Univ.-Prof. Dr. Ingeborg Zerbes
Mag. Shirin Ghazanfari

Schenkenstraße 4
A-1010 Wien

T +43 1 4277 34661

ingeborg.zerbes@univie.ac.at
shirin.ghazanfari@univie.ac.at

Organisationsassistentin
Kathrin Kirschner, BA

T +43 1 4277 34660

kathrin.kirschner@univie.ac.at

Wien, am 21.11.2022

Stellungnahme

im Auftrag des Instituts für Anwaltsrecht der Universität Wien zum Thema der Sicherstellung und Auswertung von Daten und Datenträgern

I. Vorbemerkung: zur Unabhängigkeit von der politischen Brisanz des Themas

Die „Handybeschlagnahme“ – gemeint ist die Sicherstellung von Mobiltelefonen und anschließende Auswertung sämtlicher über diese verfügbaren Daten, insbesondere der Kommunikationsdaten – ist in Österreich in jüngerer Zeit mit politischen Skandalen verbunden. Hintergrund bilden die vor allem durch die WKStA sichergestellten Handys von hochrangigen Politikern und weiteren öffentlich exponierten Personen. Die umfassende Auswertung dieser Kommunikationsgeräte – vor kurzem wurde kolportiert, dass um die 300.000 Chatnachrichten auf dem Gerät einer einzigen Person ausgewertet werden – hat höchst brisante Kenntnisse über die Denkweise und Aktionen der betroffenen Personen in die Öffentlichkeit getragen und letzten Endes zu deren politischem Sturz geführt.

Die vorliegende Analyse ist keinesfalls als Stellungnahme zu diesen Geschehnissen zu verstehen: Sie bezieht sich auf eine bereits zuvor identifizierte Schieflage zulasten der Verteidigung, der kein rechtliches Gehör im Auswertungsprozess von fallweise enormen Datenmengen eingeräumt wird.

II. Ausgangspunkt

Ausgangspunkt ist, dass sich die Sicherstellungsbefugnisse nach der StPO ihrer vor dem Zeitalter von „Big Data“ und moderner Informationstechnologie ansetzenden Geschichte entsprechend auf sämtliche Gegenstände beziehen. Die Ermittlungsbehörden dürfen diese zur Verwendung als Beweis in ihre Verfügungsmacht bringen. Zur Entstehungszeit der Normen war freilich nicht absehbar, dass damit heute auch Datenträger aller Art wie etwa Mobiltelefone, Laptops, PCs, Tablets und unter Umständen sogar ganze Server erfasst sind: Sie werden als **Gegenstände** nach §§ 109 ff StPO sichergestellt und die durch sie zugänglichen Daten werden umfassend ausgelesen. Auch der auf Daten zugeschnittene § 111 Abs 2 StPO wurde zu einer Zeit konzipiert, in der die Masse, die Reichweite und die Qualität der dadurch verfügbaren Informationen noch nicht vorherzusehen waren.

Angesichts dessen sind „Handydaten“ – Chatverläufe, E-Mails, aus dem Internet heruntergeladene Daten, Fotos, Ortsfeststellungen, kurzum alle Daten, die bei der umfassenden Nutzung eines Smartphones anfallen – den Strafverfolgungsbehörden leicht durch Sicherstellung zugänglich. Die Voraussetzungen zur Ausübung dieser Befugnis sind äußerst niederschwellig angesetzt.

Wenn die Ermittlungsbehörden jedoch nicht auf den Datenträger des Betroffenen zugreifen können, sind ihnen die gleichen Daten nur durch spezifische, an den **Charakter der Daten als „Nachrichten und Informationen“** gebundene Ermittlungsmaßnahmen zugänglich: Rahmendaten einer Kommunikation durch Auskunft über Daten einer Nachrichtenübermittlung und Kommunikationsinhalte durch Nachrichtenüberwachung. Die zuletzt genannten Maßnahmen sind an anspruchsvolle rechtsstaatliche Grenzen gebunden. Ein solcher Unterschied zwischen (Kommunikations-) Daten, die im Zuge einer Sicherstellung des Mobiltelefons verfügbar werden, und der Sache nach gleichen Daten, die die Behörde durch Nachrichtenüberwachung an sich bringt, ist historisch gewachsen, in der heutigen Zeit aber sachlich nicht mehr gerechtfertigt.

III. Skizze der geltenden Rechtslage

1. Zugang zu Daten durch Sicherstellung

1.1. Unumstrittener Bereich: Auslesen offline

1.1.1. Bindung an die Sicherstellung von Datenträgern

Mit § 111 Abs 2 wird die Sicherstellung geregelt, die den Strafverfolgungsbehörden den Zugang zu digital gespeicherten Daten („Informationen") verschaffen soll: „Sollen auf Datenträgern gespeicherte Informationen sichergestellt werden", lautet die Einleitung. Die Formulierung führt insofern zu Widersprüchen, als sie nicht der hier relevanten[1] Definition der Sicherstellung als „Begründung der Verfügungsmacht über Gegenstände" (§ 109 Z 1 lit a) entspricht: „Informationen" – „immaterielle Objekte", so die Materialien[2] – sind ja gerade keine Gegenstände. Sie können daher nicht als solche sichergestellt werden, sondern nur durch Sicherstellung eines Datenträgers, zB einer CD, einer DVD, eines USB-Sticks, einer Festplatte oder auch eines PCs, Laptops, Tablets oder Handys. Anders ausgedrückt: Ohne die Sicherstellung derartiger Hardware, die den Zugang zu Informationen ermöglicht, erlauben die §§ 109 Z 1, 110 ff keinen Zugang zu digital gespeicherten Informationen. Die Sicherstellung der Hardware kann auch nur vorübergehend erfolgen, etwa, indem die Ermittlungsorgane den Rechner des Betroffenen vor Ort auslesen.

Es gibt dementsprechend nur *einen* Zeitpunkt der Sicherstellung: den Zeitpunkt der Sicherstellung des Speichermediums – danach erfolgt keine Sicherstellung mehr, sondern (nur mehr) die Auslesung dieses Speichermediums (dazu sogleich 1.1.2.), obwohl dieser Vorgang bislang nicht ausdrücklich gesetzlich geregelt ist. Dass § 111 Abs 2 die Sicherstellung missverständlich direkt auf die Daten bezieht und damit eigentlich auf den Auslesevorgang, liegt wohl daran, dass dieser das eigentliche virtuelle Pendant zur „Verfügungsmacht über Gegenstände" ist, auf die § 109 beschränkt ist.

1.1.2. Auslesen der am Datenträger selbst gespeicherten Daten

Unumstritten ist, dass die Befugnis zur Sicherstellung eines Datenträgers auch erfasst, sich die auf ihm selbst gespeicherten Daten zugänglich zu machen und für das Strafverfahren zu nutzen: die Daten anzusehen, sie vollständig zu kopieren oder Ton- und Bildaufnahmen von ihnen anzufertigen (zB eine Abbildung der aktuell am Bildschirm sichtbaren Inhalte), sie vor Zugriffen Dritter zu sichern, sie auszudrucken und sie auszuwerten. Insofern lassen sie sich durchaus mit in einer Kiste aufbewahrten Unterlagen vergleichen. So wie die Unterlagen in einer solchen Kiste angesehen und ausgewertet werden dürfen, darf auch ein Datenträger nicht nur von außen betrachtet, sondern darf auch auf seinen Inhalt – das sind die auf ihm gespeicherten Daten – zugegriffen werden.

Das gilt auch für Nachrichten wie Mails, *WhatsApp*-Nachrichten, SMS etc. Denn wenn diese auf einem Datenträger gespeichert sind, wurden sie ja bereits empfangen, noch nicht abgeschickt oder nach dem Abschicken dort abgespeichert. Ihre Übertragung ist somit bereits abgeschlossen oder noch gar nicht eingeleitet. Sie sind zwar zweifellos „Nachrichten" vor oder nach einem Übertragungsvorgang iSd § 134 Z 2 und 3, ihre Auslesung nach einer

[1] Das Verbot der Herausgabe iS der lit b spielt für Informationen eine untergeordnete Rolle, weil sie vor allem als Beweismittel (ausgedruckt) zum Akt genommen werden sollen.
[2] EBRV 25 BlgNR 22 zu § 111 Abs 2.

offen durchgeführten Sicherstellung des betreffenden Speichermediums beim Beschuldigten ist allerdings keine Überwachung iS von § 135 Abs 2 und 3 .[3]

Selbst passwortgeschützte Daten dürfen zugänglich gemacht werden. Sind den Ermittlungsbehörden die Passwörter nicht bekannt, ist derjenige, der sie mutmaßlich kennt, dazu zu vernehmen. Ist er ein Zeuge, muss er sie preisgeben, bei Verweigerung droht ihm eine Beugestrafe (§ 93 Abs 2),[4] der Beschuldigte ist als Schweigeberechtigter freilich von Beugemitteln befreit. Erhalten die Ermittlungsorgane die Zugangsdaten nicht, können sie Cracking-Software einsetzen, so wie sie eine sichergestellte versperrte Kiste aufbrechen dürften. Haben sie damit Erfolg, gelten dieselben Grenzen wie für ausgedruckte Unterlagen oder sonstige Gegenstände: Wenn keine auf den Inhalt bezogenen Sicherstellungsverbote bestehen, wie etwa für Anwaltsdaten, dürfen sie ausgewertet und zum Akt genommen werden.

1.2. Graubereich: externe Speicherplätze

Anders als körperliche Gefäße bieten Handys, Computer udgl nicht nur den eigenen (Daten-) Inhalt: Die durch sie zugänglichen Daten liegen zu einem großen Teil auf externen Servern, zB in einer Cloud, auf den Servern von *Facebook*, *Amazon*, Banken, Betreibern von Kommunikationsdiensten etc, auf den Rechnern von Übersetzungsdiensten oder sonstigen IT-Diensten. Denn fast jeder Nutzer bedient sich mittlerweile externer Speicherplätze aller Art; so spart er einerseits Speicherplatz auf dem einzelnen Kommunikationsgerät, andererseits kann er ausgelagerte Texte, Bilder, Videos, Flugtickets, Bankdaten, Postings, „Likes" etc von beliebigen Standorten und Geräten aus abrufen und verändern.

Ermittlungsbehörden, die ein Kommunikationsgerät sichergestellt haben, haben jedenfalls keine „körperliche Verfügungsmacht über [jene] Gegenstände", auf die der Nutzer Daten auslagert.[5] Sollen „auf Datenträgern gespeicherte Informationen sichergestellt werden" verpflichtet § 111 Abs 2 jeden, den Ermittlungsbehörden bloß „Zugang zu diesen Informationen zu gewähren". Je nach Auslegung dieser Bestimmung ist umstritten, ob die Regeln der Sicherstellung auch erfassen, diese – vom sichergestellten Gegenstand geographisch weit entfernten – Speicherplätze auszulesen und auszuwerten.

1.2.1. Enger Zugang in Abgrenzung zur Nachrichtenüberwachung

§ 111 Abs 2 eng zu verstehen und die Sicherstellung allein auf die am sichergestellten Gerät selbst gespeicherten Daten zu beziehen, entspricht einerseits der expliziten **gegenständlichen Bindung** der Sicherstellung. Denn körperliche Verfügungsmacht wird nur über den *Datenträger* begründet; damit liegt nahe, dass nur dieser das Objekt der Auswertung ist, nicht aber die über ihn bloß *vermittelten* Daten.[6]

Darüber hinaus lässt sich auf diese Weise eine klare Grenze zu jenen Ermittlungsmaßnahmen ziehen, die auf Datenübermittlungen zugeschnitten sind, das sind die Auskunft über Daten einer Nachrichtenübermittlung (§ 134 Z 2) und die (inhaltliche) Überwachung von Nachrichten (§ 134 Z 3). Diese Ermittlungsmaßnahmen erlauben mittlerweile den Zugriff auf sämtliche Daten, die – verallgemeinert ausgedrückt – bei einer Datenübermittlung unter

---

[3] *Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO § 134 Rz 53; *Zerbes,* Einsatz von Spionagesoftware bei Sicherstellung und Durchsuchung, in *Lewisch* (Hrsg), Wirtschaftsstrafrecht und Organverantwortlichkeit, Jahrbuch 2014, 199 (203); aus Deutschland: BVerfG, 16. 6. 2009, 2 BVR 902/06, NJW 2009, 2431.

[4] *Hinterhofer/Oshidari,* System des österreichischen Strafverfahrens (2017) Rz 7.197.

[5] *Wicker,* Durchsuchung in der Cloud. Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden, MMR 2013, 765 (766).

[6] *Reindl-Krauskopf/Salimi/Stricker,* IT-Strafrecht (2018) Rz 5.11.

Nutzung eines öffentlichen[7] Übertragungsdienstes („Kommunikationsnetz … oder Dienst der Informationsgesellschaft", § 134 Z 3) gespeichert werden. Die Nutzung externer Speicherplätze erfolgt nämlich nicht anders als durch eine solche Übermittlung. Inhalte, die dort von einer natürlichen Person hinterlassen werden, sind nach § 134 Z 3 entweder „Nachrichten" – dann, wenn sie wie zB E-Mails an einen bestimmten Adressatenkreis gerichtet sind („Kommunikation im sozialen Sinn"[8]) –, oder, eingefügt durch das StPRÄG II 2018[9], (sonstige) „Informationen", die bei einem Kontakt zu einem externen Rechner entstehen, etwa beim Aufruf einer Webseite oder beim Abspeichern von Dokumenten in einer Cloud („Kommunikation im technischen Sinn"[10]). Beides ist den Ermittlungsbehörden unter den Voraussetzungen des § 135 Abs 3 durch eine „Überwachung von Nachrichten" zugänglich. Werden nicht die Inhalte, sondern nur formale Rahmendaten einer solchen Übertragung – „Verkehrsdaten …, Zugangsdaten … und Standortdaten" – ermittelt, handelt es sich um eine „Auskunft über Daten einer Nachrichtenübermittlung" nach § 134 Z 2, die nach § 135 Abs 2 zulässig ist.

Diese ursprünglich aus der Telefonüberwachung entstandenen Methoden sind Eingriffe in das Fernmeldegeheimnis und allein deswegen im Vergleich zur Sicherstellung an deutlich engere Voraussetzungen geknüpft (zu diesen unten IV. 4.); das gilt insbesondere für die inhaltliche Überwachung von Nachrichten. Geht man davon aus, dass sie *exklusiv* für von einem Kommunikationsgerät aus übertragene Daten gelten, ergibt sich eine klare und systematisch einwandfreie Unterscheidung: Die §§ 109 ff decken nur eine Untersuchung des sichergestellten Mobiltelefons selbst, während die über dieses möglichen Einblicke in externe Speichermedien an die höheren Voraussetzungen der §§ 134, 135 gebunden sind.[11]

1.2.2. Weiter Zugang

Die Materialien gehen offenbar davon aus, dass die Befugnis zur Sicherstellung eines Mobiltelefons, eines Laptops oder eines sonstigen internetfähigen Geräts auch erlaubt, in die vom sichergestellten Gerät aus **bloß erreichbaren Datenbestände** einzudringen.[12] Sie erstrecken damit die Untersuchung des Geräts auf Gegenstände, die räumlich weit entfernt sind und als solche gar nicht sichergestellt wurden. Die Anordnung, dass „jedermann Zugang zu … [gespeicherten] Informationen zu gewähren" hat (§ 111 Abs 2), sei nämlich auch dann anwendbar, wenn „auf dem eigentlich durchsuchten Rechner keine relevanten Datenbestände auffindbar sind, weil diese auf einem [...] Datenserver gespeichert sind"[13].

Dahinter steht, dass bei vielen modernen Anwendungen zunehmend die Grenzen zwischen lokalen und externen Daten verwischt werden, zumindest aus dem Blickwinkel des Nutzers. Oft verbirgt die Benutzungsoberfläche sogar gezielt, wo die Daten abgelegt werden. So wird dem Nutzer gar nicht mehr bewusst, ob ein Foto oder sonstiges Dokument nun am Mobiltelefon verbleibt oder – zB um Speicherplatz zu sparen – in eine Cloud verschoben wird, zumal Synchronisierungsprozesse häufig automatisch ablaufen. Insofern fühlen sich

---

[7] *Reindl-Krauskopf/Salimi/Stricker,* IT-Strafrecht (2018) Rz 5.103.
[8] *Reindl-Krauskopf/Salimi/Stricker,* IT-Strafrecht (2018) Rz 5.102.
[9] BGBl I 2018/27.
[10] *Reindl-Krauskopf/Salimi/Stricker,* IT-Strafrecht (2018) Rz 5.102.
[11] *Reindl-Krauskopf/Salimi/Stricker,* IT-Strafrecht (2018) Rz 5.11.
[12] In Deutschland wird dies mit BVerfG, 16.09.2009, 2 BvR 902/06, BVerfGE 124, 43, für zulässig angesehen, wobei der Zugriff an Offenheit gebunden wurde (Rn 75 der Entscheidung); *Beulke/Meininghaus,* Der Staatsanwalt als Datenreisender, in FS Widmaier 2008, 63 (78); *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 111 Rz 14 ff;
[13] EBRV 25 BlgNR 22. GP zu § 111.

heute „das Endgerät des Nutzers und die Cloud [wie] ein einheitliches informationstechnisches System“[14] an.[15]

Problematisch ist an diesem breiten Verständnis der Sicherstellungsbefugnis nicht nur, dass der Gegenstandsbezug der Sicherstellung aufgegeben wird, sondern auch, dass damit für übermittelte „Nachrichten und Informationen“ iS von § 134 Z 3 – wie erwähnt (oben 1.2.1.) sind auch ausgelagerte Daten der Sache nach nichts anderes – den strengeren Voraussetzungen ausgewichen wird, die für eine Nachrichtenüberwachung (§ 135 Abs 3) und Nachrichtendatenabfrage (§ 135 Abs 2) vorgesehen sind. Auch lässt sich etwa nach der Sicherstellung des Mobiltelefons eines Nichtbeschuldigten auch dessen Verhalten im öffentlich angebotenen Kommunikationsnetz ermitteln – dessen Kommunikation mit anderen, die von diesem aufgerufenen Webseiten, die von ihm getätigten oder „gelikten“ Postings, dessen Dokumente in einer Cloud etc –, was nach § 135 Abs 2 und 3 grundsätzlich ausgeschlossen sein soll.

2. Zugang zu Daten durch Nachrichtenüberwachung

2.1. Charakterisierung durch den Übertragungsvorgang

Nach § 134 Z 3 bedeutet Nachrichtenüberwachung die Überwachung solcher „Nachrichten und Informationen …, die von einer natürlichen Person über ein Kommunikationsnetz (§ 4 Z 1 TKG …) oder einen Dienst der Informationsgesellschaft (§ 1 Abs 1 Z 1 Notifikationsgesetz) gesendet, übermittelt oder empfangen werden.“ Verkürzt ausgedrückt geht es damit um sämtliche Daten, die nicht nur auf einem Rechner oder innerhalb eines abgegrenzten Rechnerverbundes gespeichert werden, sondern in einem **öffentlichen[16] Netz** durch elektromagnetische Signale **übertragen** werden. Dazu gehört sämtliche **„Kommunikation im sozialen Sinn“[17]** über SMS, MMS, E-Mails, Videonachrichten, akustische Telefongespräche, die nicht nur über ein Haustelefon geführt werden, Postings oder sonstige Kommentare auf Sozialen Medien etc.

Durch die Breite des Begriffs der „Information“ erfasst die Nachrichtenüberwachung mittlerweile aber auch die **„Kommunikation im [bloß] technischen Sinn“[18]** (vgl oben 1.2.1.) und damit die Daten, die beim Anklicken einer Webseite gespeichert werden, ebenso jene, die der betreffende Nutzer auf einen externen Speicherplatz wie eine Cloud udgl verschiebt – denn auch dafür wird ein öffentliches Netz bedient. Schließlich – arg „Dienst der Informationsgesellschaft“ – umfasst die Befugnis zur Nachrichtenüberwachung auch den Zugang zu Daten, die im „Fernabsatz“ (§ 1 Abs 1 Z 1 Notifikationsgesetz) von Waren oder Dienstleistungen zustande kommen, wie etwa die Daten aus der Abfrage einer Datenbank, die online-Bestellungen oder das Streaming oder Herunterladen von Audio- oder Videodateien.

2.2. Überwachung

Im Unterschied zur Sicherstellung erfolgt die an Übertragungsvorgänge gebundene Nachrichtenüberwachung **geheim.** Ihre Durchführung kann auch ohne Innehabung des benutz-

---

[14] *Grözinger*, Heimliche Zugriffe auf die Cloud – Befugnis zur Plünderung eines unermesslichen Datenschatzes? StV 2019, 406 (410 f).

[15] *Wicker,* Durchsuchung in der Cloud. Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden, MMR 2013, 765 (767), zieht daher eine von der „virtuellen“ Verfügungsgewalt über eine Cloud abgeleitete Parallele zum körperlichen Gewahrsamsbegriff.

[16] *Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO § 134 Rz 43.

[17] *Reindl-Krauskopf/Salimi/Stricker,* IT-Strafrecht (2018) Rz 5.102.

[18] *Reindl-Krauskopf/Salimi/Stricker,* IT-Strafrecht (2018) Rz 5.102.

ten Kommunikationsgeräts selbst erfolgen: Der Übertragungsvorgang ermöglicht, auch außerhalb des entsprechenden Geräts auf Nachrichten bzw Informationen zuzugreifen. Dieser Zugriff kann in Echtzeit erfolgen – insofern tatsächlich während eines Übertragungsvorganges –, aber auch danach, wenn die Nachricht zwar bereits zugestellt wurde, jedoch weiterhin auf einem der Übertragung dienenden Server verbleibt. Auch noch nicht abgeschickte Nachrichten können überwacht werden, wenn sie bereits – zur Vorbereitung der Versendung – auf dem der Übertragung dienenden Server abgelegt wurden, beispielsweise in den Entwurfsordner eines E-Mail-Programms im Online-Modus. In allen diesen Fällen findet oder fand nämlich eine Übertragung der Nachricht auf den betreffenden Server und damit „über ein Kommunikationsnetz" statt. Dementsprechend erstrecken sich die Befugnisse nach § 135 Abs 3 auf ein (Kommunikations-) Gerät, das „Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird".

Eine Überwachung zeichnet sich außerdem durch eine gewisse Dynamik aus: Sie erstreckt sich über eine bestimmte Zeitspanne. Eine Sicherstellung führt demgegenüber insofern zu einer Momentaufnahme, als das sichergestellte (Kommunikations-) Gerät einmalig untersucht und ausgewertet wird.

3. Schutz der Berufsgeheimnisse, insbesondere im Zusammenhang mit Rechtsberatung

3.1. Konzept

Vertreter bestimmter Berufe – sog Berufsgeheimnisträger – dürfen im Strafverfahren die Zeugenaussage zu bestimmten Themen verweigern (§ 157 Abs 1 Z 2-4):

- Verteidiger, Rechtsanwälte, Patentanwälte, Verfahrensanwälte in Untersuchungsausschüssen, Notare und Wirtschaftstreuhänder (§ 157 Abs 1 Z 2),
- Psychiater, Psychotherapeuten, Psychologen, Bewährungshelfer, eingetragene Mediatoren, Mitarbeiter anerkannter Einrichtungen zur psychosozialen Betreuung (Z 3)
- Medieninhaber, Herausgeber, Medienmitarbeiter und sonstige Arbeitnehmer eines Medienunternehmens oder Mediendienstes (Z 4).

Angesichts dessen, dass gerade im Zusammenhang mit **Rechtsberatung** typischerweise viel beweisrelevantes Material zustande kommt, werden die folgenden Ausführungen auf die als erstes genannte Gruppe – Verteidiger, Rechtsanwälte usw (§ 157 Abs 1 Z 2) – zugespitzt.

Jede **Umgehung** des berufsbedingten Aussageverweigerungsrechts ist mit **Nichtigkeit** bedroht (§ 157 Abs 2). Damit ist einerseits insbesondere verboten, an das berufliche Wissen der Verteidiger, Rechtsanwälte usw durch Vernehmung ihrer Hilfskräfte (für die Beratung beigezogene Dolmetscher, Kanzleiangestellte oder die EDV-Fachleute etc) oder der bei ihnen zur Ausbildung beschäftigten Personen (zB Rechtsanwaltsanwärter oder Praktikanten) heranzukommen[19]. Zum anderen dürfen keine Unterlagen oder auf Datenträgern gespeicherte Informationen sichergestellt oder beschlagnahmt werden, die derartiges Wissen abbilden. Solange kein Fall vorliegt, in dem der Berufsgeheimnisträger selbst dringend verdächtig ist (§ 144 Abs 3), darf außerdem *keine* Ermittlungsmaßnahme oder Beweisaufnahme – kein Eingriff des 8. Hauptstücks der StPO, §§ 109 ff – angeordnet oder durchgeführt werden, die eine Umgehung des berufsbedingten Aussageverweigerungsrechts zur Folge hat (§ 144 Abs 2).

[19] *Kirchbacher/Keglevic* in *Fuchs/Ratz,* WK StPO § 157 Rz 11 und Rz 32/1;

Zweck des Aussageverweigerungsrechts samt Umgehungsverbot ist der in einem Rechtsstaat unentbehrliche Schutz des Vertrauens der betreffenden Mandanten in die Diskretion ihrer Ratgeber: Jeder soll Rechtsberatung im weitesten Sinn in Anspruch nehmen können, ohne davon ausgehen zu müssen, damit in einem Strafverfahren Beweise gegen sich selbst zu schaffen.[20] Mittelbar ist damit die Selbstbelastungsfreiheit realisiert.

3.2. Sicherstellung von Datenträgern als Umgehungsmethode

Für das gegenständliche Thema, den Zugriff auf Datenträger, interessiert freilich das Verbot, das Recht von Berufsgeheimnisträgern auf Aussageverweigerung durch andere Ermittlungsmaßnahmen zu umgehen: Wie weitgehend und durch welche Abläufe sind Datenträger, die Anwaltsgeheimnisse udgl enthalten können, vor Sicherstellung geschützt?

Ausgangspunkt ist, dass das Umgehungsverbot des § 157 Abs 2 die **Sicherstellung** ausdrücklich als **mögliche Umgehungsmethode** erwähnt und sich dabei nicht nur auf analoge schriftliche Unterlagen (wie etwa Akten, manuelle schriftliche Aufzeichnungen von Besprechungen oder Übersetzungsprotokolle), sondern auch auf elektronische Datenträger bezieht, auf denen sich vertrauliche Informationen befinden (zB USB-Sticks, externe Festplatten, Server, Laptops, Mobiltelefone).

3.3. Geschützte Gewahrsamsverhältnisse

3.3.1. Datenträger im Gewahrsam des Berufsgeheimnisträgers

Jedenfalls ein Verstoß gegen das Umgehungsverbot liegt vor, wenn die Datenträger, die Berufsgeheimnisse preisgeben – etwa das beruflich genutzte Handy –, gegen den Willen[21] des Berufsgeheimnisträgers bei diesem selbst sichergestellt werden. Dabei ist unerheblich, ob die entsprechenden (Kommunikations-) Geräte in den Kanzleiräumen oder an der Privatadresse aufgefunden werden: In beiden Fällen befinden sie sich in der Verfügungsmacht des Berufsgeheimnisträgers, wo sie vor Sicherstellung geschützt sind.[22]

3.3.2. Datenträger im Gewahrsam von Hilfskräften und in Ausbildung stehenden Personen

Auch Datenträger, die sich in der Verfügungsmacht einer Hilfskraft eines Berufsgeheimnisträgers oder bei Personen, die bei diesem ausgebildet werden, befinden, dürfen nicht sichergestellt werden: So, wie ihre Vernehmung eine mit Nichtigkeit bedrohte Umgehung ist (explizit genannt in § 157 Abs 2), muss es auch der Zugriff auf Sachbeweise aus ihrer Hand sein. Das dürfte unstrittig sein[23] und gilt auch dann, wenn Hilfskräfte das geschützte Material den Strafverfolgungsbehörden freiwillig aushändigen. Ihnen kommt kein eigenes Schweigerecht zu, sie üben vielmehr das Schweigerecht des Berufsgeheimnisträgers aus, bei dem oder für den sie arbeiten, darauf können sie nicht wirksam verzichten.

---

[20] *Zerbes,* Zugriff auf Beweise zwischen Effizienz und Rechtsschutz, in *Lewisch* (Hrsg), Wirtschaftsstrafrecht und Organverantwortlichkeit, Jahrbuch 2012, 105 (108).

[21] *Müller*, Verwertung im Gewahrsam Dritter befindlicher Anwaltsunterlagen im Strafverfahren?, RZ 2015, 250 (252); *Zerbes*, Anwaltsgeheimnis: Wirkung und Fernwirkung des Umgehungsverbots, ÖJZ 2016/23, 159 (160).

[22] OLG Wien 17 Bs 27/18x, JSt-Slg 2019/3.

[23] OLG Wien 18 Bs 33/16h, JSt-Slg 2016/47; *Müller,* Verwertung im Gewahrsam Dritter befindlicher Anwaltsunterlagen im Strafverfahren?, RZ 2015, 250 (253); *Stricker,* Das Umgehungsverbot (§ 157 Abs 2 StPO) nach dem StPRÄG 2016 I, ÖJZ 2018/67, 498 (500 f); *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO Vor 110-115 Rz 28/1; *Zerbes*, Anwaltsgeheimnis: Wirkung und Fernwirkung des Umgehungsverbots, ÖJZ 2016/23, 159 (162).

Unstrittig ist auch, dass der Begriff „Hilfskraft“ weit auszulegen ist: Es ist „jede Person …, an die berufsbedingt notwendig oder typisch Unterlagen weitergegeben werden, unabhängig davon, ob es sich dabei um einen Mitarbeiter des Rechtsanwalts oder eine sonstige externe Hilfskraft (Bank, Sachverständiger etc) handelt.“[24] Dazu gehören auch externe Experten oder etwa beigezogene Dolmetscher und IT-Spezialisten.

3.3.3. Datenträger im Gewahrsam Beschuldigter

Veranlasst durch die EU-RL zum Rechtsbeistand[25], hat das StPRÄG I[26] klargestellt, dass sich das Sicherstellungsverbot auch auf Beratungsdokumente bezieht, die der Beschuldigte innehat. In diesem Sinn wurde das Umgehungsverbot nach § 157 Abs 2 um solche „Unterlagen und Informationen“ in der Verfügungsmacht eines Beschuldigten ergänzt,

- die „zum Zwecke der Beratung oder Verteidigung des Beschuldigten“ durch einen Verteidiger, einen Rechtsanwalt oder sonstigen Parteienvertreter

- und entweder von dem Verteidiger, dem Rechtsanwalt oder dem sonstigen Parteienvertreter oder vom Beschuldigten selbst – etwa zur Vorbereitung des Beratungsgesprächs

erstellt wurden.

Letztere, die vom Beschuldigten selbst verfassten Dokumente, sind bei diesem allerdings nur geschützt, soweit sie tatsächlich ein anwaltliches Aussageverweigerungsrecht zum Ausdruck bringen. Sie dürfen daher sichergestellt werden, solange sie oder ihr Inhalt noch keinem Berufsgeheimnisträger übermittelt wurden.[27]

Zur Verdeutlichung mögen folgende Szenarien dienen:

- Der Beschuldigte hat noch keinen Anwalt beauftragt. Zum Zweck seiner Verteidigung hat er Dateien erstellt, auf deren Basis er mit einem Anwalt sprechen möchte. – Mangels Mandat gibt es noch kein Aussagverweigerungsrecht und folglich kein Umgehungsverbot: Die Datenträger dürfen sichergestellt werden.
- Der Beschuldigte hat zum Zweck seiner Verteidigung Dateien erstellt, weil er sich auf deren Basis selbst verteidigen möchte. – Es besteht kein Berufsgeheimnis, daher kann auch kein solches umgangen werden; es liegt daher kein Anwendungsfall des § 157 Abs 2 vor.
- Der Beschuldigte hat vertrauliche Informationen mit einem Wirtschaftstreuhänder geteilt, bei dieser Besprechung hat er Notizen verfasst. Diese Notizen will er nunmehr einem Anwalt überreichen, mit dem zu diesem Zeitpunkt noch kein Mandatsverhältnis besteht. – Eine Sicherstellung dieser Unterlagen beim Beschuldigten ist unzulässig, da sie das Aussageverweigerungsrecht zwar nicht des Anwalts (dessen Berufsgeheimnis ist noch nicht entstanden), aber das des Wirtschaftstreuhänders umgehen würde.
- Der Beschuldigte hat einen Anwalt beauftragt. Er macht sich Notizen über Angelegenheiten, die er noch nicht mit dem Anwalt besprochen hat, die er im Zuge des nächsten Beratungsgesprächs aber einbringen möchte. – Auch in diesem Fall wäre die Sicherstellung noch keine Umgehung, denn die betreffenden Inhalte sind dem Anwalt noch gar nicht bekannt und folglich nicht Gegenstand seines Verschwiegenheitsrechts.

---

[24] OLG Wien 18 Bs 33/16h, JSt-Slg 2016/47.
[25] Richtlinie 2013/48/EU, ABl 2013 Nr. L 294/1 vom 29. 6. 2013.
[26] BGBl I 2016/26.
[27] *Stricker*, Das Umgehungsverbot (§ 157 Abs 2 StPO) nach dem StPRÄG 2016 I, ÖJZ 2018/67, 498 (501 f);

- Das Mobiltelefon des Beschuldigten soll sichergestellt werden. Er weist darauf hin, dass sich in seinem Mailprogramm auch die Korrespondenz mit seinem Verteidiger befindet. – Zu dieser Konstellation unten 3.4.2.

3.3.4. Datenträger im Gewahrsam Dritter

Soweit ersichtlich tendiert die Judikatur[28] mittlerweile dazu, Gegenstände – hier interessieren Datenträger –, die ohne Zutun der Strafverfolgungsbehörden die Machtsphäre des Berufsgeheimnisträgers verlassen haben (und sich auch nicht beim Beschuldigten befinden), der Sicherstellung preiszugeben: Eine solche sei keine Umgehung des Aussageverweigerungsrechts iS des § 157 Abs 2 StPO. Dabei wird nicht differenziert, ob der Berufsgeheimnisträger die Unterlagen in eigener Verantwortung an einen Dritten gegeben hat, oder ob diese gegen seinen Willen von Mitarbeitern „geleakt", gestohlen oder „gehackt" wurden.

Dadurch kommt allerdings im Zusammenhang mit dem Verbot, sich zur Umgehung des Aussageverweigerungsrechts an Hilfspersonen zu wenden, ein Widerspruch zustande: Wenn eine Sicherstellung bei diesen eine unzulässige Umgehung ist – insofern besteht Einigkeit (siehe oben 3.3.2.) –, dann muss das auch dann gelten, wenn Hilfskräfte die einschlägigen Datenträger den Strafverfolgungsbehörden durch Mittelspersonen zuspielen. Solche Mittelspersonen stehen zwar außerhalb der Einflusssphäre des betroffenen Rechtsberaters; übernehmen die Strafverfolgungsbehörden von ihnen jedoch vertrauliches Material, dann lassen sie letzten Endes doch Hilfspersonen über das Aussageverweigerungsrecht disponieren. Dies steht allerdings ausschließlich dem Berufsgeheimnisträger selbst zu. Ein überwiegender Teil der Literatur[29] und zumindest das OLG Linz[30] erstrecken den Schutz vor Sicherstellung daher auch auf Unterlagen, die Hilfskräfte an Dritte weitergegeben haben.

3.4. Das Recht auf Widerspruch, Versiegelung und gerichtliche Durchsicht

3.4.1. Konzept

Das Verbot, ein berufsbedingtes Aussageverweigerungsrecht durch Zugriff auf Unterlagen zu umgehen (§ 157 Abs 2), ist nach § 112 durch das Recht des Betroffenen geschützt, der Sicherstellung unter Berufung auf ein solches Aussageverweigerungsrecht zu **widersprechen.** Dieser erwirkt damit eine **Versiegelung** der betreffenden Datenträger, die in der Folge bei Gericht hinterlegt und einem gerichtlichen Sichtungsverfahren vorbehalten werden. Damit soll ein sofortiger Einblick der Ermittlungsorgane in berufsgeheime Informationen vermieden werden und deren Aussortierung dem – in die Untersuchung nicht involvierten – Haft- und Rechtsschutzrichter vorbehalten werden. Nur die vom Gericht als nicht berufsgeheim freigegebenen Unterlagen kommen in den Akt, als berufsgeheim geschützte

[28] OLG Graz 13.08.2019, 1 Bs 32/19v; OLG Wien 12.09.2014, 22 Bs 133/14w; OLG Wien 18 Bs 33/16h, JSt-Slg 2016/47; ebenso *Müller*, Verwertung im Gewahrsam Dritter befindlicher Anwaltsunterlagen im Strafverfahren? RZ 2015, 250 (252 f).

[29] *Ghazanfari,* Sicherstellung von Mobiltelefonen und Berufsgeheimnisschutz, in *Lewisch* (Hrsg), Wirtschaftsstrafrecht und Organverantwortlichkeit, Jahrbuch 2022 (erscheint im Herbst 2022); *Kollmann/Moser,* Sicherstellung von Verteidigungsunterlagen, ZWF 2016, 57 (58 f); *Öner,* Die rechtsanwaltliche Verschwiegenheit im Verfassungs- und im Strafrecht, ÖJZ 2020/58, 448 (451); *Stricker,* Der Berufsgeheimnisträger als Zeuge, in *BMJ* (Hrsg), 42. Ottensteiner Fortbildungsseminar (2015) 54 ff; *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO Vor §§ 110-115 Rz 32 f; *Zerbes,* Hotspot Anwaltsgeheimnis, in *Lewisch* (Hrsg), Wirtschaftsstrafrecht und Organverantwortlichkeit, Jahrbuch 2016, 155 (161 ff); *Zerbes*, Anwaltsgeheimnis: Wirkung und Fernwirkung des Umgehungsverbots, ÖJZ 2016/23, 159 (162 f).

[30] OLG Linz 7 Bs 188/15v, ÖJZ 2016/23 (*Zerbes*).

Unterlagen werden zurückgegeben, ohne dass die Staatsanwaltschaft Zugang zu ihrem Inhalt hat.

Zwischen Versiegelung und gerichtlicher Sichtung ist ein Verfahren zur Konkretisierung vorgesehen: Der betroffene Berufsgeheimnisträger ist insofern eingebunden, als er dazu aufgefordert wird, „jene Teile der Aufzeichnungen oder Datenträger **konkret zu bezeichnen**, deren Offenlegung eine Umgehung seiner Verschwiegenheit bedeuten würde“ (§ 112 Abs 2). Diese Vorgangsweise ist bei der Sicherstellung elektronischer Datenträger unumgänglich: In komplexeren Verfahren, in denen nicht nur einzelne analoge Aktenordner, sondern etwa sämtliche Geschäftsunterlagen und EDV-Anlagen – von Mobiltelefonen bis zu ganzen Servern – sichergestellt werden, gelangt einerseits typischerweise eine unüberschaubare Menge an Daten in die Hände der Strafverfolgungsbehörden. Die Materialien sprechen von „Datensätzen im Bereich von mehreren Giga- oder sogar Terabyte“[31]. Andererseits sind Datenträger, insbesondere Kommunikationsgeräte, zwar jeweils für sich genommen ein einzelner Gegenstand, die Nutzung erfolgt jedoch in aller Regel gemischt. Das hat zur Folge, dass auf dem betreffenden Gerät typischerweise sowohl anwaltliche und damit geschützte Korrespondenz als auch sonstige Geschäftsdokumente, Verträge oder private Kommunikation gespeichert sind. Es ist daher aus Gründen der Prozessökonomie sinnvoller, eine Vorsortierung der Inhalte auf pauschal versiegelten Datenträgern durch denjenigen zu veranlassen, dessen Berufsgeheimnisse zu schützen sind.

Um die konkrete Bezeichnung vorzunehmen, ist dem Betroffenen **Einsicht** in die sichergestellten Unterlagen zu gewähren. Die Bestimmung ist auf gegenständliche Akten zugeschnitten: Sie werden dem betroffenen Berufsgeheimnisträger ausgehändigt, der sie durchsehen und jene Unterlagen oder Gruppen von Unterlagen listen soll, die sein Verschwiegenheitsrecht betreffen. Im Fall der hier interessierenden Datenträger ist das allerdings nicht ohne weiteres möglich – sie werden ihm freilich nicht als solche wieder ausgehändigt, damit er auf ihnen selbst sucht; damit wäre die Gefahr der Manipulation verbunden. Das Gericht muss daher von entsprechend ausgebildeten Hilfskräften[32] eine vollständige (**forensische) Kopie des Datenbestands** der versiegelten elektronischen Datenträger anfertigen lassen. Diese müssen dem betroffenen Berufsgeheimnisträger zur Durchsicht übergeben werden.

Hat der Berufsgeheimnisträger die entsprechenden Dateien oder Gruppen von Dateien abgegrenzt, unterzieht das Gericht nur[33] diese einer **Sichtung**. Nach der Sichtung entscheidet es, welche Inhalte tatsächlich einem Aussageverweigerungsrecht unterliegen. Ergibt sich das für den gesamten Datenträger, wird dieser dem Betroffenen wieder ausgehändigt. Sind einzelne Dateien oder Dateiordner auf gemischt verwendeten Datenträgern betroffen, müssen sie aus der Kopie, die gesichtet wird, herausgelöscht werden. Die Daten, denen das Gericht die Qualität eines Berufsgeheimnisses abspricht, werden zum Akt genommen.

§ 112 Abs 2 sieht zwingend vor, dass der Betroffene in den Sichtungsvorgang einzubeziehen ist. Der Fall seines Nichterscheinens ist ungeregelt. Ein Verzicht auf das gerichtliche Sichtungsverfahren kann daraus jedenfalls nicht abgeleitet werden.[34]

---

[31] EBRV 1677 BlgNR 24. GP.

[32] Dazu Erlass vom 20. September 2017 über den Einsatz von IT-Experten bei Staatsanwaltschaften und Gerichten in Strafverfahren, BMJ-Pr6150/0059-III 3/2017.

[33] *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 112 Rz 13/3.

[34] *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 112 Rz 13/2.

3.4.2. Einschränkung des Widerspruchsrechts auf den Berufsgeheimnisträger selbst und seine Vertreter

§ 112 Abs 1 räumt das Widerspruchsrecht der **„von der Sicherstellung betroffenen oder anwesenden Person“** unter Berufung auf **„ein“** vor Umgehung geschütztes Recht auf **Verschwiegenheit** ein. Als von der Sicherstellung in diesem Sinn „betroffen“ qualifiziert die Judikatur[35] ausschließlich den **Berufsgeheimnisträger selbst,** der die sicherzustellenden Gegenstände innehat: „Ein“ Verschwiegenheitsrecht wird als „sein“ Verschwiegenheitsrecht gelesen. Mit den anwesenden Personen sollen hingegen nur solche gemeint sein, die ihn in seiner Abwesenheit vertreten, das sind seine Mitarbeiter oder Angehörige der einschlägigen Interessensvertretung, die bei der Hausdurchsuchung in Kanzleiräumen anwesend sind (§ 121 Abs 2).[36]

Nun sind seit 2016 die Unterlagen und Informationen aus einer Rechtsberatung auch dann geschützt, wenn der **Beschuldigte** sie innehat (§ 157 Abs 2, siehe oben 3.3.3.). Wenn seine Räumlichkeiten durchsucht und seine Datenträger sichergestellt werden, läge es daher nahe, auch ihm das **Widerspruchsrecht einzuräumen.** Das entspräche dem Wortlaut des Gesetzes: Betroffener einer Sicherstellung ist iS von § 48 Abs 1 Z 4 jeder, in dessen Verfügungsmacht sich die sichergestellten Unterlagen befinden. Und § 112 Abs 1 spricht von „einem“ Verschwiegenheitsrecht, auf das sich der Betroffene berufen muss – also nicht notwendig auf „seines“.[37]

Die **Judikatur** anerkennt das nicht und **spricht dem Beschuldigten das Recht ab,** der Sicherstellung unter Berufung auf das Verschwiegenheitsrecht seines Rechtsberaters zu widersprechen. Auch Datenträger, auf denen sich Korrespondenz oder sonstige Beratungsunterlagen iS von § 157 Abs 2 befinden, gelangen daher ohne richterliche Sichtung an die Ermittlungsbehörden. Diese haben bei ihrer Einsicht zwar von Amts wegen die Umgehungsverbote zu beachten und dürfen Daten aus einem geschützten Beratungsverhältnis nicht zum Akt nehmen. Dennoch erlangen sie Einblick und damit das Wissen über die betreffenden Inhalte – es tritt also genau die Situation ein, die § 112 vermeiden soll.

IV. Rechtsstaatliche Defizite

1. Mutmaßlicher Beweiswert als einzige Voraussetzung

Die Voraussetzungen für eine Sicherstellung und damit auch für die Sicherstellung von Datenträgern einschließlich der hier interessierenden Kommunikationsgeräte sind schnell aufgezählt: Der Beweiswert des betreffenden Gegenstandes und eine Anordnung durch die Staatsanwaltschaft genügen. Weder muss eine Anlasstat bestimmter Schwere vorliegen, noch der Tatverdacht dringend sein, richterliche Bewilligung ist keine notwendig. Ein elektronischer Datenträger kann daher immer bereits dann sichergestellt werden, wenn etwa erwartet wird, dass irgendeine Nachricht, irgendeine Notiz, irgendein Bild, irgendeine sonstige Information auf diesem selbst gespeichert oder sogar – ausgehend von einem breiten Verständnis des § 111 Abs 2 – auf einen durch ihn zugänglichen externen Speicherplatz ausgelagert ist.

---

[35] OGH 13 Os 94/17y, EvBl 2018/48; OLG Wien 17 Bs 27/18x, Jst-Slg 2019/3; OLG Graz 13.08.2019, 1 Bs 32/19v.

[36] *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 112 Rz 10/1; JAB 1700 BlgNR 24. GP zu § 112.

[37] *Ghazanfari,* Sicherstellung von Mobiltelefonen und Berufsgeheimnisschutz, in *Lewisch* (Hrsg), Wirtschaftsstrafrecht und Organverantwortlichkeit, Jahrbuch 2022 (erscheint im Herbst 2022); *Tipold/Zerbes* in *Fuchs/Ratz,* WK StPO § 112 Rz 10/2.

Stellt man diese niederschwelligen Eingriffsvoraussetzungen der eigentlichen Schwere des Eingriffs gegenüber, ergibt sich ein unausgewogenes Bild. Dazu im Folgenden.

2. Datenüberschuss und Dauer des Ausleseprozesses

Durch eine insbesondere in komplexeren Wirtschaftsstrafsachen typisch umfassende Sicherstellung von elektronischen Datenträgern werden bei weitem **nicht nur die mit dem konkreten Verdacht zusammenhängenden Daten** zugänglich. Es geraten ungleich – und ex ante nicht abschätzbar – mehr Informationen in die Hände der Strafverfolgungsbehörden: sämtliche über Jahre gespeicherte oder rekonstruierbare Nachrichtenverläufe in sämtlichen Kommunikations-Apps mit sämtlichen Freunden und Familienangehörigen, sämtliche Bilder, Adressbücher, aufgezeichnete Ortsfeststellungen, idR auch zumindest die jüngst aufgerufenen Internetseiten, alle Einträge in die durch dieses Gerät benutzten Sozialen Medien, kurzum, die Strafverfolgungsbehörden erhalten ein „Logbuch" des Lebens des Betroffenen.[38] Insofern ist dieser einem wesentlich **breiteren Einblick** in sein Leben ausgesetzt als bei einer erstens zeitlich und zweitens auf Kommunikationsdaten beschränkten Nachrichtenüberwachung. Bei einer Sicherstellung von Datenträgern in einem Unternehmen kann die einbezogene Datenmenge bis zu mehreren Terabyte betragen. Häufig werden etwa sämtliche Unterlagen über die Geschäftsvorgänge ab einem gewissen Geschäftsjahr gesucht und zu diesem Zweck Computer, Mobiltelefone, Laptops bis hin zum Firmenserver sichergestellt. Naturgemäß ist nach solchen Vorgängen nur ein Bruchteil des sichergestellten Materials tatsächlich verdachtsrelevant; die Rede ist von einem mitunter zehntausendfach größeren Datenbestand, den sich die Strafverfolgungsbehörden zugänglich machen.[39]

Derartig umfassende Sicherstellungen kommen dadurch zustande, dass die Daten idR nicht vor Ort gesichtet und aussortiert werden können: Der zu durchsuchende Datenbestand ist schlicht zu umfangreich, häufig müssen überdies technische Hürden überwunden werden.[40] Der Eingriff in die Privatsphäre des Betroffenen kann daher allein quantitativ weit über das hinausgehen, was angesichts des anlassgebenden Vorwurfs verhältnismäßig ist.

Hinzu kommt, dass auch die Strafverfolgungsbehörden selbst bei der Auswertung der ihnen vorliegenden Datenmenge über ihre Kapazitäten hinausgehend beansprucht sind. Jedenfalls wird das Ermittlungsverfahren dadurch entscheidend in die Länge gezogen. Ermittlungsverfahren in Wirtschaftsstrafsachen werden **fallweise über 10 Jahre lang** geführt; die Datenträger bleiben teilweise ebenso lang sichergestellt, sodass sie der Betroffene in dieser Zeit nicht verwenden kann, und fallweise keine Kopie der in die Auswertung einbezogenen Daten erhält.

3. Einfacher Zugriff auf Kommunikationsdaten

Mittels Sicherstellung eines Mobiltelefons oder sonstigen Kommunikationsgeräts sind zu einem guten Teil auch jene Daten verfügbar, die als **„Nachrichten und Informationen"** Gegenstand einer Nachrichtenüberwachung sind: stets dann, wenn diese nicht nur auf dem Server des betreffenden Anbieters, sondern auch auf dem Handy abgespeichert wurden. Erstreckt man die Auswertungsbefugnis eines sichergestellten Mobiltelefons *zusätzlich* auf

[38] *Rohregger/Benedik,* Aktenleaks – Status Quo und Reformüberlegungen*,* in *Lewisch* (Hrsg), Wirtschaftsstrafrecht und Organverantwortlichkeit, Jahrbuch 2021, 47 (51); *Zerbes,* Beweisquelle Handy, ÖJZ 2021/24, 176 (176).
[39] *Rohregger/Benedik,* Aktenleaks – Status Quo und Reformüberlegungen*,* in *Lewisch* (Hrsg), Wirtschaftsstrafrecht und Organverantwortlichkeit, Jahrbuch 2021, 47 (52).
[40] *Rohregger/Benedik,* Aktenleaks – Status Quo und Reformüberlegungen*,* in *Lewisch* (Hrsg), Wirtschaftsstrafrecht und Organverantwortlichkeit, Jahrbuch 2021, 47 (51).

die – durch dieses zugänglichen – externen Speicherplätze (siehe oben III.1.2.2.) kommen noch jene Daten hinzu, die nur auf diesen externen Speicherplätzen vorhanden sind und auf dem Handy bloß sichtbar gemacht werden können.

Will die Strafverfolgungsbehörde diese Daten durch **Nachrichtenüberwachung** ermitteln, ist sie allerdings an **deutlich strengere Vorgaben** gebunden als bei einer Sicherstellung. So muss der Verdacht auf eine vorsätzliche Anlasstat vorliegen, die mit über einem Jahr Freiheitsstrafe bedroht ist, dieser Verdacht muss dringend sein, außer einer Anordnung durch die Staatsanwaltschaft muss eine richterliche Bewilligung vorliegen. Zudem darf grundsätzlich nur die „Kommunikation" – die Nachrichten, die Informationen – des Beschuldigten gelesen werden. Ein Zeuge, von dem man in der Kommunikation mit einem anderen Nicht-Beschuldigten Äußerungen über die Anlasstat erwartet, darf nicht überwacht werden (§ 135 Abs 2 Z 3 und Abs 3 Z 3 lit b; eine Ausnahme besteht nur im Sonderfall der Zustimmung des überwachten Anschlusses).

Aus diesem Blickwinkel besteht ein **nicht sachgerechtes Ungleichgewicht:** Ein und dieselben Daten – solche, die durch Kommunikation zustande kommen – sind durch eine Sicherstellung ohne weiteres umfassend verfügbar, im Rahmen einer Nachrichtenüberwachung bindet der Gesetzgeber die Ermittlungsbehörden jedoch an deutlich höherschwellige Voraussetzungen.

4. Keine Regelung zum Umgang mit Zufallsfunden

Die Datenmenge, die sich nach einer umfangreichen Sicherstellung von Datenträgern bei der Strafverfolgungsbehörde befindet, ist geradezu unüberschaubar groß und vielfältig. Außer einer Vielzahl von Einblicken in höchstpersönliche Informationen des Betroffenen (dazu unten 6.), liegt es auf der Hand, dass sich aus der Auswertung Hinweise auf andere als die anlassgebende strafbare Handlung ergeben können.

Anders als im Zusammenhang mit Nachrichtenüberwachung (§ 140 Abs 1 Z 4) ist bei Sicherstellung jedoch **keine Regelung für Zufallsfunde vorgesehen.** Das ist – angesichts des quantitativ und qualitativ ausgesprochen weit über die verdachtsrelevanten Informationen hinausgehenden Materials und angesichts des Zugriffs auf Nachrichtendaten – nicht sachgerecht.

5. Versteckter Geheimnischarakter der Sicherstellung

Die im Vergleich zur Nachrichtenüberwachung geringfügigen Eingriffsschwellen der Sicherstellung werden gemeinhin damit erklärt, dass eine **Sicherstellung** dem Betroffenen gegenüber **offen** erfolgt: Vor seinen Augen wird durchsucht und werden ihm die betreffenden Datenträger abgenommen, anschließend erhält er in einer Bestätigung eine Liste der sichergestellten Gegenstände. Damit soll ihm von Anfang an rechtliches Gehör eingeräumt werden; offene Maßnahmen gelten daher traditionell als weniger schwerwiegend als verdecktes Vorgehen.

Aber: Welche Daten mit einem als solches offen sichergestellten Kommunikationsgerät tatsächlich den Behörden zugänglich werden, kann der Betroffene nicht mehr einschätzen. Ein Computer erhält seine Bedeutung nicht als Gegenstand, sondern als Träger von Information. Schon ein einziges Mobiltelefon gibt um vieles mehr preis, als der jeweilige Nutzer erkennt. Erst recht gilt das für Datenbestände auf diversen Datenträgern bis hin zu Servern eines ganzen Unternehmens. Das liegt nicht nur daran, dass sich kaum jemand erinnert, welche Daten er noch wo – nur am sichergestellten Datenträger oder auf externen Speicherplätzen – gespeichert und welche er bereits gelöscht hat. Überdies haben die Strafver-

folgungsbehörden weitgehende Möglichkeiten, bereits gelöschte Daten wiederherzustellen: Die gängigen Löschbefehle beseitigen die betreffenden Daten idR nur von der durch normale Nutzung verfügbaren Anwendung, bleiben aber rekonstruierbar.

Erst wenn die Strafverfolgungsbehörden den Datenbestand insofern ausgewertet haben, als sie das, was sie als verdachtsrelevant ansehen, zum Akt nehmen können, erhält der Beschuldigte die Möglichkeit, Akteneinsicht zu nehmen. Was ihm weiterhin unzugänglich bleibt, sind jene Daten, die die Ermittlungsbehörden aussortiert haben. Ebenso wenig kann er abschätzen, ob und auf welche Zufallsfunde die Behörden gestoßen sind und inwiefern diese Zufallsfunde weitere Ermittlungen anstoßen.

Damit ist das **rechtliche Gehör** des Beschuldigten jedenfalls iZ mit großen Datenträgern **entscheidend beschnitten:** Er ist nicht auf dem gleichen Informationsstand wie die Behörden und hat daher nur beschränkt die Möglichkeit zu beantragen, aus seiner Sicht entlastende Daten ebenfalls zum Akt zu nehmen.

6. Informationsüberfluss (auch) von Mitbeschuldigten

Die Daten, die zum Akt genommen werden, sind den Verfahrensbeteiligten im Wege der **Akteneinsicht** zugänglich. Das sind zum einen die Mitbeschuldigten (§ 49 Abs 1 Z 3). Insbesondere dann, wenn die Staatsanwaltschaft aufgrund sachlicher Konnexität **mehrere Personen** wegen mehrerer strafbarer Handlungen **als Beschuldigte** führt, kann der Kreis jener, die Einblick erhalten, bedenklich weit sein. Mitbeschuldigte haben Zugang zu dem weit überschießenden, zum Teil Persönliches preisgebenden Datenmaterial, und sie alle und ihre Verteidiger können, je nach eigenem prozesstaktischen Interesse, dieses Material (in den Grenzen des § 54 StPO) den Medien zuspielen. Ein derartig **breit zugänglicher Ermittlungsakt** setzt den Betroffenen der **Gefahr der öffentlichen Entblößung** aus.

Zum anderen haben Opfer, Privatbeteiligte und Privatankläger ein beschränktes Akteneinsichtsrecht (§ 68).

7. Mangelhafter Schutz der Berufsgeheimnisse

Die Judikatur schränkt das **Widerspruchsrecht** zum Schutz berufsbedingter Geheimnisse **allein** auf den **Berufsgeheimnisträger selbst** (und dessen Vertreter) ein. Hat der Beschuldigte hingegen Datenträger inne, auf denen (auch) Korrespondenz oder sonstige Dokumente aus Rechtsberatung gespeichert sind, kann er deren Sicherstellung daher nicht wirksam widersprechen. Damit gelangen Informationen, die nach § 157 Abs 2 (letzter Satz) auch in seinem Gewahrsam geschützt sind, ohne richterliche Sichtung an die Ermittlungsbehörden. Diese dürfen die Daten aus einem entsprechenden Beratungsverhältnis zwar nicht zum Akt nehmen, weil sie Umgehungsverbote von Amts wegen beachten müssen. Einen Einblick und damit das Wissen über die betreffenden Inhalte erhalten sie dennoch – es passiert also, was § 112 im Zusammenhang mit § 157 Abs 2 vermeiden soll (siehe oben 3.4.2.).

V. Reformvorschläge

1. Anhebung der Eingriffsvoraussetzungen im Hinblick auf Kommunikationsgeräte

Die Sicherstellung eines elektronischen Kommunikationsgeräts steht bei genauerem Hinsehen zwischen einer Sicherstellung von Gegenständen und einer Nachrichtenüberwachung. Die Wegnahme selbst erfolgt zwar offen, und **rein formal** liegt ein **Gegenstand**

vor, über den die Strafverfolgungsbehörden Verfügungsmacht begründen. Die dadurch zugänglich gemachten Informationen – unter anderem die bloßen **Rahmendaten von Kommunikation,** aber auch **Kommunikationsinhalte** – entsprechen jedoch in wesentlichen Bereichen jenen Daten, die bei einer Auskunft über Daten einer Nachrichtenübermittlung (§ 134 Z 2) oder bei der Nachrichtenüberwachung (§ 134 Z 3) anfallen.

Damit erhält die Sicherstellung eines Kommunikationsgeräts im Strafverfahren eine Bedeutung, der *de lege ferenda* durch ein eigenes, von der herkömmlichen Sicherstellung abgehobenes Regelungskonzept gerecht werden soll:

- mit der Einführung von **besonderen Bestimmungen** zur Sicherstellung von Datenträgern,
- wobei die Sicherstellung von „Datenträgern, die Ursprung oder Ziel einer Übertragung von Nachrichten und Informationen im Sinne von § 134 Z 3 sein können" – kurz: **Kommunikationsgeräte** – an **höhere Eingriffsschwellen** gebunden werden soll. Die begriffliche **Anlehnung an § 134 Z 3,** der die Nachrichtenüberwachung definiert, entspricht der Art der Daten, die nach einer Sicherstellung von Kommunikationsgeräten ausgelesen werden: Es handelt sich zu einem großen Teil um Nachrichtendaten.

Dementsprechend ist auch eine inhaltliche **Orientierung an § 135 Abs 3** sachgerecht. Insbesondere sollte die Schwelle der Anlasstaten auf das für die Nachrichtenüberwachung erforderliche Niveau – auf mit über einem Jahr Freiheitsstrafe bedrohte Straftaten – angehoben werden. Auch eine gerichtliche Bewilligung (vgl § 137 Abs 1) könnte erwogen werden.

Aus der Sicherstellung ausgeklammert werden sollte der Zugriff auf Datenbestände **externer Speicherplätze** wie zB auf Clouds udgl. Die dort gespeicherten Daten und Informationen sind ja gerade *nicht* auf dem als Gegenstand sichergestellten (Kommunikations-) Gerät selbst gespeichert. Sie sind nur *über* dieses über eine Online-Verbindung verfügbar; hierzu muss ein Kommunikationsnetz iS einer Nachrichtenüberwachung (§ 134 Z 3 StPO iVm § 4 Z 1 TKG) verwendet werden. Wir gehen daher davon aus, dass eine derartige Daten- und Informationsermittlung stets und unmittelbar nur unter die Regelungen für die **Nachrichtenüberwachung** zu fallen hat – siehe dazu III.1.2. und 2.

2. Regelung zum Umgang mit Zufallsfunden

Wiederum **an die Nachrichtenüberwachung angelehnt** wird zumindest für die Sicherstellung von Kommunikationsgeräten vorgeschlagen, die Verwendbarkeit von Zufallsfunden auf strafbare Handlungen zu beschränken, die auch Anlass zu einer derartigen Sicherstellung hätten geben können. Im Zusammenhang mit der notwendigen Hochstufung der Anlasstat (siehe oben 1.) wären damit nur solche Zufallsfunde verwendbar, die auf eine mit über einem Jahr Freiheitsstrafe bedrohte strafbare Handlung hinweisen.

3. Transparenz gegenüber dem Beschuldigten und Löschung

Ausgangspunkt ist wiederum, dass mit der Sicherstellung eines Smartphones oder eines sonstigen Kommunikationsgeräts ein enormer Überschuss an Daten sichergestellt wird. Die Strafverfolgungsbehörden müssen daher einen Auswahlprozess vornehmen:

- Das, was für den Fall **relevant** ist, soll **zum Akt** genommen werden;
- über **Zufallsfunde** soll ein **eigener Akt** anzulegen sein (siehe oben IV.4.);
- **alles andere** wird nicht weiter benötigt und ist **zu löschen.**

Dieser Auswahlprozess erfolgt freilich nicht direkt am sichergestellten Kommunikationsgerät: Damit wäre die Gefahr einer Manipulation des betreffenden Datenbestandes verbunden. Zudem ist einerseits nicht alles, was am Kommunikationsgerät gespeichert ist, ohne

weiteres ersichtlich. Viele darauf befindliche Daten – Nachrichten, Bilder, der Verlauf aufgerufener Webseiten usw – wurden durch den Nutzer oder auch automatisch gelöscht, sind daher (vorerst) verborgen, aber weitgehend rekonstruierbar. Andererseits gibt es automatische Löschvorgänge zB bestimmter Nachrichtenprogramme, die Daten innerhalb relativ kurzer Zeit sogar spurlos – jedenfalls nicht oder kaum rekonstruierbar – verschwinden lassen. Derartige Daten könnten im Zeitpunkt der Sicherstellung zwar noch vorhanden sein, sie drohen aber verloren zu gehen.

Um den gesamten Datenbestand eines Kommunikationsgeräts verfügbar zu machen, sind daher folgende Schritte erforderlich:

- Erstens ist eine sog **bit-idente forensische Kopie des Datenträgers** herzustellen: Sie bildet diesen 1:1 ab und gibt damit den Strafverfolgungsbehörden somit alle *offline* – vgl oben V.1. – ohne weiteres zugänglichen Daten preis.
- Durch weitere Bearbeitung dieser bit-identen Kopie durch die IT-Experten der Strafverfolgungsbehörden sind zweitens jene **Daten wiederherzustellen,** die zwar (vordergründig) gelöscht wurden, aber aus ihren Spuren rekonstruierbar sind.
- Ferner sind mitunter im Zeitpunkt der Sicherstellung – gemeint ist: bei der Begründung der körperlichen Verfügungsmacht über das Kommunikationsgerät – gewisse **Daten volatil,** insbesondere Nachrichten, die mit entsprechenden Löschmechanismen verschickt wurden. Sie drohen zu verschwinden, noch bevor sie kopiert und zur Auswertung herangezogen werden können. Derartige Daten können gleich bei der Sicherstellung zB durch **Screenshots**, **Videoaufnahmen** oder – falls es um akustisch wahrnehmbare Informationen geht – durch **Tonaufnahme** festgehalten werden.

Den gesamten Datenbestand eines sichergestellten Kommunikationsgeräts setzen die Strafverfolgungsbehörden daher zusammen

- aus einer **bit-identen Kopie** des Geräts,
- aus deren Ergänzung um **rekonstruierte Daten**
- sowie fallweise aus deren Ergänzung um **Ton- oder Bildaufnahmen** von automatisch verschwindenden Nachrichten und sonstigen Inhalten.

Das alles wird dem Auswahlprozess zugrunde gelegt.

Hier interessiert, wie sich dadurch technisch einigermaßen einfach bewerkstelligen ließe, das oben bemängelte **Defizit an Information des Betroffenen** (siehe oben IV.5.) **auszugleichen:** Ihm müssten bloß **sämtliche Teile** – bit-idente Kopie, Kopie der nachträglich wiederhergestellten Daten und der „konservierten" flüchtigen Daten – auf einem (oder mehreren) Datenträgern ebenfalls **zur Verfügung gestellt** werden. Damit würde der ihm nach einer Sicherstellung verfügbare Datenbestand mit jenem, an dem die Ermittlungsbehörden arbeiten, vollständig übereinstimmen, er könnte auf dieser Basis seine **Beteiligungsrechte** wahrnehmen und **beantragen,**

- weiteres seiner Ansicht nach **entlastendes Material zum Akt** zu nehmen, das die Behörde als irrelevant aussortiert hat, sowie
- solche Daten, die er verdachtsbezogen als **irrelevant** betrachtet, **nicht zum Akt** zu nehmen.

Nur ein derartig **transparentes Vorgehen** würde dem Verständnis der Sicherstellung als **nicht geheime** Maßnahme gerecht werden. Es entspräche zudem den auf eine Nachrichtenüberwachung folgenden Offenlegungspflichten (§ 139 StPO).

Um die mitunter unzumutbar lange **Dauer** der Auswertungsprozesse **zu verkürzen,** schlagen wir iS der Verfahrensbeschleunigung vor, die Schritte, durch die der Betroffene zu informieren ist, an Fristen zu binden:

- **Zwei Wochen** dürften für die **Aushändigung einer bit-identen Kopie** des sichergestellten Kommunikationsgeräts und für die Herausgabe von mitunter unverzüglich „konservierten" Inhalten idR genügen. In Fällen, in denen der Betroffene den Zugang zu seinen Daten an Passwörter gebunden hat, die er nicht preisgibt, müssen allerdings Entschlüsselungstechniken eingesetzt werden, bevor eine Kopie hergestellt werden kann. Um den mit einem solchen Prozess verbundenen Zeitaufwand zu berücksichtigen, kann die Zweiwochenfrist auf insgesamt acht Wochen verlängert werden.
- Werden nach Aushändigung der ersten (ergänzten) Kopie an den Betroffenen weitere Inhalte wiederhergestellt – etwa gelöschte Daten, die erst rekonstruiert werden mussten – so erscheinen **sechs Wochen** ab Herstellung der (ursprünglichen) Kopie als eine Nachreichfrist für diese rekonstruierten Inhalte angemessen,

womit sich im Normalfall eine (Auslese-, und Verständigungs-) **Frist von höchstens acht Wochen ab dem Zeitpunkt der Sicherstellung des Kommunikationsgeräts** ergibt; nur im Sonderfall einer Verschlüsselung beträgt diese Frist vierzehn Wochen. Danach sind die Inhalte verdachtsbezogen auszuwerten: Sie sind zum Akt zu nehmen oder zu löschen.

Nur demjenigen, der von der Sicherstellung betroffen ist – das ist idR der Beschuldigte, in seltenen Fällen ein Zeuge –, dürfte dieser Gesamtdatensatz zugänglich gemacht werden: Es handelt sich um seine Daten. Anderen – etwa Mitbeschuldigten – soll dieser Datensatz nicht ausgehändigt werden. Sie erhalten nur Akteneinsicht und können damit ausschließlich zum Akt genommene Inhalte einsehen (beachte jedoch den Vorschlag zur Erweiterung des § 49 Abs 2, dazu unten 4.). Das entspricht der Akteneinsicht in der analogen Welt: Zu den Unterlagen, die nicht zum Akt genommen werden, haben Mitbeschuldigte ebenfalls keinen Zugang.

4. Beschränkung der Akteneinsicht von Mitbeschuldigten

Viele der am sichergestellten Gerät vorhandenen Daten können bis in die Intimität hineinreichende Einblicke in das Leben des Betroffenen geben, die für den anlassgebenden Verdacht keinerlei Bedeutung haben. Zum Schutz der Privatsphäre des jeweils Betroffenen wird daher vorgeschlagen, die **Beschränkung der Akteneinsicht,** die sich nach geltender Rechtslage nur auf Opfer, Privatbeteiligte und Privatankläger bezieht, **auf Mitbeschuldigte anwendbar zu machen** – freilich nur soweit deren Interessen nicht beeinträchtigt werden. Damit soll der Einblick in bloßstellende Inhalte, die für den einen Mitbeschuldigten betreffenden Verdacht irrelevant sind, vermieden werden. Auch verringert sich dadurch das Risiko ihrer (medialen) Verbreitung.

5. Anerkennung eines Widerspruchsrechts des Beschuldigten bezüglich Rechtsberatungsunterlagen

Ausgangspunkt ist, dass das Widerspruchsrecht nach § 112 parallel zum Umgehungsverbot berufsbedingter Verschwiegenheitsrechte gewährleistet sein müsste. Dementsprechend sollte es sowohl dem **Beschuldigten** als auch **kanzleiexternen Hilfskräften** des Berufsgeheimnisträgers wie Übersetzern, Banken oder Privatsachverständigen ausdrücklich zustehen, soweit diese sich auf ein – aus ihrer Sicht fremdes – Verschwiegenheitsrecht eines Berufsgeheimnisträgers berufen.

Damit ist jedoch folgendes Problem verbunden: Der Beschuldigte könnte bei einer Vielzahl der bei ihm sicherzustellenden Datenträger mit dem Hinweis widersprechen, dass darauf

Kommunikation mit zB einem Anwalt gespeichert sei. Nach dem derzeitigen Konzept des § 112 ist sodann der Berufsgeheimnisträger selbst aufzufordern, eine konkretisierende Bezeichnung der – aufgrund des Widerspruchs versiegelten – Datenträger vorzunehmen. Dies könnte mit einem enormen Arbeitsaufwand für ihn verbunden sein, wenn er nicht einmal mehr ein Mandatsverhältnis mit dem Beschuldigten pflegt: Er müsste aufgefordert werden, aus vom Beschuldigten naturgemäß gemischt verwendeten Datenträgern jene Dateien herauszusuchen, die sein Verschwiegenheitsrecht betreffen – und zwar ohne Kenntnis über die Systematik, nach der der Beschuldigte seine Daten abgelegt hat.

Einen derartigen Aufwand von einem Berufsgeheimnisträger zu verlangen, erscheint unverhältnismäßig. Es wird daher als eine – ein wenig komplexe – Kompromisslösung vorgeschlagen, zunächst dem widersprechenden Beschuldigten selbst eine Bezeichnungsobliegenheit und damit die Aufgabe der Aussortierung des Materials aufzuerlegen. Im Anschluss daran soll der betroffene Berufsgeheimnisträger dieses bereits vorsortierte Material sichten. Ob sich dies in der Praxis bewerkstelligen lässt, ist allerdings unsicher.

Aus dem eigentlichen Schutzziel der Berufsgeheimnisse ließe sich sogar erwägen, das Widerspruchsrecht für Mandanten noch weiter auszubauen: *Diesen* soll eine vor staatlichen Einblicken geschützte (insbesondere rechtliche) Beratung garantiert sein. So wäre es aus Sicht der Verteidigung durchaus ein Anliegen, dem Beschuldigten bezogen auf die ihn betreffenden Rechtsberatungsunterlagen stets das Recht einzuräumen, einer Sicherstellung zu widersprechen, unabhängig davon, wo sie sich befinden.

Vorschlag zur Gesetzesänderung

Textgegenüberstellung

Geltende Fassung	Vorgeschlagene Fassung
3. Hauptstück **ZWEITER ABSCHNITT**	
§ 49. (1) Der Beschuldigte hat insbesondere das Recht, …	**§ 49.** (1) Der Beschuldigte hat insbesondere das Recht, …
(2) Der Beschuldigte hat das Recht, dass Opfern, Privatbeteiligten oder Privatanklägern Akteneinsicht (§ 68) nur insoweit gewährt wird, als dies zur Wahrung ihrer Interessen erforderlich ist.	(2) Der Beschuldigte hat das Recht, dass Opfern, Privatbeteiligten oder Privatanklägern sowie Mitbeschuldigten Akteneinsicht (§ 68 bzw §§ 51 bis 53) nur insoweit gewährt wird, als dies zur Wahrung ihrer Interessen erforderlich ist.
§ 51. (1) Der Beschuldigte ist berechtigt, in die der Kriminalpolizei, der Staatsanwaltschaft und dem Gericht vorliegenden Ergebnisse des Ermittlungs- und des Hauptverfahrens Einsicht zu nehmen. Das Recht auf Akteneinsicht berechtigt auch dazu, Beweisgegenstände in Augenschein zu nehmen, soweit dies ohne Nachteil für die Ermittlungen möglich ist. …	**§ 51.** (1) Der Beschuldigte ist berechtigt, in die der Kriminalpolizei, der Staatsanwaltschaft und dem Gericht vorliegenden Ergebnisse des Ermittlungs- und des Hauptverfahrens Einsicht zu nehmen, soweit diese nicht im Sinne von § 49 Abs. 2 ausgenommen wurden. Das Recht auf Akteneinsicht berechtigt auch dazu, Beweisgegenstände in Augenschein zu nehmen, soweit dies ohne Nachteil für die Ermittlungen möglich ist. …
8. Hauptstück **ERSTER ABSCHNITT**	
§ 109. Im Sinne dieses Gesetzes ist 1. „Sicherstellung“	**§ 109**. Im Sinne dieses Gesetzes ist 1. „Sicherstellung“

a. die vorläufige Begründung der Verfügungsmacht über Gegenstände und
b. das vorläufige Verbot der Herausgabe von Gegenständen oder anderen Vermögenswerten an Dritte (Drittverbot) und das vorläufige Verbot der Veräußerung oder Verpfändung solcher Gegenstände und Werte,

2. „Beschlagnahme“
a. eine gerichtliche Entscheidung auf Begründung oder Fortsetzung einer Sicherstellung nach Z 1 und
b. das gerichtliche Verbot der Veräußerung, Belastung oder Verpfändung von Liegenschaften oder Rechten, die in einem öffentlichen Buch eingetragen sind,
…

§ 110. (1) Sicherstellung ist zulässig, wenn sie
1. aus Beweisgründen,
2. zur Sicherung privatrechtlicher Ansprüche oder
3. zur Sicherung der Konfiskation (§ 19a StGB), des Verfalls (§ 20 StGB), des erweiterten Verfalls (§ 20b StGB), der Einziehung (§ 26 StGB) oder einer anderen gesetzlich vorgesehenen vermögensrechtlichen Anordnung
erforderlich scheint.

a. die vorläufige Begründung der Verfügungsmacht über Gegenstände und
b. das vorläufige Verbot der Herausgabe von Gegenständen oder anderen Vermögenswerten an Dritte (Drittverbot) und das vorläufige Verbot der Veräußerung oder Verpfändung solcher Gegenstände und Werte,

1a. „Sicherstellung von Datenträgern“
erfasst auch das Auslesen und Auswerten der zum Zeitpunkt der Sicherstellung auf diesen gespeicherten Daten und jener Daten, die in einem nicht öffentlichen Netzwerk über diese Datenträger verfügbar sind,

2. „Beschlagnahme“
a. eine gerichtliche Entscheidung auf Begründung oder Fortsetzung einer Sicherstellung nach Z 1 und Z 1a
b. das gerichtliche Verbot der Veräußerung, Belastung oder Verpfändung von Liegenschaften oder Rechten, die in einem öffentlichen Buch eingetragen sind,
…

§ 110. (1) Sicherstellung ist zulässig, wenn sie
1. aus Beweisgründen,
2. zur Sicherung privatrechtlicher Ansprüche oder
3. zur Sicherung der Konfiskation (§ 19a StGB), des Verfalls (§ 20 StGB), des erweiterten Verfalls (§ 20b StGB), der Einziehung (§ 26 StGB) oder einer anderen gesetzlich vorgesehenen vermögensrechtlichen Anordnung
erforderlich scheint.

(1a) Sicherstellung von Datenträgern, die Ursprung oder Ziel einer Übertragung von Nachrichten und Informationen im Sinne von § 134 Z 3 sein können (kurz: Kommunikationsgeräte) ist zulässig,
1. wenn und solange der dringende Verdacht besteht, dass eine von der Sicherstellung betroffene Person eine andere entführt oder sich sonst ihrer bemächtigt hat, und sich die Auswertung auf Daten beschränkt, von denen anzunehmen ist, dass sie

	zur Zeit der Freiheitsentziehung vom Beschuldigten gespeichert, empfangen oder gesendet wurden, 2. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann, sofern der Inhaber des Kommunikationsgeräts zustimmt, 3. wenn dies zur Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, erforderlich erscheint oder die Aufklärung oder Verhinderung von im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278 bis 278b StGB) begangenen oder geplanten Straftaten ansonsten wesentlich erschwert wäre und a. der Inhaber des Kommunikationsgeräts der vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, oder einer Straftat gemäß §§ 278 bis 278b StGB dringend verdächtig ist, oder b. auf Grund bestimmter Tatsachen anzunehmen ist, dass eine der Tat (lit a) dringend verdächtige Person das Kommunikationsgerät benützt hat oder mit ihr eine Verbindung hergestellt hatte; 4. wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann.
(2) Sicherstellung ist von der Staatsanwaltschaft anzuordnen und von der Kriminalpolizei durchzuführen.	(2) Sicherstellung nach Abs. 1 ist von der Staatsanwaltschaft anzuordnen und von der Kriminalpolizei durchzuführen. Sicherstellung nach Abs. 1a ist von der Staatsanwaltschaft aufgrund gerichtlicher Bewilligung anzuordnen. Nachdem die Kriminalpolizei die körperliche Verfügungsmacht begründet hat, haben die Strafverfolgungsbehörden die Auslesung und Auswertung vorzunehmen.
(3) Die Kriminalpolizei ist berechtigt, Gegenstände (§ 109 Z 1 lit. a) von sich aus sicherzustellen, 1. wenn sie a. in niemandes Verfügungsmacht stehen, b. dem Opfer durch die Straftat entzogen wurden,	(3) Die Kriminalpolizei ist berechtigt, Gegenstände (§ 109 Z 1 lit. a) von sich aus sicherzustellen, 1. wenn sie a. in niemandes Verfügungsmacht stehen, b. dem Opfer durch die Straftat entzogen wurden,

c. am Tatort aufgefunden wurden und zur Begehung der strafbaren Handlung verwendet oder dazu bestimmt worden sein könnten, oder
d. geringwertig oder vorübergehend leicht ersetzbar sind,

2. wenn ihr Besitz allgemein verboten ist (§ 445a Abs. 1),
3. die im Rahmen einer Durchsuchung nach § 120 Abs. 2 aufgefunden werden oder mit denen eine Person, die aus dem Grunde des § 170 Abs. 1 Z 1 festgenommen wird, betreten wurde oder die im Rahmen ihrer Durchsuchung gemäß § 120 Abs. 1 zweiter Satz aufgefunden werden, oder
4. in den Fällen des Artikels 18 der Verordnung (EU) Nr. 608/2013 zur Durchsetzung der Rechte geistigen Eigentums durch die Zollbehörden und zur Aufhebung der Verordnung (EG) Nr. 1383/2003 des Rates, ABl. Nr. L 181 vom 29.06.2013 S. 15.

(4) Die Sicherstellung von Gegenständen aus Beweisgründen (Abs. 1 Z 1) ist nicht zulässig und jedenfalls auf Verlangen der betroffenen Person aufzuheben, soweit und sobald der Beweiszweck durch Bild-, Ton- oder sonstige Aufnahmen oder durch Kopien schriftlicher Aufzeichnungen oder automationsunterstützt verarbeiteter Daten erfüllt werden kann und nicht anzunehmen ist, dass die sichergestellten Gegenstände selbst oder die Originale der sichergestellten Informationen in der Hauptverhandlung in Augenschein zu nehmen sein werden.

§ 111. (1) Jede Person, die Gegenstände oder Vermögenswerte, die sichergestellt werden sollen, in ihrer Verfügungsmacht hat, ist verpflichtet (§ 93 Abs. 2), diese auf Verlangen der Kriminalpolizei herauszugeben oder die Sicherstellung auf andere Weise zu ermöglichen. Diese Pflicht kann erforderlichenfalls auch mittels Durchsuchung von Personen oder Wohnungen erzwungen werden; dabei sind die §§ 119 bis 122 sinngemäß anzuwenden.

(2) Sollen auf Datenträgern gespeicherte Informationen sichergestellt werden, so hat jedermann Zugang zu diesen Informationen zu gewähren und auf Verlangen einen

c. am Tatort aufgefunden wurden und zur Begehung der strafbaren Handlung verwendet oder dazu bestimmt worden sein könnten, oder
d. geringwertig oder vorübergehend leicht ersetzbar sind,

2. wenn ihr Besitz allgemein verboten ist (§ 445a Abs. 1),
3. die im Rahmen einer Durchsuchung nach § 120 Abs. 2 aufgefunden werden oder mit denen eine Person, die aus dem Grunde des § 170 Abs. 1 Z 1 festgenommen wird, betreten wurde oder die im Rahmen ihrer Durchsuchung gemäß § 120 Abs. 1 zweiter Satz aufgefunden werden, oder
4. in den Fällen des Artikels 18 der Verordnung (EU) Nr. 608/2013 zur Durchsetzung der Rechte geistigen Eigentums durch die Zollbehörden und zur Aufhebung der Verordnung (EG) Nr. 1383/2003 des Rates, ABl. Nr. L 181 vom 29.06.2013 S. 15.

(4) Die Sicherstellung von Gegenständen aus Beweisgründen (Abs. 1 Z 1) ist nicht zulässig und jedenfalls auf Verlangen der betroffenen Person aufzuheben, soweit und sobald der Beweiszweck durch Bild-, Ton- oder sonstige Aufnahmen oder durch Kopien schriftlicher Aufzeichnungen oder automationsunterstützt verarbeiteter Daten erfüllt werden kann und nicht anzunehmen ist, dass die sichergestellten Gegenstände selbst oder die Originale der sichergestellten Informationen in der Hauptverhandlung in Augenschein zu nehmen sein werden.

§ 111. (1) Jede Person, die Gegenstände oder Vermögenswerte, die sichergestellt werden sollen, in ihrer Verfügungsmacht hat, ist verpflichtet (§ 93 Abs. 2), diese auf Verlangen der Kriminalpolizei herauszugeben oder die Sicherstellung auf andere Weise zu ermöglichen. Diese Pflicht kann erforderlichenfalls auch mittels Durchsuchung von Personen oder Wohnungen erzwungen werden; dabei sind die §§ 119 bis 122 sinngemäß anzuwenden.

(2) Sollen Datenträger sichergestellt werden (§ 109 Z 1a), so hat jedermann Zugang zu diesen und den darauf gespeicherten Daten zu gewähren. Überdies ist er verpflichtet, auf Verlangen einen Datenträger auszufolgen oder herstellen zu lassen, auf dem sich diese Daten in einem allgemein gebräuchlichen Format befinden. Auch hat

elektronischen Datenträger in einem allgemein gebräuchlichen Dateiformat auszufolgen oder herstellen zu lassen. Überdies hat er die Herstellung einer Sicherungskopie der auf den Datenträgern gespeicherten Informationen zu dulden.

(3) Personen, die nicht selbst der Tat beschuldigt sind, sind auf ihren Antrag die angemessenen und ortsüblichen Kosten zu ersetzen, die ihr durch die Trennung von Urkunden oder sonstigen beweiserheblichen Gegenständen von anderen oder durch die Ausfolgung von Kopien notwendigerweise entstanden sind.

(4) In jedem Fall ist der von der Sicherstellung betroffenen Person sogleich oder längstens binnen 24 Stunden eine Bestätigung über die Sicherstellung auszufolgen oder zuzustellen und sie über das Recht, Einspruch zu erheben (§ 106) und eine gerichtliche Entscheidung über die Aufhebung oder Fortsetzung der Sicherstellung zu beantragen (§ 115), zu informieren. Von einer Sicherstellung zur Sicherung einer Entscheidung über privatrechtliche Ansprüche (§ 110 Abs. 1 Z 2) ist, soweit möglich, auch das Opfer zu verständigen.

er die Herstellung einer Kopie oder von Bild- und Tonaufnahmen der auf dem Datenträger gespeicherten Informationen zu dulden.

(3) Personen, die nicht selbst der Tat beschuldigt sind, sind auf ihren Antrag die angemessenen und ortsüblichen Kosten zu ersetzen, die ihr durch die Trennung von Urkunden oder sonstigen beweiserheblichen Gegenständen von anderen oder durch die Ausfolgung von Kopien notwendigerweise entstanden sind.

(4) In jedem Fall ist der von der Sicherstellung betroffenen Person sogleich oder längstens binnen 24 Stunden eine Bestätigung über die Sicherstellung auszufolgen oder zuzustellen und sie über das Recht, Einspruch zu erheben (§ 106) und eine gerichtliche Entscheidung über die Aufhebung oder Fortsetzung der Sicherstellung zu beantragen (§ 115), zu informieren. Von einer Sicherstellung zur Sicherung einer Entscheidung über privatrechtliche Ansprüche (§ 110 Abs. 1 Z 2) ist, soweit möglich, auch das Opfer zu verständigen.

§ 111a. (1) Wurde ein Datenträger sichergestellt, so ist eine Kopie der darauf gespeicherten sowie der in einem nicht öffentlichen Netzwerk über diesen Datenträger verfügbaren Daten anzufertigen, an der die Strafverfolgungsbehörden die Auslesung und Auswertung vornehmen. Solche Daten, die nur in verborgener Form darauf vorhanden sind, dürfen innerhalb von sechs Wochen wiederhergestellt werden. Die Staatsanwaltschaft hat diejenigen Daten zum Akt zu nehmen, die für das Verfahren von Bedeutung sind und als Beweismittel verwendet werden dürfen (Abs. 5, §§ 144, 152 Abs. 2).

(2) Der von der Sicherstellung eines Datenträgers betroffenen Person ist unverzüglich, längstens jedoch binnen vierzehn Tagen, eine Kopie der Daten auszuhändigen, die mit der Kopie, an der die Strafverfolgungsbehörden ihre Auslesung und Auswertung vornehmen (Abs. 1 Satz 1), vollständig übereinstimmt. Wenn dies wegen besonderer Schwierigkeiten nicht möglich ist, erstreckt sich dies Frist auf acht Wochen. Wurden weitere Daten rekonstruiert (Abs. 1 Satz 2), so ist der betroffenen Person unverzüglich auch eine Kopie der wiederhergestellten Inhalte auszuhändigen. Sofern

der Rückstellung des Originaldatenträgers keine Gründe gemäß § 110 Abs. 1 Z 2 und 3 entgegenstehen, ist dieser der betroffenen Person zurückzustellen.

(3) Auf Antrag der betroffenen Person oder von Amts wegen sind die von einem sichergestellten Datenträger kopierten Daten (Abs. 1) zu löschen, wenn diese für ein Strafverfahren nicht von Bedeutung sein können oder als Beweismittel nicht verwendet werden dürfen.

(4) Auf Antrag des Beschuldigten, der von der Sicherstellung eines Datenträgers betroffen ist, sind weitere Daten zum Akt zu nehmen, wenn diese für das Verfahren von Bedeutung sind und ihre Verwendung als Beweismittel zulässig ist (Abs. 5, § 144, 157 Abs. 2).

(5) Als Beweismittel dürfen die durch das Auslesen und Auswerten eines Kommunikationsgerätes ermittelten Daten bei sonstiger Nichtigkeit nur verwendet werden,

1. wenn die Voraussetzungen für die Ermittlungsmaßnahme nach § 110 Abs. 1a vorlagen,

2. wenn die Ermittlungsmaßnahme gemäß § 110 Abs. 2 zweiter Satz rechtmäßig angeordnet und bewilligt wurde,

3. wenn sie unter Einhaltung der Fristen nach Abs. 2 mitgeteilt wurden und

4. nur zum Nachweis einer vorsätzlich begangenen strafbaren Handlung, derentwegen die Ermittlungsmaßnahme angeordnet wurde oder hätte angeordnet werden können.

(6) Werden bei Auslesen und Auswerten eines Kommunikationsgerätes (§ 110 Abs. 1a) Hinweise auf die Begehung einer anderen strafbaren Handlung als derjenigen, die Anlass zur Sicherstellung gegeben hat, gefunden, so ist mit diesem Teil ein gesonderter Akt anzulegen, soweit die Verwendung als Beweismittel zulässig ist (Abs. 3a, § 144, § 157 Abs. 2).

§ 112. (1) Widerspricht die von der Sicherstellung betroffene oder anwesende Person, auch wenn sie selbst der Tat beschuldigt ist, der Sicherstellung von schriftlichen Aufzeichnungen oder Datenträgern unter Berufung auf ein gesetzlich anerkanntes Recht auf Verschwiegenheit, das bei sonstiger Nichtigkeit nicht durch Sicherstellung umgangen werden darf, so sind diese Unterlagen auf geeignete Art und Weise gegen unbefugte Einsichtnahme oder Veränderung zu sichern und bei Gericht zu hinterlegen. Auf Antrag des Betroffenen sind die Unterlagen jedoch bei der Staatsanwaltschaft zu hinterlegen, die sie vom Ermittlungsakt getrennt aufzubewahren hat. In beiden Fällen dürfen die Unterlagen von Staatsanwaltschaft oder Kriminalpolizei nicht eingesehen werden, solange nicht über die Einsicht nach den folgenden Absätzen entschieden worden ist.

(2) Der Betroffene ist aufzufordern, binnen einer angemessenen, 14 Tage nicht unterschreitenden Frist jene Teile der Aufzeichnungen oder Datenträger konkret zu bezeichnen, deren Offenlegung eine Umgehung seiner Verschwiegenheit bedeuten würde; zu diesem Zweck ist er berechtigt, in die hinterlegten Unterlagen Einsicht zu nehmen. Unterlässt der Betroffene eine solche Bezeichnung, so sind die Unterlagen zum Akt zu nehmen und auszuwerten. Anderenfalls hat das Gericht, im Fall eines Antrags nach Abs. 1 vorletzter Satz jedoch die Staatsanwaltschaft die Unterlagen unter Beiziehung des Betroffenen sowie gegebenenfalls geeigneter Hilfskräfte oder eines Sachverständigen zu sichten und anzuordnen, ob und in welchem Umfang sie zum Akt genommen werden dürfen. Unterlagen, die nicht zum Akt genommen werden, sind dem Betroffenen auszufolgen. Aus deren Sichtung gewonnene Erkenntnisse

§ 112. (1) Widerspricht die von der Sicherstellung betroffene Person oder eine zu ihrer Vertretung anwesende Person, auch wenn die betroffene Person selbst der Tat beschuldigt ist, der Sicherstellung von schriftlichen Aufzeichnungen oder Datenträgern unter Berufung auf ein der betroffenen Person zukommendes gesetzlich anerkanntes Recht auf Verschwiegenheit, das bei sonstiger Nichtigkeit nicht durch Sicherstellung umgangen werden darf, so sind diese Unterlagen auf geeignete Art und Weise gegen unbefugte Einsichtnahme oder Veränderung zu sichern und bei Gericht zu hinterlegen. Auf Antrag des zur Verschwiegenheit berechtigten Betroffenen sind die Unterlagen jedoch bei der Staatsanwaltschaft zu hinterlegen, die sie vom Ermittlungsakt getrennt aufzubewahren hat. In beiden Fällen dürfen die Unterlagen von Staatsanwaltschaft oder Kriminalpolizei nicht eingesehen werden, solange nicht über die Einsicht nach den folgenden Absätzen entschieden worden ist.

(1a) Das Widerspruchsrecht nach Abs. 1 kommt dem Beschuldigten und einer nicht zur Vertretung des verschwiegenheitsberechtigten Betroffenen befugten Hilfskraft in Bezug auf solche Aufzeichnungen und Datenträger zu, durch deren Sicherstellung ein Verschwiegenheitsrecht im Sinne von Abs. 1 umgangen werden könnte (§ 157 Abs. 2).

(2) Der zur Verschwiegenheit berechtigte Betroffene (Abs. 1) ist aufzufordern, binnen einer angemessenen, 14 Tage nicht unterschreitenden Frist jene Teile der Aufzeichnungen oder Datenträger konkret zu bezeichnen, deren Offenlegung eine Umgehung seines Verschwiegenheitsrechts bedeuten würde; haben Hilfskräfte oder Beschuldigte widersprochen (Abs. 1a), so sind davor diese zur Bezeichnung aufzufordern. Zum Zweck der Bezeichnung sind der zur Verschwiegenheit berechtigte Betroffene sowie die in Abs. 1a erwähnten Personen berechtigt, in die hinterlegten Unterlagen Einsicht zu nehmen. Unterlassen sie eine solche Bezeichnung, so sind die Unterlagen zum Akt zu nehmen und auszuwerten. Anderenfalls hat das Gericht, im Fall eines Antrags nach Abs. 1 vorletzter Satz jedoch die Staatsanwaltschaft die Unterlagen unter Beiziehung der zur Verschwiegenheit berechtigten Betroffenen sowie

dürfen bei sonstiger Nichtigkeit nicht für weitere Ermittlungen oder als Beweis verwendet werden.	gegebenenfalls geeigneter Hilfskräfte oder eines Sachverständigen zu sichten und anzuordnen, ob und in welchem Umfang sie zum Akt genommen werden dürfen. Unterlagen, die nicht zum Akt genommen werden, sind dem Betroffenen auszufolgen. Aus deren Sichtung gewonnene Erkenntnisse dürfen bei sonstiger Nichtigkeit nicht für weitere Ermittlungen oder als Beweis verwendet werden.
(3) Gegen die Anordnung der Staatsanwaltschaft kann der Betroffene Einspruch erheben, in welchem Fall die Unterlagen dem Gericht vorzulegen sind, das zu entscheiden hat, ob und in welchem Umfang sie zum Akt genommen werden dürfen; Abs. 2 letzter Satz gilt. Einer Beschwerde gegen den Beschluss des Gerichts kommt aufschiebende Wirkung zu.	(3) Gegen die Anordnung der Staatsanwaltschaft kann der zur Verschwiegenheit berechtigte Betroffene Einspruch erheben, in welchem Fall die Unterlagen dem Gericht vorzulegen sind, das zu entscheiden hat, ob und in welchem Umfang sie zum Akt genommen werden dürfen; Abs. 2 letzter Satz gilt. Einer Beschwerde gegen den Beschluss des Gerichts kommt aufschiebende Wirkung zu.

ZEHNTER ABSCHNITT

§ 157. (1) Zur Verweigerung der Aussage sind berechtigt: … (2) Das Recht der in Abs. 1 Z 2 bis 5 angeführten Personen, die Aussage zu verweigern, darf bei sonstiger Nichtigkeit nicht umgangen werden, insbesondere nicht durch Sicherstellung und Beschlagnahme von Unterlagen oder auf Datenträgern gespeicherten Informationen oder durch Vernehmung der Hilfskräfte oder der Personen, die zur Ausbildung an der berufsmäßigen Tätigkeit nach Abs. 1 Z 2 bis 4 teilnehmen. Dies gilt ebenso für Unterlagen und Informationen, die sich in der Verfügungsmacht des Beschuldigten oder eines Mitbeschuldigten befinden und zum Zwecke der Beratung oder Verteidigung des Beschuldigten durch eine in Abs. 1 Z 2 genannte Person von dieser oder vom Beschuldigten erstellt wurden.	**§ 157. (**1) Zur Verweigerung der Aussage sind berechtigt: … (2) Das Recht der in Abs. 1 Z 2 bis 5 angeführten Personen, die Aussage zu verweigern, darf bei sonstiger Nichtigkeit nicht umgangen werden, insbesondere nicht durch Sicherstellung und Beschlagnahme von Unterlagen oder Datenträgern oder durch Vernehmung der zur Aufgabenerfüllung eingesetzten internen oder externen Hilfskräfte oder der Personen, die zur Ausbildung an der berufsmäßigen Tätigkeit nach Abs. 1 Z 2 bis 4 teilnehmen. Dies gilt ebenso für Unterlagen und Informationen, die sich in der Verfügungsmacht des Beschuldigten oder eines Mitbeschuldigten befinden und zum Zwecke der Beratung oder Verteidigung des Beschuldigten durch eine in Abs. 1 Z 2 genannte Person von dieser oder vom Beschuldigten erstellt wurden.