zur Passwortherausgabe angewiesen werden können (hierzu auch Franck, RDV 2013, 287, 288; Gercke, MMR 2008, 291, 298). Einen Verstoß gegen die Selbstbelastungsfreiheit oder den fair-trial-Grundsatz aus Art. 6 EMRK hatte das Supreme Court (England und Wales) hierin nicht gesehen (R v S & Anor [2008] EWCA Crim 2177 vom 09. Oktober 2008). Denn das Passwort sei als bloßer Schlüssel selbst nicht belastend, sondern lediglich die verschlüsselten Daten. Zudem vergleicht der Supreme Court das Passwort und die dadurch geschützten Daten mit Blut-, Urin- und Gewebeproben, die unabhängig vom Willen des Beschuldigten existieren.

Zwar stellte auch der EGMR fest, dass Beweismaterial, das vom Beschuldigten durch Zwang gewonnen werden kann, aber unabhängig vom Willen des Betroffenen vorhanden ist (z. B. Schriftstücke, die auf Grund einer Beschlagnahme erlangt werden, Proben von Atemluft, Blut, Urin, Haaren und Körpergewebe zu Zwecken von DNA-Analysen) nicht der Selbstbelastungsfreiheit unterliegt (EGMR (Große Kammer), Urteil vom 11. 7. 2006 - 54810/00Jalloh/Deutschland, NJW 2006, 3117, 3123). Für Passwörter wird man dies hingegen ebenfalls nur bei einer entsprechenden gesonderten Dokumentation des Passworts annehmen können (LG Trier, Beschluss vom 16. Oktober 2003 - 5 Qs 133/03, NJW 2004, 869, Greven, in: KK-StPO, § 94, Rn. 4c).

Hieraus folgt konsequent, dass ein „Angebot" zur Beschleunigung der Durchsicht durch Herausgabe des Passworts nicht bei der Verhältnismäßigkeitsprüfung zu berücksichtigen ist. Anstelle eines solchen Angebots wird die Staatsanwaltschaft den gleichen Gedanken jedoch dahingehend verpacken können, dass die noch andauernde Durchsicht der Entschlüsselung des Geräts und damit der Schwierigkeit der Auswertung – aufgrund des Passwortschutzes des Geräts – geschuldet ist (BGH, Beschluss vom 05. August 2003 - 2 BJs 11/03-5 - StB 7/03, NStZ 2003, 670, 671; OLG Koblenz, Beschluss vom 30. März 2021 – 5 Ws 16/21, NZWiSt 2021, 386, 389; Hausschild, in MüKo, § 110 StPO, Rn. 10). Eine solche Begründung würde allerdings voraussetzen, dass eine Auswertung – anders als im entscheidungsgegenständlichen Fall – bereits begonnen hat oder zügig begonnen werden soll.

Rechtsanwalt Dr. Elias Schönborn
und Mag. Jan Uwe Thiel, LL.B., beide Wien

Österreichischer Verfassungsgerichtshof: Gesetzliche Regelungen zur Handy-Sicherstellung sind verfassungswidrig

Mit Erkenntnis vom 14. Dezember 2023 (G 352/2021) hat der Verfassungsgerichtshof (im Folgenden: VfGH) in Österreich die Bestimmungen der österreichischen Strafprozessordnung (im Folgenden: StPO) über die Sicherstellung von Mobiltelefonen und anderen Datenträgern als verfassungswidrig aufgehoben, weil sie gegen die Grundrechte auf Achtung des Privatlebens nach Art 8 der Europäischen Menschenrechtskonvention („EMRK") und auf Datenschutz gemäß § 1 des österreichischen Datenschutzgesetzes („DSG") verstoßen. Die Entscheidung leitet einen Paradigmenwechsel im österreichischen Strafprozessrecht ein und hat international Beachtung gefunden, zumal es sich - soweit ersichtlich - um das erste europäische Verfassungsgericht handelt, das sich in dieser Tiefe mit Fragen der Verhältnismäßigkeit dieser besonders eingriffsintensiven Ermittlungsmaßnahme auseinandersetzt.[1] Die rechtlichen Voraussetzungen für die Sicherstellung/Beschlagnahme von Datenträgern sind in Österreich, Deutschland und der Schweiz in vielen Punkten ähnlich geregelt. Die Verhältnismäßigkeitserwägungen des VfGH können daher auch außerhalb Österreichs als Anregung für eine tiefergehende Auseinandersetzung mit der Thematik in Wissenschaft und Praxis dienen, sodass sich eine nähere Beschäftigung mit der Entscheidung lohnen kann.

I. Einleitung

1. Allgemeines

Die Sicherstellung von Handys und anderen elektronischen Datenträgern wird in Österreich in den § 110 Abs 1 Z 1 und Abs 4 sowie § 111 Abs 2 StPO geregelt. Der Kern der Debatte, illustriert durch die Entscheidung des VfGH, dreht sich um die **Verhältnismäßigkeit** solcher Ermittlungsmaßnahmen und den damit einhergehenden tiefgreifenden Eingriff in **Grund- und Freiheitsrechte** der betroffenen Personen. In Österreich stehen sowohl die EMRK samt 1 Zusatzprotokoll[2] als auch § 1 DSG im Verfassungsrang.

Indem der VfGH eine **unverhältnismäßige Beeinträchtigung** des **Rechts auf Datenschutz** nach § 1 DSG sowie in das **Recht auf Achtung des Privat- und Familienlebens** nach Art 8 EMRK durch die angefochtenen Bestimmungen feststellte, adressiert er eine **universelle Problematik** im digitalen Zeitalter: Wie weit dürfen staatliche Eingriffe gehen, um eine effiziente Strafverfolgung zu gewährleisten, ohne dabei fundamentale Freiheiten seiner Rechtsunterworfenen zu untergraben?

Es darf wohl als allgemeiner Konsens angesehen werden, dass es „in einem Rechtsstaat keine Wahrheitsfindung um jeden Preis geben" darf.[3] In einem Zeitalter, in dem (grenz-

[1] Soyer/Marsch, Handysicherstellung ohne vorherige richterliche Bewilligung verfassungswidrig, JSt-Slg 2024/4, 57 (68); vgl auch Soyer/Marsch, VfGH und Handysicherstellung – technische und rechtliche Fragen aus dem Verfahren, AnwBl 2024, 164 (164ff).
[2] Art II Z 7 BVG, BGBl 1964/59; VfGH 11.4.2017, G 5100/1965.
[3] Cepic/Gilhofer, Die Löschung von rechtswidrig ermittelten personenbezogenen Daten in der Strafrechtspflege – Ein- und Auswirkungen von § 75 StPO, JBl 2023, 409 (419).

überschreitende) Datenübermittlungen in nie dagewesenem Umfang fließen und digitale Überwachungsmöglichkeiten stetig wachsen, wird die Entscheidung des VfGH zu einem wichtigen Bezugspunkt für die Debatte um Datenschutz und Grundrechte auf globaler Ebene. Ein von einem Beschuldigten intensiv genutztes Endgerät wie Computer, Mobiltelefon oder Laptop kann durch die Ansammlung persönlicher Datenmengen zum „ultimativen Beweismittel"[4] werden, was die Bedeutung eines ausgewogenen Verhältnisses zwischen effektiver Strafverfolgung und dem Schutz individueller Freiheiten verdeutlicht.[5]

2. Derzeitige (verfassungswidrige) Rechtslage zur Sicherstellung von Datenträgern

Die **Sicherstellung** eines Handys oder anderen elektronischen Datenträgers ist dann zulässig, wenn sie für das Ermittlungsverfahren aus **Beweisgründen erforderlich** erscheint (§ 110 Abs 1 Z 1 StPO).[6] Die Sicherstellung ist die vorläufige Begründung der Verfügungsmacht über den Gegenstand durch die Strafverfolgungsbehörden (§ 109 Z 1 lit a StPO).[7] Für die Anordnung einer Sicherstellung bedarf es eines **Anfangsverdachtes** (§ 1 Abs 3 StPO), somit bestimmter Anhaltspunkte, die die Annahme rechtfertigen, dass eine Straftat begangen worden ist.

§ 111 Abs 1 und Abs 2 StPO sehen eine **Herausgabepflicht** des Betroffenen vor. Jedermann ist verpflichtet, die erforderlichen Gegenstände herauszugeben oder die Sicherstellung auf andere Weise zu ermöglichen. In dieser Bestimmung ist grundsätzlich auch eine Herausgabepflicht von Passwörtern elektronischer Datenträger umfasst, außer es handelt sich um einen Beschuldigten oder Zeugen, dem eine Schweigepflicht zukommt.[8]

Die **Anordnung** der Sicherstellung muss von der Staatsanwaltschaft begründet werden, indem dargelegt wird, welche Gegenstände von ihr erfasst sind und wofür diese von Relevanz sein könnten.[9] Eine **richterliche Bewilligung**, die beispielsweise für eine (anschließende) Beschlagnahme (§ 115 StPO) notwendig ist, ist **nicht erforderlich**. Die Sicherstellung ist lediglich von der Staatsanwaltschaft anzuordnen und von der Kriminalpolizei durchzuführen (§ 110 Abs 2 StPO).[10]

Jede **bewegliche körperliche Sache** kann sichergestellt werden.[11] Somit sind neben Datenträgern (Laptop, Mobiltelefon, etc) auch **sonstige Gegenstände** iSd § 109 Z 1 lit a StPO umfasst. Darüber hinaus kommt auch eine **Datenspiegelung** in Betracht. Im Rahmen einer Datenspiegelung wird nicht der physische Gegenstand, sondern lediglich die sich auf diesem befindenden Daten sichergestellt.[12] Diese Möglichkeit ergibt sich aus § 110 Abs 4 und § 111 Abs 2 StPO.

Im Unterschied zur Sicherstellung von sonstigen Gegenständen wird es den Ermittlungsbehörden im Rahmen der Sicherstellung von Datenträgern ermöglicht, **Rückschlüsse** auf bestimmte Personen zu ziehen.[13] Sie können sich dadurch ein **umfassendes Bild** über die Vergangenheit und der Gegenwart der betroffenen Person machen. Weiters können die Ermittler auch auf **extern gespeicherte Daten** (z.B. externe Festplatte, Cloud) uneingeschränkt zugreifen.[14] Es gibt **keine konkrete Vorschrift** darüber, **wie die Auswertung zu erfolgen** hat. Aus rechtsstaatlicher Sicht ist diese Tatsache äußerst problematisch.

Zugegriffen darf nur auf jene Daten werden, die **im Zeitpunkt der Sicherstellung** lokal oder extern gespeichert waren. Auf Daten, die erst nachträglich auf den sichergestellten Datenträger übertragen wurden, darf nicht zugegriffen werden, da dies nicht von der Sicherstellungsbefugnis gemäß § 110 Abs 1 Z 1 StPO gedeckt ist.[15]

Der Gesetzgeber verlangt auch **keine bestimmte Schwere der Straftat**, weshalb eine Sicherstellung bei Vorliegen eines Anfangsverdachts bei jedem Delikt in Frage kommt. Selbst **(nicht verdächtige) Dritte** müssen sich einer Sicherstellung beugen,[16] wenn gegen eine (andere) Person ein Anfangsverdacht im Sinne des § 1 Abs 3 StPO besteht und der – im Besitz des (nicht verdächtigen) Dritten stehende – Gegenstand ein relevantes Beweismittel im strafrechtlichen (Ermittlungs-) Verfahren ist.[17]

§ 110 Abs 4 StPO normiert, dass die Sicherstellung von Gegenständen aus Beweisgründen gemäß § 110 Abs 1 Z 1 StPO nicht zulässig und jedenfalls auf Verlangen der betroffenen Person aufzuheben ist, 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.[18]

Betroffene einer Sicherstellung können neben dem Antrag auf **Herausgabe** (§ 110 Abs 4 StPO) einen **Einspruch** wegen

[4] Grzesiek/Zühlke, Die Entschlüsselung von Smartphones gegen den Willen des Beschuldigten zum Zwecke der Durchführung des Strafverfahrens, StV-S 2021, 117 (122).
[5] Seidl/Schönborn, Dürfen Strafverfolgungsbehörden Beschuldigte zur (biometrischen) Entschlüsselung von Endgeräten zwingen? JBl 2022, 361 (361).
[6] Tipold/Zerbes in Fuchs/Ratz, WK StPO § 110 Rz 5 (Stand 1.3.2021, rdb.at).
[7] Tipold/Zerbes/Flora in Fuchs/Ratz, WK StPO § 109 Rz 2 (Stand 13.11.2017, rdb.at).
[8] Reindl-Krauskopf/Salimi/Stricker, IT-Strafrecht, 2018, Rz 5.9.
[9] Seidl/Schönborn, Dürfen Strafverfolgungsbehörden Beschuldigte zur (biometrischen) Entschlüsselung von Endgeräten zwingen? JBl 2022, 361 (364); Tipold/Zerbes in Fuchs/Ratz, WK StPO § 110 Rz 59 (Stand 1.3.2021, rdb.at).
[10] Tipold/Zerbes in Fuchs/Ratz, WK StPO § 110 Rz 57 (Stand 1.3.2021, rdb.at).
[11] Tipold/Zerbes in Fuchs/Ratz, WK StPO § 110 Rz 3 (Stand 1.3.2021, rdb.at).
[12] Schönborn/Morwitzer, Criminal Compliance (2023) Rz 11.64; McAllister in Kier/Wess, HB Strafverteidigung² (2022) Rz 8.64.
[13] Soyer/Marsch, Handysicherstellung ohne vorherige richterliche Bewilligung verfassungswidrig, JSt-Slg 2024/4, 57 (67).
[14] Vgl. ErläutRV 25 BlgNR 22. GP; Tipold/Zerbes in Höpfel/Ratz, WK StPO § 111 Rz 14 (Stand 1.3.2021, rdb.at); aA Reindl-Krauskopf/Salimi/Stricker, IT-Strafrecht, 2018, Rz 5.11.
[15] Vgl Tipold/Zerbes in Höpfel/Ratz, WK StPO § 111 Rz 17/2 (Stand 1.3.2021, rdb.at).
[16] Tipold/Zerbes in Höpfel/Ratz, WK StPO § 110 Rz 2 (Stand 1.3.2021, rdb.at).
[17] Tipold/Zerbes in Höpfel/Ratz, WK StPO Vor §§ 110-115 Rz 7 (Stand 1.3.2021, rdb.at).
[18] Tipold/Zerbes in Fuchs/Ratz, WK StPO § 110 Rz 50 (Stand 1.3.2021, rdb.at).

Rechtsverletzung (§ 106 Abs 1 StPO) erheben sowie eine gerichtliche Entscheidung über die Fortsetzung bzw Aufhebung der Sicherstellung beantragen (§ 115 iVm § 111 Abs 4 StPO). Zudem können Betroffene gemäß § 75 StPO einen Antrag auf **Berichtigung, Löschung** oder **Vervollständigung** von unrichtigen, unvollständigen oder entgegen den Bestimmungen der Strafprozessordnung 1975 ermittelten personenbezogenen Daten stellen.[19]

II. Entscheidung des Verfassungsgerichtshofes vom 14.12.2023 (G 352/2021)

1. Vorverfahren

Die Staatsanwaltschaft Klagenfurt führte gegen den Beschuldigten, einen Geschäftsführer eines Unternehmens in Kärnten, ein Ermittlungsverfahren wegen des Verdachts auf Untreue gemäß § 153 Abs 1 und Abs 3 zweiter Fall StGB. Am 21. Juli 2021 ordnete die Staatsanwaltschaft Klagenfurt die Sicherstellung des Mobiltelefons sowie des Outlook-Kalenders des Beschuldigten an. Dagegen erhob der Beschuldigte **Einspruch wegen Rechtsverletzung** (§ 106 Abs 1 StPO). Er führte begründend aus, dass die Ermittlungsmaßnahme unverhältnismäßig sei, da das Mobiltelefon einen uferlosen Zugriff auf die Lebensumstände und die Lebensgeschichte eines Menschen ermögliche, zumal durch das Mobiltelefon auch Daten zugänglich würden, die in der Cloud gespeichert seien.[20]

Das Landesgericht Klagenfurt **wies** den Einspruch wegen Rechtsverletzung mit der Begründung **ab**, dass die Sicherstellung des Mobiltelefons aus Beweisgründen **geeignet** und **erforderlich** sei und zudem das **gelindeste Mittel** darstelle.[21]

Gegen diesen Beschluss erhob der Beschuldigte fristgerecht **Beschwerde** (§ 87 StPO) an das Oberlandesgericht Graz und stellte aus Anlass dieses Rechtsmittels den **Antrag auf Normenkontrolle gemäß Art 140 Abs 1 Z 1 lit d B-VG an den VfGH**.[22] Diese Bestimmung ermöglicht es einer Person, die als Partei einer von einem ordentlichen Gericht in erster Instanz entschiedenen Rechtssache wegen Anwendung eines verfassungswidrigen Gesetzes in ihren Rechten verletzt zu sein behauptet, aus Anlass eines gegen diese Entscheidung erhobenen Rechtsmittels, die **Verfassungswidrigkeit eines Gesetzes** geltend zu machen.[23]

Diese Möglichkeit ist von der deutschen „Verfassungsbeschwerde" (§§ 90 ff dt. BVerfGG) zu unterscheiden, die es einer natürlichen oder juristischen Person ermöglicht, das Bundesverfassungsgericht anzurufen, wenn sie geltend macht, durch die öffentliche Gewalt in einem ihrer Grundrechte verletzt zu sein. Diese Möglichkeit kennt der österreichische Gesetzgeber nicht. Beim sogenannten **Parteiantrag auf Normenkontrolle**[24] wird nicht behauptet, das Gericht habe Grundrechte verletzt, sondern dass das Gericht ein **verfassungswidriges Gesetz** angewendet hat. Es wird somit der **Inhalt des Gesetzes** bekämpft.[25]

a. Argumente des Antragstellers

Der Antragsteller argumentierte, dass die Sicherstellung eines Smartphones aus Beweisgründen angesichts der Fülle der auf dem Smartphone enthaltenen Daten **tiefe Einblicke** in das Leben und die Privatsphäre des Betroffenen erlaube. Ein Blick in das Mobiltelefon genüge und man wisse alles über einen Menschen, was es zu wissen gebe. Gleichwohl bedürfe die Sicherstellung nur einer **Anordnung der Staatsanwaltschaft** im Zuge eines strafrechtlichen Ermittlungsverfahrens, für dessen Einleitung wiederum lediglich ein **Anfangsverdacht** (§ 1 Abs 3 StPO) Voraussetzung sei. Für sämtliche Ermittlungsmaßnahmen, die mit vergleichbaren Eingriffen verbunden seien, würden **strengere materielle und formelle Voraussetzungen** gelten. Dies betreffe etwa die Identitätsfeststellung nach § 118 StPO, bei der das Vorliegen **bestimmter Tatsachen** erforderlich sei. Ähnliches gelte für die Auskunft über Bankdaten gemäß § 116 StPO, die überdies einer **gerichtlichen Bewilligung** bedürfe. Auch für eine Durchsuchung von Orten und Gegenständen ("Hausdurchsuchung") (§ 120 StPO) und eine molekulargenetische Untersuchung (§ 124 StPO) bedürfe es jeweils einer **gerichtlichen Bewilligung**. Die körperliche Untersuchung (§ 123 StPO) dürfe nur bei Vorliegen **bestimmter**, im Gesetz näher genannter **Tatsachen** erfolgen und unterliege zudem einer strengen Verhältnismäßigkeitsprüfung. Observation und verdeckte Ermittlung (§§ 130 ff StPO) wiederum unterlägen **strengen zeitlichen Beschränkungen**. Für die Beschlagnahme von Briefen, die Auskunft über Daten einer Nachrichtenermittlung sowie die Lokalisierung einer technischen Einrichtung und die Überwachung von Nachrichten enthielten die §§ 134 ff StPO detaillierte Voraussetzungen, wobei überdies jeweils **richterliche Bewilligungen** erforderlich seien.[26] Bei verdeckten Ermittlungen und der Überwachung verschlüsselter Nachrichten bestehe gemäß § 147 StPO **Rechtsschutz** durch den Rechtsschutzbeauftragten.[27]

Eine einfache Anordnung der Sicherstellung könne diese detaillierten Anforderungen ohne Rechtsschutz im Hauptverfahren (§§ 210 ff StPO) umgehen, da es dafür **keine Nichtigkeitssanktion** gebe.[28]

---

[19] Vgl. OGH 13.10.2020, 11 Os 56/20z; 1.6.2021, 14 Os 35/21k.

[20] Punkt 2. bzw Rz 4 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.

[21] Punkt 3. bzw Rz 5 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.

[22] Punkt 4. bzw Rz 6 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.

[23] Näher dazu Rohregger, Der Parteiantrag auf Normenkontrolle („Gesetzesbeschwerde"), AnwBl 2015, 188 (188); Herbst/Wess, Der Parteiantrag auf Normenkontrolle im Bereich der Strafgerichtsbarkeit, ZWF 2015, 64 (64).

[24] Art 140 Abs 1 Z 1 lit d B-VG.

[25] Bußjäger in Kahl/Khakzadeh/Schmid, Kommentar zum Bundesverfassungsrecht B-VG und Grundrechte Art. 140 B-VG Rz 12 (Stand 1.1.2021, rdb.at); Rohregger, Der Parteiantrag auf Normenkontrolle („Gesetzesbeschwerde"), AnwBl 2015, 188 (188); Herbst/Wess, Der Parteiantrag auf Normenkontrolle im Bereich der Strafgerichtsbarkeit, ZWF 2015, 64 (64).

[26] Seidl/Schönborn, Dürfen Strafverfolgungsbehörden Beschuldigte zur (biometrischen) Entschlüsselung von Endgeräten zwingen? JBl 2022, 361 (370).

[27] Punkt 4.1. bzw Rz 7 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.

[28] Punkt 4.2. bzw Rz 8 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.

Die Sicherstellung eines Mobiltelefons greife folglich auf **unverhältnismäßige Weise** in Art 8 EMRK sowie § 1 DSG ein. Einerseits fehle es an der ausreichenden gesetzlichen Determinierung, andererseits könne die Sicherstellung, die einen zeitlich und inhaltlich uferlosen Eingriff in die Privatsphäre erlaube, bereits unter geringsten Voraussetzungen angeordnet werden, nämlich bei Vorliegen eines **bloßen Anfangsverdachtes** sowie bei der Eignung des Mobiltelefons als Beweismittel. Insoweit verstoße die Rechtslage auch gegen den Gleichheitsgrundsatz (Art 2 StGG, Art 7 Abs 1 B-VG), weil die erwähnten Bestimmungen der StPO den Ermittlungsbehörden erhebliche materielle und formelle Schranken setzten, wohingegen dies bei der Sicherstellung von Mobiltelefonen nicht der Fall sei.[29]

b. Argumente der Bundesregierung

Die Bundesregierung teilte die verfassungsrechtlichen Bedenken des Antragstellers nicht. In Verteidigung der Sicherstellungsbestimmungen führte die Bundesregierung insbesondere Folgendes aus: Die Sicherstellung eines Datenträgers gehe nicht notwendig mit dessen Auswertung einher, vielmehr bedürfe diese einer eigenen Anordnung. Der vermeintlichen Schrankenlosigkeit des Eingriffes sei entgegenzuhalten, dass die Ermittlungsbehörden Daten **nur zum Zwecke der Strafverfolgung** auswerten und strafrechtsunerhebliche Informationen nicht zum Akt nehmen dürften (vgl § 74 Abs 1 StPO; OGH 13.10.2020, 11 Os 56/20z). Entgegen den Bestimmungen der Strafprozessordnung 1975 **ermittelte Daten** seien von Amts wegen oder auf Antrag **zu löschen** (§ 75 Abs 1 StPO). Weder sei notwendigerweise jener Gegenstand sicherzustellen, in dem der Datenträger eingebaut sei, noch sei jener Datenträger sicherzustellen, auf dem die relevanten Daten originär gespeichert worden seien, weil andernfalls die in § 111 Abs 2 StPO normierte Pflicht, den Ermittlungsbehörden Zugang zu gespeicherten Daten zu verschaffen, insbesondere bei der Nutzung externer Speicherplätze leerliefe (OGH 11.9.2018, 14 Os 51/18h). Zudem dürfe das sichergestellte Gerät von den Strafverfolgungsorganen nicht dazu verwendet werden, um auf zukünftig dezentral gespeicherte Daten zuzugreifen. Vielmehr seien alle Verbindungen zu trennen und das Mobiltelefon auf **„Flugmodus"** zu setzen, sodass sich die Sicherstellung nur auf jene Daten beziehe, die über das Mobiltelefon im Zeitpunkt der Maßnahme verfügbar gewesen seien (Zerbes, Beweisquelle Handy. Ermittlungen zwischen Sicherstellung und Nachrichtenüberwachung, ÖJZ 2021, 176 [180]). Zudem habe es bereits der Europäische Gerichtshof für Menschenrechte für **zulässig** erachtet, dass die Staatsanwaltschaft bei Beschlagnahme einer größeren Datenmenge das **beschlagnahmte Datenmaterial sichte** (EGMR 4.6.2019, 39.757/15, Sigurður Einarsson, Z 90).[30]

Gemäß § 1 Abs 3 StPO bedürfe die Sicherstellung eines Anfangsverdachtes, also bestimmter Anhaltspunkte, welche die Annahme rechtfertigten, dass eine Straftat begangen worden sei. Die im Parteiantrag zitierten, in anderen Bestimmungen erwähnten „bestimmten Tatsachen" seien ein Verweis auf eben diesen Anfangsverdacht, wie insbesondere das Beispiel der Identitätsfeststellung nach § 118 StPO zeige. Ferner bedürfe die Anordnung einer Sicherstellung einer **Begründung**: Es sei darzulegen, **welche Gegenstände** von ihr erfasst und wofür diese von **Relevanz** seien. Im Übrigen sei auch bei Sicherstellungen der Grundsatz der **Verhältnismäßigkeit** gemäß § 5 Abs 1 und 2 StPO unter Berücksichtigung grundrechtlicher Vorgaben, insbesondere von Art 8 EMRK bzw § 1 DSG, zu wahren (OGH 28.7.2020, 11 Os 51/20i; 13.10.2020, 11 Os 56/20z), wobei dem Betroffenen zur Geltendmachung dieser Rechte das **Rechtsmittel des Einspruches** wegen Rechtsverletzung offenstehe.[31]

Die Sicherstellung sei überdies eine **bloß vorläufige Maßnahme**. Erst die nachfolgende Beschlagnahme bedürfe der richterlichen Bewilligung, wobei der Betroffene die Möglichkeit habe, nach § 115 StPO eine gerichtliche Entscheidung über die Aufhebung oder Fortsetzung der Sicherstellung zu beantragen.[32]

Die im Antrag angesprochenen Überwachungsmaßnahmen nach §§ 130 ff StPO **unterschieden sich grundlegend** von der Sicherstellung eines Datenträgers. Überwachungsmaßnahmen erfolgten regelmäßig im **Verborgenen**, wobei das Verhalten von Personen ohne deren Kenntnis typischerweise über einen gewissen Zeitraum beobachtet werde, wohingegen die Sicherstellung lediglich eine **Momentaufnahme** sei. Eine Überwachung könne nur in Echtzeit stattfinden und erfordere die Einbindung eines Dritten, des Kommunikationsdienstes. Sobald sich die Daten in der Sphäre des jeweiligen Nutzers befänden, könne dieser über sie disponieren und es unterlägen die Daten der Sicherstellung. Daraus ergebe sich ein **unterschiedliches Schutzniveau** im Verhältnis zum (im Fernmeldegeheimnis geschützten) Vertrauen auf die Integrität des Übertragungsweges, dem die Gesetzgebung durch unterschiedliche Regelungen Rechnung trage. Im Übrigen erachte der Europäische Gerichtshof für Menschenrechte selbst bei (geheimen) Überwachungsmaßnahmen eine nachträgliche richterliche Überprüfung als hinreichend (EGMR 2.9.2010, 35.623/05, Uzun, Z 71 bis 74; 12.1.2016, 37.138/14, Szabó und Vissy, Z 77).[33]

Soweit der Antragsteller darüber hinaus geltend mache, dass es im Hinblick auf die Datenvielfalt einer speziellen Regelung für die Sicherstellung von Smartphones bedürfe, verlange er vom Gesetzgeber eine **Differenzierung** danach, welchen potentiellen Beweiswert ein sichergestellter Gegenstand haben könnte, was aber **faktisch unmöglich** sei, weil dazu die Ermittlungsergebnisse antizipiert werden müssten. Ein Smartphone enthalte zwar eine Vielzahl an Informationen in kumulierter Form, gleichwohl wäre es auch möglich, diese Informationen durch Sicherstellung anderer, allenfalls mehrerer Gegenstände (Notizbücher, Taschenkalender etc.) zu gewinnen. Folglich erschiene es unsachlich, die Sicherstellung eines Mobiltelefons an **strengere Voraussetzungen**

[29] Punkt 4.3. bzw Rz 9 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[30] Punkt 9.1. bzw Rz 15 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[31] Punkt 9.2. bzw Rz 16 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[32] Punkt 9.3. bzw Rz 17 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[33] Punkt 9.4. bzw Rz 18 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.

als die Sicherstellung sonstiger persönlicher Gegenstände zu knüpfen.[34]

2. Erwägungen des VfGH

a. Verhältnismäßigkeit

Durch die Befugnis zur Sicherstellung und Auswertung von (personenbezogener) Daten, deren Rechtsgrundlage sich aus § 110 Abs 1 Z 1 und § 111 Abs 2 StPO ergibt, wird in das Recht auf Datenschutz nach § 1 DSG sowie in das **Recht auf Achtung des Privat- und Familienlebens** nach Art 8 EMRK **eingegriffen**.[35]

Nach Ansicht des VfGH handelt es sich bei dem durch §§ 110 ff StPO angestrebten Ziel, nämlich der Verfolgung von strafbaren Handlungen mittels Sicherstellung von Beweismitteln, um ein **legitimes Ziel** im Sinne des § 1 Abs 2 DSG und Art 8 Abs 2 EMRK. Weiters sind die angefochtenen Bestimmungen **abstrakt geeignet**, das angestrebte (legitime) Ziel zu erreichen.[36]

Hingegen **fehlt** es an der **Verhältnismäßigkeit** und damit der **Zulässigkeit** des Eingriffs: Eine weiteres Kriterium für die Verhältnismäßigkeit und somit die Zulässigkeit von Eingriffen in das Grundrecht auf Datenschutz gemäß § 1 DSG sowie das Recht auf Achtung des Privat- und Familienlebens gemäß Art 8 EMRK besteht nämlich darin, dass die Intensität des spezifischen Eingriffs nicht das Gewicht und die Bedeutung der mit dem Eingriff verfolgten Ziele übersteigt.[37] § 1 Abs 2 zweiter Satz DSG sieht im Hinblick auf besonders schutzwürdige Daten eine weitere Eingriffsschranke vor, nämlich, dass die Verwendung solcher Daten nur zur Wahrung wichtiger öffentlicher Interessen vorgesehen werden darf und dass das jeweilige Gesetz angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen muss.[38]

Die Sicherstellung und Auswertung von Daten sind nicht mit der Sicherstellung von **sonstigen Gegenständen** vergleichbar. Einer der **wesentlichen Unterschiede** zwischen der Sicherstellung von Datenträgern und der Sicherstellung sonstiger Gegenstände im Sinne des § 109 Z 1 lit a StPO liegt nicht in der (Anordnung der) Sicherstellung selbst, sondern in der **Möglichkeit der Auswertung** der auf einem Datenträger gespeicherten Daten und der damit verbundenen Rückschlüsse auf die betroffene Person. Die auf einem sichergestellten Datenträger **gespeicherten Daten sind potentiell äußerst umfangreich** und können unter anderem mit sonst verfügbaren Daten (nicht nur der Strafverfolgungsorgane) **verknüpft** und gespeichert werden. Diese Daten können (auch bei Verknüpfung mit sonstigen Daten) ein **umfassendes Bild** über das bisherige und aktuelle Leben des von der Sicherstellung Betroffenen geben, wie dies bei der Auswertung sonstiger Gegenstände im Sinne des § 109 Z 1 lit a StPO in der Regel nicht der Fall ist.[39]

Der Zugriff auf potentiell sämtliche auf einem Datenträger gespeicherte Daten ermöglicht den Strafverfolgungsorganen nicht bloß ein punktuelles Bild über das Verhalten des Verdächtigen oder des Betroffenen (im Sinne des § 48 Abs 1 Z 1 und 4 StPO). Die auf einem sichergestellten Datenträger, wie zB einem Laptop, einem PC oder einem Smartphone, (lokal oder extern) gespeicherten Daten, auf welche die Strafverfolgungsorgane potentiell im Rahmen der Auswertung Zugriff haben, ermöglichen den Strafverfolgungsorganen vielmehr einen **umfassenden Einblick in wesentliche Teile des bisherigen und aktuellen Lebens** der betroffenen Person. Den Strafverfolgungsorganen wird die Befugnis in die Hand gegeben, sämtliche Inhalts- und Verbindungsdaten aus sämtlichen (unter Umständen auch bereits gelöschten) Kommunikationsvorgängen zu ermitteln, zu speichern und mit anderen, insbesondere im Internet oder in Datenbanken verfügbaren Daten zu verknüpfen, abzugleichen und zu systematisieren. Auf diese Weise können umfassende **Persönlichkeits- und Bewegungsprofile** erstellt werden, die detailreiche Rückschlüsse auf das Verhalten, die Persönlichkeit und die Gesinnung des Betroffenen zulassen. Die auf dem Datenträger gespeicherten Verbindungsdaten können auch Vermutungen über Kommunikationsinhalte nahelegen, weil offengelegt wird, ob, wann, wie oft und mit wem auf welchem Weg Kontakt aufgenommen wurde (vgl dazu schon VfSlg 19.892/2014; EuGH 8.4.2014, Digital Rights Ireland ua, C-293/12 ua, Rz 27; EuGH 13.5.2014, Google Spain und Google, C-131/12, Rz 80 ff; EuGH 21.12.2016, Tele2 Sverige AB, C-203/15, Rz 98 f).[40]

Darüber hinaus haben Strafverfolgungsorgane – unabhängig von Kommunikationsvorgängen des Betroffenen – potentiell Zugriff auf alle sonstigen auf dem Datenträger (lokal oder extern) gespeicherten (sensiblen oder sonstigen personenbezogenen) Daten unterschiedlicher Art. Dies kann etwa **Fotos, Videos, Standortdaten, Suchverläufe oder Gesundheitsdaten** betreffen, die insgesamt den Strafverfolgungsorganen gemeinsam mit den oben erwähnten, gespeicherten Kommunikationsinhalten die Erstellung eines vollständigen Profils des Betroffenen ermöglichen.[41]

Eine weitere Besonderheit der Auswertung von auf einem Datenträger (lokal oder extern) gespeicherten Daten liegt darin, dass bei Vorhandensein bestimmter Daten(mengen) über die betroffene Person mittels prädiktiver Analyse sogar dann **Rückschlüsse auf das Verhalten**, die Vorlieben, die Gesinnung und damit ganz allgemein auf die Persönlichkeit des Betroffenen gezogen werden können, wenn diesbezüglich keine konkreten Daten auf dem sichergestellten Datenträger vorhanden sind.[42]

[34] Punkt 9.5. bzw Rz 19 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[35] Punkt 2.2.3. bzw Rz 61 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[36] Punkt 2.2.3. bzw Rz 62 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[37] Vgl VfSlg. 19.738/2013, 19.892/2014; EGMR 4.12.2008 [GK], Fall S. und Marper, Appl. 30.562/04, [Z 101]).
[38] Punkt 2.2.4. bzw Rz 63 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[39] Punkt 2.2.5. bzw Rz 65 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[40] Punkt 2.2.5. bzw Rz 66 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[41] Punkt 2.2.5. bzw Rz 67 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[42] Punkt 2.2.5. bzw Rz 68 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.

Außerdem ist wesentlich, dass dieser potentiell umfassende Einblick der Strafverfolgungsorgane in die auf einem sichergestellten Datenträger (lokal oder extern) gespeicherten Daten sich nicht bloß auf Datenträger bezieht, die im Gewahrsam der einer Straftat verdächtigen Person sind, sondern **auch Datenträger erfasst, die ein (der Tat nicht verdächtiger) Dritter innehat**.[43]

Angesichts der auf Datenträgern (wie zB PC, Notebook und Smartphone) in der Regel vorhandenen **Datenmenge**, des **Dateninhaltes** und der Möglichkeit, die ermittelten Daten mit anderen Daten zu **verknüpfen**, abzugleichen und unter Umständen gelöschte Daten wiederherzustellen, kann die Sicherstellung eines Datenträgers und insbesondere die Auswertung der darauf (lokal oder extern) gespeicherten Daten daher **nicht** mit der Sicherstellung und Auswertung anderer Gegenstände im Sinne des § 109 Z 1 lit a StPO **verglichen** werden.[44]

b. Weitere Gründe für die besondere Eingriffsintensität

Nach Auffassung des Verfassungsgerichtshofes kommt der Ermittlungsmaßnahme der Sicherstellung von Datenträgern und deren anschließende Auswertung gemäß § 110 Abs 1 Z 1 und § 111 StPO auch aus den folgenden Gründen eine **besondere Eingriffsintensität** zu[45]:

Zum Ersten können die Strafverfolgungsorgane die in § 110 Abs 1 Z 1 und § 111 StPO vorgesehenen Maßnahmen (Sicherstellung von Datenträgern und Auswertung der darauf gespeicherten Daten) bereits bei einem **Anfangsverdacht** im Sinne des § 1 Abs 3 StPO ergreifen; zum Zweiten genügt der **Verdacht irgendeiner Straftat** und nicht einer Straftat bestimmter Schwere; zum Dritten können diese Maßnahmen nicht nur gegenüber einem Verdächtigen, sondern auch gegenüber einem (nicht verdächtigen) **Dritten** erfolgen; zum Vierten haben die Strafverfolgungsorgane potentiell **Zugriff auf sämtliche (auch sensible) Daten**, die auf dem sichergestellten Datenträger (lokal oder extern) gespeichert sind oder gespeichert waren, somit zu allen inhaltlichen Daten und Verbindungsdaten. Die Sicherstellung (Zugriff und Auswertung) von auf Datenträgern wie PC, Notebook oder Mobiltelefon gespeicherten Daten ermöglicht den Zugriff auf **Informationen über sämtliche Lebensbereiche der betroffenen Person**. Durch die (technische) Möglichkeit, bereits gelöschte Daten zu rekonstruieren, erstreckt sich die den Strafverfolgungsorganen durch die Sicherstellung von Datenträgern ermöglichte Einsicht auch auf Daten, die **(potenziell unbegrenzt) in der Vergangenheit** auf dem Datenträger verfügbar waren. Von der Ermittlungsmaßnahme betroffen sind nicht nur Personen, gegen die ein Anfangsverdacht der Begehung einer Straftat besteht, sondern **sämtliche Personen, deren Daten sich auf dem sichergestellten Datenträger befinden.**[46]

All dies zeigt, dass die durch **§ 1 Abs 1 DSG iVm Art 8 Abs 1 EMRK** geschützte Grundrechtssphäre durch die Befugnisse der Strafverfolgungsorgane gemäß § 110 Abs 1 Z 1 und § 111 StPO im Hinblick auf die Intensität des Eingriffes **in besonderer Weise bedroht ist**.[47]

Der VfGH verweist in diesem Zusammenhang auf die Rechtsprechung des EGMR, der wiederholt die Gefahr betont, dass Systeme der (geheimen) Überwachung die **Demokratie** – unter dem Schutzmantel ihrer Verteidigung – **untergraben** oder gar zerstören können. Daraus lässt sich ableiten, dass der EGMR bei seiner Prüfung die Bestimmtheit der gesetzlichen Grundlage, Art und Dauer der Maßnahme, die für die Genehmigung, Durchführung und Kontrolle der Maßnahme zuständigen Behörde, den Rechtsschutz und vorgesehene Garantien gegen Missbrauch in Relation zueinander setzt.[48]

Der VfGH erkennt zwar an, dass es sich bei der Sicherstellung und Auswertung von Datenträgern nicht um **„geheime"** oder **„verdeckte"** Maßnahmen handelt, spricht jedoch auch aus, dass auch nicht von **„offenen"** Maßnahmen gesprochen werden kann, da für den Betroffenen nicht ersichtlich ist, in welcher Form die Auswertung der auf dem Datenträger (extern oder lokal) gespeicherten Daten erfolgt. Einerseits könnten **gelöschte Daten wiederhergestellt**, andererseits **Verknüpfungen** mit anderen Daten vorgenommen werden, ohne dass der Betroffene davon Kenntnis erlangen könnte.[49]

Des Weiteren weist der VfGH darauf hin, dass staatliches Handeln durch die rasche Verbreitung der Nutzung „neuer" Kommunikationstechnologien (z.B. Smartphones) in vielerlei Hinsicht – nicht zuletzt auch im Rahmen der Bekämpfung der Kriminalität, der die Sicherstellung von Datenträgern dienen soll – vor besondere Herausforderungen gestellt wurde und wird. Dieses geänderte Umfeld polizeilicher Ermittlungen ist nach der Rechtsprechung des VfGH maßgeblich.[50] In diesem Zusammenhang ist aber auch zu erwähnen, dass die Erweiterung der technischen Möglichkeiten der Strafverfolgungsorgane auch dazu führt, dass den Gefahren, die diese Erweiterung für die Freiheit des Menschen birgt, in einer dieser Bedrohung **adäquaten Weise** entgegengetreten werden muss.[51]

In einer Konstellation, in dem der Gesetzgeber den Strafverfolgungsbehörden umfangreiche Eingriffsbefugnisse gewährt, fordern § 1 DSG iVm Art 8 EMRK einen **effektiven Rechtsschutz**. Dieser soll sicherstellen, dass sowohl die erforderlichen Bedingungen für die Sicherstellung und Auswertung von auf Datenträgern gespeicherten Informationen als auch die Prävention von **Befugnismissbrauch** effizient

[43] Punkt 2.2.5. bzw Rz 69 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[44] Punkt 2.2.5. bzw Rz 70 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[45] Punkt 2.2.6. bzw Rz 71 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[46] Punkt 2.2.6 bzw Rz 72 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[47] Punkt 2.2.6. bzw Rz 73 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[48] Punkt 2.2.7. bzw Rz 74 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023; vgl. EGMR 6.9.1978, Fall Klass, Appl. 5029/71, [Z 49 f.]; sowie z.B. EGMR 4.12.2015 [GK], Fall Zakharov, Appl. 47.143/06, [Z 232 f.], und 12.1.2016, Fall Szabo und Vissy, Appl. 37.138/14, [Z 57 und 77 mwN]).
[49] Punkt 2.2.7. bzw Rz 75 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[50] Vgl. z.B. VfSlg. 16.149/2001, 16.150/2001, 18.830/2009, 18.831/2009, 19.657/2012.
[51] Punkt 2.2.8. bzw Rz 76 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023; vgl. auch 19.892/2014, 20.356/2019.

überprüft werden. Diese Forderung gilt insbesondere für die Verarbeitung von Daten, die gemäß § 1 Abs 2 zweiter Satz DSG als **besonders schutzwürdig** angesehen werden, wie beispielsweise Gesundheitsdaten.[52]

Wie der Verfassungsgerichtshof bereits in seiner Entscheidung VfSlg. 19.892/2014 feststellte, ist für einen wirksamen Rechtsschutz die **Überwachung durch ein Gericht erforderlich**. Dies ist besonders wichtig angesichts der weitreichenden und intensiven Eingriffsbefugnisse, die den Strafverfolgungsorganen zugesprochen werden, und der Notwendigkeit, Missbrauch zu verhindern. Nur durch **gerichtliche Kontrolle** kann ein effektiver Schutz der Grundrechte sichergestellt werden.[53] Der Verfassungsgericht hält fest, dass auch bei der Sicherstellung von Datenträgern ein **Richtervorbehalt** notwendig ist. Er belässt es aber nicht nur bei dieser formellen Voraussetzung:

In Anbetracht der weitreichenden Befugnisse, die den Strafverfolgungsbehörden durch § 110 Abs 1 Z 1 und § 111 Abs 2 der StPO eingeräumt werden, ist es **Aufgabe des Gerichts**, bei der Bewilligung einer Sicherstellung eines Datenträgers und dessen späterer Auswertung **genau festzulegen**, welche Arten von **Daten, Dateninhalte, für welchen Zeitraum und zu welchen Untersuchungszwecken** ausgewertet werden dürfen.[54]

Der Verfassungsgerichtshof sieht, insbesondere im Kontext der Sicherstellung und späteren Auswertung von Daten auf Datenträgern, **keinen sachlich gerechtfertigten Grund**, warum eine gerichtliche Bewilligung lediglich für die Beschlagnahme von (in der Regel zunächst sichergestellten) Gegenständen gemäß § 109 Z 1 lit a StPO erforderlich ist, und nicht bereits für die Sicherstellung (vgl § 115 Abs 2 StPO).[55]

Bei sichergestellten Datenträgern liegt nach einer grundsätzlich zulässigen Auswertung der gespeicherten Daten kaum ein zusätzlicher Nutzen in der formellen Beschlagnahme des Datenträgers nach § 115 StPO; die entscheidenden Ermittlungsschritte beschränken sich meist auf das Kopieren aller Daten des gesicherten Datenträgers auf ein Medium der Strafverfolgungsbehörden und deren nachfolgende Auswertung. Durch die Auswertung und Speicherung oder anderweitige Sicherung der von den Strafverfolgungsbehörden ermittelten Daten werden diese **de facto beschlagnahmt**, ohne dass die Schutzmaßnahmen des § 115 Abs 2 StPO beachtet werden müssen.[56]

Die Ermittlungsbefugnisse, die der Staatsanwaltschaft (und der Kriminalpolizei) durch § 110 Abs 1 Z 1 und § 111 Abs 2 StPO gewährt werden, **ohne** dass eine **vorherige gerichtliche Bewilligung** erforderlich ist, stehen somit im **Widerspruch** zu § 1 Abs 2 DSG iVm Art 8 Abs 2 EMRK.[57]

Des Weiteren besteht nach der derzeit geltenden Rechtslage weder im Ermittlungsverfahren noch im anschließenden gerichtlichen Hauptverfahren ein **ausreichender Rechtsschutz** für Betroffene einer Sicherstellung.[58] Nach Ansicht des VfGH bieten die bestehenden Rechtsschutzmöglichkeiten **keinen adäquaten Schutz** gegen die umfangreichen Ermittlungsbefugnisse, die den Strafverfolgungsorganen durch § 110 Abs 1 Z 1 und § 111 Abs 2 der StPO eingeräumt werden, im Lichte des § 1 des DSG iVm Art 8 der EMRK.[59]

So erlaubt § 110 Abs 4 StPO einem Betroffenen zwar, die Aufhebung der Sicherstellung bei Gericht zu beantragen; dieses prüft jedoch nicht, ob die bereits erfolgte Sicherstellung und die darauf folgende Auswertung der Daten **rechtmäßig** waren.[60] Die Möglichkeit des Einspruchs nach § 106 StPO bei Rechtsverletzungen durch Ermittlungsmaßnahmen und das Recht auf Berichtigung, Ergänzung oder Löschung unrichtiger Daten nach § 75 StPO können zwar in gewissem Maße Schutz bieten, gewährleisten jedoch **keinen umfassenden Rechtsschutz**, da Betroffene oft gar nicht von möglichen Rechtsverletzungen wissen oder keine Kenntnis von den genauen Vorgängen bei der Datenauswertung haben. Dies beeinträchtige die Verteidigungsmöglichkeiten erheblich.[61]

Angesichts der im Zusammenhang mit der Auswertung der auf einem Datenträger (lokal oder extern) gespeicherten Daten den Strafverfolgungsorganen zur Verfügung stehenden, mannigfaltigen technischen Möglichkeiten und rechtlichen Befugnisse, welche intensive Eingriffe in das Grundrecht auf Datenschutz gemäß § 1 DSG und das Grundrecht auf Privat- und Familienleben gemäß Art 8 EMRK ermöglichen, **genügt es** nach Auffassung des Verfassungsgerichtshofes **nicht**, wenn der Gesetzgeber den Strafverfolgungsorganen die Wahrung des allgemeinen **Verhältnismäßigkeitsgrundsatzes** in § 5 StPO aufträgt.[62]

Mit diesen Argumenten begründet der VfGH einen Verstoß der angefochtenen Bestimmungen gegen das Recht auf Datenschutz nach § 1 Abs 2 DSG sowie das Recht auf Privat- und Familienleben nach Art 8 Abs 2 EMRK. Sie sind somit verfassungswidrig.

Die angefochtenen Bestimmungen treten (spätestens) zum **1. Januar 2025** außer Kraft, wodurch dem Gesetzgeber bis zu diesem Zeitpunkt eine sogenannte **Reparaturfrist** eingeräumt wird. Dieser hat bis dahin für eine verfassungskonforme Neuregelung zu sorgen.

c. Schlussfolgerungen und Hinweise an den Gesetzgeber

Der VfGH hält einen **Richtervorbehalt** bloß zu Beginn, nämlich bei der Bewilligung der Anordnung zur Sicherstellung

[52] Punkt 2.2.9. bzw Rz 77 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[53] Punkt 2.2.9. bzw Rz 78 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[54] Punkt 2.2.9. bzw Rz 79 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[55] Punkt 2.2.9.1. bzw Rz 80 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[56] Punkt 2.2.9.1. bzw Rz 81 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[57] Punkt 2.2.9.1. bzw Rz 82 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023; vgl auch VfSlg. 19.892/2014.
[58] Punkt 2.2.10. bzw Rz 83 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[59] Punkt 2.2.10.2. bzw Rz 86 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[60] Punkt 2.2.10.2. bzw Rz 87 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[61] Punkt 2.2.10.2. bzw Rz 88 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[62] Punkt 2.2.10.3. bzw Rz 92 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.

von Datenträgern, für **unzureichend**, da dies angesichts der technischen Möglichkeiten und rechtlichen Befugnisse der Strafverfolgungsbehörden nicht genug Schutz für die Betroffenen gemäß § 1 DSG und Art 8 EMRK bietet.[63] Vielmehr ist es auch erforderlich, dass im Vorfeld festgelegt wird, welche **Datenkategorien**, welche **Dateninhalte**, welcher **Zeitraum** zu welchem **Zweck** ausgewertet werden dürfen.[64]

Der Gesetzgeber muss den strafprozessualen Rahmen der Ermittlungsmaßnahmen zur Sicherung und Auswertung von Daten auf Datenträgern so gestalten, dass sowohl das **öffentliche Interesse** an der Strafverfolgung als auch die **Grundrechte** der Betroffenen, insbesondere der Schutz der Geheimhaltungsinteressen und der Schutz der Privatsphäre, angemessen berücksichtigt werden.[65]

Die Anforderungen an den rechtlichen Rahmen für die Sicherung und Auswertung von Daten variieren je nach der **Intensität des Eingriffs**, die durch die spezifischen gesetzlichen Regelungen entsteht.[66] Der Gesetzgeber muss dabei unter anderem folgende Punkte berücksichtigen:

Generell kann es laut VfGH bedeutsam sein, ob die Gesetzgebung die Sicherstellung und Auswertung von Daten auf Datenträgern bei einem Anfangsverdacht einer Straftat erlaubt, **ohne** die **Schwere der Tat**, das durch die Straftat geschützte **Rechtsgut** oder den spezifischen Datenträger, der typischerweise bei solchen Straftaten verwendet wird, zu berücksichtigen, oder ob solche Maßnahmen ausschließlich für **bestimmte Straftaten** vorgesehen sind.[67]

Des Weiteren ist für die verfassungsrechtliche Bewertung der Sicherstellung von Datenträgern entscheidend, ob gesetzliche Maßnahmen ergriffen wurden, um die Auswertung der sichergestellten Daten auf das **notwendige Maß zu beschränken** und sowohl organisatorisch als auch technisch **transparent** und **überprüfbar** zu gestalten.[68]

Der Gesetzgeber muss sicherstellen, dass Personen, deren Daten sichergestellt und ausgewertet werden, angemessen über die für die **Verteidigung ihrer Rechte** im Ermittlungsverfahren (und möglicherweise im anschließenden Hauptverfahren) erforderlichen Informationen verfügen können.[69]

Zudem ist es von Bedeutung, dass im Zuge der **Abwägung** zwischen dem **Interesse der Strafverfolgung** und dem **Schutz der Rechte der Betroffenen**, insbesondere in Bezug auf den Umfang und die Art der auf einem sichergestellten Datenträger zugänglichen und ausgewerteten Daten, effektive Maßnahmen einer **unabhängigen Aufsicht** vorgesehen werden. Diese soll überwachen, ob die Strafverfolgungsbehörden innerhalb der gesetzlichen und gerichtlichen Vorgaben agieren und ob die Rechte der Betroffenen hinsichtlich des Schutzes der Privatsphäre und der Geheimhaltungsinteressen während der Datenauswertung angemessen gewahrt bleiben, selbst wenn die Betroffenen bei der Auswertung ihrer Daten nicht anwesend sind.[70]

3. Auswirkungen der Entscheidung G 352/2021 des VfGH auf Fälle im Jahr 2024

Bis zum Inkrafttreten der Neuregelung der Sicherstellungsbestimmungen von Datenträgern im Jahr 2025 sind die grundrechtlichen Erwägungen und Ausführungen des Verfassungsgerichtshofes zur Verhältnismäßigkeit keineswegs bloße Theorie, sondern **unmittelbar und bereits zum jetzigen Zeitpunkt in verfassungskonformer Interpretation der §§ 5, 110 ff StPO zu berücksichtigen**.[71] Die sehr weitreichenden Ausführungen des VfGH stellen einen **höchstgerichtlich eingeleiteten Paradigmenwechsel im Strafprozessrecht** dar.

Praktikable Verhältnismäßigkeitserwägungen setzen voraus, dass die laut Verfassungsgerichtshof notwendige Festlegung von Datenkategorien, Dateninhalten, Zeiträumen und Zwecken zur Eingrenzung der Datenauswertung auf den sichergestellten Endgeräten **auch von der Staatsanwaltschaft berücksichtigt werden**.

Für die Kriterien der Auswertung können beispielsweise die Schwere des Verdachtsgrades, die Strafdrohung sowie der Deliktstypus eine Rolle spielen. **Die Auswertung ist auf das, was aufgrund der Verdachtslage konkret gesucht wird, zu beschränken**. Die Strafverfolgungsbehörden müssen nicht auf eine Sanierung der verfassungswidrigen Sicherstellungsbestimmungen warten,[72] sondern sind verpflichtet, die vom Verfassungsgerichtshof für erforderlich erachteten Verhältnismäßigkeitserwägungen bereits jetzt über **§ 5 StPO** zu berücksichtigen und in **verfassungskonformer Interpretation (§ 1 DSG, Art 8 EMRK) der relevanten Bestimmungen nach §§ 5, 110 StPO umsetzen**. In diese Richtung argumentiert auch Brandstetter, wenn er ausführt, dass es „geboten [ist], die jetzt bis Jahresende noch bestehende Regelung im Lichte der Entscheidung verfassungskonform und dementsprechend vorsichtig zu interpretieren, zumal davon nicht nur § 1 DSG und Art 8 EMRK (Persönlichkeitsschutz), sondern in jüngster Zeit auch die Art 6 EMRK (faires Verfahren) und Art 10 EMRK (Medienfreiheit) und naturgemäss [sic!] auch die entsprechenden Grundrechtsgarantien in der EU-Grundrechtecharta (insbes Art 7, 8, 11 und 48) betroffen waren und sind".[73]

[63] Vgl. auch VfSlg. 20.356/2019.
[64] Punkt 2.2.9. bzw Rz 79 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023; vgl idZ auch Soyer/Marsch, Handysicherstellung ohne vorherige richterliche Bewilligung verfassungswidrig, JSt-Slg 2024/4, 57 (67f).
[65] Punkt 2.2.11.5 bzw Rz 97 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[66] Punkt 2.2.11.5 bzw Rz 98 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[67] Punkt 2.2.11.5 bzw Rz 99 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[68] Punkt 2.2.11.5 bzw Rz 100 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[69] Punkt 2.2.11.5 bzw Rz 101 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[70] Punkt 2.2.11.5 bzw Rz 102 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[71] So auch Soyer/Marsch, Handysicherstellung ohne vorherige richterliche Bewilligung verfassungswidrig, JSt-Slg 2024/4, 57 (67).
[72] Soyer/Marsch, Handysicherstellung ohne vorherige Bewilligung verfassungswidrig, Anmerkung zu VfGH 14.12.2023, G 352/2021, JSt 2024, Heft 1, 57 (68).
[73] Brandstetter, VfGH: Neue Vorgaben für die Sicherstellung von Mobiltelefonen, MR 1/24, 25 (27).

Eine Änderung des Gesetzes ist hierfür ebenso wenig notwendig wie ein Erlass[74] des Justizministeriums. Hinzuweisen ist auch auf den Umstand, dass die Bundesregierung – und damit auch die Justizministerin als Spitze der Weisungskette der Staatsanwaltschaften – im Verfahren vor dem Verfassungsgerichtshofes einstimmig[75] die Ansicht vertrat, dass bei der Sicherstellung und Auswertung von Datenträgern von den **Strafverfolgungsbehörden der Grundsatz der Verhältnismäßigkeit gemäß § 5 Abs 1 und 2 StPO unter Berücksichtigung grundrechtlicher Vorgaben, insbesondere von Art 8 EMRK und § 1 DSG zu berücksichtigen ist**.[76] Dies betont auch der Verfassungsgerichtshof in der zitierten Entscheidung[77] – und bereits seit 2020 im Hinblick auf die EMRK auch der Oberste Gerichtshof.[78]

4. Exkurs: Der Stampiglienbeschluss im Lichte der VfGH-Entscheidung

Selbst wenn der Gesetzgeber in der Neuregelung einen Richtervorbehalt vorsieht, sind dadurch längst nicht alle Probleme in der Paxis gelöst. Durch die Entscheidung des VfGH rückt nämlich ein bestehendes Problem erneut in den Fokus: der sogenannte **Stampiglienbeschluss**.

Der Stampiglienbeschluss bezieht sich auf eine Praxis, bei der im österreichischen Ermittlungsverfahren der **Haft- und Rechtsschutzrichter** (auch HR-Richter genannt) die Anordnungen der Staatsanwaltschaft für Ermittlungsmaßnahmen wie Hausdurchsuchungen mit einer **Bewilligungsstampiglie** versehen, die bei Übernahme der Argumentation der Staatsanwaltschaft durch das Gericht im Wesentlich besagt: **„Die Anordnung wird aus den in der Anordnung angeführten Gründen bewilligt."**[79] Diese Praxis erlaubt es dem Richter, sich die Begründung der Staatsanwaltschaft **„zu eigen"** zu machen, ohne eine eigenständige richterliche Begründung zu formulieren, sofern seine Ansicht mit der Begründung der Staatsanwaltschaft übereinstimmt.[80]

a. Kritik

Diese Vorgehensweise wird in der juristischen Fachliteratur **kritisiert**, da sie den HR-Richtern die **Abwägungsarbeit** abnehmen würde, die mit einer eigenständigen schriftlichen Begründung einer Ermittlungsmaßnahme verbunden wäre.[81] Ein weiterer Kritikpunkt ist, dass der richterliche Abwägungsprozess hinsichtlich des **Grundrechtseingriffs** für die Betroffenen nicht nachvollziehbar sei, da die Gewichtung einzelner Argumente der staatsanwaltschaftlichen Begründung unklar bliebe. Dies schränke die **Verteidigungsmöglichkeiten** der Betroffenen erheblich ein, da eine eigenständige richterliche Begründung in der Regel nur durch eine Beschwerde gegen die gerichtliche Bewilligung erlangt werden könne.[82]

Die Verwendung einer Stampiglie bzw anderer Beschlussvordrucken zur Genehmigung von Zwangsmitteln erscheint auch **nicht gesetzeskonform**[83], da § 86 Abs 1 StPO vorsieht, dass ein Beschluss (i) Spruch, (ii) Begründung und (iii) Rechtsmittelbelehrung zu enthalten hat. § 86 Abs 1 StPO betont zudem, dass in der Begründung die tatsächlichen Feststellungen und die rechtlichen Überlegungen auszuführen sind, die der Entscheidung zugrundegelegt werden. Auch wenn der Oberste Gerichtshof[84] die Praxis der Stampiglienbeschlüsse in einigen Fällen für **zulässig** angesehen hat, indem er argumentierte, dass ein Verweis des Richters auf die Begründung der Staatsanwaltschaft als eigene Begründung angesehen werden kann, ist dennoch zu berücksichtigen, dass dies die **im Gesetz vorgesehene ausdrückliche Begründungspflicht faktisch untergräbt**.[85]

Kritisch zu sehen ist vor allem, dass eine solche Vorgehensweise die Gefahr birgt, dass die **richterliche Unabhängigkeit** und die tiefergehende Auseinandersetzung mit dem Fall in den Hintergrund rücken könnten.[86]

Auch das Ansehen der Justiz und **die rechtsstaatlichen Prinzipien**[87] können darunter leiden, zumal bei derart eingriffsintensiven Vorgehensweisen der Grundsatz „Justice must not only be done, it must also be seen to be done"[88] in besonderer Weise zu berücksichtigen ist.

b. Statistik und Anscheinsproblematik

Auch die **hohe Bewilligungsquote** von Ermittlungsmaßnahmen durch staatsanwaltschaftliche Anordnungen deutet auf eine mögliche Schieflage in der richterlichen Prüfpraxis hin. So werden etwa **98,7 Prozent** der beantragen Hausdurchsuchungen der WKStA schlussendlich auch bewilligt.[89] Diese hohe Bewilligungsquote und die überwiegende Verwendung des Stampiglienbeschlusses bei der Bewilligung werfen rechtsstaatliche Fragen auf, die auch im Gesetzgebungsprozess zur Neuregelung zu berücksichtigen sind.

Im Hinblick auf die besonders intensiven Grundrechtseingriffe ist die Praxis des Stampiglienbeschlusses unseres Erachtens **zu überdenken**. Es bedarf einer **klaren gesetzliche**

[74] Vgl. zur Möglichkeit eines Erlasses durch das Justizministerium: Krakow, Der VfGH-Entscheid zur Handy-Abnahme kann rasch umgesetzt werden, DerStandard, 21.12.2023.
[75] Vgl. Soyer/Marsch, Handysicherstellung ohne vorherige richterliche Bewilligung verfassungswidrig, JSt 2024, Heft 1, 57 (69); zur im Normprüfungsverfahren vertretenen Rechtsansicht der Bundesregierung im Detail Prior, Sicherstellung Auswertung elektronischer Daten, AnwBl 2023, 554.
[76] Vgl. Punkt 9.2. zu Punkt I. (Antrag) bzw Rz 16 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[77] Punkt 2.1.5. und 2.2.10.3 bzw Rz 46 und 91 der Entscheidung G 352/2021 des Verfassungsgerichtshofes vom 14.12.2023.
[78] OGH 28.07.2020, 11 Os 51/20i; OGH 13.10.2020, 11 Os 56/20z.
[79] Schönborn/Seidl, Stampiglienbeschluss als rechtsstaatliches Feigenblatt, Die Presse 2024/05/05.
[80] Tipold in Fuchs/Ratz, WK StPO § 86 Rz 8/1 (Stand 15.3.2023, rdb.at).
[81] So z.B. Tipold in Fuchs/Ratz, WK StPO § 86 Rz 8/3 (Stand 15.3.2023, rdb.at); Schönborn/Seidl, Stampiglienbeschluss als rechtsstaatliches Feigenblatt, Die Presse 2024/05/05.
[82] Schönborn/Seidl, Stampiglienbeschluss als rechtsstaatliches Feigenblatt, Die Presse 2024/05/05.
[83] Tipold in Fuchs/Ratz, WK StPO § 86 Rz 8/1 (Stand 15.3.2023, rdb.at); Bertel/Flora/Venier, Komm StPO2 § 86 Rz 2ff; Venier/Tipold, Strafprozessrecht15 Rz 103; aA Köhl, Stampiglienbeschlüsse: Verbot brächte „überflüssiges Schreibwer", Die Presse 2024/06/06.
[84] OGH 14 Os 109/08y EvBl 2008/173 = SSt 2008/57.
[85] Tipold in Fuchs/Ratz, WK StPO § 86 Rz 8/3 (Stand 15.3.2023, rdb.at).
[86] Tipold in Fuchs/Ratz, WK StPO § 86 Rz 8/3 (Stand 15.3.2023, rdb.at).
[87] Tipold in Fuchs/Ratz, WK StPO § 86 Rz 8/3 (Stand 15.3.2023, rdb.at); Bertel/Flora/Venier, Komm StPO2 § 86 Rz 3.
[88] EGMR 17.1.1970, 2689/65, Delcourt/Belgien.
[89] Anfragebeantwortung BMJ vom 31.3.2023, 13539/AB zu 1375/J 27 GP.

Vorgabe für eine eigenständige Begründungspflicht des bewilligenden Gerichts. Dies würde auch eine **Aufstockung des Personals** bei HR-Richtern erforderlich machen, um die **Qualität** der richterlichen Prüfung und die **Grundrechtskonformität** der Ermittlungsmaßnahme zu gewährleisten. Die Entscheidung des VfGH zur Handysicherstellung bietet somit eine Gelegenheit, die richterliche Beschlusspraxis im Hinblick auf **Grundrechte** und **Datenschutz** zu überdenken und zu reformieren. Sollte es der Gesetzgeber verabsäumen, Änderungen dahingehend vorzunehmen, würde nach einer Neuregelung der (verfassungswidrigen) Bestimmungen über die Sicherstellung von Datenträgern das nächste Problem bereits warten, das **verfassungsrechtliche Fragen** aufwerfen würde.

III. Conclusio

Der VfGH hat festgestellt, dass die **angefochtenen Bestimmungen** des § 110 Abs 1 Z 1 und Abs 4 sowie § 111 Abs 2 StPO, die den Ermittlungsbehörden die Sicherstellung von Mobiltelefonen und anderen Datenträgern aus Beweiszwecken ohne richterliche Bewilligung ermöglichen, **verfassungswidrig** sind. Diese Entscheidung betont, dass die derzeitige Rechtlage nicht den Anforderungen des Rechts auf Datenschutz nach § 1 DSG sowie des Rechts auf Privat- und Familienleben nach Art 8 EMRK entspricht.

Die Sicherstellung und Auswertung von Daten auf Mobiltelefonen und anderen Datenträgern wird aufgrund der potentiellen Zugänglichkeit umfangreicher persönlicher Informationen als **besonders eingriffsintensiv** betrachtet. Diese Maßnahmen ermöglichen es den Strafverfolgungsbehörden, ein umfassendes Profil der betroffenen Person zu erstellen, was einen **tiefgreifenden Eingriff in die Privatsphäre** darstellt.

Die Entscheidung des VfGH hebt hervor, dass bei der Anwendung von Ermittlungsmaßnahmen das **Verhältnismäßigkeitsprinzip** zu wahren ist. Insbesondere müssen der Sicherstellung und Auswertung der Daten eine **richterliche Bewilligung** vorausgehen und darüber hinaus muss dieser Vorgang auf das für die Strafverfolgung notwendige Maß beschränkt und transparent sowie überprüfbar gestaltet sein.

Der Gesetzgeber hat eine Reparaturfrist bis 1. Januar 2025 eingeräumt bekommen, um eine verfassungskonforme Neuregelung der Sicherstellungsbestimmungen von Datenträgern zu schaffen. Es besteht nun die Notwendigkeit für den österreichischen Gesetzgeber, die rechtlichen Bestimmungen zur Sicherstellung und Auswertung von Daten auf Datenträgern zu überarbeiten. Dabei müssen insbesondere die Anforderungen des **Datenschutzes** und der **Privatsphäre** stärker berücksichtigt werden. Die neuen Regelungen sollten klare Vorgaben bezüglich der Voraussetzungen, des Umfangs und der Verfahren bei der Sicherstellung und Auswertung von Daten enthalten.

Die Entscheidung des VfGH unterstreicht die zunehmende Bedeutung des Schutzes persönlicher Daten und der Privatsphäre im digitalen Zeitalter. Die Überarbeitung der gesetzlichen Bestimmungen bietet die Chance, die Grundrechte betroffener Personen weiter zu stärken und den Datenschutz effektiver zu gestalten.

Die Entscheidung könnte auch **über Österreich hinaus** Bedeutung erlangen, indem sie als Referenzpunkt für ähnliche rechtliche Überprüfungen und allfällige gesetzliche Anpassungen in anderen Jurisdiktionen dient. Sie setzt ein starkes Signal für die Notwendigkeit, bei der strafrechtlichen Ermittlung und Beweisführung den Datenschutz und die Privatsphäre zu wahren.

Insgesamt fordert die Entscheidung des VfGH eine **sorgfältige Abwägung** zwischen den **Notwendigkeiten der Strafverfolgung** und dem **Schutz der Grundrechte**, insbesondere in Bezug auf Datenschutz und Privatsphäre. Die zukünftige gesetzliche Neugestaltung wird zeigen, wie Österreich diesen Herausforderungen begegnet und welche Standards für den Umgang mit persönlichen Daten im Rahmen von strafrechtlichen Ermittlungen gesetzt werden.

Oberstaatsanwalt a.D. Raimund Weyand, St. Ingbert

Entscheidungen zum Insolvenzstrafrecht

I. Strafprozessrecht

1. Befangenheitsantrag der Staatsanwaltschaft – § 24 StPO

Bei den gesetzlichen Vorschriften, nach denen ein Richter wegen Besorgnis der Befangenheit abgelehnt werden kann (§ 24 Abs. 1 und 2, § 31 StPO), handelt es sich nicht um Rechtsnormen, die im Sinne des § 339 StPO lediglich zugunsten des Angeklagten wirken. Die Staatsanwaltschaft kann in Ausübung ihrer Rolle als „Wächterin des Gesetzes" Rechtsfehler im Zusammenhang mit der Entscheidung über von ihr gestellte Ablehnungsgesuche ungeachtet von deren Angriffsrichtung mit der Revision rügen. Ein Ablehnungsgesuch der Staatsanwaltschaft ist gerechtfertigt, wenn sie bei verständiger Würdigung der ihr bekannten Umstände Grund zu der Besorgnis hat, dass der Richter gegenüber dem rechtlich zu würdigenden Sachverhalt oder den daran Beteiligten nicht unvoreingenommen und unparteilich ist.

BGH, Urteil vom 25.10.2023 – 2 StR 195/23, NJW 2024, 846.

In der entschiedenen Sache hatte eine Schöffin die lediglich weitläufige persönliche Bekanntschaft mit einem Angeklagten angezeigt, was die Strafkammer aber nicht als Befangenheitsgrund ansah. Nach Auffassung des BGH hat die Kammer die angesichts der konkreten Umstände der Angelegenheit gebotene Gesamtschau des Sachverhalts vernachlässigt: Der