermittlungsbehörden schwer, sich auf der Suche nach beweisrelevanten Daten auf den fremden Rechnern zurechtzufinden.

Andererseits begegnet die Praxis, im Regelfall den gesamten Datenbestand eines Rechners oder ganzer Serverlaufwerke zu spiegeln und „mitzunehmen", mit Blick auf Wortlaut, Sinn und Zweck des § 110 StPO sowie das vom Bundesverfassungsgericht neu geschaffene Grundrecht auf Gewährung der Integrität und Vertraulichkeit informationstechnischer Systeme[10] erheblichen Bedenken. Nachfolgend werden die Stufen der Datendurchsicht beschrieben und deren Reichweite und Grenzen beleuchtet.

III. Vorläufige Sicherstellung zum Zwecke der Datendurchsicht

Mit der Durchsicht i. S. von § 110 StPO soll der Staatsanwaltschaft Gelegenheit zur Klärung und Entscheidung gegeben werden, ob die Unterlagen sicherzustellen bzw. zu beschlag-

[5] *BVerfG* NJW 2005, 1917, 1922.
[6] *BVerfG* NJW 2005, 1917, 1922.
[7] Ähnlich schon *Park* wistra 2000, 453 allerdings in Bezug auf die Abschaffung zunächst des richterlichen Sichtungsprivilegs (BGBl. I 1974, 3393). Später wurde auch das rein staatsanwaltschaftliche Sichtungsprivileg abgeschafft (BGBl. I 2004, 2198).
[8] Vgl. KK-StPO/*Nack*, § 110 Rn. 4.
[9] *Bäcker/Freiling/Schmitt* DuD 2010, 80, 81.
[10] *BVerfGE* 120, 274 = NJW 2008, 822.

nahmen sind.[11] Die Durchsicht von Daten ist damit Bestandteil der Durchsuchung,[12] wobei es aufgrund der Fülle und der damit einhergehenden Unübersichtlichkeit der Daten oftmals als erforderlich angesehen wird, diese mitzunehmen und erst später in der Behörde durchzusichten. In diesem Fall werden die zu durchsichtenden Papiere und Daten zum Zwecke der Mitnahme an den Dienstort „vorläufig sichergestellt".[13]

1) Begriff der vorläufigen Sicherstellung

Kompensation der vorläufigen Sicherstellung durch Kurzfrist

Den Begriff der „vorläufigen Sicherstellung" sucht man in der StPO vergeblich. Gleichwohl passt er für zur Durchsicht mitgenommene Papiere und Datenträger durchaus. Es herrscht denn auch grundsätzlich Einigkeit darüber, dass eine „vorläufige Sicherstellung" dieser Daten zulässig ist.[14] Dass im Wege der vorläufigen Sicherstellung Daten mitgenommen werden, die für das zugrunde liegende Strafverfahren nicht relevant sind oder die sogar einem Beschlagnahmeverbot unterliegen, liegt in der Natur der Sache. Dieser Umstand soll dadurch kompensiert werden, dass die Durchsicht nur eine kurzfristige, eben „vorläufige Sicherstellung" darstellt und nur ein grobes Überfliegen der Daten erfordert. Die „vorläufige Sicherstellung" geht also der Durchsicht der Daten voraus; sie ist – wie gesehen – Bestandteil der Durchsuchung und noch keine Beschlagnahme.[15] Alternativ kann die vorläufige Sicherstellung in Form einer Spiegelung von Daten durchgeführt werden. Hierbei handelt es sich um einen Datenverarbeitungsvorgang, bei dem die „vorläufig sichergestellten" Daten auf Datenträger der Ermittlungsbehörden kopiert werden. Als „Minus" im Vergleich zu einer vorläufigen Sicherstellung von Datenträgern des Betroffenen dürfte sie grundsätzlich zulässig sein.[16] Denn die Mitnahme von Datenträgern über einen längeren Zeitraum schränkt die Funktionsfähigkeit eines Unternehmens jedenfalls zeitweise erheblich ein, schließt sie mitunter sogar aus. Die Anfertigung einer Kopie bewirkt, dass die Daten dem Unternehmen weiterhin zur Verfügung stehen und stellt somit im Vergleich zur Mitnahme der Originale grundsätzlich eine mildere – die Berufsausübungsfreiheit schützende – Maßnahme dar.

2) Grenzen der vorläufigen Sicherstellung

Keine vorläufig Sicherstellung offensichtlich verfahrensirrelevanter Daten

Schon die vorläufige Sicherstellung unterliegt Grenzen, die der Durchsuchungsbeschluss bestimmt. Für eine der vorläufigen Sicherstellung nachfolgende Durchsicht gem. § 110 StPO ist kein Raum, wenn ein Papier oder ein Datenbestand schon aufgrund der Beschreibung im Durchsuchungs- und Beschlagnahmebeschluss gezielt ausgesondert und sogleich beschlagnahmt werden kann.[17] Umgekehrt ist die Durchsicht nur solcher Papiere und Daten zulässig, die überhaupt als Beweismittel für den im Durchsuchungs- und Beschlagnahmebeschluss umrissenen Vorwurf in Betracht kommen.[18] Daraus folgt, dass jedenfalls *offensichtlich* verfahrensirrelevante Beweisstücke bereits vor der vorläufigen Sicherstellung auszusondern sind. Soll z. B. eine das Jahr 2009 betreffende Steuerhinterziehung aufgeklärt werden, dürfen die Belege anderer Jahre nur durchgesehen werden, wenn aus ihnen Schlüsse auf die Vorgänge des Jahres 2009 denkbar sind.[19] Von vornherein unzulässig ist die Durchsicht auch, wenn offensichtlich ist, dass bzgl. des Schriftstücks ein Beschlagnahmeverbot besteht. So darf Email-Verkehr des Beschuldigten mit seinem Verteidiger schon nicht zur Durchsicht vorläufig sichergestellt werden. Auch soweit bereits vor Ort offensichtlich ist, dass bestimmte Daten für das zugrunde liegende Strafverfahren nicht relevant sein können, müssen diese bereits vor der Durchsicht zurückgegeben werden.[20]

Die technische Möglichkeit zur Mitnahme des gesamten Datenträgers oder der Spiegelung desselben befreit nicht von einer Vorsortierung des Datenbestandes vor Ort anhand der im Durchsuchungsbeschluss umrissenen Grenzen. In jedem Einzelfall muss die Begrenzung einer „überschießenden Datenerhebung" schon im Vorfeld der vorläufigen Sicherstellung

[11] *BGH* NJW 1995, 3397.
[12] *BGHSt* 44, 265, 273 = NJW 1999, 730; *BGH* NJW 1995, 3397.
[13] *BGH* NJW 1995, 3397.
[14] Vgl. allein *Meyer-Goßner*, StPO, 55. Aufl. 2012, § 110 Rn. 10.
[15] *BVerfG* NJW 2009, 2431, 2438; *OVG Hamburg*, Beschl. v. 03.07.2012 – 12 Bf 58/12.F, Rn. 20 (abrufbar unter www.juris.de); *LG Limburg* PStR 2011, 112 f.; *Meyer-Goßner*, § 110 Rn. 10.
[16] A. A. wohl *Kemper* NStZ 2005, 538, 541.
[17] *Park* wistra 2000, 453.
[18] Vgl. *Schäfer* in: Löwe-Rosenberg, § 110 Rn. 1.
[19] Vgl. *Schäfer* in: Löwe-Rosenberg, § 110 Rn. 1.
[20] Vgl. *Meyer-Goßner*, § 110 Rn. 2.

Beweismittel ist die Datei, nicht der Datenträger

zumindest erwogen werden.[21] Diese Erwägung muss sich auch aus der Dokumentation der strafprozessualen Maßnahme erkennen lassen, damit sie gerichtlich nachprüfbar ist.[22] Dies gebietet zum einen der Schutz u. U. zahlreicher Personen, die durch die Spiegelung einer Vielzahl verfahrensunerheblicher (auch personenbezogener) Daten in den Wirkungsbereich der Maßnahme mit einbezogen werden, obwohl sie in keiner Beziehung zum Tatvorwurf stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben.[23] Zum zweiten ist aber auch der Eingriff in personenbezogene Daten des Betroffenen verhältnismäßig zu gestalten, mithin auf das erforderliche und angemessene Maß zu beschränken.

Die sorgfältige Durchsicht und Aussonderung nicht beweisrelevanter Daten darf auch nicht mit dem Hinweis unterbleiben, der auf einem Datenträger befindliche Datenbestand sei ein Beweismittel im Ganzen, der unteilbar der Beschlagnahme unterliege.[24] Denn Beweismittel ist Inhalt der Dateien, nicht der gesamte Datenträger.[25] Nur weil sich beweisrelevante Daten auf einem bestimmten Serverlaufwerk identifizieren lassen, ergibt sich hieraus nicht die Erforderlichkeit, den gesamten auf dem Serverlaufwerk befindlichen Datenbestand zu kopieren oder gar den gesamten Datenträger mitzunehmen.

Die nach diesen Maßstäben erforderliche Begrenzung des „vorläufig sicherzustellenden" Materials kann etwa anhand der Struktur des Datenbestandes, durch Identifizierung der Zugriffsmöglichkeiten von Beschuldigten oder sonst verfahrensrelevanten Personen sowie anhand des Speicherdatums, des Verfassers bzw. Adressaten oder Absenders einer Email erfolgen. Nur dann, wenn „die Eigenheiten des jeweiligen strafrechtlichen Vorwurfs und die – auch technische – Erfassbarkeit des jeweiligen Datenbestands eine unverzügliche Zuordnung nicht erlauben, muss die Prüfung der Verfahrensrelevanz der gespeicherten Daten im Rahmen der vorläufigen Sicherstellung erwogen werden."[26] Dies bedeutet, dass bereits vor einer „vorläufigen Sicherstellung" eine Abwägung stattzufinden hat, welche Datensätze an Ort und Stelle überprüft werden können und welche nicht. Dabei ist zu beachten, dass eine Durchsicht vor Ort durchaus Zeit kosten darf und auch muss: Denn eine Mitnahme von Daten zur Durchsicht führt insoweit zu einer nahezu vollständigen Durchsuchung „im Geheimen". Der gem. § 106 StPO gesetzlich angeordnete „offene" Charakter einer Durchsuchung wird dadurch faktisch unterlaufen.[27] Dazu kommt, dass durch die Mitnahme von Daten der unzulässigen[28] zielgerichteten Suche nach Zufallsfunden Tür und Tor geöffnet wird. Diese Negativeffekte müssen durch eine sorgfältige Abwägung und Begrenzung der mitzunehmenden Daten im Vorfeld der vorläufigen Sicherstellung beschränkt werden.

Die in der Praxis geradezu selbstverständlich gewordene Mitnahme sämtlicher auf einem bestimmten Speichermedium befindlicher Daten stellt sich vor diesem Hintergrund in einer Vielzahl der Fälle als nicht zulässig dar. Freilich bleiben Fälle denkbar, in denen sich nach der groben Vorsichtung des Datenbestandes und der vorgenannten Abwägung die Erforderlichkeit einer Komplettspiegelung bzw. Sicherstellung ganzer Datenträger oder Laufwerke ergibt, dies etwa weil es sich aufgrund der unübersichtlichen Ablagestruktur geradezu aufdrängt, dass beweiserhebliche Dateien vor Ort nicht identifiziert werden können. Dies dürfte allerdings nur ausnahmsweise der Fall sein.

IV. Die Datendurchsicht

Nach der vorläufigen Sicherstellung und Mitnahme der Daten in die Behördenräume erfolgt deren eigentliche Durchsicht. Den Ablauf der Durchsicht regelt die StPO nicht. Jedoch ergeben sich aus dem Charakter der Durchsicht als Teil der Durchsuchungsmaßnahme und aus den im gesamten Ermittlungsverfahren zu berücksichtigen Verfassungsprinzipien Grundsätze, die das Verfahren der Durchsicht bestimmen.

---

[21] *BVerfG* NJW 2005, 1917, 1921.
[22] Zu den Rechtsschutzmöglichkeiten siehe Punkt VII.
[23] *BVerfG* NJW 2005, 1917, 1921.
[24] *BVerfG* NJW 2005, 1917, 1923.
[25] Vgl. *LG Bonn* wistra 2005, 76.
[26] *BVerfG* NJW 2005, 1917, 1921.
[27] Zur Erforderlichkeit der Hinzuziehung des Dateninhabers zur Durchsicht siehe noch sogl. Punkt IV. 2.
[28] Vgl. *Meyer-Goßner*, § 108 Rn. 1.

1) Zulässige Dauer

Je nach Umfang und Komplexität der Daten muss die Durchsicht nicht binnen kürzester Zeit erfolgen; die Rechtsprechung hat hier ausdrücklich keine festen Grenzen gesetzt. Die sechsmonatige „Haltbarkeitsgrenze", derzufolge eine Durchsuchungsanordnung spätestens nach Ablauf eines halben Jahres seine rechtfertigende Kraft verliert,[29] betrifft nur den Fall, dass mit der Durchsuchung innerhalb von sechs Monaten nicht einmal begonnen wurde. Wurde diese Frist eingehalten, besteht keine feste zeitliche Grenze für die Durchsicht der vorläufig sichergestellten Daten. Während der Gesamtdauer der Durchsicht müssen jedenfalls aber die Eingriffsvoraussetzungen der §§ 102, 103 StPO vorliegen. Insbesondere muss ein konkreter und nicht nur vager Auffindeverdacht vorliegen. Die allgemeine Angabe, dass nicht auszuschließen sei, dass sich relevante Daten auf der Festplatte befänden, reicht hierzu nicht aus.

Unzumutbar lange darf die Durchsicht mit Blick auf das in Art. 6 Abs. 1 EMRK enthaltene Beschleunigungsgebot[30] indes nicht dauern. Bei der Durchsicht i. S. von § 110 StPO ist zu verlangen, dass die Ermittlungsbehörde sich zügig an die Durchsicht der vorgefundenen und mitgenommenen Unterlagen macht mit dem Ziel, in angemessener Zeit potentiell Beweiserhebliches zu identifizieren und zu beschlagnahmen. Die übrigen Unterlagen sind an den Betroffenen wieder herauszugeben. Welche Dauer hierzu angemessen ist, hängt wesentlich von der Menge des zu überprüfenden Materials und der Schwierigkeit der Auswertung ab. Das LG Frankfurt hat in einem Fall der Durchsicht 15 Monate für „noch als hinnehmbar" angesehen,[31] dies allerdings nur wegen „außerordentlich umfangreicher" Unterlagen sowie „der internationalen Bezüge" des Verfahrensgegenstandes.

2) Anwesenheit des Betroffenen bei der Datendurchsicht

Insbesondere wenn umfassende Datenmitnahmen erfolgt sind, empfiehlt es sich, dass die Behörden die Durchsicht gemeinsam mit dem Inhaber der Daten durchführen, um auf diese Weise effektiv verfahrens(ir)relevante Datenbestände identifizieren zu können. Zwar wurde das ursprünglich bestehende Anwesenheitsrecht des Inhabers der betroffenen Papiere und Daten durch das 1. Justizmodernisierungsgesetz[32] ersatzlos gestrichen. Dies geschah jedoch, da § 110 Abs. 3 StPO a. F. eine Versiegelung der vorläufig sichergestellten Daten vorsah, die verhindern sollte, dass die Ermittlungsbeamten der Staatsanwaltschaft Einsicht in diese Daten bekommen. Nach der Erweiterung der Sichtungsbefugnis zugunsten dieser Ermittlungspersonen war dies nun obsolet. Gleichzeitig aber entfiel ohne nähere Begründung auch die Regelung, nach der der Inhaber für den Fall der demnächst anzuordnenden Durchsicht der Papiere nach Möglichkeit zur Teilnahme aufzufordern war.[33] Zu Recht hält es das BVerfG zur „Sicherung der Verhältnismäßigkeit des Eingriffs" im Einzelfall für geboten, trotz Wegfalls dieser Regelung den Inhaber des jeweiligen Datenbestandes in die Prüfung der Verfahrenserheblichkeit einzubeziehen.[34] Dies erscheint auch mit Blick auf § 106 StPO systematisch geboten.

Gerade in Wirtschaftsstrafverfahren kann die Anwesenheit des Betroffenen, eines mit der IT-Struktur des betroffenen Unternehmens vertrauten Mitarbeiters und des Unternehmensanwalts zudem zu einer erheblichen Beschleunigung der Aussonderung verfahrensirrelevanter Dateien und zu einer schnelleren Identifikation relevanter Beweismittel führen. Ohne Hilfestellung eines anwesenden Mitarbeiters des jeweiligen Unternehmens wird eine Datenaussonderung innerhalb vertretbarer Zeit kaum zu bewerkstelligen sein.

Dazu kommt, dass die Anwesenheit des Betroffenen die Gefahr der „gezielten Suche" nach Zufallsfunden minimiert. Als Faustregel sollte gelten: Je weiter und undifferenzierter der Umfang der zur Sichtung mitgenommenen Datenbestände ist, desto schwerer wiegt das Interesse des Inhabers der Daten, bei der Aussonderung verfahrensirrelevanter Daten anwesend zu sein und diese zu begleiten.

---

[29] *BVerfGE* 96, 44 = *BVerfG* NJW 1997, 2165.
[30] Näher zum Beschleunigungsgebot im Allgemeinen KK-StPO/*Schädler*, 6. Aufl. 2008, Art. 6 EMRK Rn. 34, 39; *Meyer-Ladewig* in: ders., EMRK, 3. Aufl. 2011, Art. 6 Rn. 199 ff.
[31] *LG Frankfurt* NStZ 1997, 564, 565.
[32] BGBl. I 2004, 2198.
[33] Vgl. *BVerfGE* 113, 29 = wistra 2005, 295.
[34] *BVerfG* NJW 2005, 1917, 1922.

V. Beendigung der Durchsicht und Rückgabe

Die Durchsicht endet mit der Entscheidung der Staatsanwaltschaft, welche Papiere bzw. Daten beweisrelevant sind.[35] Die als verfahrensunerheblich bzw. beschlagnahmefrei identifizierten Papiere müssen an den Inhaber zurückgegeben werden.[36]

1) Rückgabe oder Vernichtung ausgesonderter Daten

Das Rückgabegebot gilt im Grundsatz auch für Daten, da diese dem extensiven Papierbegriff des § 110 StPO unterfallen. Eine physische Rückgabe an den Inhaber kommt jedoch nur dann in Betracht, wenn der Originaldatenträger vorläufig sichergestellt wurde und dieser ausschließlich verfahrensirrelevante Daten enthält. Enthält der Datenträger beweisrelevante Daten, kommt in Betracht, den Datenträger zu kopieren und auf der Kopie die ausgesonderten Daten (endgültig) zu löschen. Die Kopie verbleibt bei den Ermittlungsbehörden, und das Original wird an den Dateninhaber zurückgegeben.

Vernichtung irrelevanter Daten geboten

Erfolgte die vorläufige Sicherstellung durch eine Datenspiegelung oder die Anfertigung von Kopien einzelner Dateien bzw. Dateiordner, ist eine Rückgabe an den Inhaber obsolet, weil dieser die Originaldaten noch hat. Sinn der Rückgabe im Wortsinn ist es freilich nicht allein, dass der ursprüngliche Gewahrsamsinhaber seinen Gewahrsam an dem Papier bzw. dem Datenbestand zurückerlangt. Entscheidend ist vielmehr, dass gleichzeitig der Gewahrsam der Strafverfolgungsbehörde endet: Die Behörde darf nach Abschluss der Durchsicht und dem damit einhergehenden Abschluss der Durchsuchung keine Zugriffsmöglichkeit mehr auf die ausgesonderten Daten haben. Der mit dem Zugriff auf verfahrensirrelevante Daten und Unterlagen verbundene Eingriff in das Recht der informationellen Selbstbestimmung wird nämlich nur dadurch angemessen beschränkt, dass den Ermittlungsbehörden diese nicht länger als für die Dauer der Durchsicht zur Verfügung stehen. Behält die Strafverfolgungsbehörde die Daten, obwohl sie beweisirrelevant sind, läge darin eine unzulässige Vorratsdatenspeicherung. Dies ergibt sich jedenfalls für personenbezogene Daten bereits aus § 483 Abs. 1 StPO: Danach dürfen Strafverfolgungsbehörden personenbezogene Daten nur speichern, verändern und nutzen, soweit dies für Zwecke des konkreten[37] Strafverfahrens erforderlich ist. Beweisirrelevante Daten sind in diesem Sinne nicht mehr erforderlich, sodass eine weitere Speicherung rechtswidrig wäre. Ebenso wie gem. § 110 StPO durchsichtete und als irrelevant identifizierte Papiere dem Inhaber zurückgegeben werden, ohne dass Kopien asserviert werden, müssen von Strafverfolgungsbehörden zu Zwecken der Durchsicht gespeicherte Daten vernichtet werden, sobald ihre Beweisirrelevanz festgestellt ist.

Die Praxis sieht anders aus: Ermittlungsbehörden wenden gegen eine teilweise Löschung des vorläufig sichergestellten Datenbestandes bisweilen ein, dass es sich hierbei um einen „Eingriff in die Beweiskette" handele, der den Beweiswert mindere. Gegen diese Auffassung spricht schon, dass der auf einem Datenträger gespeicherte Datenbestand gerade nicht unteilbar der Beschlagnahme unterliegt, sondern auch hier zu prüfen ist, ob eine Aussonderung verfahrensirrelevanter Daten möglich und vertretbar ist. Zu Recht bemerkt das BVerfG, dass die entgegenstehende Auffassung die „von Verfassungs wegen gebotene Prüfung der Umstände des Einzelfalls" nicht zulässt.[38]

Insbesondere in Zollstrafverfahren wird von den Fahndungsbeamten zur Abwendung der Datenvernichtung zudem auf eine angebliche „Speicherpflicht" der Zollbehörden hingewiesen. Eine *Befugnis* (!) zur Speicherung existiert indes lediglich im Hinblick auf Daten „aus dem Strafverfahren" bzw. zur Erfüllung der zollfahndungsbehördlichen Aufgaben (§§ 17, 27 Zollfahndungsdienstgesetz). Als im Rahmen der Durchsicht beweisirrelevant qualifizierte Daten gehören nicht dazu. Eine außerstrafrechtliche Speicherpflicht oder auch nur -befugnis besteht insoweit also nicht.

---

[35] *BGH* NJW 1995, 3997.
[36] Vgl. KK-StPO/*Nack*, § 110 Rn. 4.
[37] Vgl. *Meyer-Goßner*, § 483 Rn. 2.
[38] *BVerfG* NJW 2005, 1917, 1923 in Ablehnung der gegenteiligen Auffassung des LG Hamburg.

2) Unmöglichkeit der Aussonderung bei der Verwendung sog. „Containerdateien"

Gelegentlich erweist sich die Aussonderung irrelevanter Daten durch selektive Löschung jedoch als technisch unmöglich, weil die von den Ermittlungsbehörden zur forensischen Sicherung verwendeten Computerprogramme eine derartige Funktion erst gar nicht vorsehen. Dies ist dann der Fall, wenn der gesamte gespiegelte Datenbestand in einer einzigen sog. „Containerdatei" abgespeichert wird. Diese ist einer nachträglichen Änderung (z. B. Entnahme nicht vom Beschlagnahmebeschluss erfasster Dateien) nicht zugänglich. Die Verwendung derartiger Programme und Containerdateien wird damit begründet, dass die mangelnde Eingriffsmöglichkeit in die Containerdatei den Beweiswert sichere.

Die Verwendung solcher Containerprogramme führt dazu, dass in der Praxis unter Berufung auf § 110 StPO eine größere Anzahl an Daten „faktisch beschlagnahmt" wird, als nach §§ 94, 98 StPO möglich wäre. Der Gegenstand der Beschlagnahme richtet sich in solchen Fällen nicht nach den in §§ 94, 98 StPO normierten Maßstäben, sondern nach technischen Möglichkeiten. Eine Kompensation dafür, dass im Rahmen der vorläufigen Sicherstellung auf die Durchsuchungsanordnung „überschießende" Datenbestände zugegriffen wird, findet nicht statt. § 110 StPO führt in diesen Fällen entgegen seiner Schutzfunktion zu einer Schlechterstellung des von einer umfassenden Datendurchsicht Betroffenen. Die Verwendung von Containerdateien stellt damit einen dauerhaften, rechtswidrigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung des Dateninhabers und solcher Personen dar, deren personenbezogene Daten sich im „überschießenden" Datenbestand befinden.

Verwendung von Containerdateien verhindert Datenrückgabe / -vernichtung

Bei Lichte betrachtet liegt in der Verwendung von Containerdateien erstellenden Programmen eine Umgehung der verfassungsgerichtlichen Rechtsprechung zur Beschränkung des umfassenden Informationszugriffs durch die Datendurchsicht gem. § 110 StPO. Die technische Unmöglichkeit, nicht verfahrensrelevante bzw. nicht vom Beschlagnahmebeschluss erfasste Daten auszusondern und dem hiervon Betroffenen zurückzugeben, führt in den meisten Fällen faktisch zu einer rechtswidrigen Sicherstellung des gesamten gespiegelten Datenbestandes. (Nichts Anderes gilt im Übrigen, wenn eine Aussonderung zwar technisch möglich ist, durch die Ermittlungsbehörden aber nicht durchgeführt wird.) Die Verwendung von Programmen zur Herstellung derartiger Container muss daher schon aus Rechtsgründen unterbleiben. Ansonsten bleibt nur ein Weg: Die als verfahrensrelevant identifizierten Dateien sind auszudrucken oder auf einen gesonderten Datenträger zu kopieren, um sie in dieser Form zu den Asservaten zu nehmen. Im Anschluss daran ist die Containerdatei zu vernichten.

Eine gelegentlich befürchtete Minderung des „Beweiswerts" durch Entnahme einzelner Dateien oder Ordner aus einer Ablagestruktur kann dadurch verhindert werden, dass im Rahmen der Datensicherung die Ordnerstruktur des gesicherten Laufwerks beibehalten wird, während Verfahrensirrelevantes aus diesen Ordnern gelöscht wird. Ggf. ist zu überlegen, die „leeren", weil verfahrensirrelevanten Ordner umzubenennen (z. B. in „XXX01", „XXX02" usw.). Die Löschungen sind in ein Löschprotokoll aufzunehmen, sodass das Vertrauen in die „Beweiskette" und damit im Beweiswert der verbliebenen Dateien fortbesteht. Alternativ könnte ein Screenshot der Ordnerstruktur im Explorer erfolgen oder der genaue Pfad dokumentiert werden. Zusammenfassend sind sämtliche Maßnahmen in Betracht zu ziehen, die eine Zuordnung der beweisrelevanten Datei zwar zulassen, dabei aber das Recht auf informationelle Selbstbestimmung nicht mehr tangieren als erforderlich und angemessen ist.

3) Beweisverwertungsverbot

Die Rechtsprechung hat sich bislang nicht durchringen können, bzgl. sichergestellter verfahrensirrelevanter Daten ein Beweisverwertungsverbot anzunehmen. Ob ein solches zum Schutz des Rechts auf informationelle Selbstbestimmung erforderlich ist, ist höchstrichterlich noch ungeklärt. Jedenfalls bei schwerwiegenden, bewussten oder willkürlichen Verfahrensverstößen, in denen die Beschränkung auf den Ermittlungszweck der Datenträgerbeschlagnahme planmäßig oder systematisch außer Acht gelassen wird, ist ein Beweisverwertungsverbot als Folge einer fehlerhaften Durchsuchung und Beschlagnahme von Datenträgern und der darauf vorhandenen Daten geboten.[39] Dies ist insbesondere dann der Fall,

[39] Vgl. *BVerfG* NJW 2005, 1917, 1923.

wenn eine generelle Anordnung besteht, grundsätzlich alle Daten mitzunehmen und „nichts liegen zu lassen". Erfolgt die Datensicherung dann auch noch in einer Containerdatei, dürfte kein Zweifel an der bewussten Umgehung der Zielrichtung des § 110 StPO bestehen. Da hier das Schutzinstrumentarium der §§ 52, 53, 97 und 160a StPO bewusst ignoriert wird, muss ein Verwertungsverbot die Folge sein.

4) Rechtsschutz

Soweit Zweifel an der Erforderlichkeit der Mitnahme von Daten bestehen, sind diese analog § 98 Abs. 2 Satz 2 StPO geltend zu machen. Da die Entscheidung über die vorläufige Sicherstellung der Staatsanwaltschaft bzw. ihren Ermittlungspersonen obliegt, ist ein Antrag auf richterliche Bestätigung dieser Anordnung der richtige Rechtsbehelf.[40] Dasselbe gilt, wenn die Unzumutbarkeit der Dauer der Durchsicht gerügt werden soll und eine Freigabe der vorläufig sichergestellten Unterlagen erstrebt wird.[41]

VI. Zusammenfassung

Bei der Durchsicht von Daten i. S. von § 110 StPO im Rahmen von Durchsuchungsmaßnahmen sind zusammenfassend folgende Maßgaben zu beachten:

Der Durchsicht von Daten gem. § 110 StPO hat eine Vorauswahl des zu durchsichtenden Datenbestandes vorauszugehen. Diese Vorauswahl hat sich am Inhalt des Durchsuchungsbeschlusses zu orientieren. Eine vorläufige Sicherstellung zu Zwecken der Durchsicht von Daten, die schon nicht beweisgeeignet für den im Durchsuchungsbeschluss genannten Vorwurf sind, ist nicht zulässig. Ebenso dürfen keine Daten vorläufig sichergestellt werden, die einem Beweiserhebungsverbot unterliegen. Die Voraussonderung zur Identifikation gem. § 110 StPO zu durchsichtender Daten darf und muss Zeit kosten. Die Spiegelung ganzer Datenträger oder Laufwerke zum Zwecke der späteren Aussonderung dürfte im Regelfall rechtswidrig, da nicht erforderlich sein.

Die im Anschluss stattfindende Durchsicht sollte im Regelfall in Anwesenheit des Dateninhabers erfolgen. So kann einem Missbrauch vorgebeugt werden und das Vertrauen des Betroffenen in die Durchsuchungsmaßnahme gestärkt werden. Außerdem werden durch die dadurch eintretende Beschleunigung des Verfahrens auch die Ermittlungspersonen selbst entlastet.

Eindeutig nicht verfahrensrelevante Daten sind zurückzugeben bzw. zu vernichten. Die Vernichtung entspricht der Rückgabe nicht beweisrelevanter Papiere nach der Durchsicht. Eine Verweigerung der Vernichtung unter Hinweis, die Beweiskette dürfe nicht unterbrochen werden, ist unzulässig. Dies gilt auch, wenn zur Datensicherung sog. Containerdateien verwendet werden, in die ein späterer Eingriff zu Zwecken der Aussortierung nicht möglich ist. Die willkürlich geschaffene Unmöglichkeit einer Aussonderung vorläufig sichergestellter Daten darf sich nicht zulasten des von der Durchsuchung Betroffenen bzw. des jeweils betroffenen Informationsträgers auswirken.

Jedenfalls in Fällen, in denen das Schutzinstrumentarium der §§ 52, 53, 97 und 160a StPO durch die vorläufige Sicherstellung von Daten ohne anschließende Aussonderung verfahrensirrelevanter Dateien ausgehebelt wird, ist ein Beweisverwertungsverbot hinsichtlich des „überschießenden" Datenbestandes zu verlangen.

---

[40] *LG Limburg*, Beschl. v. 15.02.2011 – 1 QS 20/11 = BeckRS 2011, 05150; *Meyer-Goßner*, StPO, § 110 Rn. 10.
[41] Vgl. *LG Frankfurt* NStZ 1997, 564 ff.