INTERNATIONALES

Oliver M. Loksa, Rechtsanwalt, Wien, und
Präsident der Austrian White Collar Crime Association

Länderbericht Österreich: Die Neuregelung der „Handy-Sicherstellung"

Mit 01.01.2025 sind in Österreich neue gesetzliche Bestimmungen in Kraft getreten, die die Möglichkeiten der Sicherstellung von Handys und auf ihnen befindliche bzw über sie einsehbare Daten für deren Auswertung regeln. Der vorliegende Beitrag bietet einen Überblick über die wichtigsten Eckpunkte und beleuchtet Kritikpunkte:

1. Hintergrund der Neuregelung

Bis zum Inkrafttreten der Neuregelung konnten Datenträger und Daten unter denselben Voraussetzungen sichergestellt werden wie gewöhnliche Gegenstände. Diese fehlende Unterscheidung zu einem Gerät, mit dem ein detaillierter Einblick in das Leben und die Persönlichkeit nicht nur des:der konkret Betroffenen, sondern auch Dritter gewonnen werden kann, stieß vielfach und langjährig auf Kritik unter Experten. Tätig wurde der Gesetzgeber schlussendlich, als der VfGH Mitte Dezember die bisherige Regelung aufhob.[1] In das Endstadium des Gesetzwerdungsprozesses hinein erließ überdies der EuGH eine separate Entscheidung, die bzgl einer europarechtskonformen Auslegung der österreichischen Rechtslage zu einem ähnlichen Schluss kam.[2]

Auch wenn sich (in Österreich) das Wort „Handysicherstellung" eingebürgert hat, handelt es sich nunmehr um eine Beschlagnahme, konkret um *„eine gerichtliche Entscheidung auf Begründung einer Sicherstellung von a. Datenträgern und Daten, b. Daten, die an anderen Speicherorten als einem Datenträger gespeichert sind, soweit auf sie von diesem aus zugegriffen werden kann, oder c. Daten, die auf Datenträgern oder an anderen Speicherorten gespeichert sind (lit. a und b), die zuvor nach Z 1 lit. a sichergestellt wurden"* (§ 109 Z 2a StPO).

Zweck der Ermittlungsmaßnahme ist jedenfalls stets die **Auswertung von Daten**. Um zu dieser zu gelangen, sind in den §§ 115f-115l StPO drei Schritte vorgesehen:

2. 3 Schritte von der Beschlagnahme zur Auswertung

2.1 Schritt 1: Beschlagnahme von Daten und Datenträgern (§ 115f StPO)

Eine Beschlagnahme ist zulässig, wenn sie aus Beweisgründen erforderlich scheint und aufgrund bestimmter Tatsachen anzunehmen ist, dass dadurch Informationen ermittelt werden können, die für die Aufklärung einer Straftat wesentlich sind (Abs 1). Ein Anfangsverdacht muss zu diesem Zeitpunkt bereits bestehen. Es ist demnach unzulässig, erst durch die Beschlagnahme einen Anfangsverdacht begründen zu wollen.

Um eine Beschlagnahme zu erwirken, bedarf es einer Anordnung der Staatsanwaltschaft, die vom zuständigen Haft- und Rechtsschutzgericht (Landesgericht) bewilligt werden muss. Mittels dieses Beschlusses wird anschließend die Kriminalpolizei um Durchführung der Ermittlungsmaßnahme ersucht (Abs 2). Das Prozedere entspricht im Wesentlichen jenem, das auch zB für die Durchführung einer Hausdurchsuchung vorgesehen ist.

Der Gesetzgeber hat damit bedauerlicherweise trotz immer wieder geäußerter Kritik[3] nicht die Chance genutzt, den sogenannten „Stampiglienbeschluss" abzuschaffen. Darunter ist die Praxis gemeint, gemäß der das Gericht keinen Be-

[1] VfGH 14. 12. 2023, G 352/2021 h.
[2] EuGH C-548/21, Bezirkshauptmannschaft Landeck, 04.10.2024.
[3] ZB: Schönborn/Seidl, Stampiglienbeschluss als rechtsstaatliches Feigenblatt, Die Presse 2024/05/05; Tipold in Fuchs/Ratz, WK StPO § 86 Rz 8/1 (Stand 15.3.2023, rdb.at); Reindl-Krauskopf, Das reformierte strafprozessuale Ermittlungsverfahren, ÖJZ 2020/78.

schluss separat verfasst, sondern die Anordnung der Staatsanwaltschaft „abstempelt". Der OGH vertritt die Auffassung, dass ein solches Vorgehen rechtskonform ist.[4]

Die staatsanwaltschaftliche Anordnung und die gerichtliche Bewilligung müssen eine **Beschreibung der zu beschlagnahmenden Datenkategorien und -inhalte** enthalten. Unter ersterem gemeint ist die Spezifizierung dessen, ob z. B. Kommunikationsdaten, Metadaten, Fotos, Videos, Standortdaten etc gesucht werden. Letzteres zielt auf das gesuchte Beweismaterial ab. Außerdem muss aus den Unterlagen ersichtlich sein, aus welchem **Zeitraum** Daten gesucht werden. Eine Ausnahme macht hiervon der Gesetzgeber in Fällen, in denen Daten aus technischen Gründen nicht einem bestimmbaren Zeitraum zuordenbar sind. Dies soll insb gelöschte und wiederhergestellte Daten betreffen, die keinen Zeitstempel aufweisen.

2.2 Schritt 2: Technische Aufbereitung der Daten

In der Praxis werden regelmäßig überschießend Daten sichergestellt (bzw beschlagnahmt). Daher ist in § 115h StPO nunmehr in einem zweiten Schritt eine **Reduktion** des beschlagnahmten Datensatzes auf jenen vorgesehen, der dem Beschluss entspricht (sogenanntes „Ergebnis der Datenaufbereitung" gem § 109 Z 2e StPO).

Dafür wird zunächst eine Originalsicherung der beschlagnahmten Daten erstellt. Anschließend wird daraus eine Arbeitskopie angefertigt, auf deren Basis die Herstellung des Ergebnisses der Datenaufbereitung erfolgt. Um die Transparenz und Nachvollziehbarkeit des Verfahrens zu gewährleisten, muss dieser Prozess umfassend in dokumentiert werden. Ausschließlich dieser Datensatz wird im anschließenden Schritt durchsucht und ausgewertet.

Dennoch sind die Originalsicherung und die Arbeitskopie bis zum rechtskräftigen Abschluss des Strafverfahrens **aufzubewahren**. Auf diese darf unter bestimmten Voraussetzungen auch **erneut zugegriffen** werden – vorausgesetzt, es wird hierfür eine neue gerichtliche Bewilligung eingeholt. Ein solches Bedürfnis wird sich ergeben und ist rechtens, wenn *„konkrete Tatsachen oder Umstände darauf schließen lassen, dass ein weiterer Zugriff […] erforderlich ist"* (§ 115f Abs. 5 StPO). Die Gesetzesmaterialien haben dabei Fälle im Blick, wenn zB ein Zeitraum von der gerichtlichen Bewilligung nicht erfasst war, sich aber aufgrund der Ermittlungen materialisierte, dass auch dieser zur Aufklärung der Straftat wesentlich ist; oder wenn technische Umstände bekannt werden, die die Prüfung der Verlässlichkeit der Daten erfordern.

2.3 Schritt 3: Auswertung von Daten

§ 115i Abs. 1 StPO sieht nunmehr ausdrücklich vor, dass StA und Kriminalpolizei Suchparameter zur gezielten Filterung der Daten festlegen und benutzen können (aber nicht müssen). Die verwendeten Suchparameter und die Anzahl der Treffer sind zu protokollieren.

Ziel dieses als **„Relevanzprüfung"** bezeichneten Prozesses ist die Identifizierung jener Informationen, die für das Verfahren relevant sind und als Beweismittel verwendet werden dürfen – und somit Aktenbestandteil werden.

3. Vorgehen bei Zufallsfunden

Nicht zuletzt bedingt durch die bekannten Korruptionsprozesse war der Umgang mit Zufallsfunden im Gesetzwerdungsprozess höchst umstritten. Denn diese Verfahren gründeten zu einem signifikanten Teil nicht auf Funden, wegen der Ermittlungsmaßnahmen ursprünglich angeordnet und durchgeführt worden waren.

Schlussendlich einigte sich der Gesetzgeber darauf, dass die Verwertung von Zufallsfunden wie bisher **verwertbar** bleibt. Die Chance bzw das Risiko auf solche zu treffen, soll jedoch reduziert werden. Erreicht werden soll dies dadurch, dass die Ermittlungsbehörde eben nicht mehr den gesamten, von ihr beschlagnahmten Datensatz ihren Ermittlungen zugrunde legen darf, sondern nur das Ergebnis der Datenaufbereitung. Die Datenmenge, die einen Zufallsfunde zu Tage fördern kann, ist somit eine **geringere**.

Gerät die Ermittlungsbehörde dennoch auf einen Zufallsfund, so muss ein neuer Ermittlungsakt angelegt werden, sofern die neuen Beweise verwertbar sind (§ 115j Abs. 2 StPO). Zulässig wird dann auch sein, erneut auf die Originalsicherung oder Arbeitskopie zugreifen zu können, wofür die Einholung eines neuen Beschlusses notwendig ist.

4. Rechtsschutzmöglichkeiten

Neben den im Wesentlichen unverändert anwendbaren allgemeinen Rechtsbehelfen (Kapitel 4.1) sieht die neue Rechtslage durchaus umfangreich und nicht auf Anhieb einfach zu überblickende weitere Rechtsschutzmöglichkeiten vor (Kapitel 4.2 – 4.4):

4.1 Rechtsbehelfe

Gegen die Anordnung der Beschlagnahme steht Betroffenen das Rechtsmittel des Einspruchs wegen Rechtsverletzung und gegen die gerichtliche Bewilligung das der Beschwerde zu. Der **Beschwerde** kommt keine aufschiebende Wirkung zu. Wird ihr jedoch insofern Folge gegeben, dass das Vorliegen eines Anfangsverdachts verneint wird, sind die beschlagnahmten Daten zu vernichten bzw ist der beschlagnahmte Datenträger zurückzustellen.

Sollte **vertrauliche Anwaltskorrespondenz** betroffen sein, so ist die Erhebung eines Widerspruchs gem § 112 StPO möglich. Mit diesem Rechtsbehelf werden die Daten vorerst vor Einsichtnahme durch die Ermittlungsbehörden geschützt und zum Gegenstand eines Sichtungsverfahrens, an dessen Ende eine gerichtliche Entscheidung über die (Nicht-)Freigabe der Daten steht.

Gemäß ausdrücklicher gesetzlicher Bestimmung dürfen dem Anwaltsprivileg unterliegende Erkenntnisse nicht für weitere Ermittlungen oder als Beweis verwendet werden (§ 112 Abs. 2 letzter Satz StPO). Diese Bestimmung stellt die einzige in der

[4] OGH 26.08.2008, 14 Os 109/08y.

StPO dar, mit der eine Fernwirkung eines Beweiserhebungsverbots vorgesehen ist (fruit of the poisenous tree). Ansonsten besteht gemäß ständiger Rechtsprechung keine Fernwirkung von Beweisverwertungsverboten in der Hinsicht, dass Beweismittel, die auf Grund unverwertbaren Beweismaterials aufgefunden wurden, ihrerseits aus diesem Grund jedenfalls unverwertbar wären.[5]

4.2 Beantragung zusätzlicher Datenauswertungen

Beschuldigte und Opfer (und damit auch Privatbeteiligte) können die **Verwendung weiterer Suchparameter** beantragen § 115i Abs. 2 StPO. Durch den Verweis auf das Beweisantragsrecht nach § 55 StPO ist davon auszugehen, dass ein solcher Antrag auf den Einsatz von Suchparametern die allgemeinen Voraussetzungen eines Beweisantrags erfüllen muss und damit insb die Beweisrelevanz. Dies gilt gemäß bestehender Rechtsprechung dann nicht, wenn diese durch das mit dem Fall und den Akten vertraute Gericht erschließbar ist.[6]

4.3 Einsichtsrechte Beteiligter

Beschuldigte und Opfer haben das Recht, das Ergebnis der Datenaufbereitung vor Ort und unter Aufsicht einzusehen (§ 115i Abs. 2 StPO). Andere Beteiligte (insb Mitbeschuldigte) erhalten kein generelles Einsichtsrecht, sondern sind auf die Akteneinsicht beschränkt. Dritte Personen (die nicht Beschuldigte oder Opfer sind) haben nur ein eingeschränktes Einsichtsrecht soweit sie selbst betroffen sind (§ 115i Abs. 4 StPO). Hierfür muss die Staatsanwaltschaft die betroffenen Personen informieren, sofern ihre Identität bekannt oder ohne unverhältnismäßigen Aufwand feststellbar ist.

4.4 Vernichtung nicht relevanter Daten

Nicht relevante oder nicht verwertbare Daten müssen gemäß § 115i Abs. 5 StPO vernichtet werden. Private Daten ohne Bezug zum Tatverdacht sind von den Ermittlungsbehörden von Amts wegen zu löschen. Beschuldigte, Opfer oder der Rechtsschutzbeauftragte können die Löschung beantragen.

4.5 Rechtsschutzbeauftragte:r

Neu gestaltet und aufgewertet wurde die Rolle des:der Rechtsschutzbeauftragten. Dieser obliegt allgemein die Wahrnehmung des besonderen Rechtsschutzes im Sinne der StPO. Im Rahmen der Daten(träger)beschlagnahme kommen ihr umfangreiche Kontrollrechte zu und sie ist zur Erhebung von Rechtsmitteln berechtigt.

5. Ausnahmen

5.1 Gefahr im Verzug

In Fällen, in denen der Verlust wichtiger Beweismittel droht, dürfen Ermittlungsbehörden auch ohne vorherige Genehmigung handeln. Ein typisches Beispiel wäre die Festnahme eines Beschuldigten, der sein Handy verschlüsseln oder Chats löschen könnte.

Die Maßnahme muss detailliert dokumentiert und umgehend der Staatsanwaltschaft gemeldet werden. Spätestens innerhalb von 14 Tagen muss eine nachträgliche richterliche Bewilligung beantragt werden. Falls das Gericht diese verweigert, dürfen die gesicherten Daten nicht weiter genutzt und müssen unverzüglich gelöscht werden.

5.2 Punktuelle Daten

Überhaupt keiner gerichtlichen Bewilligung bedarf es, wenn nur punktuelle Daten gesucht und sichergestellt werden sollen. So kann es bspw genügen, einen einzelnen Vertrag aus einer Unternehmensdatenbank zu sichern, ohne dass die gesamte Geschäftskorrespondenz des Unternehmens beschlagnahmt werden muss.

Selbiges gilt auch für die Sicherstellung von Daten aus Beweisgründen, die durch Bild- und Tonaufzeichnungsgeräte an öffentlichen oder öffentlich zugänglichen Orten aufgenommen wurden (zB die Aufnahmen einer Bankomatkamera).

6. Überlegungen des Autors

Dass zB neuerliche Zugriffe auf Originalsicherung bzw Arbeitskopie nur unter bestimmten Voraussetzungen erfolgen dürfen, ist positiv. Wenn jedoch die Praxis dazu führen wird, dass hierfür notwendige Beschlüsse relativ einfach eingeholt werden könnten, dann wäre *in puncto* Datenminimierung und Verfahrenseffizienz wenig gewonnen. Vor diesem Hintergrund begegnet gerade die Aufbewahrung der Originalsicherung und der Arbeitskopie bis zum rechtskräftigen Abschluss des Strafverfahrens nicht zu Unrecht Kritik.

Inwiefern die Regelung den gewünschten Zweck, die Auswertung von Daten effizient und transparent durchzuführen, tatsächlich erreichen wird, bleibt abzuwarten. Viel wird von der praktischen Umsetzung abhängen.

Nichtsdestotrotz gilt: Wenn auch die Neuregelung durch den VfGH und auch den EuGH erzwungen wurde, ist es ohne Zweifel zu begrüßen, dass die StPO nunmehr ein eigenes Regime für die „Handysicherstellung" vorsieht.

[5] RIS-Justiz RS0130052.
[6] Schmoller in Fuchs/Ratz, WK StPO § 55 Rz 63 (Stand 1.9.2022, rdb.at); OGH 16.09.2008, 11 Os 119/08x; OGH 19.12.2005, 14 Os 129/0k.