Sicherstellung im digitalen Zeitalter

Cloud Computing und Verschlüsselung bergen Hürden für Ermittler

Christopher Schrank / Alexander Stücklberger / Aaron Kleinbrod

Das digitale Zeitalter hat die Funktionsweise der Datenspeicherung revolutioniert. Was für die meisten eine Erleichterung bedeutet, bereitet Strafverfolgungsbehörden mitunter Kopfschmerzen. Dies wird insb bei der Sicherstellung digitaler Daten sichtbar, bei der moderne Cloud-Speicher und ausgereifte Verschlüsselungsmethoden die Ermittler vor neue Herausforderungen stellen. Dieser Beitrag untersucht, wie weit die Befugnisse der Behörden in Verbindung mit neuen Technologien tatsächlich reichen und wo die StPO an ihre Grenzen stößt.

1. Auf der Suche nach Daten

Die neben Vernehmungen wohl wichtigste Ermittlungshandlung bei Wirtschaftsstrafsachen ist die Sicherstellung. In einer digitalisierten (Wirtschafts-)Welt gewinnen dabei vor allem Daten zunehmend an Bedeutung und haben die Relevanz physischer Unterlagen längst überholt.

Moderne digitale Lösungen stellen die Ermittler jedoch häufig vor Probleme: Die Sicherstellung als Begründung physischen Gewahrsams stößt nämlich gerade dann an ihre Grenzen, wenn sich die gesuchten Daten nicht auf dem jeweils verfügbaren Gerät befinden, sondern vom jeweiligen Gerät nur über Netzwerke, insb das Internet, abgerufen werden können. Dies ist vor allem bei den stark auf dem Vormarsch befindlichen Cloud-Lösungen, in die ganze Unternehmen ihre Datenspeicherung auslagern, problematisch: Mit der Gewahrsame am Endnutzergerät, zB einem Computer, geht dann nämlich nicht auch die Gewahrsame an den Daten einher, weil sich diese nicht am Gerät befinden. Dadurch verlagern sich die Ermittlungen faktisch häufig weg von den tatsächlich am untersuchten Sachverhalt beteiligten Personen bzw Örtlichkeiten hin zu den Dienstanbietern, die sich ihrerseits mit Sicherstellungen und anderen Ermittlungsmaßnahmen konfrontiert sehen.

Des Weiteren stoßen Ermittler häufig an ihre Grenzen, wenn Daten verschlüsselt gespeichert werden. Viele kostengünstige oder gar gratis verfügbare Verschlüsselungssysteme sind so sicher, dass – ohne Herausgabe von Zugangsdaten oder Entschlüsselungscodes und damit der Kooperation Betroffener, die in vielen Fällen auch Beschuldigte sind – faktisch kein Auslesen der Daten möglich ist. Die Ermittler suchen daher häufig Wege, unverschlüsselte bzw unversperrte Endnutzergeräte sicherzustellen oder – mangels Kooperation der Verfügungsberechtigten – die Zugangscodes anderweitig herauszufinden.

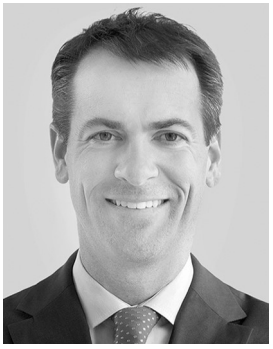
Beide in einer digitalisierten Welt durchaus notwendigen Ermittlungswege dürfen selbstverständlich nur im Rahmen der bestehenden StPO gegangen werden, die für diese Schritte keine maßgeschneiderten Lösungen anbietet. Dieser Beitrag untersucht, was Ermittler tatsächlich dürfen und wo sie faktisch wie rechtlich an ihre Grenzen stoßen.

2. Reichweite der Sicherstellung bei Cloud Services

Solange die Kriminalpolizei in der Lage ist, Datenträger und Geräte sicherzustellen, auf denen unverschlüsselte oder entschlüsselbare Daten gespeichert sind, ist die Rechtslage klar: Die Ermittler dürfen und können alle auf einem physisch sichergestellten Datenträger lokal gespeicherten (= statischen) Daten auswerten und benötigen dafür weder gesonderte Anordnungen noch gerichtliche Bewilligungen. Der Gesetzgeber unterscheidet nicht danach, ob Informationen auf Papier oder zB in einem Textverarbeitungsprogramm festgehalten werden. Dies gilt auch für Daten aus Kommunikation (zB E-Mails, Chats), die bereits gesendet bzw empfangen wurden und noch immer auf dem Datenträger gespeichert sind. Nicht heranzuziehen sind in diesem Fall die Bestimmungen über die Nachrichtenüberwachung, weil eine solche eben gerade nicht vorliegt. Zwar handelt es sich bei E-Mails um Nachrichten iSd § 134 Z 3 StPO, jedoch erfolgt hier der Zugriff losgelöst von einer laufenden Kommunikation in der Sphäre des Betroffenen. Dieser ist sohin selbst dafür verantwortlich, ob er die E-Mails weiterhin auf dem Datenträger belässt (und sie somit gegebenenfalls dem Zugriff der Strafverfolgungsbehörden aussetzt) oder löscht.

2.1. Externe Server

Die digitale Infrastruktur in Unternehmen ändert sich jedoch. Interne und externe Fileserver sowie generell die Auslagerung von Rechen- und Speicherleistung an externe Dienstleister in der Cloud werden immer mehr zum Regelfall. Die gesuchten Daten befinden sich dann eben nicht auf dem physischen Datenträger vor Ort, den die Ermittler sicherstellen können und wollen. Vielmehr ist es zum Erhalt der Daten erforderlich, einen Telekommunikationsvorgang zwischen dem lokalen Gerät und dem externen Rechner auszulösen.



MMag. Dr. Christopher Schrank ist Partner der Brandl & Talos Rechtsanwälte GmbH in Wien.

Mag. Alexander Stücklberger ist Rechtsanwaltsanwärter bei der Brandl & Talos Rechtsanwälte GmbH in Wien.

Aaron Kleinbrod ist juristischer Mitarbeiter bei der Brandl & Talos Rechtsanwälte GmbH in Wien.

Das deutsche Strafprozessrecht hat diesen Fall bereits aufgegriffen. So regelt § 110 Abs 3 dStPO die Durchsicht elektronischer Speichermedien und verweist dabei explizit auch auf *„räumlich getrennte Speichermedien"* (sog Online-Sichtung). Voraussetzung ist jedoch, dass die Durchsicht dieser Serverdaten vom Speichermedium aus erfolgt. Die deutsche Rechtslage ermöglicht es den Ermittlern daher, auch externe Datenbestände auszuwerten, allerdings nur vom zuvor sichergestellten Datenträger aus.[1]

Die StPO regelt dieses Thema hingegen nicht ausdrücklich. Die Mat zu § 111 Abs 2 StPO[2] beziehen zwar auch externe Datenbestände mit ein. Der Begriff des externen Datenbestands darf allerdings nicht zu weit verstanden werden. Die ErlRV wählen in diesem Zusammenhang nämlich den Ausdruck *„im Netzverbund befindlicher Datenserver"* und dehnen somit den Anwendungsbereich der §§ 110 ff StPO gerade nicht für sämtliche externe Datenbestände aus. Demnach dürfen uE lediglich jene externen Daten, also Daten auf einem anderen Gerät als dem sichergestellten, sichergestellt werden, die sich im Zeitpunkt der Sicherstellung in einem lokalen Netzwerk (= Netzverbund) befinden. Zu denken ist etwa an lokale File- oder Mailserver, wobei sich die Sicherstellungsanordnung freilich auch auf diese Server beziehen muss.[3] Nicht erfasst sind hingegen Daten, die sich auf Cloud-Speichern wie etwa *iCloud* oder *Google Drive* befinden und nur über eine aktive Internetverbindung abgerufen werden können. Dies würde der Gegenstandsbezogenheit der Sicherstellung zuwiderlaufen.[4] Dass die Ermittler nämlich Daten, die sich im Sicherstellungszeitpunkt weder am Datenträger noch am Fileserver befinden, zuerst von einem Cloud-Speicher herunterladen und sodann sicherstellen, geht offenkundig über die Ermächtigung der §§ 110 ff StPO hinaus.

Am Beispiel von E-Mail-Kommunikation bedeutet dies somit Folgendes: Die Strafverfolgungsbehörden dürfen die auf einem Smartphone oder PC im Zeitpunkt der Sicherstellung befindlichen E-Mails sicherstellen. Dies gilt unabhängig davon, ob diese auf dem sicherzustellenden Gerät selbst abgespeichert sind oder nur über den lokalen Mailserver abgerufen werden können. In letzterem Fall ist Voraussetzung, dass das Endgerät direkt mit dem Mailserver verbunden ist (Netzverbund) und es keiner aktiven Internetverbindung zur Beschaffung der E-Mails bedarf.

Logische Schlussfolgerung dieser Abgrenzung ist auch, dass nur jene (im Beispiel) E-Mails sichergestellt werden dürfen, die sich im Zeitpunkt der Sicherstellung bereits vollständig am Endgerät bzw am Mailserver befunden haben. Die Sicherstellung ermöglicht damit eine Momentaufnahme des Datenbestands.[5] Das Auslesen der laufenden Kommunikation durch späteres Aktualisieren des Mailservers wäre hingegen nicht mehr zulässig, weil dazu eine Internetverbindung und damit Telekommunikation erforderlich ist.

2.2 Erhebungen beim Internetdienstleister

Die bisherigen Ausführungen haben sich darauf bezogen, dass die Strafverfolgungsbehörden beweiserhebliches Datenmaterial bei Endnutzern sicherstellen. Mitunter richten die Behörden ihre Anordnungen jedoch auch direkt an Internetdienstleister, um an die dort gespeicherten Nutzerdaten zu gelangen. Dienstleister wie *Google* und *Facebook* führen weitreichende Datenbanken, in denen neben *„ausdrücklicher"* Kommunikation auch Standortdaten oder Gesundheitsdaten gespeichert werden, die für Strafverfolgungsbehörden von großem Interesse sein können. Die weitreichenden Möglichkeiten dieser Daten und auch die Gefahr dahinter zeigt ein Beispiel aus dem US-Bundesstaat Florida, wo ein ahnungsloser Radfahrer eines Einbruchsdiebstahls bezichtigt wurde, weil er innerhalb einer Stunde zufälligerweise dreimal am Tatort vorbeifuhr. Dabei verwendete er eine Fitness-App, die seine Standortdaten nutzte, wobei diese Daten auch an *Google* weitergeleitet wurden. Durch eine simple Standortabfrage bei *Google* entdeckte die US-amerikanische Polizei sodann das verdächtige Bewegungsprofil des Radfahrers und fokussierte ihre Ermittlungen auf ihn. Das Missverständnis konnte jedoch aufgeklärt werden.[6]

Ungeachtet dieses unglücklichen Einzelfalls liegt es auf der Hand, dass derartige Daten die Arbeit von Ermittlern erheblich vereinfachen können.[7] Auf den ersten Blick wäre es naheliegend, dass im Rahmen der StPO schlicht eine Sicherstellung der Datenträger beim Dienstleister vorgenommen wird.[8] Da dieser in aller Regel nicht selbst beschuldigt sein wird, träfe diesen sogar eine (zwangsweise durchsetzbare) Herausgabeverpflichtung (§ 111 Abs 1 StPO). Tatsächlich ist dies aber zu kurz gedacht:

Soweit das gegenwärtige bzw künftige Kommunikationsverhalten des Users untersucht

1 *Zerbes/El-Ghazi*, Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung, ZStW 2015, 425 (428); vgl auch *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 5.12.

2 ErlRV 25 BlgNR 22. GP zu § 111 StPO.

3 *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO, § 111 Rz 14.

4 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht, Rz 5.11, 5.15.

5 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht, Rz 5.16.

6 Siehe https://www.derstandard.at/story/2000115521019/wie-ein-radfahrer-wegen-google-daten-des-einbruchs-verdaechtigt-wurde (Zugriff am 2. 11. 2020).

7 Wenngleich die Dienstleister in einigen Fällen selbst nicht über die gesuchten Daten in unverschlüsselter Form verfügen, zB bei verschlüsselten Instant Messaging Services.

8 Dies ist die – tatsächlich rechtswidrige – häufig gewählte Vorgehensweise der österreichischen Strafverfolgungsbehörden.

werden soll, liegt ohnehin unzweifelhaft eine Überwachung von Nachrichten (§ 134 Z 3 StPO) vor, deren Voraussetzungen sich nach den §§ 134 ff StPO richten. Als Dienste der Informationsgesellschaft (§ 134 Z 3 StPO iVm § 1 Abs 1 Z 2 NotifG) unterliegen dabei alle gängigen Anbieter, darunter etwa auch *Google* und *Facebook*,[9] den vorgenannten Bestimmungen. Überwacht werden dabei Kommunikationsinhalte (Inhaltsdaten), wobei der Kommunikationsbegriff (spätestens) seit dem StPRÄG 2018[10] ein klar technischer ist. Umfasst ist neben dem Austausch von Nachrichten zwischen zwei natürlichen Personen (zB via *Gmail*) auch die Übermittlung von Inhalten von einer Person zu einem Rechner.[11] Werden also etwa Daten zur Speicherung in eine Cloud hochgeladen (zB via *Google Drive*) oder Kalendereinträge mit einem Server synchronisiert (zB via *Google Calendar*), so gilt dies ebenfalls als Kommunikation. All diese Datentransfers können somit bei Vorliegen der Voraussetzungen der §§ 134 ff StPO ebenfalls überwacht werden – was aber an sehr hohe Anforderungen und eine gerichtliche Bewilligung geknüpft ist.

Dasselbe gilt jedoch auch für vergangene Zeiträume: Da hier in aller Regel kein aktiver Eingriff in den Kommunikationsprozess mehr erfolgt, wäre eine Sicherstellung dieser Datenbestände theoretisch zwar denkbar. Die wohl überwiegende Lit[12] hat dazu jedoch einen überzeugend differenzierten Lösungsansatz geschaffen: Werden die Daten eines vergangenen Zeitraums beim Internetdienstleister ermittelt, müssen die Voraussetzungen der §§ 134 ff StPO weiterhin vorliegen, und zwar selbst dann, wenn der User die am Server des Internetdienstleisters vorhandenen Daten bereits abgerufen (etwa heruntergeladen) hat. Dies wird zutreffend damit begründet, dass ein höheres Schutzbedürfnis des Users besteht, wenn Inhaltsdaten beim Internetdienstleister ermittelt werden.[13] Der entscheidende Gesichtspunkt ist dabei, dass in diesen Fällen der Betroffene die Herrschaft über seine persönlichen Daten teilweise dem Internetdienstleister anvertraut. Selbst wenn der User nämlich Datenpakete abruft, bleiben diese weiterhin am Server gespeichert und befinden sich somit (auch) im Einflussbereich des Internetdienstleisters. Dadurch hat der User wiederum nicht die letzte Entscheidung darüber, was mit seinen Daten geschieht. So kann es etwa passieren, dass der User E-Mails auf seinem Endgerät löscht, diese aber weiterhin am Server des Internetdienstleisters gespeichert bleiben und somit dem Zugriff der Strafverfolgungsbehörden ausgesetzt sind. Diese fehlende Beherrschbarkeit rechtfertigt die strengeren Eingriffsvoraussetzungen der §§ 134 ff StPO, möchten die Ermittler die Daten direkt vom Internetdienstleister erhalten. Erheben die Strafverfolgungsbehörden die Daten hingegen nicht beim Internetdienstleister, sondern beim User selbst, kommen die allgemeinen Regeln der Sicherstellung zur Anwendung.[14] Hier gilt das zur Sicherstellung von Kommunikationsdaten bereits Gesagte (vgl Pkt 1. und 2.).

3. Umgang mit verschlüsselten Daten

Ein eigenes Problemfeld bilden verschlüsselte Daten. Stellen die Strafverfolgungsbehörden nämlich einen Datenträger sicher, müssen sie diesen häufig entsperren bzw entschlüsseln, bevor sie auf die darauf befindlichen Daten zugreifen können. Hierfür benötigen sie die Zugangscodes des Verfügungsberechtigten. Abhängig davon, ob es sich beim Verfügungsberechtigten um einen bloß Betroffenen oder aber um einen Beschuldigten (bzw eine andere Person mit Schweigerecht) handelt, bestehen unterschiedliche Herausgabe- und Mitwirkungspflichten.[15] Bloß Betroffene sind verpflichtet, allfällige Zugangscodes bzw Passwörter nach Aufforderung preiszugeben. Weigern sie sich, können ihnen gegenüber Beugemittel verhängt werden.[16] Beschuldigte dürfen hingegen nicht zur Mitwirkung (dh auch nicht zur Herausgabe von Zugangscodes) gezwungen werden. Dies ergibt sich aus dem Verbot des Zwangs zur Selbstbelastung (*Nemo-tenetur*-Prinzip), das in § 7 Abs 2 StPO statuiert ist und sich auch aus Art 90 Abs 2 B-VG (Anklagegrundsatz) sowie Art 6 EMRK (Recht auf ein faires Verfahren) ableitet.[17]

Beschuldigte müssen es allerdings dulden, dass die Strafverfolgungsbehörden versuchen, den Datenträger auf eigene Faust zu entsperren. Insofern die Ermittler den Datenträger dabei nicht beschädigen (etwa durch Verwendung schädlicher Software), ist ihnen die Wahl allfälliger Entschlüsselungsmethoden frei überlassen.[18] Neben der Verwendung von Entschlüsselungs- und Cracking-Programmen kommt auch die Zuhilfenahme externer Dienstleister in Betracht.[19] Was theoretisch einfach klingt, ist praktisch jedoch mit sehr viel Aufwand und oftmals

9 *Thiele*, Persönlichkeitsschutz in Neuen Medien – Facebook, Google & Co, AnwBl 2013, 11 (13).

10 BGBl I 2018/27.

11 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht, Rz 5.18.

12 *Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO, § 134 Rz 49 ff; *Venier* in *Bertel/Venier*, Komm StPO, § 111 Rz 2; zweifelnd *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO, § 111 Rz 16.

13 *Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO, § 134 Rz 51, 53; die staatsanwaltschaftliche Praxis sieht freilich in vielen Fällen anders aus.

14 *Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO, § 134 Rz 52; *Venier* in *Bertel/Venier*, Komm StPO, § 135 Rz 7; sinngemäß OGH 15. 2. 2007, 15 Os 20/06i.

15 *Bauer*, Ausgewählte beweissichernde Zwangsmittel in der neuen StPO, ÖJZ 2008, 754 (755).

16 *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO, § 111 Rz 8, 13; *Vogl* in *Fuchs/Ratz*, WK StPO, § 93 Rz 46.

17 *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO, Vor §§ 110–115 Rz 40 mwN; OGH 27. 8. 2015, 1 Ob 123/15t.

18 *Zerbes*, Einsatz von Spionagesoftware bei Sicherstellung und Durchsuchung, in *Lewisch* (Hrsg), Wirtschaftsstrafrecht und Organverantwortlichkeit. Jahrbuch 14 (2014) 199 (204).

19 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht, Rz 5.5.

auch hohen Kosten verbunden – sofern es überhaupt möglich ist.[20] Dieses Umstands sind sich die Ermittler bewusst, weshalb sie in der Praxis auf zum Teil trickreiche Methoden zurückgreifen, um den relevanten Datenträger (zB ein Smartphone) möglichst im entsperrten Zustand sicherzustellen oder die Zugangscodes herauszufinden.

Die Kriminalpolizei kann einen günstigen Zeitpunkt abwarten, in dem der Beschuldigte unbedacht sein Smartphone entsperrt. Entreißen (vgl § 93 Abs 1 StPO) sie dem Beschuldigten das entsperrte Telefon, ist dies keine Verletzung des *Nemo-tenetur*-Prinzips, weil kein Zwang zur aktiven Mitwirkung an der Schaffung von selbstbelastendem Material geübt wurde.[21] Die Polizisten haben letztlich in keiner Weise auf den Willen des Beschuldigten eingewirkt, sondern sich lediglich sein unvorsichtiges Verhalten zu Nutze gemacht. In dieser Hinsicht wäre der Beschuldigte dann zur Duldung der zwangsweisen Sicherstellung verpflichtet.

Eine andere Möglichkeit bildet das Entsperren von Datenträgern mittels biometrischer Verfahren. Wenngleich die Ausübung von Zwang zur Erlangung (neuer) selbstbelastender Äußerungen des Beschuldigten unzulässig ist, dürfen bereits bestehende Beweismaterialien verwertet werden. Der EGMR hat diesbezüglich unter Bezugnahme auf Art 6 EMRK judiziert,[22] dass etwa die Erhebung von Blutproben, DNA-Material und Fingerabdrücken gegen den Willen des Beschuldigten zulässig ist. Grund dafür ist, dass diese Indizien unabhängig vom Willen des Beschuldigten existieren und es keiner aktiven Mitwirkung des Beschuldigten zur Erlangung dieser Beweismaterialien bedarf.[23] Möchte die Kriminalpolizei daher die Fingerabdrücke des Beschuldigten zur Identitätsfeststellung registrieren (§ 118 Abs 2 StPO), so muss dieser das dulden.[24] Gekoppelt mit einer Sicherstellungsanordnung nach §§ 110 ff StPO wird es (in Anlehnung an das deutsche Schrifttum[25]) aber auch zulässig sein, den Finger des Beschuldigten zur Geräteentsperrung an den Fingerabdrucksensor zu halten. Gleiches muss sinngemäß für Iris- und Gesichtskennungen gelten. Hier wird nämlich wiederum ein bloßes Dulden des Beschuldigten als *„objektiver Personalbeweis"* gefordert. Das *Nemo-tenetur*-Prinzip wird dadurch nicht verletzt.

Andere Methoden der Ermittler gehen dahin, dem Beschuldigten mittels vermeintlich kooperativen Verhaltens falsche Intentionen vorzuspiegeln. Die Kriminalpolizisten „empfehlen" dem Beschuldigten zB zu Beginn der anstehenden Hausdurchsuchung, seinen Anwalt zu kontaktieren. Beim Entsperren des Smartphones beobachtet nun einer der Ermittler den Beschuldigten und findet so den Zugangscode heraus – oder die Kriminalpolizisten entreißen dem Beschuldigten das Smartphone nach dem Entsperren bzw während des Telefonats und verschaffen sich dadurch Zugang zum (entsperrten) Gerät. Diese Situationen mögen auf den ersten Blick jener zuvor gleichen (Beschuldigter entsperrt unbedacht sein Smartphone), weisen jedoch ein ganz wesentliches Unterscheidungsmerkmal auf: Im zuerst behandelten Fall entsperrt der Beschuldigte das Smartphone nämlich ohne Zutun der Ermittler, wohingegen die Ermittler in den hier genannten Fällen auf den Beschuldigten aktiv einwirken. Darin kann – insb wenn der Beschuldigte zuvor bereits die Herausgabe seiner Zugangsdaten verweigert hat – ein Täuschungsmanöver der Ermittler gesehen werden, um den Willen des Beschuldigten zu beugen bzw zu umgehen: Dem Beschuldigten wird suggeriert, dass er seinen Zugangscode „in Sicherheit" eingeben kann. Selbst wenn er es im Zeitpunkt des Entsperrens noch nicht weiß, unterstützt er dadurch allerdings die Behörden bei den Ermittlungen gegen ihn. Zu dieser Handlung wurde er zwar nicht durch unmittelbaren Zwang genötigt, durch Vorspiegelung falscher Kooperationsbereitschaft jedoch bewogen, was uE eine Umgehung des *Nemo-tenetur*-Prinzips darstellt.

Der EGMR postuliert in seiner Rsp zu Art 6 EMRK nämlich einen weitgehenden Umgehungsschutz des *Nemo-tenetur*-Prinzips.[26] Demnach muss der Staat den Willen des Beschuldigten, schweigen zu wollen, respektieren. Daran fehlt es aber unzweifelhaft, wenn der Staat die Freiwilligkeit zwar nicht durch Druck, wohl aber durch Täuschungen untergraben darf. Der Rückgriff auf Informationen, die aus Täuschungen stammen und anderweitig nicht hätten erlangt werden können, sind daher mit dem Recht auf ein faires Verfahren unvereinbar.[27] Zwar bezieht sich diese Rsp auf Vernehmungen des Beschuldigten (und nicht auf Ermittlungsmaßnahmen im Rahmen einer Hausdurchsuchung). Das Verbot des Zwangs zur Selbstbelastung nach Art 6 EMRK gilt jedoch für das gesamte Strafverfahren, weshalb die Rsp des EGMR als solche auch analog auf Ermittlungshandlungen angewendet werden kann. Im Ergebnis ist ein aktives Hinwirken staatlicher Er-

[20] Siehe https://futurezone.at/netzpolitik/was-ermittler-mit-straches-handy-anstellen-koennen/400585820 (Zugriff am 2. 11. 2020).

[21] Vgl OGH 11. 10. 2016, 11 Os 60/16g.

[22] EGMR 17. 12. 1996, Bsw 19187/91, *Saunders* gg Großbritannien; 11. 7. 2006, Bsw 54810/00, *Jalloh* gg Deutschland; ÖJZ [MRK] 1998/1, 32.

[23] *Gaede* in MünchKomm StPO, Art 6 EMRK Rz 321; OGH 11. 10. 2016, 11 Os 60/16g.

[24] *Birklbauer* in *Fuchs/Ratz*, WK StPO, § 118 Rz 18 f.

[25] *Rottmeier/Eckel*, Die Entschlüsselung biometrisch gesicherter Daten im Strafverfahren, NStZ 2020, 193; *Bäumerich*, Verschlüsselte Smartphones als Herausforderung für die Strafverfolgung, NJW 2017, 2718.

[26] EGMR 5. 11. 2002, Bsw 48539/99, *Allan* gg Großbritannien.

[27] *Gaede*, Entscheidung des EGMR im Fall Allan v. Großbritannien, StV 2003, 257 (260 ff); *Gaede* in MünchKomm StPO, Art 6 EMRK Rz 331.

mittlungsbehörden darauf, dass ein Beschuldigter zB sein Handy entsperrt und so entweder der Zugangscode oder das entsperrte Gerät erlangt wird, unzulässig.

► Auf den Punkt gebracht

Stellen die Strafverfolgungsbehörden im Zuge einer Ermittlungsmaßnahme einen Datenträger sicher, dürfen sie diesen auswerten. Von der Reichweite der Sicherstellungsbefugnis umfasst sind dabei jedenfalls statische Daten, dh solche, die sich direkt auf dem Gerät befinden. Darüber hinaus dürfen die Ermittler auch auf solche Daten zugreifen, die sich (wie oft iZm E-Mail-Kommunikation) zwar nicht am Endgerät selbst, aber in einem mit diesem Endgerät gemeinsamen lokalen Netzverbund befinden (zB Mail- oder Dateiserver). Nicht erlaubt ist uE hingegen eine Ausweitung der Sicherstellungsbefugnis auch auf Cloud-Speicher, weil dies insb der Gegenstandsbezogenheit der Sicherstellung und deren Merkmal als Momentaufnahme zuwiderläuft. Ebenfalls unzulässig sind Sicherstellungen iZm Erhebungen direkt beim Internetdienstleister. Aufgrund des erhöhten Schutzbedürfnisses des Nutzers müssen die Ermittler hier auf die Nachrichtenüberwachung ausweichen und deren wesentlich höhere Anforderungen erfüllen.

Bei gesperrten oder verschlüsselten Datenträgern ist insb die Bedeutung des *Nemo-tenetur*-Prinzips hervorzuheben. So dürfen Beschuldigte nicht mittels Gewalt oder unter Androhung von Zwang genötigt werden, Passwörter udgl zur Entschlüsselung eines Datenträgers preiszugeben. Nicht verboten ist es dagegen, biometrische Merkmale von Beschuldigten zu nutzen, um damit moderne Verschlüsselungstechniken (Fingerabdruckscanner, Face-ID) zu bedienen. Dies aber auch nur insoweit, als die (mitunter trickreichen) Handlungen der Ermittler keine Umgehung des *Nemo-tenetur*-Prinzips begründen.