

Bericht

des Budgetausschusses

über den Antrag 6/A der Abgeordneten Mag. Harald Stefan, Kolleginnen und Kollegen betreffend ein Bundesgesetz, mit dem die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz, das Gerichtsorganisationsgesetz, das Finanzstrafgesetz, das Justizbetreuungsagentur-Gesetz und das Allgemeine Verwaltungsverfahrensgesetz 1991 geändert werden (Strafprozessrechtsänderungsgesetz 2024)

Die Abgeordneten Mag. Harald **Stefan**, Kolleginnen und Kollegen haben den gegenständlichen Initiativantrag am 24. Oktober 2024 im Nationalrat eingebracht und wie folgt begründet:

„Hauptgesichtspunkte des Antrags:

Der vorliegende Antrag soll die bisher bestehende Möglichkeit der Sicherstellung ‚aus Beweisgründen‘ in Folge des Erkenntnisses des VfGH vom 14.12.2023, G 352/2021, einem grundlegenden und den Anforderungen des VfGH entsprechenden Rechtsrahmen zuführen und zu einer Stärkung von Beschuldigten- und Opferrechten sowie zu einer Erhöhung der Effizienz und Beschleunigung von Ermittlungsverfahren führen sowie auf Basis von Erfahrungen und Reformvorschlägen aus dem Bereich der Staatsanwaltschaften betreffend den Bereich der Cyberkriminalität und unter Berücksichtigung aktueller Rechtsprechung und Literatur beruhende legistische Anpassungen vornehmen.

Die Vorschläge zu einer Stärkung von Beschuldigten- und Opferrechten sowie zu einer Erhöhung der Effizienz und Beschleunigung von Ermittlungsverfahren dienen auch der **Umsetzung mehrerer Punkte des Regierungsprogramms der Bundesregierung 2020-2024 ‚Aus Verantwortung für Österreich‘** (in Folge ‚Regierungsprogramm‘), und zwar:

- Erhöhung der Qualität von SV-Gutachten (S. 22),
- verpflichtende Veröffentlichung im RIS zumindest von Urteilen der Oberlandesgerichte (S. 22),
- Stärkung der Staatsanwaltschaften zur unabhängigen Ermittlungsarbeit im verfassungsrechtlichen Rahmen durch (u.a.) Verkürzung der Ermittlungsverfahren und durch Entfall von vermeidbaren Berichten (S. 25 f.),
- Prüfung der Ausweitung des Antrags auf Einstellung nach § 108 StPO (S. 28).

I. Allgemeiner Teil

I. Änderungen in Folge des Erkenntnisses des VfGH vom 14. Dezember 2023, G 352/2021 und des Urteils des EuGH vom 4. Oktober 2024, Rechtssache C 548/21, der Richtlinie (EU) 2016/680 sowie der Verordnung (EU) 2024/1689

Nach dem Erkenntnis des VfGH, mit dem er die Bestimmungen der **§ 110 Abs. 1 Z 1** und **Abs. 4 StPO** sowie **§ 111 Abs. 2 StPO**, wegen Verstoßes gegen das Grundrecht auf Datenschutz nach **§ 1 DSGVO** und das Recht auf Achtung des Privat- und Familienlebens nach **Art. 8 EMRK** mit **Ablauf des 31.12.2024 als verfassungswidrig aufgehoben** hat, variieren – abhängig von der durch die konkrete gesetzliche Ausgestaltung bewirkten Intensität des Eingriffes – die verfassungsrechtlichen Anforderungen an die neu zu schaffenden Regelungen. Im Lichte des vom VfGH dargestellten beweglichen Systems, in welchem jedoch neben der Erforderlichkeit und Verhältnismäßigkeit der Maßnahme sowie der gerichtlichen

Bewilligung vom Gesetzgeber wesentliche Schranken für die Zulässigkeit festzulegen sind, die Eingriffsschranke des § 1 Abs 2 zweiter Satz DSGVO zu beachten ist, sowie der im Begutachtungsverfahren geäußerten Bedenken, werden Neuregelungen vorgeschlagen, die das öffentliche Interesse an der Verfolgung und Aufklärung von Straftaten mit den grundrechtlich geschützten Interessen der Betroffenen gegeneinander abwägt und entsprechend in Ausgleich bringt, dabei jedoch die gesetzlichen Leitungs- und Kontrollbefugnisse der Staatsanwaltschaft gegenüber der Kriminalpolizei und das öffentliche Interesse an der Strafverfolgung berücksichtigt.

Das Urteil des EuGH verlangt neben der Erforderlichkeit der Maßnahme und der gerichtlichen Bewilligung für die Zulässigkeit einen konkreten Tatverdacht (objektive Anhaltspunkte), eine Definition von Art und Kategorien der aufzuklärenden Taten, die Berücksichtigung bestimmter Kriterien bei der Verhältnismäßigkeitsprüfung, insbesondere ob die Daten beim Beschuldigten oder anderen Betroffenen sichergestellt werden, eine Unterscheidung nach Datenkategorien (nur Standort oder Fotos, Kommunikation oder sogar besonders geschützte Daten) sowie eine Verarbeitung und Speicherung der Daten nur im erforderlichen Umfang und der erforderlichen Dauer. Darüber hinaus muss eine Gefahr in Verzug-Regelung getroffen werden.

Zusätzlich ist nach dem Erkenntnis des VfGH Befugnismissbrauch zu unterbinden. Die RL (EU) 2016/680 verlangt die Wahrung von Integrität und Vertraulichkeit der personenbezogenen Daten und Verfahren für ihre Vernichtung, um hinreichende Garantien gegen die Gefahr des Missbrauchs und der Willkür zu bieten. Es sind geeignete technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung in Übereinstimmung mit dieser Richtlinie erfolgt. Besonders sensible personenbezogene Daten müssen hinreichend gesichert und der Zugang der Mitarbeiterinnen und Mitarbeiter der zuständigen Behörde zu den Daten strenger geregelt werden.

Soweit die Richtlinie (EU) 2016/680 nicht bis 2018 umgesetzt wurde, ist sie direkt anwendbar. Wenn – wie im Fall der Sicherstellung und Beschlagnahme von Datenträgern und Daten – die nationalen Regelungen nicht unionsrechtskonform interpretiert werden können, dürfen sie nicht angewendet werden (EuGH vom 7. September 2023 Rz 58 ff).

Zu beachten ist darüber hinaus die am 1. August 2024 in Kraft getretene und ab 1. Februar 2025 stufenweise anwendbare Verordnung (EU) 2024/1689, die auch Bereiche der Strafverfolgung und Justizverwaltung betrifft und in diesem Zusammenhang klare Anforderungen an KI-Systeme stellt.

Folglich sollen auch diverse Aspekte, die derzeit nicht gesetzlich geregelt sind, abgebildet werden:

- Einführung einer neuen Ermittlungsmaßnahme für die **„Beschlagnahme von Datenträgern und Daten“**, die eine **vorherige gerichtliche Entscheidung** auf Begründung einer Sicherstellung über Datenträger und Daten **zum Zweck der Auswertung** verlangt. Dadurch sollen im Sinne des Erkenntnisses des VfGH Fälle der Sicherstellung von Gegenständen generell von jenen von Datenträgern, die potentiell sensible Daten enthalten, sowie von Daten getrennt und diese an eine vorherige richterliche Kontrolle geknüpft werden. Das Abstellen auf den Zweck der Auswertung soll zudem den Praxisbedürfnissen Rechnung tragend die vom Erkenntnis des VfGH unberührt gebliebene Möglichkeit der Sicherstellung von Datenträgern zu anderen gesetzlichen Zwecken (§ 110 Abs. 1 Z 2 und 3 StPO) weiterhin erlauben, solange nicht in weiterer Folge eine Auswertung erfolgen soll. Ebenso soll die Sicherstellung und Auswertung von Daten, die mittels Bild- und Tonaufzeichnungsgeräten an öffentlich oder öffentlich zugänglichen Orten aufgenommen wurden, weiterhin möglich sein. In allen übrigen Fällen ist eine gerichtliche Beschlagnahme von Datenträgern und Daten erforderlich, für die folgende Vorgaben gelten:
- **Erhöhung der Begründungspflicht** für die Anordnung der Staatsanwaltschaft und die gerichtliche Entscheidung durch Anlehnung an andere bereits bestehende Ermittlungsmaßnahmen (etwa Auskunft von Daten einer Nachrichtenübermittlung nach §§ 135 ff StPO). Die zusätzlich vorgeschlagene **Verpflichtung der Einschränkung durch Umschreibung der Datenkategorien und Dateninhalte**, die zu beschlagnahmen sind, und in Bezug auf welchen **Zeitraum** dies zu erfolgen hat, soll bereits **zum Zeitpunkt der Antragstellung bei Gericht** erforderlich sein. Die auf Ebene der Einzelfallprüfung stattzufindende Verhältnismäßigkeitsprüfung sowohl durch die Staatsanwaltschaft im ersten Schritt als auch durch den Richter bzw. die Richterin im entscheidenden Schritt soll letztlich zielgerichtet eine klare Abwägung ermöglichen.
- Ausdrückliche gesetzliche Verankerung der Möglichkeit der Beschlagnahme auch von Daten, die in anderen (externen) Speicherorten als einem Datenträger gespeichert sind, soweit auf sie von diesem aus zugegriffen werden kann. Damit sollen sämtliche Fälle umfasst werden, die aufgrund der technischen Entwicklung eine Auslagerung der Speicherkapazitäten vom Datenträger erlauben (z. B.

Cloud-Computing, Server) und auf die vom beschlagnahmten Datenträger aus zugegriffen werden kann.

- Einführung einer **Nichtigkeitssanktion** von Ergebnissen einer Auswertung, wenn die Ermittlungsmaßnahme nicht rechtmäßig angeordnet und bewilligt wurde.
- Die vorgeschlagene Neugestaltung der gesetzlichen Voraussetzungen und Durchführungsbestimmungen verbunden mit einer Gliederung der Beschlagnahme von Datenträgern und Daten in mehrere **Phasen** soll zu einer **erhöhten Transparenz beitragen** und eine **stärkere rechtliche Determinierung insbesondere der Beteiligungsmöglichkeiten von Beschuldigten und Opfern bei der Selektion von erheblichen Tatsachen**, von **Informationspflichten** der Behörden **an alle betroffene Personen** und somit einen erhöhten Rechtsschutz gewährleisten.
- Schaffung einer organisatorischen Transparenz durch Trennung zwischen der Phase der (technischen) Aufbereitung von Daten und der Phase der (inhaltlichen) Auswertung von Daten unter Berücksichtigung der grundsätzlichen Leitungsfunktion der Staatsanwaltschaft im Ermittlungsverfahren, der jedoch gerichtliche Beweisaufnahme (§§ 101 Abs 2 zweiter Satz; 104 StPO; 126 Abs 5 StPO idgF) und selbstverständlich umfassender gerichtlicher Rechtsschutz nicht entgegenstehen. Dadurch könnte auch die befürchtete unzulässige Beschränkung der Befugnisse der EUSTa (EPPO) hintangehalten werden, deren Staatsanwältinnen und Staatsanwälte „selbst Durchsuchungen von Computersystemen anordnen und die Herausgabe gespeicherter Computerdaten im Original oder in anderer Form erwirken können oder solche Ermittlungsmaßnahmen bei Gericht beantragen dürfen“ sollen.
- Die **Phase der Aufbereitung von Daten** unter Einhaltung forensischer Standards soll die – sofern überhaupt erforderlich – **Entsperrung von Speichermedien** (z. B. Datenträger, Cloudspeicher, Server), die **Sicherung von Daten** (allenfalls samt **Wiederherstellung gelöschter Daten**) in Form einer **Originalsicherung (der Rohdaten) des gesamten Datenbestandes** sowie die **Erstellung einer Arbeitskopie** (eine Kopie der Originalsicherung, anhand derer die **konkrete forensisch-technische Aufbereitung** durch das - abgesehen von wenigen gesetzlich geregelten Ausnahmen - ausschließlich für die forensische Aufbereitung zuständige Gericht erfolgt) umfassen.
- Auf die Originalsicherung und Arbeitskopie, deren Verwahrung zur Kontrolle der Rechtmäßigkeit der nachfolgenden Aufbereitungs- und Auswertungsprozesse und der Integrität der Daten erforderlich ist, soll ausschließlich im Fall einer (neuerlichen) **richterlichen Entscheidung zugegriffen** werden können, was auch durch eine entsprechende Verwahrung sowie Schutz vor unbefugter Einsichtnahme oder Veränderung sicherzustellen ist. Die **Arbeitskopie** dient der **Umsetzung des Ergebnisses der Datenaufbereitung iSd gerichtlichen Entscheidung** (in Bezug auf die Datenkategorien und den Zeitraum, die keine inhaltliche Auseinandersetzung mit den Daten erfordern. Diese Phase ist durch besondere Vorkehrungen gekennzeichnet: Das ausschließlich für die forensische Aufbereitung zuständige Gericht hat **anhand der Arbeitskopie die Aufbereitung der Daten durchzuführen** und das **Ergebnis** der Datenaufbereitung **herzustellen und** samt einem **Aufbereitungsbericht an die für die Führung des Ermittlungsverfahrens zuständige Staatsanwaltschaft** zu übermitteln. Damit ist gewährleistet, dass die Arbeitskopie ausschließlich für die Umsetzung der gerichtlichen Entscheidung verwendet wird und der für die Führung des Ermittlungsverfahrens zuständigen Staatsanwaltschaft oder Kriminalpolizei eine Einsichtnahme nur in jene Daten zukommt, die in Bezug auf die Dateninhalte, Datenkategorien und den Zeitraum der gerichtlichen Bewilligung entsprechen. Auf diese Weise ist sichergestellt, dass ein im Vergleich zur derzeitigen Praxis weit geringerer Datensatz den eigentlichen strafrechtlichen Ermittlungen zugrunde liegt, wodurch auch die Betroffenheit jener Personen, deren Datensätze und Daten von einer Beschlagnahme betroffen sind, deutlich gemindert wird. Zugleich ermöglicht der Aufbereitungsbericht eine nachprüfende Kontrolle, ob die gerichtliche Entscheidung in diesem Umfang richtig und vollständig umgesetzt wurde.
- Die **Phase der Auswertung von Daten** soll daher nur mehr diesen **begrenzten Datenbestand** umfassen, der als **Ergebnis der Datenaufbereitung** gewonnen wurde. Die **Kriminalpolizei und die Staatsanwaltschaft** haben diesen Datenbestand sodann im Rahmen der gerichtlichen Bewilligung auf **erhebliche Tatsachen** zu untersuchen, wobei sie auch **Suchparameter zum Zweck der Auswertung** festlegen können. Um die Transparenz der (konkreten) Auswertung zu gewährleisten, müssen die Ergebnisse und gegebenenfalls die Suchparameter im Akt **dokumentiert** werden. Zusätzlich soll ausdrücklich auch **Beschuldigten und Opfern das Recht eingeräumt werden, weitere Suchparameter zu beantragen**, womit zum einen die **Waffengleichheit iSd Art. 6 EMRK** hergestellt wird und zum anderen **Opferschutzinteressen** Rechnung getragen wird. Jene Personen, deren Datenträger und Daten beschlagnahmt wurden, sollen überdies die Möglichkeit haben,

Einsicht zu nehmen. Dies erscheint zweckmäßig, um u.a. die Waffengleichheit mit den Strafverfolgungsbehörden herzustellen; andere (Mit-)Beschuldigte und Opfer sollen hingegen aufgrund des unverhältnismäßigen Eingriffs in die Persönlichkeitssphäre einer anderen Person nicht das Recht haben, in das Ergebnis der Datenaufbereitung Einsicht zu nehmen. Ein Ausgleich soll jedoch dadurch geschaffen werden, dass sie die Möglichkeit haben sollen, Suchparameter zu beantragen und auf diese Weise gegebenenfalls weitere erheblichen Tatsachen zu ermitteln.

- Darüber hinaus wird vorgeschlagen, auch sämtliche betroffene Personen – sohin auch sonstige Personen, deren Daten (mit)gesichert, ausgelesen, aufbereitet und letztlich ausgewertet wurden – das Recht einzuräumen, in die Originalsicherung **insoweit einzusehen, als ihre Daten betroffen sind**. Zu diesem Zweck sollen – vergleichbar der Überwachung von Nachrichten – die Personen über dieses Recht **informiert** werden, **sofern ihre Identität bekannt ist oder ohne besonderen Verfahrensaufwand feststellbar** ist und auf ihren Antrag oder von Amts wegen **Ergebnisse der Auswertung vernichtet** werden, wenn sie nicht bereits in einem anderen Strafverfahren Verwendung finden oder als Beweismittel nicht verwendet werden dürfen. **Gleiches gilt auf Antrag des bzw. der Beschuldigten**, der bzw. die damit eine (partielle) Datenlöschung erreichen kann.
- Die vorgeschlagene Regelung für **Zufallsfunde** kann aufgrund der vorgeschlagenen Vorgehensweise (insb. Zugriff auf die Originalsicherung oder Arbeitskopie nur bei einer – erneuten – gerichtlichen Entscheidung) ausschließlich **die Phase der Auswertung von Daten** in Bezug auf das **Ergebnis der Datenaufbereitung** betreffen. Darüber hinaus gehende Daten können davon per se nicht betroffen sein, weil den Strafverfolgungsbehörden ein rechtmäßiger Zugriff darauf durch den Bewilligungsumfang verwehrt ist. Die Verwertbarkeit von Zufallsfunden orientiert sich überdies an der vergleichbaren Regelung des § 140 Abs 1 Z 4 und Abs 2 StPO.- Ergänzend soll im Sinne der Anforderungen des VfGH eine (zusätzliche) **unabhängige Aufsicht** dadurch verankert werden, in dem die Befugnisse der bzw. des langjährigen und bewährt in der Strafrechtspflege tätigen **Rechtsschutzbeauftragten der Justiz** auch in Bezug auf die neue vorgeschlagene Ermittlungsmaßnahme ausgebaut werden sollen. Seine bzw. ihre vorgeschlagenen besonderen Befugnisse erfordern nicht nur die gesetzliche Verankerung von Informations-, Auskunfts- und Akteneinsichtsrechten, sondern zur Gewährleistung einer effektiven Kontrolle auch die Zurverfügungstellung der zu seiner bzw. ihrer Tätigkeit notwendigen Sach- und Personalressourcen, wobei die Unabhängigkeit insbesondere auch dadurch sichergestellt werden soll, dass bei ihr bzw. ihm ausschließlich Personen tätig sind, die nicht auch in Gerichten oder Staatsanwaltschaften tätig sind. Neben juristischen Mitarbeiterinnen und Mitarbeitern wird dabei auch an technische Expertinnen bzw. Experten zu denken sein, die ihn bzw. sie etwa bei der Kontrolle unterstützen können, ob die Aufbereitung von Daten oder die Auswertung von Daten hinsichtlich eines Zeitraumes der gerichtlichen Entscheidung tatsächlich entspricht. Darüber hinaus soll der bzw. die Rechtsschutzbeauftragte der Justiz Zutrittsrechte in Räume haben, in denen Originalsicherungen, Datenträger und Ergebnisse der Datenaufbereitung aufbewahrt werden und die Aufbereitung von Daten vorgenommen wird. Der Jahresbericht des bzw. der Rechtsschutzbeauftragte über seine bzw. ihre Tätigkeit und Wahrnehmungen im Rahmen seiner bzw. ihrer Aufgabenerfüllung soll künftig auch die neue Ermittlungsmaßnahme umfassen.

Die datenschutzrechtliche Verantwortlichkeit entspricht den für Ermittlungsmaßnahmen generell üblichen Maßstäben. Verantwortlicher gemäß § 36 Abs. 2 Z 8 DSGVO im Bereich der Strafjustiz ist die zuständige Behörde, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Demgegenüber ist Auftragsverarbeiter nach § 36 Abs. 2 Z 9 DSGVO jene Behörde, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Bedient sich nun die Staatsanwaltschaft zur Durchführung einer Analyse einer (zuständigen) Spezialabteilung im Bundesministerium für Inneres, so bleibt die Staatsanwaltschaft Verantwortlicher der Datenverarbeitung. Die unterstützende Einheit wird zum Auftragsverarbeiter. Ersucht daher die Staatsanwaltschaft darum, eine bestimmte Ermittlungshandlung durchzuführen, welche die Verarbeitung personenbezogener Daten zum Gegenstand hat (etwa die Auswertung sichergestellter Daten), ist die Kriminalpolizei als Auftragsverarbeiterin anzusehen (vgl. *Kristoferitsch/Bugelnig* in *Fuchs/Ratz*, WK StPO § 74 Rz 32 und 38), datenschutzrechtlich verantwortlich ist die jeweilig zuständige Staatsanwaltschaft.

II. Stärkung der Beschuldigten- und Opferrechte sowie Maßnahmen zur Verfahrensbeschleunigung

1. Der Stärkung der Beschuldigtenrechte dient dabei insbesondere die Neuregelung bei Beginn und Beendigung des Ermittlungsverfahrens. Durch die vorgeschlagene Beseitigung von ‚Vorfeldermittlungen‘ iSd § 91 Abs. 2 letzter Satz StPO als Schwelle zum Beginn des Ermittlungsverfahrens und die Einbeziehung von im 1. Teil der StPO verorteten Handlungen sollen derzeit bestehende Rechtsschutzdefizite während der (mitunter längerdauernden) Phase der ‚Vorfeldermittlungen‘, deren Umfang durch die Rechtsprechung zudem in den vergangenen Jahren deutlich ausgeweitet wurde,

beseitigt werden. Es soll gesetzlich klargestellt werden, dass ein Ermittlungsverfahren gegen angezeigte Personen bereits dann eingeleitet wird, wenn und sobald die Staatsanwaltschaft oder Kriminalpolizei aufgrund einer Anzeige oder eines Verdachts tätig werden, und damit auch der europarechtlich gebotene Zustand (vgl. S. 41) (wieder) hergestellt werden. Davon ausgenommen sollen lediglich Erkundigungen zur Klärung bleiben, ob auf Grund bestimmter Anhaltspunkte angenommen werden kann, dass ein Sachverhalt einem gesetzlichen Tatbild entspricht (§ 91 Abs. 3 StPO). Damit soll der Kriminalpolizei in einem eng definierten Bereich (in der Regel nach einem Geschehen unmittelbar vor Ort) ebenso wie der Staatsanwaltschaft (im Regelfall bei Eingaben im Hinweisgebersystem; § 2a Abs. 6 StAG) auch weiterhin das Verlangen von Auskunft und das Entgegennehmen einer Mitteilung von einer Person möglich sein, ob überhaupt eine Straftat vorliegt; gegen eine Person gerichtete Tätigkeiten der Strafverfolgungsbehörden sollen jedoch in jedem Fall ein Ermittlungsverfahren auslösen. Damit soll die Rechtssicherheit erhöht werden, weil die Unklarheit, ob eine Tätigkeit der Strafverfolgungsbehörden bereits ein Ermittlungsverfahren auslöst, entfällt. Gegenüber der geltenden Rechtslage werden dadurch (mit Ausnahme der weiterhin bestehenden engen Möglichkeit von Erkundigungen nach § 91 Abs. 3 StPO) zwar im Fall eines Tätigwerdens von Kriminalpolizei oder Staatsanwaltschaft Personen früher als Verdächtiger bzw. Verdächtige erfasst, allerdings wird ihr Rechtsschutz deutlich erhöht: so sollen ihnen künftig ab jeglichem Tätigwerden einer Strafverfolgungsbehörde – anders als derzeit – auch alle Verfahrensgarantien und Beschuldigtenrechte (wie etwa das Recht auf Akteneinsicht oder auf Einspruch wegen Rechtsverletzung) zustehen und – entsprechend der Intention des Strafprozessreformgesetzes, BGBl. I Nr. 19/2004, – (wieder) eine Verrechtlichung des Ermittlungsverfahrens erreicht werden. Ein Schutz vor der anlasslosen Einleitung eines Strafverfahrens besteht auch weiterhin, weil Ermittlungsverfahren auslösende Ermittlungen weiterhin nur bei Vorliegen eines Anfangsverdachts zulässig sind.

Dem bzw. der Angeklagten soll zudem auch richtlinienkonform die Möglichkeit eingeräumt werden, am Gerichtstag zur öffentlichen Verhandlung vor dem Obersten Gerichtshof teilzunehmen.

2. Auch die vorgeschlagenen Maßnahmen zur **Verfahrensbeschleunigung** dienen infolge der dadurch bedingten Verfahrensverkürzung letztlich der Stärkung der Beschuldigtenrechte. Die Arbeitsgruppe im Projekt ‚Qualitätssicherung und Effizienz im Ermittlungsverfahren‘ sprach sich betreffend die **Höchstdauer von Ermittlungsverfahren** (§ 108a StPO) überwiegend gegen die Einführung eines neuen Einstellungsgrunds der langen Verfahrensdauer und für die Beibehaltung des geltenden § 108a StPO mit der Abänderung aus, dass die Einstellung nur auf Antrag möglich sein und die Berechnung der Fristen beschuldigtenbezogen erfolgen sollte. Im Zusammenhang mit der amtswegig vorzunehmenden Überprüfung der Höchstdauer des Ermittlungsverfahrens konstatierte der Wahrnehmungsbericht von Vizekanzler und Bundesminister für Justiz a.D. DDr. Clemens Jabloner einen sich daraus ergebenden hohen Verwaltungsaufwand durch die erforderliche Kalendrierung von Akten, die Vorlage an das Gericht und die Abgabe einer Stellungnahme. Er sprach sich dafür aus, den Verwaltungsaufwand durch eine antragsgebundene Ausgestaltung zu verringern. Die Staatsanwaltschaft müsste dann nicht von sich aus an das Gericht herantreten, sondern der Beschuldigte würde die Möglichkeit einer entsprechenden Antragstellung in die Hand bekommen. Dies könnte dadurch ausgeglichen werden, dass die normierte Höchstdauer von drei auf zwei Jahre herabgesetzt wird.

Auf dieser Basis und unter Berücksichtigung aktueller Rechtsprechung und Literatur ist aus systematischen Gründen künftig eine Differenzierung zwischen § 108 StPO und § 108a StPO kaum mehr argumentierbar, weshalb eine Zusammenführung der beiden Bestimmungen vorgeschlagen wird. Durch die vorgeschlagenen Änderungen zum Antrag auf Einstellung sowie der Überprüfung der Höchstdauer des Ermittlungsverfahrens und deren Zusammenführung in einem neu gestalteten § 108 StPO sollen für Beschuldigte die in der praktischen Anwendung mit Unklarheiten behafteten Fristen für die Erhebung von Anträgen auf Einstellung entfallen. Zudem soll klargestellt werden, dass auch **Anträge auf und die Einstellung von einzelnen Fakten** zulässig sind, was zu einer Verschlinkung und somit Beschleunigung des Verfahrens führen soll. Daran gebunden ist die Erwartung, dass diese erweiterte Reaktionsmöglichkeit auch zu einer Reduzierung jener Fälle führt, in denen die Höchstdauer des Ermittlungsverfahrens überhaupt erreicht oder überschritten wird.

Darüber hinaus soll ein Gericht im Rahmen der Prüfung eines Antrages auf Einstellung – unabhängig von einer allfälligen Überschreitung der Höchstdauer des Verfahrens – bei einer behaupteten Verletzung des Beschleunigungsgebots (§ 9 StPO) der Staatsanwaltschaft stets **konkrete verfahrensbeschleunigende Maßnahmen auftragen** können, wenn eine Verletzung des Beschleunigungsgebots festgestellt wurde und dadurch zu einer fokussierten Führung des Ermittlungsverfahrens beitragen; der bzw. die Beschuldigte soll nicht wie bisher diesbezüglich auf die (zusätzliche) Erhebung eines Einspruchs wegen Rechtsverletzung angewiesen sein. Änderungen im Bereich der Fristenberechnung sollen ebenfalls zu einer Verfahrensbeschleunigung beitragen.

Dem Vorschlag von Bundesminister a.D. DDr. Jabloner folgend soll zudem die **Höchstdauer des Ermittlungsverfahrens von drei auf zwei Jahre herabgesetzt** werden; überdies soll auch die allfällige **Verlängerung** des Verfahrens nicht mehr zwingend um die Dauer von zwei Jahren zu erfolgen haben, vielmehr soll das Gericht die Dauer einzelfallbezogen um **bis zu zwei Jahre** verlängern können, womit ebenfalls die Erwartung einer Verfahrensbeschleunigung einhergeht. An Stelle des Neubeginns der Höchstdauer des Ermittlungsverfahrens nach Fortführung oder Wiederöffnung soll überdies künftig die bereits begonnene Frist nach Wegfall der Einstellung bzw. Abbrechung weiterlaufen, was ebenfalls zu einer Verkürzung der Fristen führen und damit der Verfahrensbeschleunigung dienen soll.

Betreffend die **Trennung von Verfahren** soll einerseits klargestellt werden, dass die bislang bereits in § 27 StPO aufgezählten Gründe demonstrativer Natur sind, gleichzeitig soll als ein weiterer Grund für die Trennung von Verfahren die **Wahrung schutzwürdiger Geheimhaltungsinteressen (§ 1 Abs. 1 DSG) eines bzw. einer Beschuldigten** ergänzt werden. Zur Stärkung der Beschuldigtenrechte soll Beschuldigten ein **subjektives Recht** auf Trennung von Verfahren eingeräumt und damit sichergestellt werden, dass das pflichtgebundene Ermessen einer Staatsanwaltschaft im Rahmen eines Einspruchs wegen Rechtsverletzung (§ 106 StPO) überprüfbar ist (§ 49 Abs. 1 StPO).

Insbesondere vor dem Hintergrund der Entscheidung des Obersten Gerichtshofes vom 24. August 2022, 14 Os 82/22y, wonach § 51 Abs 2 stoppt – nach Maßgabe der in § 74 Abs 2 StPO idgF normierten allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten – die zulässigen Beschränkungen der Akteneinsicht bei Beschuldigten abschließend regelt, sodass in Bezug auf den Umfang der Akteneinsicht im Verhältnis zu Mitbeschuldigten – anders als bei Opfern, Privatbeteiligten oder Privatanklägerinnen bzw. Privatanklägern – keine Interessenabwägung vorzunehmen ist, stellt die vorgeschlagene Ergänzung des § 27 StPO einen datenschutzrechtlich und grundrechtlich gebotenen Ausgleich dar, um die verfassungsrechtlich gewährleisteten Rechte der bzw. des Beschuldigten nach § 1 DSG und Art 8 EMRK zu wahren.

Darüber hinaus steht diese OGH-Entscheidung auch in Widerspruch zur Rechtsprechung der gegenüber Staatsanwaltschaften (nicht jedoch gegenüber den Gerichten) ebenfalls zuständigen Datenschutzbehörde und des Bundesverwaltungsgerichts zum Recht auf Akteneinsicht im Ermittlungsverfahren, wonach keine Beschränkung der Parteienrechte einer bzw. eines Mitbeschuldigten vorliegt, wenn dieser bzw. diesem keine Einsicht in Aktenteile bzw. personenbezogene Daten von Personen in Verfahren (richtig: Verfahrenskomplexen) gewährt wird, an denen sie bzw. er selbst nicht beteiligt ist (BVwG 18.12.2019, GZ W211 2213604-1), hingegen eine Verletzung der bzw. des Beschuldigten in ihrem bzw. seinem Recht auf Geheimhaltung gegeben ist, wenn einer bzw. einem Mitbeschuldigten antragsgemäß – und nach der Rechtsprechung des OGH zutreffend – vollständige Akteneinsicht (§ 51 StPO) auch in Aktenteile gewährt wird, die in keinem sachlichen Zusammenhang mit seiner Tat stehen (DSB 11.03.2021, GZ 2021-0.017.641 [Verfahrenszahl D124.2337]).

Die vorgeschlagene Neuregelung des § 27 StPO würde es der Staatsanwaltschaft sohin ermöglichen, auf entsprechende Entscheidungen der DSB und des BVwG zu reagieren ohne von der für sie selbstverständlich ebenfalls maßgeblichen Rechtsprechung des OGH abzuweichen und dadurch dem doppelten Rechtsschutz im Ermittlungsverfahren Rechnung tragen. Auch wenn die bzw. der Beschuldigte – wie der OGH in ihrer bzw. seiner Stellungnahme zutreffend ausführt – mit einem Einspruch wegen Rechtsverletzung nur einen Ermessensmissbrauch geltend machen kann (§ 106 Abs 1 letzter Satz StPO) und in die Prüfung, ob ein solcher vorliegt, wohl auch die Interessen der Mitbeschuldigten einbezogen werden müssen, ist der praktische Wert der Neuregelung gegeben, weil nicht ersichtlich, inwieweit eine gemeinsame Verfahrensführung insbesondere bei unterschiedlichen Verfahrenskomplexen in Großverfahren geeignet sein soll, Verzögerungen zu vermeiden oder die Haft zu verkürzen, sieht § 27 StPO doch schon jetzt die Trennung des Ermittlungsverfahrens just aus diesen Gründen vor.

Es kann kein Zweifel daran bestehen, dass ein schlanker, übersichtlicher und somit strukturierter Akt dem grundrechtlich geschützten Beschleunigungsgebot (§ 9 StPO) entspricht (Ratz, Führung von Ermittlungsverfahren und Ermittlungsakt, ÖJZ 2020/103 [872]). Geheimhaltungsinteressen von Mitbeschuldigten, aber auch Opfern, insbesondere wenn durch die Tat ihr höchstpersönlicher Lebensbereich betroffen ist, werden dadurch gewahrt.

Darüber hinaus sollen Gerichte künftig im Rahmen der Rufbereitschaft bzw. des Journaldienstes im Fall der mündlichen Bewilligung einer Zwangsmaßnahme den wesentlichen Inhalt des Vorbringens der Staatsanwaltschaft sowie die Gründe für die Dringlichkeit in einem zum Ermittlungsakt zu nehmenden Amtsvermerk festhalten müssen. (§ 105 Abs. 3 StPO). Auch die Staatsanwaltschaft hat die Gründe für die Dringlichkeit der Antragstellung in einem Amtsvermerk festzuhalten. Klargestellt werden soll zudem, dass eine Bewilligung von Zwangsmitteln im Rahmen der Rufbereitschaft bzw. des Journaldienstes nur

erfolgen darf, wenn damit nicht bis zum Beginn der nächsten gerichtlichen Dienststunden zugewartet werden kann. Dementsprechend ist auch die Gültigkeit der gerichtlichen Bewilligung für die Anordnung der Staatsanwaltschaft eng zu befristen.

Ebenso kommen die vorgeschlagenen **Änderungen im Gerichtssachverständigenwesen** vor dem Hintergrund der dadurch intendierten Verfahrensbeschleunigung sowie der Sicherung der Qualität der Sachverständigengutachten dem bzw. der Beschuldigten zugute. Zunächst soll dem bzw. der Sachverständigen (wie auch Dolmetschern bzw. Dolmetscherinnen) künftig im Zuge seiner bzw. ihrer Bestellung eine angemessene Frist zu setzen sein, binnen der Befund oder Gutachten (bzw. Übersetzung) zu erstatten ist. Diese sollen im Zeitpunkt der Befassung bzw. Bestellung künftig nicht nur den Umstand aktueller Fristüberschreitungen bei bereits erfolgten gutachterlichen Beauftragungen in mehr als zehn Verfahren gegenüber der Staatsanwaltschaft oder dem Gericht bekanntzugeben, sondern überdies – von wenigen Ausnahmen abgesehen – auch glaubhaft zu machen haben, dass für die Einhaltung der gesetzten Frist zur Gutachtenserstattung hinreichend vorgekehrt ist, anderenfalls sie nicht bestellt werden dürfen.

3. Darüber hinaus sollen mit dem Antrag auch die jahrzehntelangen stetigen **Verbesserungen im Bereich des Opferschutzes** weiter fortgesetzt werden. So soll das bestens etablierte und international anerkannte Instrument der psychosozialen und juristischen Prozessbegleitung im Strafverfahren neuerlich ausgeweitet werden. Da für Minderjährige das Miterleben jeglicher Form von Gewalt und die neuerliche Konfrontation damit im Rahmen der Vernehmung bei der Polizei oder bei Gericht eine schwerwiegende psychische Belastung darstellen kann, die professioneller Unterstützung bedarf, soll der Anspruch auf psychosoziale und juristische **Prozessbegleitung** im Strafverfahren künftig nicht mehr auf Minderjährige beschränkt sein, die Zeuginnen bzw. Zeugen von Gewalt im sozialen Nahraum (Gewalt in der Familie, Gewalt an Kindern) waren, sondern **allen Minderjährigen, die Zeuginnen bzw. Zeugen von Gewalt waren**, zustehen. Opfer sollen zudem die Übermittlung ihrer personenbezogenen Daten an eine durch die Bundesministerin für Justiz vertraglich mit der Wahrnehmung von Prozessbegleitung beauftragte Opferschutzeinrichtung (§ 66b Abs. 3 StPO) ihrer Wahl verlangen können, soweit dies zum Zweck einer Kontaktaufnahme und Beratung iZm der Inanspruchnahme von psychosozialer und/oder juristischer Prozessbegleitung erforderlich ist.

Im Bereich der Neuregelung bei Beginn und Beendigung des Ermittlungsverfahrens soll – anders als bisher – durch die Möglichkeit der Stellung eines Antrags auf Verfolgung ein **gerichtlicher Rechtsschutz gegen das Absehen von der Einleitung des Ermittlungsverfahrens für Personen, die Opfer** der angezeigten Tat sein könnten, geschaffen werden. Überdies soll durch die massive Einschränkung zulässiger ‚Vorfeldermittlungen‘ auch der Rechtsschutz für Opfer weiter ausgebaut werden, indem ihnen ab Tätigwerden von Kriminalpolizei oder Staatsanwaltschaft (abgesehen vom Fall der Durchführungen von Erkundigungen nach § 91 Abs. 3 StPO) bereits die Opferrechte zukommen.

Darüber hinaus sollen in **Privatanklageverfahren** zur Erwirkung von Anordnungen nach § 135 Abs. 1a oder Abs. 2 Z 2 StPO zur Ausforschung des Täters (§ 71 Abs. 1 StPO) bei typischen ‚Hass-im-Netz-Delikten‘ Opfern von **Hass im Netz** durch Klarstellungen zur Zuständigkeit bei der Akteneinsicht der Zugang zum Recht erleichtert und Zuständigkeitsprobleme vermieden werden. Darüber hinaus soll auch die durch das Hass-im-Netz-Bekämpfungsgesetz (HiNBG, BGBl. I Nr. 148/2020) entfallene Klarstellung, dass in Privatanklageverfahren ein Ermittlungsverfahren nicht stattfindet, wieder in den Gesetzestext aufgenommen werden; eine inhaltliche Änderung ist damit nicht verbunden.

Für die Einbringung eines Fortführungsantrags sollen formale Voraussetzungen, die bei anderen Rechtsmitteln und Rechtbehelfen nicht vorgesehen sind und insbesondere für anwaltlich oft nicht vertretene Opfer eine große Hürde darstellen können, entfallen.

4. Letztlich sollen die vorgeschlagenen Änderungen auch zu einer Entlastung der Staatsanwaltschaften führen, die es ihnen erleichtern soll, sich auf die eigentliche Ermittlungstätigkeit zu fokussieren. So sollen durch den Entfall des § 91 Abs. 2 letzter Satz StPO und die Ermöglichung nur sehr eingeschränkter, klar determinierter ‚Vorfeldermittlungen‘ mitunter rechtlich komplexe Überlegungen, ob eine Tätigkeit bereits ein Ermittlungsverfahren auslösen kann, hinfällig werden. Ebenso soll das Vorgehen bei einer Einstellung eines Ermittlungsverfahrens durch Beseitigung von Abgrenzungsschwierigkeiten hinsichtlich der beiden Ziffern des § 190 StPO entfallen. Eine gewisse Entlastung soll zudem mit der Umgestaltung der Überprüfung der Höchstdauer des Ermittlungsverfahrens von einem amtswegigen Vorgehen der Staatsanwaltschaft zu einer Prüfung im Rahmen eines Antrags des bzw. der Beschuldigten auf Einstellung des Ermittlungsverfahrens erfolgen.

III. Darüber hinaus sollen mit dem gegenständlichen Antrag auf Basis von Erfahrungen und Reformvorschlägen aus dem Bereich der Staatsanwaltschaften betreffend den Bereich der Cyberkriminalität (insbesondere der Sonderreferentinnen bzw. –referenten der Kompetenzstellen sowie Kontakt- und Verbindungsstellen Cybercrime im Rahmen des rezent etablierten Cybercrime-

Qualitätszirkels im Bundesministerium für Justiz), Reformvorschlägen der Vereinigung Österreichischer Staatsanwältinnen und Staatsanwälte (StAV) und unter Berücksichtigung aktueller Rechtsprechung und Literatur sollen weitergehende **legistische Anpassungen im Bereich der Sicherstellung, Beschlagnahme, Ausfolgung und (auch vorzeitigen) Verwertung** vorgenommen werden. Damit soll zum einen **Bedürfnissen der Praxis und der technischen Entwicklung Rechnung getragen** werden, die **Terminologie und Systematik** der StPO in diesem Bereich **vereinheitlicht** und insgesamt zu einem **modernerem und besseren Verständnis** der Gesetzesbestimmungen als auch zu einer **deutlichen Verbesserung der Rechtsposition der Opfer im Bereich der Entschädigung** beigetragen werden.

Mit den vorgeschlagenen Änderungen soll insbesondere von der bislang zum Teil bestehenden Gegenstandsbezogenheit der Bestimmungen über die Sicherstellung, Beschlagnahme, Ausfolgung und Verwertung abgegangen und das System breitflächig um (auch immaterielle) Vermögenswerten ergänzt werden. Unter einem soll in Umsetzung der Richtlinie 2024/1260/EU über die Abschöpfung und Einziehung von Vermögenswerten – der Begriff der Vermögenswerte klar, umfassend und technologieneutral in die StPO eingeführt werden.

IV. Überdies sollen verschiedene in der strafprozessualen Praxis zu Tage getretene Problemstellungen gesetzlich geregelt bzw. klargestellt werden:

So soll eine ausdrückliche Rechtsgrundlage für Kriminalpolizei, Staatsanwaltschaft und Gericht für die Bekanntgabe von personenbezogenen Daten aus einem Strafverfahren im Rahmen einer ‚Fallkonferenz Staatsschutz‘ (§ 6a Abs. 1 SNG) geschaffen werden.

Trotz verfassungsrechtlich höherwertiger Absicherung des Fernmeldegeheimnisses (Art. 10a StGG) gegenüber dem Bankgeheimnis (§ 38 Abs. 2 Z 1 BWG) haben derzeit Kredit- und Finanzinstitute bei der Auskunft über Bankkonten und Bankgeschäfte (§ 116 StPO) mehr Rechtsschutz und Zugang zu personenbezogenen Daten aus einem Strafverfahren als Anbieter von Telekommunikationsdiensten bei der Überwachung von Nachrichten nach § 138 StPO. Diese Ungleichbehandlung soll behoben und der **Schutz personenbezogener Daten der von der durch eine Auskunft über Bankkonten und Bankgeschäfte betroffenen Personen gestärkt** werden, indem künftig die verfahrensrechtlichen Bestimmungen für Kredit- und Finanzinstitute an die bereits seit Jahren geltenden Regelungen für Anbieter von Telekommunikationsdiensten angeglichen werden.

Darüber hinaus sollen **für den Bereich der Staatsanwaltschaften** mit der Ablöse der bisherigen ‚Einschau‘ durch zwei gesonderte Systeme, nämlich die ‚**Innenrevision**‘ einerseits und die ‚**Nachschau**‘ andererseits, nach dem schon bewährten Modell im Gerichtsbereich im Rahmen der Aufsicht unterschiedlich risikogeneigte Bereiche auf zwei komplementäre Prüfkreise verteilt werden. Diese sollen in verschiedenen Intervallen zum Einsatz kommen und einen jeweils unterschiedlichen Fokus bei der Durchführung der Prüfung legen, womit ein wirksames und effizientes System zur Qualitätssicherung bei den Staatsanwaltschaften eingerichtet wird.

V. Schließlich sollen in Entsprechung der im aktuellen Regierungsprogramm verankerten Zielsetzung, die letztinstanzlichen rechtskräftigen Entscheidungen der Oberlandesgerichte in der Entscheidungsdokumentation Justiz zu veröffentlichen, eine **allgemeine Veröffentlichungspflicht der rechtskräftigen Entscheidungen der Oberlandesgerichte, aber auch der Landesgerichte als Rechtsmittelgerichte** (§ 48a GOG) verankert und damit Entscheidungen der Gerichte besser zugänglich werden. Weiters sollen Spezialzuständigkeiten für Verfahren wegen Gewalt im sozialen Nahraum bei den Bezirksgerichten und Gerichtshöfen erster Instanz gesetzlich verankert werden.

VI. Die vorgeschlagenen Änderungen im Bereich der StPO hinsichtlich des Ermittlungsverfahrens sollen auch für den Bereich des **FinStrG** nachvollzogen sowie Regelungen zum Verteidigungskostenersatz vorgeschlagen werden. So sollen § 201 FinStrG („Zu § 108“) und § 205 FinStrG („Zu den §§ 195 196, 197b und 197c“) an den vorliegenden Antrag angepasst werden. Darüber hinaus soll neben rein sprachlichen Änderungen (Umwandlung des als veraltet und diskriminierend eingestuften Begriffes ‚stumm‘ in ‚hochgradig sprachbehindert‘) **§ 228a FinStrG**, der bis dato den Verteidigungskostenersatz in gerichtlichen Finanzstrafverfahren regelt, indem er auf den – mit Erkenntnis des VfGH vom 22.9.2022, G 90/2022 aufgehoben – § 393 Abs. 2 StPO verweist, in Hinblick auf den Verteidigungskostenbeitrag dem Regime der StPO (§§ 196a, 393a StPO) angepasst und insofern auch hier der Stärkung der Beschuldigtenrechte Rechnung getragen werden.

VII. Im Justizbetreuungsagentur-Gesetz (JBA-G) ist eine geringfügige Erweiterung des Geschäfts- und Aufgabenbereiches der Justizbetreuungsagentur vorgesehen.

Die Zuständigkeit des Bundes zur Erlassung dieses Bundesgesetzes ergibt sich aus Art. 10 Abs. 1 Z 6 B-VG („Strafrechtswesen“) und Art. 11 Abs. 2 B-VG („Verwaltungsverfahren“).

VIII. Im Allgemeinen Verwaltungsverfahrensgesetz 1991 (AVG) soll – in Präzisierung der verfassungsgesetzlichen Amtshilferegelung des Art. 22 B-VG – eine gemäß § 76 Abs. 4 StPO erforderliche ausdrückliche gesetzliche Ermächtigung geschaffen werden, um den Behörden eine ordnungsgemäße Vollziehung zu ermöglichen (vgl. OGH 10.12.2019, 11 Os 76/19i).

Kompetenzgrundlage:

Die Zuständigkeit des Bundes zur Erlassung dieses Bundesgesetzes ergibt sich aus Art. 10 Abs. 1 Z 6 B-VG („Strafrechtswesen“) und Art. 11 Abs. 2 B-VG („Verwaltungsverfahren“).

Besonderheiten des Normerzeugungsverfahrens:

Keine.

Verhältnis zu Rechtsvorschriften der Europäischen Union:

§ 69 Abs. 3, § 109 Z 1 lit. a, § 109 Z 1a, § 110 Abs. 3, § 113 Abs. 2, § 114 Abs. 1, Abs. 1a und 2, § 115 Abs. 1, § 115e Abs. 2, § 367, § 379 und § 408 Abs. 2 StPO dienen der Umsetzung der Richtlinie 2024/1260/EU über die Abschöpfung und Einziehung von Vermögenswerten, ABl. Nr. L 1260 vom 24.04.2024 S. 1. § 115i StPO dient der Umsetzung der Richtlinie 2016/680/EU zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. Nr. L 119 vom 27.4.2016 S. 1. § 195 Abs. 2, § 197b und § 197c StPO dienen der Umsetzung der Richtlinie 2012/29/EU über Mindeststandards für die Rechte, die Unterstützung und den Schutz von Opfern von Straftaten sowie zur Ersetzung des Rahmenbeschlusses 2001/220/JI, ABl. Nr. L 315 vom 14.11.2012 S. 57. § 286 Abs. 1 und 2, § 294 Abs. 5, § 296 Abs. 3 und § 471 StPO dienen der Umsetzung der Richtlinie 2016/343/EU über die Stärkung bestimmter Aspekte der Unschuldsvermutung und des Rechts auf Anwesenheit in der Verhandlung im Strafverfahren, ABl. Nr. L 65 vom 11.03.2016 S. 1.

II. Besonderer Teil

Soweit sich im Folgenden keine gesonderte Begründung findet, wird zur Vermeidung von Wiederholungen im Wesentlichen auf die Ausführungen im ursprünglichen Ministerialentwurf und im gleichlautenden Initiativantrag verwiesen

Zu Artikel 1 (Änderung der Strafprozeßordnung 1975)

I. Änderungen aus Anlass des Erkenntnisses des VfGH vom 14. Dezember 2023, G 352/2021 **und dem Urteil des EuGH vom 4. Oktober 2024, Rechtssache C 548/21.**

Allgemeines zu den Änderungen in (Eintrag im Inhaltsverzeichnis zur Überschrift des 1. Abschnitts des 8. Hauptstücks und zu den § 115 folgenden Einträgen, § 47a Abs. 4a und 7, Überschrift 1. Abschnitts des 8. Hauptstücks, § 109 Z 1 lit. a, Z 2a bis Z 2e, § 110 Abs. 1 Z 1 und Abs. 4, § 111 Abs. 1 und 2, § 112 Abs. 1 und 2, § 112a Abs. 1, § 115f bis § 115l, § 157 Abs. 2 und § 281 Abs. 1 Z 3 StPO):

Zu den aufgehobenen Bestimmungen und den vom VfGH und zuletzt auch vom EuGH festgelegten Anforderungen an die neu zu erlassenden gesetzlichen Regelungen:

Der VfGH hat sich aus Anlass eines auf Art. 140 Abs. 1 Z 1 lit d B-VG gestützten Antrags auf Normenkontrolle mit den Bestimmungen zur Sicherstellung intensiv auseinandergesetzt und nach Durchführung einer mündlichen Verhandlung in seinem Erkenntnis vom 14.12.2023, G 352/2021, die Bestimmungen der § 110 Abs. 1 Z 1 und Abs. 4 sowie § 111 Abs. 2 StPO wegen Verstoßes gegen das Grundrecht auf Datenschutz nach § 1 DSG und das Recht auf Achtung des Privat- und Familienlebens nach Art. 8 EMRK mit Ablauf des 31.12.2024 als verfassungswidrig aufgehoben.

In seinem Erkenntnis G 352/2021 erkannte der VfGH grundsätzlich die Bedeutung der Sicherstellung an und hob hervor, dass die Verfolgung strafbarer Handlungen mittels Sicherstellung von Beweismitteln ein legitimes Ziel iSd § 1 Abs. 2 DSG und Art. 8 Abs. 2 EMRK darstellt. Die Befugnisse der Strafverfolgungsorgane zur Sicherstellung seien grundsätzlich auch abstrakt geeignet, dieses Ziel zu erreichen. Der Eingriff sei jedoch im Fall der Sicherstellung von Datenträgern, die die Sicherstellung von potentiell sensiblen Daten letztlich einschließe, unverhältnismäßig und nicht mit der Sicherstellung von gewöhnlichen (nicht auslesbaren) Gegenständen vergleichbar. § 1 Abs. 2 DSG ziehe die Grenzen für Eingriffe in das Grundrecht enger als dies im Hinblick auf Art. 8 Abs. 2 EMRK der Fall sei; an die Verhältnismäßigkeit einer materienspezifischen Regelung, die die Fälle zulässiger Eingriffe in das

Grundrecht auf Datenschutz konkretisiere und begrenze, müsse iSd **§ 1 Abs. 2 DSG ein strengerer Maßstab** angelegt werden, als er sich bereits aus Art. 8 EMRK ergebe.

Aus Sicht des VfGH ist aufgrund der besonderen Eingriffsintensität der Ermittlungsmaßnahme die **richterliche Vorabkontrolle alleine nicht ausreichend, sondern sind weitere (besondere) Garantien erforderlich**. Zur Begründung weist der VfGH neben der (potentiellen) Schwere des Eingriffs zusätzlich darauf hin, dass die (technischen) Veränderungen an sichergestellten Daten im Nachhinein nicht nachvollziehbar seien bzw. nicht feststellbar sei, welche Daten konkret geändert worden seien. Er orte während des Ermittlungsverfahrens und im anschließenden (Haupt-)Verfahren für die von einer Sicherstellung (Zugriff und Auswertung) von Datenträgern Betroffenen zudem keinen angemessenen Rechtsschutz. Obwohl teilweise geeignete Rechtsschutzmöglichkeiten bestünden, um gegen eine Sicherstellung vorzugehen oder unrechtmäßige Datenverarbeitungen zu beseitigen (vgl. § 106 StPO und § 75 StPO), seien diese nicht vollumfänglich. Zudem sei für alle Personen, die von der Sicherstellung betroffen sind, der Prozess der Auswertung nicht transparent und dritte Personen, deren Daten verarbeitet werden, hätten keine Kenntnis von der Verarbeitung. In Bezug auf Beschuldigte würde dies erhebliche Auswirkungen auf die Verteidigungsmöglichkeit haben.

Der Gesetzgeber müsse bei der Neuregelung der Sicherstellung (Zugriff und Auswertung) von Datenträgern das öffentliche Interesse an der Strafverfolgung und die Grundrechte der Betroffenen gegeneinander abwägen und in Ausgleich bringen. Es genüge allerdings nicht, dass der Gesetzgeber den Strafverfolgungsorganen die (allgemeine) Geltung des § 5 StPO im Rahmen der ‚Auswertung‘ auftrage; dies mit Blick auf die *‚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‘* (vgl. Rn. 92).

Insofern müsse der Gesetzgeber selbst die wesentlichen Schranken für die Zulässigkeit *‚der jeweils zu setzenden Ermittlungsschritte‘* festlegen (Rn. 94), womit der faktische *‚Zugriff‘* auf den Datenträger als weniger intensiv und die *‚nachfolgende Auswertung‘* als intensiver Grundrechtseingriff zu verstehen ist (Rn. 91 ff). Welchen verfassungsrechtlichen Anforderungen dieser Ausgleich genügen muss, hänge im Ergebnis davon ab, wie intensiv der Grundrechtseingriff sei. Der Gesetzgeber habe daher – abhängig von der durch die konkrete gesetzliche Ausgestaltung bewirkten Intensität des Eingriffs – exemplarisch mehrere **Gesichtspunkte** für die Prüfung der **Verhältnismäßigkeit auf Gesetzesebene** zu berücksichtigen.

Für den VfGH ist – **neben der geforderten gerichtlichen Vorabkontrolle** der Ermittlungsmaßnahme (Beschlagnahme von Datenträgern und Daten) – **das Informationsrecht** einer betroffenen Person ein **wesentlicher Eckpfeiler**: Demnach hat der Gesetzgeber **zu gewährleisten**, dass die von der Sicherstellung eines Datenträgers und der Auswertung der darauf (lokal oder extern) gespeicherten Daten Betroffenen in geeigneter Weise jene **Informationen** erhalten (können), die zur Wahrung ihrer Rechte im (Ermittlungs- und allenfalls nachfolgenden Haupt-) Verfahren notwendig sind.

Ein vom VfGH als erforderlich angesehener Richtervorbehalt bloß zu Beginn, nämlich bei der Bewilligung der Anordnung der Sicherstellung (Zugriff und Auswertung) eines Datenträgers, stelle im Lichte der technischen Möglichkeiten und rechtlichen Befugnisse der Strafverfolgungsorgane unter dem Blickwinkel des § 1 DSG und Art. 8 EMRK keinen ausreichenden Rechtsschutz für die von einer Sicherstellung von Datenträgern Betroffenen dar. Daneben **kann** es nach dem VfGH – innerhalb eines beweglichen Systems – einen Unterschied machen,

- ☐ ob eine **Sicherstellung von Datenträgern bei allen oder nur bei bestimmten Straftaten** vorgesehen wird, z. B. nur bei schweren Straftaten oder etwa nur bei Cyberkriminalität,
- ☐ ob der Gesetzgeber Vorkehrungen trifft, dass die Auswertung nachvollziehbar sowie überprüfbar ist und der Datenträger nur im erforderlichen Ausmaß ausgewertet wird, und
- ☐ ob der Gesetzgeber für Betroffene – im Hinblick auf die **Art und den Umfang** der auf einem sichergestellten Datenträger zugänglichen Daten und deren **Auswertung – effektive Maßnahmen einer unabhängigen Aufsicht** vorsieht, die gewährleistet, dass sich die Strafverfolgungsorgane bei der Auswertung von Daten im Rahmen der gerichtlichen Bewilligung bewegen und die Rechte der Betroffenen in verhältnismäßiger Weise gewahrt sind.

Zudem würden § 1 DSG iVm Art. 8 EMRK, wenn der Gesetzgeber den Strafverfolgungsorganen weitgehende Eingriffsbefugnisse einräumt, einen wirksamen Rechtsschutz erfordern, durch den die Auswertung der auf einem sichergestellten Datenträger gespeicherten Daten ebenso effektiv geprüft wie ein Befugnismissbrauch unterbunden wird. Dies umso mehr im Fall der Verarbeitung von (unter anderem) Daten, die im Sinne des § 1 Abs. 2 zweiter Satz DSG als besonders schutzwürdig gelten.

Der Gesetzgeber habe zu gewährleisten, dass die von der Sicherstellung eines Datenträgers und der Auswertung der darauf (lokal oder extern) gespeicherten Daten Betroffenen in geeigneter Weise jene Informationen erhalten (können), die zur Wahrung ihrer Rechte im (Ermittlungs- und möglicherweise nachfolgenden Haupt-) Verfahren notwendig sind.

Nach Ansicht des EuGH ist die Sicherstellung eines Mobiltelefons und bereits der bloße Versuch, darauf gespeicherte personenbezogene Daten auszulesen oder abzufragen, eine Verarbeitung im Sinne von Art. 3 Nr. 2 der Richtlinie 2016/680, die auf die Gewährleistung eines hohen Schutzniveaus für personenbezogene Daten natürlicher Personen abziele.

Nach Art. 4 Abs. 1 Buchst. c der Richtlinie 2016/680 müssen die Mitgliedstaaten vorsehen, dass personenbezogene Daten dem Verarbeitungszweck entsprechen, maßgeblich und in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sind. Diese Bestimmung verlangt somit von den Mitgliedstaaten die Einhaltung des Grundsatzes der ‚Datenminimierung‘, in dem der Grundsatz der Verhältnismäßigkeit zum Ausdruck gebracht wird.

Die nach der Richtlinie 2016/680 zulässigen Einschränkungen des in Art. 8 der Charta vorgesehenen Rechts auf Schutz personenbezogener Daten und des durch Art. 7 der Charta geschützten Rechts auf Achtung des Privat- und Familienlebens, wie im 104. Erwägungsgrund der Richtlinie hervorgehoben werde, seien im Einklang mit den Anforderungen von Art. 52 Abs. 1 der Charta auszulegen, zu denen die Wahrung des Grundsatzes der Verhältnismäßigkeit gehöre. Diese Grundrechte würden nämlich nicht uneingeschränkt gelten, sondern müssten im Hinblick auf ihre gesellschaftliche Funktion gesehen und gegen andere Grundrechte abgewogen werden. Jegliche Einschränkung ihrer Ausübung müsse gemäß Art. 52 Abs. 1 der Charta gesetzlich vorgesehen sein, ihren Wesensgehalt achten sowie den Grundsatz der Verhältnismäßigkeit wahren. Nach diesem Grundsatz dürften Einschränkungen nur vorgenommen werden, wenn sie erforderlich seien und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen würden. Sie müssten sich auf das absolut Notwendige beschränken, und die Regelung, die die fraglichen Einschränkungen enthalte, müsse klare und präzise Regeln für ihre Tragweite und ihre Anwendung vorsehen.

Bei einer Verarbeitung personenbezogener Daten im Rahmen polizeilicher Ermittlungen zur Ahndung einer Straftat – wie einem Versuch, auf die auf einem Mobiltelefon gespeicherten Daten zuzugreifen – sei grundsätzlich davon auszugehen ist, dass sie einer von der Union anerkannten dem Gemeinwohl dienenden Zielsetzung im Sinne von Art. 52 Abs. 1 der Charta tatsächlich entspreche, doch sei die Voraussetzung, dass eine solche Einschränkung erforderlich sein müsse, nicht erfüllt, wenn die angestrebte, dem Gemeinwohl dienende Zielsetzung in zumutbarer Weise ebenso wirksam durch andere Mittel erreicht werden könne, die weniger stark in die Grundrechte der betroffenen Personen eingreifen würden.

Darüber hinaus impliziere die Verhältnismäßigkeit einer Einschränkung der Ausübung der in den Art. 7 und 8 der Charta verbürgten Grundrechte, die sich aus solchen Verarbeitungen ergäbe, eine Gewichtung aller relevanten Gesichtspunkte des Einzelfalls, zu denen u. a. die Schwere der damit verbundenen Einschränkung der Ausübung der in Rede stehenden Grundrechte, die von der Natur und der Sensibilität der Daten abhängen, zu denen die zuständigen Polizeibehörden Zugang erlangen könnten, die Bedeutung des mit dieser Einschränkung verfolgten, dem Gemeinwohl dienenden Ziels, die Verbindung zwischen dem Eigentümer des Mobiltelefons und der in Rede stehenden Straftat oder die Relevanz der fraglichen Daten für die Feststellung des Sachverhalts.

Je nachdem, welche Inhalte sich auf dem in Rede stehenden Mobiltelefon befinden und welche Entscheidungen die Polizeibehörden treffen würden, könne sich ein solcher Zugang nicht nur auf Verkehrs- und Standortdaten erstrecken, sondern auch auf Fotos und den Verlauf der Navigation im Internet mit diesem Telefon oder sogar auf einen Teil des Inhalts der mit diesem Telefon geführten Kommunikationen, insbesondere durch die Abfrage der darauf gespeicherten Nachrichten.

Der Zugang zu einem solchen Datensatz könne sehr genaue Schlüsse auf das Privatleben der betroffenen Person zulassen, etwa auf ihre Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Person und das soziale Umfeld, in dem sie verkehre. Schließlich könne nicht ausgeschlossen werden, dass zu den auf einem Mobiltelefon gespeicherten Daten besonders sensible Daten – wie personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen und religiöse oder weltanschauliche Überzeugungen hervorgehen – gehören könnten, deren Sensibilität den besonderen Schutz rechtfertige, den sie nach Art. 10 der Richtlinie 2016/680 genießen und der sich auch auf Daten erstrecken würde, aus denen sich mittels eines Denkvorgangs der Ableitung oder des Abgleichs indirekt derartige Informationen ergeben würden.

Der Eingriff in die in den Art. 7 und 8 der Charta verbürgten Grundrechte, zu dem die Anwendung einer solchen Maßnahme führen könne, sei daher als schwerwiegend oder sogar besonders schwerwiegend einzustufen.

Die Schwere der Straftat, die Gegenstand der Ermittlungen sei, stelle daher einen der zentralen Parameter bei der Prüfung der Verhältnismäßigkeit des schwerwiegenden Eingriffs dar, um den es sich beim Zugang zu den auf einem Mobiltelefon gespeicherten personenbezogenen Daten handeln würde, die es erlaube, genaue Schlüsse auf das Privatleben der betroffenen Person zu ziehen.

Die Rechtsgrundlage, die eine solche Einschränkung gestatte, müsse deren Tragweite hinreichend klar und präzise definieren. Um diesem Erfordernis zu genügen, müsse der nationale Gesetzgeber die zu berücksichtigenden Gesichtspunkte, insbesondere die Art oder die Kategorien der betreffenden Straftaten, hinreichend präzise definieren.

Die Verbindung zwischen dem Eigentümer des Mobiltelefons und der in Rede stehenden Straftat sowie die Relevanz der in Rede stehenden Daten für die Feststellung des Sachverhalts betreffenden Gesichtspunkt ergäbe sich aus Art. 6 der Richtlinie 2016/680, dass der Begriff ‚betroffene Person‘ verschiedene Kategorien von Personen umfasse, und zwar im Wesentlichen Personen, gegen die ein begründeter Verdacht bestehe, dass sie eine Straftat begangen hätten oder in naher Zukunft begehen würden, verurteilte Straftäter, Opfer oder potenzielle Opfer solcher Straftaten sowie andere Parteien im Zusammenhang mit einer Straftat, die bei Ermittlungen in Verbindung mit der betreffenden Straftat oder beim anschließenden Strafverfahren als Zeugen in Betracht kommen würden. Nach diesem Artikel müssten die Mitgliedstaaten vorsehen, dass der für die Verarbeitung Verantwortliche gegebenenfalls und so weit wie möglich zwischen den personenbezogenen Daten dieser verschiedenen Kategorien betroffener Personen klar unterscheidet.

Insoweit müsse insbesondere in Bezug auf den Zugang zu Daten, die wie im Ausgangsverfahren auf dem Mobiltelefon der Person, gegen die strafrechtlich ermittelt wird, gespeichert sind, der begründete Verdacht, dass diese Person eine Straftat begangen habe, begehe oder zu begehen plane oder dass sie in irgendeiner Weise in eine solche Straftat involviert sei, durch hinreichende objektive Anhaltspunkte untermauert werden.

Um namentlich sicherzustellen, dass der Grundsatz der Verhältnismäßigkeit in jedem Einzelfall durch eine Gewichtung aller relevanten Gesichtspunkte gewahrt werde, sei es von wesentlicher Bedeutung, dass der Zugang der zuständigen nationalen Behörden zu personenbezogenen Daten, wenn er die Gefahr eines schwerwiegenden oder sogar besonders schwerwiegenden Eingriffs in die Grundrechte der betroffenen Person mit sich bringe, von einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle abhängig gemacht wird.

Diese vorherige Kontrolle setze voraus, dass das mit ihr betraute Gericht oder die mit ihr betraute unabhängige Verwaltungsstelle über alle Befugnisse verfüge und alle Garantien biete, die erforderlich seien, um zu gewährleisten, dass die verschiedenen einander gegenüberstehenden berechtigten Interessen und Rechte in Einklang gebracht würden. Speziell im Fall strafrechtlicher Ermittlungen verlange eine solche Kontrolle, dass das Gericht in der Lage ist, für einen gerechten Ausgleich zwischen den berechtigten Interessen, die sich aus den Erfordernissen der Ermittlungen im Rahmen der Kriminalitätsbekämpfung ergeben, und den Grundrechten auf Achtung des Privatlebens und den Schutz personenbezogener Daten der Personen, auf deren Daten zugegriffen werde, zu sorgen.

Diese unabhängige Kontrolle müsse vor jedem Versuch, Zugang zu den betreffenden Daten auf einem Mobiltelefon zu erlangen, erfolgen, außer in hinreichend begründeten Eilfällen, in denen die Kontrolle kurzfristig erfolgen müsse. Eine spätere Kontrolle würde es nämlich nicht ermöglichen, dem Ziel der vorherigen Kontrolle zu entsprechen, das darin bestehe, zu verhindern, dass ein über das absolut Notwendige hinausgehender Zugang zu den fraglichen Daten gewährt werde.

Insbesondere seien bei der Verarbeitung sensibler Daten die Anforderungen zu berücksichtigen, die in Art. 10 der Richtlinie 2016/680 aufgestellt würden, dessen Zweck darin bestehe, einen erhöhten Schutz vor solchen Verarbeitungen zu gewährleisten, die, wie sich aus dem 37. Erwägungsgrund der Richtlinie ergäben, erhebliche Risiken für die in den Art. 7 und 8 der Charta verbürgten Grundrechte und Grundfreiheiten wie das Recht auf Achtung des Privat- und Familienlebens und das Recht auf Schutz personenbezogener Daten mit sich bringen könnten. Zu diesem Zweck sei, wie sich bereits aus dem Wortlaut von Art. 10 der Richtlinie ergäbe, die Einschränkung, dass die Verarbeitung solcher Daten ‚nur dann erlaubt [ist], wenn sie unbedingt erforderlich ist‘, dahin auszulegen, dass sie verschärfte Voraussetzungen für die Rechtmäßigkeit der Verarbeitung sensibler Daten festlege, verglichen mit denjenigen, die sich aus Art. 4 Abs. 1 Buchst. b und c sowie aus Art. 8 Abs. 1 der Richtlinie ergeben würden, in denen lediglich von der ‚Erforderlichkeit‘ einer allgemein in den Anwendungsbereich der Richtlinie fallenden Verarbeitung von Daten die Rede ist (Urteil vom 26. Januar 2023, Ministers

Die vorgeschlagenen Änderungen orientieren sich an den Ausführungen des VfGH und des EuGH, aber auch der RL (EU) 2016/680 indem in organisatorischer und rechtlicher Hinsicht gesetzlich geregelt wird, dass der Zugriff auf Datenträger und Daten an eine richterliche Vorabkontrolle geknüpft wird und ab der haptischen Wegnahme des Datenträgers jegliche Zugriffe und Zugriffsversuche durch die ermittelnden Strafverfolgungsbehörden erforderlich, richterlich begrenzt, nachvollziehbar und überprüfbar sind. Der Zugriff auf und die Verarbeitung von Daten soll letztlich nur im erforderlichen Ausmaß und nur dann erfolgen, wenn weniger grundrechtsinvasive geeignete Ermittlungsmaßnahmen nicht zur Verfügung stehen, und in unterschiedlichen Phasen des Auswertungsprozesses (auch nachprüfend) der unabhängigen Aufsicht durch die Rechtsschutzbeauftragte bzw. den Rechtsschutzbeauftragten der Justiz unterzogen werden (können). Die Informationsrechte und die Beteiligungsmöglichkeiten von Beteiligten des Strafverfahrens sollen einen grundlegenden Ausgleich gewährleisten.

Einführung einer neuen Ermittlungsmaßnahme:

De lege lata besteht (unabhängig von einer vorangegangenen Sicherstellung und damit vor einem Zugriff) die Möglichkeit einer – der richterlichen Vorabkontrolle zugänglichen – Beschlagnahme von (körperlichen) Gegenständen; gleichfalls ist auch die Beschlagnahme von auf Datenträgern abgespeicherten Daten nicht ausgeschlossen (vgl. *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht 5.22). In der Praxis gewann allerdings das Antragsrecht der Staatsanwaltschaft (§ 115 Abs. 2 StPO) auf eine (ursprüngliche) Begründung einer Sicherstellung im Wege der Beschlagnahme kaum an Bedeutung; selbst im Regelfall, in dem eine Beschlagnahme zur Fortsetzung der Sicherstellung möglich ist, wird davon kaum Gebrauch gemacht, was unter anderem auch daran liegt, dass betroffene Personen ihr Antragsrecht nicht ausüben (vgl. § 115 Abs. 2 StPO) und § 113 Abs. 3 StPO lediglich im Fall des § 109 Z 1 lit. b StPO eine unverzügliche Pflicht der Staatsanwaltschaft zur Beantragung der Beschlagnahme vorsieht.

Um die vom VfGH verlangte allgemeine Garantie der vorherigen gerichtlichen Genehmigung bereits bei der Begründung der Verfügungsmacht über einen Datenträger umzusetzen, wird vorgeschlagen, an die schon nach der geltenden Rechtslage bestehende Möglichkeit der Beschlagnahme (arg. *„gerichtliche Entscheidung auf Begründung einer Sicherstellung“*; vgl. § 109 Z 2 lit. a StPO) anzuknüpfen. Damit soll die Systematik der (vorläufigen) Sicherstellung und der Beschlagnahme, die auch nach der hM Fälle einer gerichtlichen Entscheidung auf (ursprüngliche) Begründung einer Sicherstellung umfasst (vgl. *Tipold/Zerbes*; *Flora in Fuchs/Ratz*, WK StPO § 109 Rz. 5; *Keplinger/Prunner/Pühringer/Rebisant in Birklbauer/Haumer/Nimmervoll/Wess* (Hrsg), stopp – Linzer Kommentar zur Strafprozessordnung zu § 109 StPO Rn. 12f.; ebenda *Rebisant* zu § 115 StPO Rz. 1), beibehalten werden. Dabei soll in § 115f Abs. 2 und Abs. 3 stopp – wie auch bei vergleichbaren Ermittlungsmaßnahmen (z. B. §§ 134 ff StPO) – die Bewilligung einer staatsanwaltschaftlichen Anordnung zu erfolgen haben.

Dogmatisch handelt es sich bei der Neuregelung um eine neue Ermittlungsmaßnahme, die sich von der Sicherstellung von Gegenständen grundlegend unterscheidet und zudem eine Reihe von Begleitbestimmungen erforderlich macht. Es wird vorgeschlagen, die Ermittlungsmaßnahme als Sonderform der Beschlagnahme (*„gerichtliche Entscheidung auf Begründung einer Sicherstellung“*) in §§ 115f bis 115l StPO zu verorten. Dies scheint auch zur klaren Abgrenzung von jenen Fällen erforderlich, in denen im geltenden Recht (und auch künftig) vor oder nach einer Sicherstellung iSd obigen Ausführungen eine Beschlagnahme möglich (bzw. im Fall des § 109 Z 1 lit. b StPO zwingend) ist.

Die vorgeschlagene Ermittlungsmaßnahme der *„Beschlagnahme von Datenträgern und Daten“* (§ 115f StPO) unterscheidet sich von der Beschlagnahme nach § 115 StPO nicht nur durch die zwingende Voraussetzung einer vorherigen gerichtlichen Bewilligung, womit eine ohne gerichtliche Bewilligung erfolgende Sicherstellung (mit Ausnahme der in § 115f Abs. 5 StPO geregelten Fälle) weder notwendig noch zulässig ist, sondern auch dadurch, dass sie einen spezifischen Anwendungsbereich sowie besondere Voraussetzungen normiert.

Neben der Einführung von Legaldefinitionen in § 109 StPO, die zu einer besseren Verständlichkeit des Gesetzestexts beitragen sollen, sollen die inhaltlichen und formalen Voraussetzungen der *„Beschlagnahme von Datenträgern und Daten“* in § 115f StPO geregelt werden. In den darauffolgenden Bestimmungen sollen die etablierten, mehrstufigen und mit jeweils unterschiedlichen rechtsstaatlichen Garantien ausgestatteten Phasen des Auswertungsvorgangs, nämlich die *„Aufbereitung von Daten“* (§ 115h StPO) und die *„Auswertung von Daten“* (§ 115i und § 115j StPO), übersichtlich dargestellt und normiert sowie die vom VfGH geforderte Nachvollziehbarkeit und Überprüfbarkeit gewährleistet werden. Weiters vorgesehen sind besondere Vorschriften für die *„Verwahrung von Datenträgern und Daten“* (§ 115k StPO) und für den *„Rechtsschutz“* (§ 115l StPO). Dabei bildet § 111 Abs. 2 StPO eine grundsätzliche Ausnahme zur *„Beschlagnahme von Datenträgern und Daten“*: demnach fallen geringwertige oder punktuelle Daten oder Daten, die mittels Bild- und Tonaufzeichnungsgeräten an

öffentlichen oder öffentlich zugänglichen Orten aufgenommen wurden, nicht unter diese Ermittlungsmaßnahme. § 109 Z 1 lit. a StPO ermöglicht daher die Sicherstellung von Gegenständen (somit auch Datenträgern) und Daten, die unter den (materiellen) Voraussetzungen des § 111 Abs. 2 StPO ausgewertet werden können (wobei bereits de lege lata die Auswertung nach § 91 Abs. 2 dritter Fall StPO möglich ist und auch künftig möglich sein soll).

Um die vorgeschlagene Ermittlungsmaßnahme der ‚Beschlagnahme von Datenträgern und Daten‘ möglichst friktionsfrei in das bestehende System strafprozessualer Regelungen einzufügen, soll umfangreich auf bewährte Bestimmungen der StPO aus dem Bereich der Sicherstellung und Beschlagnahme, der Durchsuchung von Orten und Gegenständen und der vergleichbar grundrechtsinvasiven Auskunft über Daten einer Nachrichtenüberwachung zurückgegriffen werden.

Die vom VfGH und vom EuGH geforderten Garantien sowie die prozessualen und organisatorischen Vorkehrungen stellen im Übrigen ohnedies hohe Anforderungen an die Beschlagnahme von Datenträgern und Daten (z. B. gerichtliche Genehmigung vor dem Zugriff auf den Datenträger und die Daten). Rechtsvergleichend ist daher festzuhalten, dass etwa in Deutschland die Durchsicht vorläufig sichergestellter Unterlagen und elektronischer Daten ohne vorherige gerichtliche Bewilligung und ohne Strafschwelle möglich ist. Ein solches Durchsverfahren hat zum Ziel, erst den verfahrensrelevanten Teil des Datenbestandes der gerichtlichen Beschlagnahme zu unterwerfen (vgl. § 110 sowie § 94 Abs. 2 iVm § 98 Abs. 1 erster Satz sowie § 94 Abs. 2, § 98 Abs. 1 erster Satz iVm Abs. 2 erster Satz dStPO; vgl. *Park*, Aktuelle Fragen zur Durchsuchung und Beschlagnahme in Wirtschaftsstrafsachen, NSTZ 11/2023, S. 646 ff.). Ein Gestaltungsspielraum, der eine Ausgestaltung der Neuregelung nach diesem Vorbild sowie eine (vorläufige) Sicherstellung weiterhin ermöglicht hätte, scheidet aber aus, weil VfGH und EuGH die richterliche Vorabkontrolle grundsätzlich bereits für den Zugriff auf den Datenträger verlangen. Die Beschlagnahme von Daten soll daher von der Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung angeordnet werden können; die Durchführung der Ermittlungsmaßnahme soll grundsätzlich – dem System der StPO folgenden – der Kriminalpolizei zukommen (§ 115f Abs. 2 StPO), sodass die Leitungsfunktion nicht beeinträchtigt wird. Die gerichtliche Aufbereitung und der umfassende gerichtliche Rechtsschutz stehen dieser Leitungsfunktion der Staatsanwaltschaft nicht entgegen, zumal ihr Antragsrechte und die Befugnis zu Auswertung zukommen,

Die Anforderungen insbesondere des EuGH an die Zulässigkeit der Maßnahme soll in § 115h Abs 1 Rechnung getragen werden, wobei in § 115f Abs 4 die von VfGH und EuGH sowie weitere wesentliche Kriterien für die Verhältnismäßigkeitsprüfung enthalten soll. § 115 Abs 5 soll die vom EuGH geforderten Ausnahmen bei Gefahr in Verzug vorsehen.

Unter Berücksichtigung des Grundsatzes der Datenminimierung und der Schwere des Grundrechtseingriffs sollen zudem umfassende Informations- und Antragsrechte der Betroffenen, Beweisverwertungsverbote, Vernichtungsgebote und eine aufschiebende Wirkung von Rechtsmitteln und Rechtsbehelfen vorgesehen werden, soweit sie sich gegen die Zulässigkeit der Maßnahme richten.

Zu (Eintrag im Inhaltsverzeichnis zur Überschrift des 1. Abschnitts des 8. Hauptstücks und zu den § 115 folgenden Einträgen sowie Überschrift des 1. Abschnitts des 8. Hauptstücks):

Die Einführung der neuen Ermittlungsmaßnahme ist konsequenter Weise in die Überschrift des Bezug habenden 1. Abschnitts des 8. Hauptstücks der StPO aufzunehmen; überdies hat die Ergänzung des Inhaltsverzeichnisses um die vorgeschlagene neue Ermittlungsmaßnahme und deren Begleitbestimmungen zu erfolgen, wobei auch der bislang aufgrund eines Redaktionsversehens fehlende Eintrag im Inhaltsverzeichnis zu den Bestimmungen § 115a bis § 115e StPO vorgenommen werden soll.

Zu (§ 109 Z 1 lit. a und Z 2a bis Z 2e):

Die neue Ermittlungsmaßnahme soll systemkonform in § 109 StPO definiert werden. Es wird vorgeschlagen, in einem neu zu schaffenden **§ 109 Z 2a StPO** die Beschlagnahme von Datenträgern und Daten zu umschreiben. Künftig sollen ausdrücklich drei Fälle unterschieden werden, nämlich ‚die Beschlagnahme von Datenträgern und darauf gespeicherten Daten‘ (lit. a), ‚Daten, die an anderen Speicherorten als dem Datenträger gespeichert sind, soweit auf sie von diesem aus zugegriffen werden kann‘ (lit. b) und ‚Daten, die auf Datenträgern oder an anderen Speicherorten gespeichert sind, (lit. a und b), die zuvor für andere Zwecke nach Z 1 lit. a sichergestellt wurden‘ (lit. c).. Grundvoraussetzung soll in allen drei Fällen sein, dass die Begründung der Verfügungsmacht über die Datenträger und/oder Daten erfolgt, um diese unter den (materiellen) Voraussetzungen der §§ 115f ff StPO auszuwerten (§ 109 Z 2a StPO). Soll eine Ermittlungstätigkeit eine Auswertung von Daten iSd § 115i StPO (und nicht bloß eine Auswertung iSd § 111 Abs. 2 StPO iVm § 91 Abs. 2 dritter Fall StPO) erfordern, sind die neuen Regelungen zur Beschlagnahme von Datenträgern und Daten anzuwenden. Nach der Legaldefinition in § 109 Z 2b StPO muss daher zunächst eine Sicherung und Vorabbegrenzung eines Datenbestandes im Umfang der richterlichen Bewilligung vorgenommen werden. Anschließend ist die Auswertung

(Selektion) erheblicher Tatsachen durch die Strafverfolgungsbehörden vorzunehmen, um die Daten zielgerichtet auszuwerten. Dadurch soll eine klare Abgrenzung zu anderen Ermittlungsmaßnahmen erreicht werden, insbesondere zur Sicherstellung (s. dazu insb. § 111 Abs 2 und die Ausführungen zu § 109 Z 2a lit. c StPO). Zur eindeutigen Trennung der Fälle der Sicherstellung (§§ 110 ff. StPO) von den Fällen der Beschlagnahme von Datenträgern und Daten (§§ 115f ff. StPO) wird zudem auch vorgeschlagen, bereits in der Legaldefinition der Sicherstellung in § 109 Z 1 lit. a StPO in Zusammenhang mit § 110 Abs. 1 Z 1 StPO klarzustellen, dass eine Sicherstellung von Datenträgern (die unter den Begriff des Gegenstandes bzw. Vermögenswerts zu subsumieren sind) und Daten nach § 109 Z 2a StPO auch weiterhin möglich ist, sofern die Voraussetzungen des § 111 Abs. 2 StPO vorliegen. Damit soll der gesetzgeberische Wille zum Ausdruck gebracht werden, dass eine Sicherstellung niemals (auch nicht vorsorglich, um in weiterer Folge auf (gespeicherte) Daten zugreifen zu können) erfolgen kann, wenn die Bestimmungen über die Beschlagnahme von Datenträgern und Daten zur Anwendung kommen.

§ 109 Z 2a **lit. a** StPO umfasst den Fall der Beschlagnahme von Datenträgern und Daten, die auf einem Datenträger (*,darauf'*) originär gespeichert sind (z. B. die Beschlagnahme eines USB-Sticks, einer externen Festplatte oder eines Smartphones und der auf diesen Datenträgern gespeicherten Daten).

Im geltenden Recht ist der Zugriff auf Daten bei ausgelagerter Datenbetreuung nicht ausdrücklich geregelt. Nach der Rechtsprechung des OGH muss die Sicherstellung nicht zwingend auch die Gegenstände umfassen, in denen der sicherzustellende Datenträger eingebaut ist (wie etwa PCs, Laptops udgl.). Weiters müsse sich die Sicherstellung nicht zwingend auf den Datenträger beziehen, auf dem (neben anderen) jene Daten originär gespeichert wurden, die für das Ermittlungsverfahren relevant sind. Es gibt nach der Rechtsprechung des OGH nicht den einzig möglichen Gegenstand der Sicherstellung von (originalen) Datenträgern – vor allem mit Rücksicht darauf, dass betroffene Personen mitunter über den Datenträger gar nicht verfügen, wie etwa bei der Nutzung externer Speicherplätze, *,vor allem – in Zeiten internetbasierter Netzwerke regelmäßiger – ausgelagerter Datenbetreuung durch Cloud-Computing- oder Cloud-Storage-Dienste'* (14 Os 51/18h). Die hL bejaht zwar, dass die ausgelagerten bzw. auf räumlich entfernten Servern gespeicherten Datenbestände von der Sicherstellung umfasst sind, allerdings wurde zum Teil auch eine ausdrückliche gesetzliche Grundlage für die Möglichkeit der Sicherstellung solcher extern gespeicherten Daten gefordert (vgl. *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 111, Rz. 14 ff.; *Zerbes*, Durchsuchung und Beschlagnahme in Wirtschaftsstrafsachen, ÖJZ 2012/93, 845 ff.; *Zerbes*, Beweisquelle Handy, ÖJZ 2021/24, 176 ff. mwN; zum Teil aa *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht Rz. 5.11 ff.; *Schrank/Stücklberger/Kleinbrod*, Sicherstellung im digitalen Zeitalter, ZWF 2020, 289; *Ainedter/Poppenwimmer*, Sicherstellung und Auswertung von auf Datenträgern gespeicherten Informationen – aktuelle Rechtsprobleme, ZWF 2022, 17). Die Einführung des § 109 Z 2a **lit. b**. StPO soll dieser Kritik begegnen und eine explizite gesetzliche Rechtsgrundlage für den Zugriff auf Daten, die an anderen Speicherorten als dem Datenträger selbst gespeichert sind, schaffen. Dadurch wird klargestellt, dass auch die Beschlagnahme extern gespeicherter Daten, soweit auf sie von dem beschlagnahmten Datenträger aus zugegriffen werden kann, nach den Voraussetzungen der Beschlagnahme von Datenträgern und Daten nach §§ 115f ff. StPO zulässig ist. Die Bestimmung orientiert sich dabei weitgehend an der deutschen Bestimmung des § 110 Abs. 3 dStPO.

§ 109 Z 2a **lit. c** StPO soll schließlich die Beschlagnahme von Daten umfassen, die auf Datenträgern oder an anderen Speicherorten gespeichert sind (lit. a und b), die zuvor nach lit. a sichergestellt wurden. Davon sollen ausschließlich Fälle umfasst sein, in denen ein Datenträger nicht zum Zweck der Auswertung der auf ihm (lokal oder extern) gespeicherten Daten sichergestellt wurde, sondern lediglich für einen anderen in § 110 Abs. 1 StPO genannten Zweck. Dies betrifft etwa den Fall, dass ein Datenträger ursprünglich aus Beweisgründen (§ 110 Abs. 1 Z 1 StPO), etwa zur Sicherung von Spuren (z. B. Blutspuren, Fingerabdrücken udgl.), sichergestellt wurde, im Nachhinein jedoch darauf gespeicherte Daten ausgewertet werden sollen. Praktisch bedeutsam sein könnte § 109 Z 2a lit. c StPO etwa auch für die Sicherstellung eines (mit einem Datenträger ausgestatteten modernen) Fahrzeugs zur Sicherung privatrechtlicher Ansprüche (§ 110 Abs. 1 Z 2 StPO) oder zur Sicherung vermögensrechtlicher Anordnungen (§ 110 Abs. 1 Z 3 StPO). Erscheint eine – über die Befugnis nach § 111 Abs. 2 StPO hinausgehende – Auswertung von Daten, die auf solchen Datenträgern gespeichert sind, zu einem späteren Zeitpunkt aus Beweisgründen erforderlich, sollen auch hier die Voraussetzungen der Beschlagnahme von Datenträgern und Daten nach § 115f ff. StPO gelten. Da in diesen Fällen die Verfügungsmacht über den Datenträger bereits hergestellt ist, beschränkt sich die Zwangsbefugnis auf den Zugriff auf die Daten (vgl. dazu auch die Ausführungen zu § 115f StPO).

§ 109 Z 2b StPO soll die *,Aufbereitung von Daten'* als eine aus Beweisgründen erfolgende technische Aufbereitung, einschließlich der Wiederherstellung von Daten, und deren Einschränkung auf jenen Umfang, der der gerichtlichen Entscheidung nach § 109 Z 2a StPO in Bezug auf die Datenkategorien, Dateninhalte und den Zeitraum entspricht, definieren. Grundlage für die im Zuge der Aufbereitung von

Daten vorzunehmenden Einschränkung der Daten soll daher ausschließlich die gerichtliche Bewilligung sein. Um in technischer Hinsicht jenes Ergebnis herzustellen, das der gerichtlichen Bewilligung in Bezug auf die Datenkategorien, Dateninhalte und den Zeitraum entspricht, sind zwei Schritte notwendig: Die Herstellung einer ‚*Originalsicherung*‘ und die Herstellung einer ‚*Arbeitskopie*‘:

§ 109 Z 2c StPO definiert die ‚*Originalsicherung*‘ als eine unter Verwendung forensischer Sicherungsmechanismen gewonnene Kopie des Originaldatenbestandes. Diese hat – wie derzeit – in der forensischen Arbeit als Imagesicherung (eine 1:1-Kopie des Datenträgers) zu erfolgen und ist unter Verwendung von entsprechenden forensischen Sicherungsmechanismen (Schreibschutz, Schreibblocker) zu erstellen. Diese gewährleisten, dass ab dem Beginn der Imageerstellung kein Schreibvorgang auf dem zu sichernden Datenträger mehr möglich ist. Die Gewährleistung der Datenintegrität liefert der Hash-Wert (Prüfsumme auf Grund eines mathematischen Algorithmus), der sich auf den Dateninhalt des gesicherten Mediums zum Zeitpunkt der Sicherung und den Dateninhalt des angefertigten Images bezieht. Dies dient der Beweisbarkeit der Unveränderlichkeit des Images, somit, dass keine Veränderung von Daten stattgefunden hat). Nach der – schon aus technischen Gründen notwendigen und auch derzeit gesetzlich vorgesehenen (vgl. § 111 Abs. 2 letzter Satz StPO, wonach die Herstellung einer Sicherungskopie der auf den Datenträgern gespeicherten Informationen zu dulden ist) – Herstellung einer Originalsicherung dient diese als Grundlage für die Herstellung einer ‚*Arbeitskopie*‘, mit welcher die Aufbereitung der konkreten Daten vorgenommen wird.

§ 109 Z 2d StPO definiert die ‚*Arbeitskopie*‘ als eine Kopie der Originalsicherung, anhand derer die Aufbereitung von Daten nach § 109 Z 2b StPO erfolgt. Diese Kopie dient – anders als die Originalsicherung, die bereits aus Gründen der Nachvollziehbarkeit und Überprüfbarkeit unverändert bleiben muss – zur Umsetzung der gerichtlichen Entscheidung.

§ 109 Z 2e StPO schließlich definiert das ‚*Ergebnis der Datenaufbereitung*‘ als einen der gerichtlichen Entscheidung in Bezug auf die **Datenkategorien, Dateninhalte** und den **Zeitraum** entsprechenden Datensatz. Dieser stellt das Ergebnis der Aufbereitung von Daten nach Z 2b und somit den (reduzierten) Datensatz dar, der den Ermittlungen zugrunde gelegt werden darf.

Zu (§ 110 Abs. 1 Z 1 und Abs. 4 StPO):

Die Bestimmungen nach § 110 Abs. 1 Z 1 und Abs. 4 StPO idF BGBl. I Nr. 19/2004 wurden vom VfGH vor dem Hintergrund, dass die Sicherstellung von Daten und Datenträgern nach geltender Gesetzeslage keiner vorhergehenden Bewilligung durch das Gericht bedarf, ebenfalls als verfassungswidrig aufgehoben. Diese Regelungen sind jedoch auch weiterhin erforderlich und sollen daher (§ 110 Abs. 4 StPO mit geringfügigen sprachlichen, nicht jedoch inhaltlichen Änderungen) neu erlassen werden, weil sie für die Sicherstellung von (sonstigen) Gegenständen, die nicht ausgelesen und ausgewertet werden sollen, sowie für Vermögenswerte nach wie vor Bedeutung haben. Um eine klare Abgrenzung zu der neu vorgeschlagenen Ermittlungsmaßnahme nach §§ 115f ff StPO zu schaffen, wird in § 110 Abs. 1 Z 1 StPO auf Daten nach § 111 Abs. 2 StPO Bezug genommen.

Zu (§ 111 Abs. 1 und Abs. 2 StPO):

Der in Geltung stehende § 111 Abs. 2 StPO regelt die Sicherstellung von ‚*auf Datenträgern gespeicherten Informationen*‘; darunter ist die ‚*Auswertung*‘ als – zeitlich nachgelagerte – Phase der ‚*Sicherstellung im weiteren Sinn*‘ zu verstehen; derzeit greifen so die allgemeinen Voraussetzungen (§§ 110 ff. StPO). Insoweit ist für den Datenzugriff auch der Rückgriff auf die Erforderlichkeit ‚*aus Beweisgründen*‘ (§ 110 Abs. 1 Z 1 StPO), das Anordnungserfordernis und die Durchführungskompetenz der Kriminalpolizei (§ 110 Abs. 2 StPO), die Subsidiarität der Sicherstellung (§ 110 Abs. 4 StPO) und die Informationspflicht einer von der Sicherstellung betroffenen Person (§ 111 Abs. 4 StPO) notwendig. Die Vorschrift für den Datenzugriff in § 111 Abs. 2 StPO soll künftig aufgrund der Aufhebung durch den VfGH nur mehr einen sehr eingeschränkten Anwendungsbereich haben. Im Gegenzug sollen als *leges speciales* Bestimmungen in den §§ 115f bis 115l StPO geschaffen werden, die technologieneutral auf den Sammelbegriff Datenträger abstellen, sowie den Zugriff auf die darauf (lokal oder extern) gespeicherten Daten regeln.

Wie bisher soll nach § 111 Abs. 2 die Sicherstellung von auf Bild- und Tonaufzeichnungsgeräten gespeicherten Daten, die an öffentlichen oder öffentlich zugänglichen Orten aufgenommen wurden zulässig sein, wenn iSd Verhältnismäßigkeitsgebots (§ 5 StPO) nicht der gesamte Datenträger und sämtliche Daten sichergestellt werden sollen (vgl. 14 Os 51/18h).

Den Erwägungen des OGH in seiner Entscheidung zu 14 Os 51/18h folgend, wonach der Zugriff auf den gesamten Datenträger und alle Daten in bestimmten Fällen unverhältnismäßig sein kann und demnach nur eine gezieltere Maßnahme zulässig und geboten ist, wird vorgeschlagen, die Sicherstellung auf Daten zu beschränken, die an öffentlichen oder öffentlich zugänglichen Orten mittels Bild- und

Tonaufzeichnungsgeräten aufgenommen wurden. Von der Herausgabepflicht nach § 111 Abs. 2 StPO (vgl. zu den möglichen Folgen der Verletzung § 93 Abs. 2 StPO) sind Zugangsdaten, Daten einer Nachrichtenübermittlung, geographische Standorte sowie gesendete, übermittelte oder empfangene Nachrichten auf dem Endgerät einer Person (vgl. § 134 Z 5 StPO) ausdrücklich ausgeschlossen, weil mit diesen nach dem Erkenntnis des VfGH umfassende Persönlichkeits- und Bewegungsprofile erstellt werden können, die detailreiche Rückschlüsse auf das Verhalten, die Persönlichkeit und die Gesinnung des bzw. der Betroffenen zulassen und bereits auf einem Datenträger gespeicherte Verbindungsdaten u.a. ‚Vermutungen über Kommunikationsinhalte nahelegen, weil offengelegt wird, ob, wann, wie oft und mit wem auf welchem Weg Kontakt aufgenommen wurde‘ (vgl. Rn. 66). Gleiches gilt nach der Rsp des VfGH und des EuGH für besondere Kategorien von Daten (§ 1 Abs 2 zweiter Satz StPO; Art 9 DSGVO). Die Beschlagnahme von Kommunikationsdaten im weiteren Sinn und besonderen Kategorien von Daten unterliegt daher jedenfalls den Sonderbestimmungen nach §§ 115f ff StPO; Eine Sicherstellung nach § 111 Abs. 2 StPO ist insofern hinsichtlich dieser Daten ausdrücklich unzulässig; gleichzeitig ist – abgesehen von diesen Fällen – eine solche Möglichkeit zur Entlastung der Gerichte und zur Verfahrensbeschleunigung grundsätzlich erforderlich, wobei mit dieser Aufwand sparenden Maßnahme kein Verlust an Rechtsschutz verbunden ist.

In der Praxis soll die Bestimmung daher zur Anwendung gelangen, wenn Videomaterial sichergestellt werden soll, das ein bestimmtes Geschehen festhält (z.B. Aufnahmen von Überwachungskameras in Supermärkten und Banken, öffentlichen Verkehrsmitteln, videoüberwachten Örtlichkeiten) oder Fotos aus Bankomatkameras. Diese Unterscheidung ist auch vor dem Hintergrund der Entscheidung des OGH zu 14 Os 51/18h, in der dieser in Bezug auf Videoaufzeichnungen die Verhältnismäßigkeit des Zugriffs eingehend geprüft und bejaht hat, weiter zulässig. Den vom OGH angestellten Erwägungen steht auch das Erkenntnis des VfGH nicht entgegen. Die Verfassungswidrigkeit des § 111 Abs. 2 StPO begründete der VfGH nämlich damit, dass ‚(...) der Zugriff auf potentiell sämtliche auf einem Datenträger gespeicherten Daten (...) den Strafverfolgungsorganen nicht bloß ein punktuelles Bild über das Verhalten des Verdächtigten oder des Betroffenen (...)‘ ermöglicht; dabei wies der VfGH auf die Gefahr hin, dass umfassende Persönlichkeits- und Bewegungsprofile erstellt werden können, die detailreiche Rückschlüsse auf das Verhalten, die Persönlichkeit und die Gesinnung des Betroffenen zulassen. Demgegenüber liegt bei Aufnahmen z. B. auf für private oder berufliche Zwecke genutzten Mobiltelefonen an öffentlichen oder öffentlich zugänglichen Orten ein solcher Hinweis auf Aufnahmen nicht vor, sodass die Anwendung dieser Bestimmung auf die Erlangung solcher Daten jedenfalls nicht möglich ist; vielmehr ist nach §§ 115f ff. StPO vorzugehen.

Die vom VfGH geortete erhebliche Eingriffsintensität einer Sicherstellung von Daten(trägern) ergibt sich somit aus mehreren Faktoren, die in der Praxis jedoch nicht notwendigerweise in allen Fällen vorliegen. Ein solcher nicht eingriffsintensiver Fall liegt mit Blick auf die Rechtsprechung des OGH zu 14 Os 51/18h etwa dann vor, wenn dem **Zweck der Beweismittelsicherung** (§ 110 Abs. 1 Z 1 StPO) schon dadurch **entsprochen werden kann**, dass die Daten, die von einer Bankomatkamera angefertigt wurden, und auf der Festplatte im Bankomaten gespeichert sind, **im Wege eines – mit Kopien** dieser (solcherart **materiell verkörperten**) **Daten** – bespielten **Datenträgers** (etwa eines **USB-Sticks**) sichergestellt werden, zu dessen **Ausföhrung oder Duldung seiner Herstellung** die Bank nach § 111 Abs. 2 StPO verpflichtet ist. Diese Lösung entspricht zudem der vorgeschlagenen Systematik, wonach die Sicherstellung nicht zum ‚Zweck der Auswertung von Daten‘ (§ 109 Z 2a StPO) erfolgt. Zudem stellt das Innehaben von Kopien oder anderen Ersatzgegenständen schon nach § 110 Abs. 4 StPO keine eigenständige Ermittlungsmaßnahme dar, sondern das gelindere Mittel gegenüber einer grundsätzlich zulässigen Sicherstellung des Originals (vgl. *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 110, Rz. 76).

Die Verhältnismäßigkeit ist auch dadurch gewährleistet, dass solche Aufzeichnungen von den verpflichteten Personen (Kredit- und Finanzinstitut, Supermärkte, Betreiber öffentlicher Verkehrsmittel etc.) selbst spezifiziert und gesichert werden (können). Eine Suche nach oder eine Durchsuchung von Datenträgern ist im Falle der Sicherstellung einer Videoaufzeichnung nicht notwendig (vgl. 14 Os 51/18h). Insofern wird in der Praxis auch nicht der (alle Daten enthaltende ursprüngliche) Datenträger durch die Kriminalpolizei sichergestellt (bzw. gesichert, aufbereitet, auf Relevanz geprüft und ausgewertet), vielmehr stellt die verpflichtete Person nach Anordnung der Sicherstellung (lediglich) das **relevante Bild- oder Videomaterial in Bezug auf einen bestimmten Zeitpunkt** bereit, sodass letztlich die vom VfGH georteten Gefahren (wie etwa die Erstellung umfassender Persönlichkeits- und Bewegungsprofile durch Strafverfolgungsorgane, die detailreiche Rückschlüsse auf das Verhalten, die Persönlichkeit und die Gesinnung der Betroffenen zulassen) nicht gegeben sind.

Mit Blick auf den vom VfGH eingeräumten gesetzgeberischen Gestaltungsspielraum und unter Berücksichtigung der Rechtsprechung des OGH wird daher – den Bedürfnissen der Praxis nach effizienter Strafverfolgung Rechnung tragend – eine verhältnismäßige gesetzliche Grundlage für die

Sicherstellung von Daten, die mittels Bild- und Tonaufzeichnungsgeräten an öffentlichen oder öffentlich zugänglichen Orten aufgenommen wurden, vorgeschlagen. Darüber hinaus soll die Kriminalpolizei gemäß § 115f Abs 5 klar definierte bei Gefahr in Verzug erhalten.

Unter öffentlich zugänglichen Orten sind z.B. frei zugängliche Geschäfte oder Kaufhäuser während der Geschäftsöffnungszeiten; der Schalterraum einer Bank- oder Postfiliale; öffentliche Verkehrsmittel bzw. deren Haltebereiche; Sportplätze und Sportstadien; allgemein zugängliche Schulhöfe; der Eingangsbereich eines Hotels (Lobby); für den Publikumsverkehr geöffnete Flure, Treppenhäuser oder Parkgaragen bzw. Parkplätze etc. zu verstehen. Der Begriff ‚Ort‘ ist weit und nicht als abgeschlossener Platz oder Raum zu verstehen, es können daher auch frei zugängliche Flächen wie ein Waldgebiet, ein Park, ein Naherholungsgebiet oder die Fußgängerzone einer Stadt darunterfallen (vgl. *Thiele/Wagner*, Praxiskommentar zum Datenschutzgesetz (DSG)² § 12 Rz 44); der höchstpersönliche Lebensbereich soll hingegen von dieser Regelung nicht umfasst sein. Kommt eine mitwirkungspflichtige Person einer Anordnung nicht nach und kann auch mit Beugemitteln kein Auslangen erzielt werden (§ 93 Abs. 2 StPO), wird mit Beschlagnahme nach §§ 115f ff StPO vorzugehen sein.

Zu (§ 47a Abs. 4a und 7, §§ 115f bis 115l samt Überschriften und § 281 Abs. 1 Z 3 StPO):

Zur Beschlagnahme von Datenträgern und Daten (§ 115f und § 115g StPO):

Das bislang in der StPO verankerte grundsätzliche Konzept der Trennung in ein Stadium der (vorläufigen) Sicherstellung und der anschließenden Beschlagnahme kann bei der Neuregelung der Beschlagnahme von Datenträgern und Daten aufgrund der von VfGH und EuGH festgelegten Anforderungen nicht aufrechterhalten werden. Schon die Begründung der Verfügungsmacht über einen Datenträger sowie die darauf (lokal oder extern) gespeicherten Daten soll einer gerichtlichen Bewilligung unterliegen, wodurch es sich bei dieser Ermittlungsmaßnahme – sogleich – um eine (originäre) Beschlagnahme handelt. § 109 Z 2a StPO definiert die Beschlagnahme von Datenträgern und Daten daher – als eine ‚gerichtliche Entscheidung auf Begründung einer Sicherstellung [...] zum Zweck der Auswertung von Daten‘. § 115f Abs. 1 StPO orientiert sich ebenso in seinen materiellen Voraussetzungen am Wortlaut des § 110 Abs. 1 Z 1 StPO, wonach die Ermittlungsmaßnahme ‚aus Beweisgründen [...] erforderlich scheint‘, und nicht an jenem des § 115 Abs. 1 StPO, der konzeptuell darauf abstellt, dass ‚sichergestellte Gegenstände‘ voraussichtlich (weiterhin) als ‚Beweismittel erforderlich sein werden‘. Letztere Regelung weist eine nähere Beurteilungsgrundlage auf als in den nun vorgesehenen Fällen, in denen die Erwartung an den Beweiswert erst nach Erlangung der Verfügungsmacht über den Datenträger und den Zugriff auf die Daten messbar wird. Die Erforderlichkeit der Beschlagnahme ‚aus Beweisgründen‘ in einem bestimmten Verfahren verlangt jedoch, dass der Datenträger und die Daten geeignet sind, das Beweisthema zu führen; die Bedeutung für die konkrete Untersuchung muss – begründend – nachvollziehbar sein (vgl. die schon dahingehende Voraussetzung zur Sicherstellung, *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 110 Rz. 5).

Darüber hinaus muss die Beschlagnahme nach Ansicht des EuGH zur Aufklärung der Tat (unbedingt) erforderlich sein, sodass keine weniger grundrechtsinvasive geeignete Ermittlungsmaßnahme zur Verfügung stehen darf. Zudem soll in Entsprechung der Anforderungen des EuGH ein konkreter Verdacht einer Vorsatztat als Kategorie von Straftaten und – abhängig von der Zustimmung des Betroffenen eine Mindestschwere der Tat vorgesehen werden (vgl § 135 StPO).

In Konkretisierung der erwähnten Voraussetzungen sollen darüber hinaus bestimmte Tatsachen vorliegen müssen, dass durch die Ermittlungsmaßnahme Informationen ermittelt werden können, die für die Aufklärung einer Straftat erforderlich sind. Die Beschlagnahme darf demnach keinesfalls ‚zur Sicherheit‘, ‚bloß zur Vorsicht‘ oder erst aus Anlass einer sehr vagen Sachverhaltskonstellation durchgeführt werden, um dadurch erst einen (Anfangs-)Verdacht zu begründen (*Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 110 Rz. 10; *Kroschl* in *Schmölzer/Mühlbacher* (Hrsg), StPO Kommentar, Band 1 Ermittlungsverfahren² § 110 StPO Rz. 15; *Keplinger/Prunner/Pühringer* in *Birklbauer/Haumer/Nimmervoll/Wess* (Hrsg), StPO – Linzer Kommentar zur Strafprozessordnung zu § 110 StPO Rz. 8). Es muss somit ein begründeter Verdacht vorliegen, dass durch die Beschlagnahme von Datenträgern und Daten iSd § 115f StPO beweiserhebliche Tatsachen gewonnen werden können, die für die Aufklärung der Straftat erforderlich sind.

§ 115f Abs. 1 StPO erlaubt die Beschlagnahme von Datenträgern und Daten – neben anderen materiellen Voraussetzungen – aus Beweisgründen. § 109 Z 2a StPO legt fest, dass die Ermittlungsmaßnahme dann zulässig ist, wenn sie zum Zweck der Auswertung von Daten erfolgt. Zum Tragen kommen die Regelungen nur dann und verdrängen damit die allgemeinen Bestimmungen der Sicherstellung und Beschlagnahme (§§ 110 ff. StPO), wenn die Beschlagnahme aus Beweisgründen und zum Zweck der Auswertung der Daten erfolgt; diesfalls ist die von VfGH und EuGH erkannte Schwere des Eingriffs gegeben und sollen die Neuregelungen in §§ 115f ff. StPO zur Anwendung gelangen.

Nach **§ 115f Abs. 2 StPO** hat die Staatsanwaltschaft eine Beschlagnahme von Datenträgern und Daten aufgrund einer gerichtlichen Bewilligung gegenüber der Kriminalpolizei anzuordnen; der Kriminalpolizei obliegt die Durchführung der gerichtlich bewilligten Ermittlungsmaßnahme.

Für die gerichtliche Bewilligung der Beschlagnahme ist der Einzelrichter bzw. die Einzelrichterin des Landesgerichts zuständig (§ 31 Abs. 1 Z 2 StPO). Nach § 105 Abs. 1 StPO hat das Gericht für die Durchführung einer Zwangsmaßnahme eine Frist zu setzen. Nach Ablauf dieser Frist darf die Zwangsmaßnahme nicht mehr angeordnet werden. Der Beschluss ist den zur Beschwerde Berechtigten (§ 87 StPO) zuzustellen.

Sowohl die staatsanwaltschaftliche Anordnung als auch die gerichtliche Bewilligung müssen der in **§ 115f Abs. 3 StPO** enthaltenen erhöhten Begründungspflicht gerecht werden. Der Begründungsumfang orientiert sich an den Erfordernissen bestehender, strenger geregelter Ermittlungsmaßnahmen (etwa Auskunft von Daten einer Nachrichtenübermittlung nach § 135 StPO). Sie geht allerdings auch darüber hinaus, indem sowohl die staatsanwaltschaftliche Anordnung als auch die gerichtliche Bewilligung der Beschlagnahme von Datenträgern und Daten die **Umschreibung der Datenkategorien** und **Dateninhalte**, die zu beschlagnahmen sind, zu enthalten hat und aus ihnen auch ausreichend klar hervorgehen muss, in Bezug auf welchen **Zeitraum** die Beschlagnahme zu erfolgen hat. Unter Datenkategorien sind allgemeine Festlegungen, wie etwa Kommunikationsdaten, Metadaten, Fotos, Videos, Standortdaten, etc. zu verstehen.

Die Beschlagnahme darf jeweils nur für jenen Zeitraum angeordnet und bewilligt werden, in Bezug auf welchen dies zur Erreichung ihres Zwecks voraussichtlich erforderlich ist. Diese zusätzliche Begründungspflicht zum Zeitpunkt der Antragstellung und Bewilligung ist im Wesentlichen den Anforderungen des VfGH nachgebildet (vgl. dazu die Ausführungen in der Rn. 79 des Erkenntnisses). Damit sind die Anforderungen an die Ausgestaltung der Anordnung und Bewilligung der Beschlagnahme von Datenträgern und Daten höher als bei einer gewöhnlichen Sicherstellung (§ 110 Abs. 2 iVm § 102 Abs. 1 StPO) oder einer (allgemeinen) Beschlagnahme (§ 115 StPO). Sie sind zwar an § 138 Abs. 1 StPO angelehnt, gehen aber über die erforderlichen Angaben einer Anordnung nach § 135 Abs. 2b StPO sowie einer Anordnung und Bewilligung nach den § 135 Abs. 2, 2a und 3 StPO und § 136 StPO hinaus.

Die vorgeschlagene Verpflichtung der Einschränkung soll einen gesetzlichen Rahmen bieten, auf welche Datenkategorien und Dateninhalte sowie auf welchen Zeitraum die Beschlagnahme von Datenträgern und Daten abzielen soll. Sie bietet dadurch nicht nur eine Überprüfbarkeit, sondern auch eine Vorhersehbarkeit für betroffene Personen, welcher Datenumfang konkret ausgewertet werden soll. Letztlich wird dadurch den von einer solchen Beschlagnahme betroffenen Personen auch ermöglicht, das von den Strafverfolgungsbehörden Gesuchte selbst herauszugeben, ihrer Mitwirkungspflicht nachzukommen (vgl. unten § 115g StPO) und damit die Durchführung der Zwangsmaßnahme der Beschlagnahme von Datenträgern und Daten abzuwenden. Die nach dem Gesetz in der gerichtlichen Entscheidung zwingend enthaltenen und entsprechend begründeten Parameter dienen letztlich auch dazu, die forensische Aufbereitung von Daten zu ermöglichen (vgl. die Ausführungen zu § 115h StPO).

Die maßgebliche Richtschnur für die Beurteilung im Einzelfall ist der Grundsatz der Verhältnismäßigkeit (§ 115f Abs 4), wobei die Staatsanwaltschaft im ersten Schritt und der Richter bzw. die Richterin im folgenden Schritt die Umstände des Einzelfalls (z. B. Schwere der Straftat, Verdachtsdichte, Haftsache) sowie andere Faktoren (z. B. verhältnismäßige Eingrenzung in zeitlicher Hinsicht oder im Datenumfang) berücksichtigen muss. An die Verhältnismäßigkeit wird ein weniger strenger Maßstab anzulegen sein, wenn sich ein weiterer Zeitraum – innerhalb einer Datenkategorie bzw. eines bestimmten Programms – auf **nicht personenbezogene** Daten bezieht (z.B. Datenerfassungsprotokoll einer Registrierkasse, um Unregelmäßigkeiten oder Manipulationen festzustellen). Ein besonders strenger Maßstab wird bei der Prüfung, ob eine Beschlagnahme erforderlich ist, in jenen Fällen anzulegen sein, in denen die Ermittlungsmaßnahme bei einer nicht verdächtigen Person durchgeführt werden soll. Bei der Abwägung im Einzelfall kann es darüber hinaus einen Unterschied machen, ob die Ermittlungsmaßnahme lediglich auf Daten abzielt, die auf einem Datenträger selbst gespeichert sind (z. B. Daten, die auf einem USB-Stick oder lokal auf einem Smartphone gespeichert sind; § 109a Z 2 lit. a StPO) oder nicht. Soll daher (auch) ein Zugriff auf Daten erfolgen, die in anderen Speicherorten als dem Datenträger gespeichert sind (§ 109a Z 2 lit. b StPO), kann dies im Rahmen der Verhältnismäßigkeitsprüfung ebenso eine Rolle spielen (z. B. wenn die Gefahr besteht, dass vermehrt unbeteiligte Personen betroffen sind). Weiters kann es einen Unterschied machen, ob auf einen (weiteren) Datensatz zugegriffen wird, für den aus technischer Sicht eine eigene Originalsicherung (§ 109 Z 2c StPO) und Arbeitskopie (§ 109 Z 2d StPO) hergestellt werden muss (vgl. dazu näher die Ausführungen zu § 115h StPO). Eine solche Konstellation stellt sich vor allem im Fall des Zugangs auf Cloud-Daten, die dann erreichbar sind, wenn die auf einem Datenträger gespeicherten Daten (z. B. der Arbeitsspeicher im Online-Modus) gesichert werden und sich darin ein Schlüssel befindet, der einen Zugang zur Cloud ermöglicht.

Obwohl eine Beschlagnahme von Datenträgern und Daten grundsätzlich eine vorherige gerichtliche Bewilligung erfordert (§ 115f Abs. 2 StPO), soll in einem eng definierten Teilbereich den Interessen der Strafverfolgung in der Praxis Rechnung getragen und der Kriminalpolizei eine Sicherstellung aus eigenem bei Gefahr im Verzug sowie in den Fällen des § 110 Abs. 3 StPO und § 170 Abs. 1 Z 1 StPO möglich sein (**§ 115f Abs. 4 StPO**).

Nur ausnahmsweise soll in diesem Stadium jedoch der grundrechtsintensivere inhaltliche Zugriff auf konkret bezeichnete einzelne (punktuelle) Daten zulässig sein (der umfassende Zugriff wird eigenständig geregelt, siehe § 115h, § 115i StPO); andernfalls soll selbst ein Versuch, auf die gespeicherten Daten – mit Ausnahme der Sicherung bei Gefahr in Verzug – in irgendeiner Form zuzugreifen (z. B. Versuch der Entsperrung), ausgeschlossen sein. Vielmehr soll grundsätzlich lediglich die physische ‚Inbesitznahme‘ des Datenträgers zur Sicherung einer nachfolgenden Anordnung und Bewilligung iSd § 115f Abs. 2 und 3 StPO zulässig sein. Anwendungsfälle werden beispielsweise Fälle von Suchtgiftkriminalität sein, in denen die Kriminalpolizei die Beschuldigte bzw. den Beschuldigten auf frischer Tat betritt und ihm bzw. ihr ein Mobiltelefon abnimmt (vgl. § 110 Abs. 3 Z 3 StPO). Eine solche auf absolute – in der Regel situative – Ausnahmefälle beschränkte Befugnis der Kriminalpolizei, Datenträger von sich aus vorläufig sicherzustellen, stellt einen maßvollen Eingriff dar. Dies insbesondere vor dem Hintergrund, dass die Kriminalpolizei schließlich auch berechtigt ist, wesentlich grundrechtsintensivere Maßnahmen aus eigenem durchzuführen, etwa den Beschuldigten von sich aus festzunehmen, was letztlich auch eine praktische Fallkonstellation darstellt, auf die § 110 Abs. 3 Z 3 StPO abstellt (vgl. § 170 Abs. 1 Z 1 StPO sowie bei Gefahr im Verzug § 171 Abs. 2 Z 2 StPO).

Nach **§ 115f Abs. 6 StPO** soll ein (neuerlicher) Zugriff auf die Originalsicherung und die Arbeitskopie (vgl. die Ausführungen zu § 109 Z 2c StPO) ausschließlich dann zulässig sein, wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass ein weiterer Zugriff erforderlich ist. In diesem Fall müssen die Voraussetzungen des Abs. 1 leg. cit. erfüllt sein. Bestimmte Tatsachen sind etwa dann anzunehmen, wenn die auf Basis des aufbereiteten Datenmaterials (vgl. die Ausführungen zu § 115h StPO) vorgenommene Auswertung (vgl. die Ausführungen zu § 115i StPO) ergeben hat, dass ein Zeitraum von der gerichtlichen Bewilligung nicht erfasst ist, der aus Beweisgründen zur Aufklärung der Straftat erforderlich ist (z. B. Besitz von bildlichem sexualbezogenem Kindesmissbrauchsmaterial bereits in einem davorliegenden Zeitraum). Darüber hinaus kann auch die Tatsache, dass z. B. im Rahmen der unabhängigen Aufsicht durch den Rechtsschutzbeauftragten bzw. die Rechtsschutzbeauftragte der Justiz nach § 115l StPO technische Umstände bekannt werden, die die Prüfung der Verlässlichkeit der Daten erfordern, einen neuerlichen Zugriff erforderlich machen. Die Bestimmung stellt somit sicher, dass die Strafverfolgungsbehörden nicht – wie im geltenden Recht – auf die Originalsicherung (§ 109 Z 2c StPO) und damit auf den (nicht lesbaren) gesamten Datenbestand laufend zugreifen können; sie soll vielmehr dazu beitragen, die am geltenden Recht vom VfGH kritisierte Intransparenz des Auswertungsprozesses zu beseitigen. Umgekehrt soll die Regelung dem Interesse der Strafrechtspflege Rechnung tragen und den Strafverfolgungsbehörden verdeutlichen, dass kein Datenverlust zu befürchten ist (vgl. auch zur Bestimmung der Verwahrung die Ausführungen zu § 115k StPO), weil auf die Originalsicherung und die Arbeitskopie unter den Voraussetzungen des Abs. 1 letztlich (erneut) zugegriffen werden kann. Die Anordnung und die gerichtliche Bewilligung müssen jedoch die Voraussetzungen des Abs. 3 erfüllen.

§ 115f Abs. 7 StPO soll im Hinblick auf im Begutachtungsverfahren geäußerte Kritik für die Beschlagnahme von Datenträgern und Daten nicht lediglich die sinngemäße Anwendung der § 110 Abs. 4 und § 115 Abs. 6 StPO anordnen, sondern ausdrücklich klarstellen, dass eine Beschlagnahme von Datenträgern und Daten aus Beweisgründen nicht zulässig ist, wenn der Beweiszweck durch Bild-, Ton- oder sonstige Aufnahmen oder durch Kopien automationsunterstützt verarbeiteter Daten erfüllt werden kann und nicht anzunehmen ist, dass die Datenträger selbst oder die Originale der beschlagnahmten Daten in der Hauptverhandlung in Augenschein zu nehmen sein werden. Dadurch soll die Verhältnismäßigkeit der Beschlagnahme von Datenträgern und Daten iSd bestehenden Systematik gewahrt und weiter verstärkt werden.

Dem Grundsatz der Verhältnismäßigkeit entsprechend normiert nämlich bereits § 110 Abs. 4 StPO zur Sicherstellung, dass in einem solchen Fall die Sicherstellung unzulässig und jedenfalls auf Verlangen der betroffenen Person aufzuheben ist. Dabei kommt es nicht auf den Aufwand der Anfertigung von digitalen Bilddateien bzw. Kopien wegen einer großen Menge an. Dies dient auch einem effizient geführten Ermittlungsverfahren, um sich möglichst frühzeitig auf die strafrechtlich relevanten Sachverhalte zu konzentrieren (vgl. OLG Linz 9 Bs 73/10i). Gleiches gilt für die Beschlagnahme nach § 115 Abs. 3 StPO, die auf die dort angeführten Aufnahmen und Kopien zu beschränken ist (vgl. *Tipold/Zerbes* in Fuchs/Ratz, WK StPO Vor §§ 110–115, Rz. 8). Vor diesem Hintergrund sollen daher nach § 115f Abs. 6 StPO zumindest nach einer Sichtung der Unterlagen die Originale – nach Anfertigung entsprechender

Bild-, Ton- oder sonstiger Aufnahmen bzw. Kopien – ausgefolgt werden; die (weitere) Beschlagnahme ist dann unzulässig.

Da die Anfertigung digitaler Bilddateien oder Kopien sowie die digitale Sicherung von Daten häufig dazu führt, dass eine physische Sicherstellung oder Beschlagnahme des Datenträgers selbst (bzw. die Herstellung einer Originalsicherung über den gesamten Datenbestand) entfällt, bietet § 110 Abs. 4 StPO bereits de lege lata eine Grundlage für eine verhältnismäßige Begrenzung des Eingriffs. Darauf aufbauend soll nunmehr auch im Gesetzestext klargestellt werden, dass unter Beibehaltung der geübten Praxis ein sofortiger Zugriff auf Datenträger und Daten sowie die Einsichtnahme in diese zulässig ist, um (lediglich) die erforderlichen Daten zu sichern. Diese Regelung soll gewährleisten, dass der Vollzug der gerichtlichen Bewilligung – auch im Hinblick auf den Grundsatz der Datenminimierung – nach einer erster Vorselektion (Erstsichtung) auf jene Sicherungsdaten beschränkt wird, die anschließend aufbereitet und ausgewertet werden sollen. Der Verweis auf § 74 Abs. 2 StPO stellt klar, dass die Sicherung dem Grundsatz der Gesetz- und Verhältnismäßigkeit (§ 5 StPO) zu entsprechen hat und im Rahmen der gerichtlichen Bewilligung auf erforderliche Daten zu beschränken ist, die Sicherung sich daher – aufgrund der schon durch das Gericht vorgenommenen Prüfung iSd § 5 stopp – jedenfalls im Rahmen der richterlichen Bewilligung bewegen muss. Erfolgt Zugriff und Einsichtnahme in überschießender Weise, greift u.a. die Rechtsfolge nach § 115j Abs. 1 StPO.

Die Beschlagnahme von Daten, einschließlich derjenigen, die auf Kopien beschränkt sind (vgl. hierzu auch die bestehende Regelung in § 115 Abs. 3 StPO für die Beschlagnahme von Kopien) ist aufzuheben, wenn die Voraussetzungen für die Beschlagnahme nicht oder nicht mehr bestehen. Die Notwendigkeit einer Beschlagnahme kann sich auch erst zu einem späteren Zeitpunkt als nicht mehr gegeben erweisen. Dies könnte etwa der Fall sein, wenn ein Original beschlagnahmt wurde, aber später digitale Kopien oder Sicherungen angefertigt werden können, oder wenn sich beschlagnahmte Kopien später als nicht relevant herausstellen (vgl. zur Beschlagnahme von Kopien *Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 110 Rz. 76).

§ 115f Abs 8 regelt die Verpflichtung zur Information der von der Sicherstellung betroffenen Personen, die – wie derzeit (vgl. § 111 Abs. 4 StPO) – längstens binnen 24 Stunden über ihre Rechte zu informieren sind.

Gemäß § 115f Abs 9 StPO kommen der Beschwerde (§ 87) und dem Einspruch (§ 106) kommt infolge ausdrücklicher Regelung aufschiebende Wirkung zu (§ 87 Abs. 3 StPO), soweit sie die Zulässigkeit der Beschlagnahme betreffen. Wird die Beschlagnahme rechtskräftig für unzulässig erklärt, sind die beschlagnahmten Daten zu vernichten (§ 115f Abs. 7 iVm § 89 Abs. 4 StPO) bzw. ist der beschlagnahmte Datenträger zurückzustellen (vgl. *Stricker* in *Birklbauer/Haumer/Nimmervoll/Wess* (Hrsg), stopp – Linzer Kommentar zur Strafprozessordnung zu § 89 StPO Rz. 26). Diese Vernichtungs- und Zurückstellungsanordnungen sollen aufgrund der von VfGH und EuGH festgestellten Eingriffsintensität und dem Grundsatz der Datenminimierung einen spürbaren Ausgleich bieten. Die ausdrückliche Vernichtungsanordnung in diesem Fall bezweckt damit nicht bloß die Anerkennung der Unzulässigkeit des Eingriffs, wie es im Fall der Rechtswidrigkeit der Durchsuchung von Orten (§ 119 ff. StPO) der Fall ist (vgl. OGH 14 Os 46/09k mit dem Hinweis, dass eine wirksame Beschwerde iSd Art. 13 EMRK im Hauptverfahren durch die Verfahrensrüge des § 281 Abs. 1 Z 4 StPO gegeben ist). Vielmehr soll im Gleichklang mit dem Fall einer (nachträglich) ausgesprochenen Unzulässigkeit einer im 5. und 6. Abschnitt des 8. Hauptstücks der StPO (§§ 134 bis 143 StPO) geregelten Ermittlungsmaßnahme festgelegt werden, dass das Gericht sogleich anzuordnen hat, dass alle durch die Ermittlungsmaßnahme gewonnenen Ergebnisse zu vernichten sind (vgl. zur Missachtung der Vernichtungsanordnung OGH 13 Os 83/08t; weiters *Ratz* in *Fuchs/Ratz*, WK StPO § 281 Rz. 368). In diesem Sinne sollen in **§ 281 Abs. 1 1 Z 3, § 345 Abs. 1 Z 4 und § 468 Abs. Z 3 StPO** die Fälle der Nichtigkeit auf § 115j Abs. 1 StPO erweitert werden.

§ 115g Abs. 1 StPO soll zum einen als *lex specialis* zu § 111 Abs. 1 StPO die Herausgabe eines Datenträgers sowie zum anderen als Nachfolgebestimmung des aufzuhebenden § 111 Abs. 2 StPO die Pflicht zur Herausgabe von auf Datenträgern gespeicherten Daten regeln und damit der Ermöglichung der Beschlagnahme von Datenträgern und Daten dienen. Die Pflicht betrifft sowohl verdächtige als auch unverdächtige Personen. Kommt eine Person der Herausgabepflicht nicht nach, so ist die Beschlagnahme mit Zwang durchzusetzen. Abs. 1 enthält in diesem Zusammenhang nunmehr klarstellend einen expliziten Hinweis auf § 93 Abs. 2 StPO. Gemäß dem in § 7 Abs. 2 StPO geregelten *nemo tenetur-Prinzip* darf ein Verdächtiger bzw. eine Verdächtige oder ein Beschuldigter bzw. eine Beschuldigte jedoch nicht gezwungen werden, sich selbst zu belasten. Dieses Verbot des Zwangs zur Selbstbelastung bezieht sich auch auf Beweismittel, zu deren eigenhändigen Herausgabe der bzw. die Beschuldigte nicht gezwungen werden darf (*Haslwanter* in *Fuchs/Ratz*, WK StPO § 7 Rz. 37). Auch bei gesetzlichen Befreiungen von der Aussagepflicht oder bei Vorliegen von Aussageverweigerungsrechten darf eine Mitwirkungspflicht nicht mittels Zwang bei Personen durchgesetzt werden, die von der Pflicht zur Aussage gesetzlich befreit

sind (§ 93 Abs. 2 StPO). Beschuldigte und bestimmte schweigeberechtigte Personengruppen dürfen also keinesfalls gezwungen werden, Zugang zu Daten zu gewähren und z. B. Zugangscode bekanntzugeben. Der Zugang darf – wenn möglich – nur anderweitig erlangt werden (z. B. durch allfällige Abnahme eines Zettels, auf dem der Zugangscode vermerkt ist). Eine Strafbarkeit nach § 295 StGB (Unterdrückung eines Beweismittels) kommt mit Blick auf § 7 Abs. 2 StPO bei Beschuldigten und schweigeberechtigten Personengruppen selbst dann nicht in Betracht, wenn sie ihrer Herausgabepflicht nicht nachkommen.

Ob bzw. inwieweit es gegebenenfalls gegen das Verbot des Zwangs zur Selbstbelastung verstoßen würde, wenn ein Mobiltelefon zum Entsperren vor das Gesicht eines bzw. einer Beschuldigten gehalten oder sein bzw. ihr Finger dafür auf den Sensor eines Mobiltelefons geführt würde, ist in der Literatur strittig und wird letztlich von den zur Beurteilung der Gesetz- und Verhältnismäßigkeit des Handelns der Strafverfolgungsbehörden zuständigen Gerichten zu beurteilen sein (vgl. *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 111 Rz. 4 und 13/1; *Zerbes*, Beweisquelle Handy, ÖJZ 2021/24; *Schrank/Stückberger/Kleinbrod*, Sicherstellung im digitalen Zeitalter, ZWF 2020, 289; *Seidl/Schönborn*, Dürfen Strafverfolgungsbehörden Beschuldigte zur (biometrischen) Entschlüsselung von Endgeräten zwingen?, JBl 2022, 361).

Die Pflichten der genannten Personengruppen, Zugang zu Daten zu gewähren, ist mit der Herausgabe des Datenträgers erschöpft (vgl. *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 111 Rz. 13/1). Aus der Pflicht, Zugang zu Daten zu gewähren, lässt sich darüber hinaus für die Entschlüsselung eines Datenträgers keine weitergehende Pflicht zur Aktivität ableiten: Ein von der gerichtlichen Beschlagnahme Betroffener bzw. eine solche Betroffene kann daher nicht zu einem persönlichen Arbeitseinsatz gezwungen werden.

Abgesehen von den genannten Personengruppen sind alle anderen Personen, die von einer Beschlagnahme betroffen sind, grundsätzlich verpflichtet, im Umfang der gerichtlichen Bewilligung Zugang zu den Daten zu gewähren. Diese Mitwirkungspflicht kommt freilich nur dann zum Tragen, wenn die Daten nicht bereits ohne weiteres ausgelesen werden können (etwa, weil das beschlagnahmte Mobiltelefon nicht durch einen Code gesperrt ist). In diesem Fall ist schon mit der Beschlagnahme des Datenträgers bzw. der Herstellung einer Originalsicherung alles Erforderliche für den Zugriff auf die Daten getan. Ist ein Datenträger hingegen durch Passwörter oder sonstige Zugangsschlüssel geschützt, können jene Personen, bei denen die Beschlagnahme durchgeführt wird, – mittels Beugemitteln – gezwungen werden, Zugangscode preiszugeben (vgl. *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 111 Rz. 13/1).

Die betroffene Person trifft die schon im geltenden Recht verankerte Pflicht, auf Verlangen Daten in einem allgemein gebräuchlichen Format zur Verfügung zu stellen. Dazu hat sie entweder Daten in einem allgemein gebräuchlichen Dateiformat auszufolgen oder durch die Kriminalpolizei herstellen zu lassen. Die sinngemäße Anwendung des § 111 Abs. 3 StPO dient dem angemessenen Kostenersatz.

Ist die von einer Beschlagnahme betroffene Person freiwillig bereit, die Beschlagnahme von Datenträgern und Daten zuzulassen, indem sie der Staatsanwaltschaft oder der Kriminalpolizei Zugang zu den Daten verschafft, kann es – je nach Einzelfall – geboten sein, die Daten auch bloß in Form eines Augenscheins (§ 149 StPO) zu sichern, etwa wenn ein Opfer der Kriminalpolizei freiwillig Einschau in sein Mobiltelefon gewährt, um einzelne Nachrichten zu sichern, in denen eine gefährliche Drohung ausgesprochen wurde. In diesem Fall sind gemäß § 149 Abs. 2 letzter Satz StPO Art und Weise der Durchführung des Augenscheins und seine Ergebnisse in einem Amtsvermerk festzuhalten.

Die sinngemäße Anwendung des § 112 StPO und des § 112a StPO in § 115g Abs. 2 StPO ist vor dem Hintergrund der Ausgestaltung der Vorschriften der §§ 115f ff. StPO als *leges speciales* erforderlich; eine inhaltliche Änderung ist damit nicht verbunden. Präzisierend wird – basierend auf Anregungen im Begutachtungsverfahren – eine Klarstellung der Vorgehensweise vorgeschlagen: der Beschlagnahme Datenbestand soll im Sinne der gerichtlichen Bewilligung der Beschlagnahme von Datenträgern und Daten zunächst vom Gericht technisch aufbereitet werden und lediglich das Ergebnis dieser Datenaufbereitung (§ 109 Z 2e StPO) der Bezeichnungspflicht zugrunde liegen. Dies soll zu einer deutlichen Beschleunigung des Sichtsungsverfahrens beitragen, indem es sich nur noch auf den verfahrensrelevanten reduzierten Datenbestand bezieht. Zum Zweck der Bezeichnung sind die betroffene Person, Behörde oder öffentliche Dienststelle berechtigt, Einsicht in das Ergebnis der Datenaufbereitung zu nehmen.

§ 115g Abs. 3 StPO regelt die Berichtspflicht der Kriminalpolizei, wenn ein Datenträger oder Daten vorläufig aus Eigenem sichergestellt wurden (§ 115f Abs. 4 StPO). Die Berichtspflicht soll unverzüglich erfolgen. Die Staatsanwaltschaft hat in diesem Fall sogleich die Beschlagnahme von Datenträgern und Daten nach § 115f StPO zu beantragen oder die Aufhebung der Sicherstellung anzuordnen (vgl. § 113 Abs. 3 StPO). Wird die Bewilligung nicht erteilt, so sind aufgrund des Beweisverwertungsverbots und des Grundsatzes der Datenminimierung die Originaldaten zurückzustellen und allfällige Kopien und

Sicherungen zu vernichten. Die Beschwerde der Staatsanwaltschaft gegen einen solchen Beschluss des Gerichts hat aufschiebende Wirkung, um - Anregungen im Begutachtungsverfahren folgend - sicherstellen, dass keine Ausfolgungsansprüche vor einer rechtskräftigen gerichtlichen Entscheidung geltend gemacht werden können und kein Verlust von Beweismitteln eintritt.

Zur Aufbereitung von Daten (§ 115h StPO):

Entsprechend dem Konzept der vorgeschlagenen neuen Ermittlungsmaßnahme soll gewährleistet werden, dass die für die Führung des Ermittlungsverfahrens zuständige Staatsanwaltschaft und die Kriminalpolizei keinen Zugang zum gesamten Datenbestand (Originalsicherung nach § 109 Z 2c oder Arbeitskopie nach § 109 Z 2d) haben, sondern – immer nach einer gerichtlichen Bewilligung – ausschließlich zum Ergebnis der Datenaufbereitung (§ 109 Z 2e StPO).

Die Aufbereitung von Daten soll künftig – abgesehen von wenigen gesetzlich geregelten Ausnahmefällen – ausschließlich das Gericht vornehmen.

Gemäß **§ 115h Abs. 1 StPO** hat das Gericht eine Originalsicherung (§ 109 Z 2c StPO), somit eine Imagesicherung (1:1-Kopie) des Datenträgers, zu erstellen und mittels entsprechender forensischer Sicherungsmechanismen (Schreibschutz, Schreibblocker) zu sichern. Damit ist gewährleistet, dass ab dem Beginn der Imageerstellung kein Schreibvorgang auf dem zu sichernden Datenträger und somit keine Änderung am Datenbestand mehr möglich ist. In der Praxis wird der Datenbestand mit einem Hash-Wert (Prüfsumme auf Grund eines mathematischen Logarithmus) versehen. Nach Herstellung einer Originalsicherung dient diese als Grundlage für die Herstellung einer ‚Arbeitskopie‘, mit welcher die Aufbereitung der konkreten (immer noch Roh-)Daten vorgenommen wird. Ist von der gerichtlichen Bewilligung auch die Beschlagnahme von Daten umfasst, die an anderen Speicherorten liegen (§ 109 Z 2a lit. b StPO), ist eine weitere Originalsicherung und Arbeitskopie erforderlich; dies ist etwa dann der Fall, wenn eigens auf einen Cloud-Speicher zugegriffen werden soll.

Damit wird dieser Aufgabenbereich gesetzlich definiert; Das anhand der gerichtlichen Bewilligung aufbereitete Datenmaterial (‚*Ergebnis der Datenaufbereitung*‘) ist in einem allgemein gebräuchlichen Dateiformat in strukturierter Form, sodass die Daten elektronisch weiterverarbeitet werden können, herzustellen. Die Wendung in Bezug auf das Dateiformat orientiert sich an § 116 Abs. 6 StPO und soll insbesondere nicht nur der leichteren Auswertung durch die Strafverfolgungsbehörden dienen, sondern auch den berechtigten Verfahrensparteien (s. § 115 Abs. 2 und 4 StPO) und dem Rechtsschutzbeauftragten im Rahmen seiner unabhängigen Aufsicht (§ 115l Abs. 4 und 5 StPO) die effektive Wahrnehmung ihrer Rechte ermöglichen.

Der Aufbereitungsbericht hat den Vorgaben des § 100 Abs. 1 erster Satz StPO zu entsprechen, somit die Ermittlungen aktenmäßig in einer Form festzuhalten, dass deren Anlass, Durchführung und Ergebnis nachvollzogen werden können. Der Bericht hat – ebenfalls aus Gründen der Transparenz – jedenfalls Informationen zum Umstand der Wiederherstellung von Daten, die Kriterien für die erfolgte Einschränkung von Daten sowie die verwendeten Softwareprogramme festzuhalten.

Mit dem Abschluss der forensischen Arbeiten (‚*Ergebnis der Datenaufbereitung*‘) und der dargestellten Berichtspflicht (‚*Aufbereitungsbericht*‘) soll die Arbeitskopie, die aufgrund der Originalsicherung hergestellt wurde, gemeinsam mit der Originalsicherung sicher verwahrt werden (§ 115k StPO). Damit wird auf gesetzlicher Ebene eine weitere organisatorische Vorkehrung getroffen, um jeden Anschein eines (vermuteten) unzulässigen Zugriffs der Strafverfolgungsbehörden auf den Gesamtdatenbestand zu beseitigen. Die Umgehung gesetzlicher Vorgaben würde einen Fehlgebrauch von Befugnissen zur Aufklärung einer Straftat begründen.

Wesentlich ist, dass die Kriminalpolizei und die Staatsanwaltschaft ausschließlich jenen reduzierten Datensatz erhalten, der das Ergebnis der Datenaufbereitung (§ 109 Z 2e StPO) ist und damit in Bezug auf die Datenkategorien, Dateninhalte und den Zeitraum dem gerichtlich bewilligten Datenumfang entspricht.

Mit der vorgeschlagenen Regelung soll eine strikte Trennung zwischen dem ausschließlich für die forensische Aufbereitung zuständigen Gericht sowie der Kriminalpolizei und der Staatsanwaltschaft gewährleistet werden, denen Einblick ausdrücklich nur in jene Daten zukommt, die in Bezug auf die Datenkategorien, Dateninhalte und den Zeitraum der gerichtlichen Bewilligung entsprechen. Auf diese Weise ist sichergestellt, dass den eigentlichen strafrechtlichen Ermittlungen künftig ein im Vergleich zur derzeitigen Praxis weit geringerer Datensatz zugrunde liegt. Damit einhergehend gewährleistet diese Trennung der Daten im Zuge ihrer Aufbereitung, dass von den – nach einer Beschlagnahme von Datenträgern – ausgewerteten Datensätzen und Daten in der Regel weitaus weniger Personen betroffen sind. Zugleich dient der Aufbereitungsbericht der Transparenz und ermöglicht eine Kontrolle, ob die gerichtliche Entscheidung in diesem Umfang richtig und vollständig umgesetzt wurde (s. in diesem

Zusammenhang auch die unabhängige Aufsicht durch den Rechtsschutzbeauftragten der Justiz, § 115l StPO).

Das Gericht soll die Aufbereitung von Daten unter Beiziehung geeigneter Hilfskräfte oder eines Sachverständigen durchzuführen haben. Als Hilfskräfte kann das Gericht Sachverständige oder die IT-Expert:innen des justizeigenen IT-Forensikzentrums beiziehen.

§ 115h Abs. 2 StPO ermöglicht der Staatsanwaltschaft und dem Beschuldigten, die Aufbereitung von Daten durch einen Sachverständigen zu beantragen, wenn dies notwendig ist, um das Verfahren zu beschleunigen (§ 9), oder weil das besondere Fachwissen eines Sachverständigen benötigt wird. Darüber hinaus können die Staatsanwaltschaft, der Beschuldigte und die betroffene Person, Behörde oder öffentlichen Dienststelle Suchparameter zum Zweck der Aufbereitung von Daten (§ 109 Z 2e) vorschlagen.

Das Erfordernis eines besonderen Fachwissens einer bzw. eines Sachverständigen betrifft insb. die forensische Aufbereitung von Daten (§ 109 Z 2e StPO) und nicht dessen sonstige Sachkunde.

Für die Bestellung von Sachverständigen sind die allgemeinen Bestimmungen nach §§ 125 ff StPO anzuwenden. Die Tätigkeit von Sachverständigen im Dienste der Strafrechtspflege bedingt – neben strengen Berufspflichten – schon durch die allgemeinen Vorgaben aus der DSGVO eine durchgängige Nachvollziehbarkeit und Protokollierung der Datenverarbeitung sowie – auch im Lichte des Grundsatzes der Datenminimierung – eine Löschung von Datenbeständen, wenn der gerichtliche Auftrag erfüllt wurde. Damit jedoch die allgemeinen Vorgaben zur Verwahrung von Datenträgern und Daten (§ 115k StPO) sowie die das Gericht in § 115 Abs. 5 StPO treffende Pflicht zur Vernichtung der Originalsicherung und der Arbeitskopie erhalten bleiben, wird die Originalsicherung und die Arbeitskopie – im Regelfall auch über einen gerichtlichen Auftrag – an das Gericht zu übermitteln sein. Dies auch vor dem Hintergrund, damit der Rechtsschutzbeauftragte (§ 115l StPO) die ihm gesetzlich zugewiesenen Aufgaben erfüllen kann.

Die vom Gericht zur Erfüllung dieser Aufgaben beigezogenen Hilfskräfte dürfen nicht auch für den Rechtsschutzbeauftragten, die Staatsanwaltschaft oder die Kriminalpolizei tätig sein (somit keine Doppel- oder Mehrfachverwendungen von Expertinnen bzw. Experten).

§ 115h Abs. 4 StPO dient dem Grundsatz der Datenminimierung. Die erforderlichen Daten dürfen nur gespeichert werden, solange sie erforderlich sind.

§ 115h Abs. 5 StPO regelt, dass die Staatsanwaltschaft die Ergebnisse der Datenaufbereitung dem Gericht bei Einbringung der Anklage zu übermitteln hat. Dadurch soll das Gericht in der Hauptverhandlung über jenen Datenbestand verfügen, der für die Auswertung von Daten (§ 115i StPO) erheblich war. Die Bestimmung sieht darüber hinaus vom Verfahrensstadium abhängige Vernichtungsverpflichtungen vor. Es sind sowohl die Ergebnisse der Datenaufbereitung selbst zu löschen als auch die Originalsicherung und die Arbeitskopie. Eine Aufbewahrung ‚auf Vorrat‘ für den Fall der allfälligen Einleitung eines (weiteren) Strafverfahrens ist daher unzulässig.

Zur Auswertung von Daten (§ 115i und § 115j StPO):

Sobald der Staatsanwaltschaft und der Kriminalpolizei das Ergebnis der Datenaufbereitung sowie den Aufbereitungsbericht vorliegt, beginnt die zentrale Phase der Auswertung von Daten. Um diese friktionsfrei in das bestehende System strafprozessualer Regelungen einzufügen, erfolgt eine weitgehende Anlehnung an die Systematik der Überwachung von Nachrichten (§ 115i Abs. 1 Satz 2 StPO ist an § 138 Abs. 4 StPO angelehnt; in gleicher Weise entsprechen § 115i Abs. 3 bis Abs. 5 StPO im Wesentlichen den bestehenden Regelungen in § 139 Abs. 2 bis Abs. 4 StPO).

Um die Auswertung des – bereits reduzierten – Datenbestandes auf das unvermeidbare Maß zu beschränken, wird in **§ 115i Abs. 1 erster Satz StPO** vorgeschlagen, dass die Staatsanwaltschaft und die Kriminalpolizei Suchparameter festlegen können; diese sowie die durch den Einsatz dieser Suchparameter erzielten Suchtreffer sind zu dokumentieren. Damit soll auf Gesetzesebene ein weiterer (grundrechtlicher) Ausgleich erfolgen, um die vom VfGH kritisierte Intransparenz der Auswertung von Daten zu beseitigen. Die Möglichkeit des Einsatzes von Suchparametern ist als eine Kann-Bestimmung ausgestaltet, um der Staatsanwaltschaft – abhängig vom Datenbestand – ein Ermessen einzuräumen. In komplexen (Wirtschafts-)Verfahren ist der Einsatz von Suchparametern aufgrund der Datenmengen, aus denen potentiell (beweis-)erhebliche Tatsachen zu extrahieren sind, weitaus häufiger anzunehmen als dies etwa bei Verfahren wegen beharrlicher Verfolgung nach § 107a StGB der Fall sein wird, wo primär der Kommunikationsverlauf zwischen den Beteiligten auszuwerten sein wird. Unter Suchparameter sind etwa Suchwortlisten und die Suche nach bestimmten Merkmalen in einer Datenstruktur zu verstehen. Wie weit der Kreis allfälliger Suchparameter gezogen werden kann, liegt letztlich im Ermessen der

Staatsanwaltschaft, deren diesbezügliche Anordnungen die Kriminalpolizei – bei divergierenden Ansichten – zu beachten hat.

§ 115i Abs. 1 letzter Satz StPO soll nunmehr für diesen Bereich ausdrücklich gesetzlich normieren, dass die Staatsanwaltschaft nur diejenigen Ergebnisse der Auswertung zu den Akten zu nehmen hat, die für das Verfahren – entsprechend dem Grundsatz der materiellen Wahrheit (§ 3 StPO) alle be- und entlastenden Tatsachen – von Bedeutung sind und als Beweismittel verwendet werden dürfen. Im Sinne der Rechtsprechung des OGH (vgl. 11 Os 56/20z) soll damit die Verpflichtung der Staatsanwaltschaft (sowie der Kriminalpolizei) gesetzlich festgelegt werden, strafrechtserhebliche Informationen (bzw. Daten) säuberlich von anderen zu trennen. Werden im Rahmen der Auswertung Informationen erhoben, deren Erheblichkeit für das konkrete Strafverfahren nicht erkennbar ist, sind sie nach der Rechtsprechung des OGH vom Verfahrensgegenstand nicht umfasst. Sie dürfen weder ermittelt noch zu den Akten genommen oder dort belassen werden. Der OGH folgert in ständiger Rechtsprechung, dass Ermittlungsakten nicht faktisch, sondern rechtlich determiniert sind (RIS-Justiz RS0133323). Insoweit erfassen Ergebnisse einer Auswertung nicht jene Tatsachen, die nicht als Beweismittel verwendet werden dürfen (konkret Fälle nach § 115j Abs. 1 StPO, § 144 StPO sowie § 157 Abs. 2 StPO).

In diesem Zusammenhang legt **§ 115i Abs. 2 StPO** fest, dass Beschuldigte und Opfer zusätzliche (eigene) Suchparameter beantragen können. Diese Regelung stärkt – auch im Sinne eines (grundrechtlichen) Ausgleichs – die Beteiligungsmöglichkeit von Beschuldigten, womit die Waffengleichheit iSd Art. 6 EMRK hergestellt wird; sie trägt darüber hinaus auch den Opferschutzinteressen gebührend Rechnung. Die sinngemäße Anwendung des § 51 Abs. 2 StPO soll sicherstellen, dass die vorgeschlagene Einsicht in das Ergebnis der Datenaufbereitung – vergleichbar den Fällen der Akteneinsicht – aus den in dieser Bestimmung genannten Gründen beschränkt werden kann.

Einen wesentlichen Beitrag zu einem (grundrechtlichen) Ausgleich soll auch die Möglichkeit schaffen, dass Beschuldigte und Opfer, die Ergebnisse der Datenaufbereitung einsehen können. Dies erscheint vor dem Hintergrund, dass es sich ohnehin um den eigenen (aufbereiteten) Datenbestand handelt, zweckmäßig, um u.a. die Waffengleichheit in diesen Konstellationen voll herzustellen; andere (Mit-)Beschuldigte und Opfer sollen hingegen nur das Recht auf Akteneinsicht haben (wobei Bezugspunkt dieses Rechts weiterhin (nur) erhebliche Tatsachen sind, die verpflichtend aktenmäßig zu dokumentieren sind; vgl. 14 Os 35/21k); aufgrund des unverhältnismäßigen Eingriffs in die Persönlichkeitssphäre einer anderen Person sollen sie hingegen nicht das Recht haben, in das Ergebnis der Datenaufbereitung Einsicht zu nehmen, weil der Datenbestand den höchstpersönlichen Lebensbereich dieser Person betrifft und ohnedies gerade Gegenstand der Auswertung (bzw. Selektion) von erheblichen Tatsachen ist. In diesen Fällen soll die vorgeschlagene Möglichkeit, Suchparameter zu beantragen, eine ausreichende – verhältnismäßige – Beteiligung sichern.

Künftig soll daher Beschuldigte oder Opfer, deren Datenträger und Daten beschlagnahmt wurden, die Möglichkeit haben, das Ergebnis der Datenaufbereitung im gleichen Umfang wie die Staatsanwaltschaft und Kriminalpolizei einzusehen. Dieses Recht ermöglicht es ihnen auch – falls von der gerichtlichen Bewilligung umfasst – die Einsichtnahme auch in wiederhergestellte Daten, die von ihm bzw. ihr ursprünglich gelöscht wurden; die bisher erfolgte bloße Zurückstellung des Datenträgers an den Beschuldigten bzw. die Beschuldigte, wodurch für ihn bzw. sie jedoch der Umfang der Auswertung nicht klar war, wird beseitigt.

Eine Ausfolgung des Ergebnisses der Datenaufbereitung soll nicht erfolgen, weil dies die Strafverfolgungsbehörden vor (zu) große praktische Hürden stellen würde. So sind beispielsweise verbotene Daten (wie etwa bildliches sexualbezogenes Kindesmissbrauchsmaterial oder Bombenbauanleitungen) zu vernichten; ob solche vorhanden sind, wird in aller Regel aber erst nach Auswertung feststehen, was insb. bei fremdsprachigen Personen und Kommunikationen eine Rolle spielen wird. Durch die geschilderten Beteiligungsmöglichkeiten soll jedoch ein angemessener grundrechtlicher Ausgleich möglich sein,

Die Bestimmungen in **§ 115i Abs. 3 bis Abs. 5 StPO** fassen – wie im geltenden Recht etwa bei der Auskunft von Daten einer Nachrichtenüberwachung (§§ 135 ff StPO) – die Rechte von Beschuldigten, Opfern und anderen betroffenen Personen auf Information, Einsicht und Vernichtung zusammen. Damit werden die für andere, strenger geregelte Ermittlungsmaßnahmen geltenden Rechte für die Beschlagnahme von Datenträgern und Daten verankert und gewährleisten in Fortsetzung der Systematik einen (grundrechtlichen) Ausgleich, um über die Ergebnisse der Auswertung informiert zu werden, diese einzusehen und – falls ein berechtigtes Interesse besteht – die Vernichtung dieser Ergebnisse zu beantragen.

Allgemein ist bei der Phase der Auswertung von Daten insbesondere auf die Bedeutung des § 74 Abs. 1 StPO hinzuweisen, wonach Kriminalpolizei, Staatsanwaltschaft und – hier nicht relevant – Gericht im

Rahmen ihrer Aufgaben (nur) die hierfür erforderlichen personenbezogenen Daten verarbeiten dürfen. § 74 Abs. 2 StPO verpflichtet beim Verwenden (Verarbeiten und Übermitteln) personenbezogener Daten dazu, den Grundsatz der Verhältnismäßigkeit (§ 5 StPO) zu beachten. Dabei sind schutzwürdige Interessen der Betroffenen an der Geheimhaltung zu wahren und der vertraulichen Behandlung von Daten Vorrang einzuräumen (vgl. *Fabrizy/Kirchbacher*, StPO¹⁴ § 74 Rz 2). In diesem Sinne wird auch in **§ 115i Abs. 4 StPO** ausdrücklich festgehalten, dass bei der Auswertung von Daten die Persönlichkeitsrechte (sämtlicher) Personen soweit wie möglich zu wahren sind; sie ist auf das unvermeidbare Maß zu beschränken.

In **§ 115j StPO** soll der – im geltenden Recht nicht ausdrücklich verankerte – Umgang mit Ergebnissen einer Auswertung und Zufallsfunden in der Phase der Auswertung von Daten geregelt werden. Nach **§ 115j Abs. 1 StPO** sollen – ergänzend zur Vernichtungsanordnung – auch Ergebnisse einer Auswertung bei sonstiger Nichtigkeit nur verwendet werden dürfen, wenn die Ermittlungsmaßnahme rechtmäßig angeordnet und bewilligt wurde. Es bedarf daher zur Verwertbarkeit der Ergebnisse der Ermittlungsmaßnahme einer ordnungsgemäßen Anordnung der Ermittlungsmaßnahme, wobei – wie schon in der Literatur zu § 140 StPO vertreten (vgl. *Rohregger in Birklbauer/Haumer/Nimmervoll/Wess* (Hrsg), StPO - Linzer Kommentar zur Strafprozessordnung [2020] zu § 140 StPO Rz 2) – für die rechtmäßige Anordnung und Bewilligung die formellen Voraussetzungen nach § 115f Abs. 2 und 5 StPO erfüllt sein müssen. Da im Sinne der Rechtsprechung des OGH ein Beweisverwendungsverbot jedoch nicht hindert, die Ergebnisse zum Anlass weiterer Erhebungen zu nehmen und die Ergebnisse dieser Erhebungen als Beweismittel zu verwerten (vgl. RIS-Justiz RS0129378), soll eine Verwendungsverbotskonsequenz in Form der Zurückstellung von Originaldaten sowie Vernichtung von Kopien und Sicherungen wie bei den (teils sogar weniger grundrechtsinvasiven Maßnahmen nach §§ 134, 135 greifen. Im Übrigen entspricht dies dem auch vom ÖRAK geforderten erhöhten Rechtsschutz.

Ergeben sich bei der Auswertung von Daten Hinweise auf die Begehung einer anderen strafbaren Handlung als derjenigen, die Anlass zur Beschlagnahme von Datenträgern und Daten gegeben hat, so ist gemäß **Abs. 2** mit diesen – einer Anregung des ÖRAK folgend – nicht nur wie ursprünglich vorgesehen ein gesondertes Protokoll zu verfassen, sondern (der Bestimmung des § 140 Abs. 2 StPO folgend) ein neuer Akt anzulegen, soweit die Verwendung als Beweismittel zulässig ist. Die Regelung verweist zur Zulässigkeit der Verwendung als Beweismitteln auf § 115j Abs. 1, § 144 und § 157 Abs. 2 StPO.

Die Anlassfälle für Zufallsfunde können künftig nur das Ergebnis der Datenaufbereitung (§ 109 Z 2e StPO) betreffen, welches im Sinne der Bewilligung hergestellt wurde. Dem Anschein, dass Strafverfolgungsbehörden auf den gesamten Datenbestand zugreifen könnten (z. B. auf die Originalsicherung oder auf die Arbeitskopie), um dort nach weiteren Straftaten zu suchen, wird auf Gesetzesebene mehrfach begegnet, nämlich durch die gesetzliche Festlegung, dass auf die Originalsicherung und die Arbeitskopie nur bei einer (erneuten) gerichtlichen Entscheidung zugegriffen werden kann, sowie durch den (optionalen) Einsatz von Suchparametern in der Phase der Auswertung. Diese gesetzlichen und organisatorischen Vorkehrungen erlauben die Entdeckung von Zufallsfunden und damit letztlich die Verarbeitung von Daten, jedoch nur im eigentlichen – richterlich genehmigten – Datenausmaß.

Vergleichbar den Fällen der § 135 Abs. 1, Abs. 2 Z 2, 3 und 4, Abs. 2a, Abs. 3 Z 2 bis 4 und § 135a darf das Ergebnis der Datenaufbereitung nur zum Nachweis einer vorsätzlich begangenen strafbaren Handlung, derentwegen die Ermittlungsmaßnahme angeordnet wurde oder hätte angeordnet werden können, erfolgen (§ 140 Abs 1 Z 4 StPO).

Zur Verwahrung von Datenträgern und Daten (§ 115k StPO):

In Bezug auf die Originalsicherung werden auf gesetzlicher Ebene mehrere Vorkehrungen getroffen: Zum einen wird die Datenintegrität durch den technisch gewonnenen Hash-Wert gesichert. Zum anderen normiert **§ 115k StPO**, dass das Gericht dafür zu sorgen hat, dass die Originalsicherung sowie die Arbeitskopie auf geeignete Art und Weise gegen unbefugte Einsichtnahme oder Veränderung gesichert und bis zur rechtskräftigen Beendigung des Strafverfahrens aufbewahrt wird. Daneben wird normiert, dass auf die Originalsicherung ausschließlich im Fall des § 115f Abs. 6 StPO (somit bei Vorliegen einer neuerlichen gerichtlich bewilligten Anordnung) und des § 115h Abs 4 zugegriffen werden kann (was von dem bzw. der Rechtsschutzbeauftragten gemäß § 115l StPO auch kontrolliert werden kann; ihm bzw. ihr ist diesbezüglich Einblick in alle der Dokumentation dienenden Unterlagen und Zutritt zu allen Räumlichkeiten zu gewähren, überdies sind ihm bzw. ihr gegenüber alle erforderlichen Auskünfte zu erteilen). In diesem Fall ist daher neuerlich eine Arbeitskopie auf Grundlage der Originalsicherung herzustellen. Nur in diesem Fall ist ein Zugriff auf die Originalsicherung zulässig. Nach Maßgabe der (neuen) gerichtlichen Bewilligung ist die Aufbereitung von Daten vorzunehmen; nach Abschluss der Arbeiten ist die Arbeitskopie neuerlich gesichert aufzubewahren und ein Aufbereitungsbericht zu

erstellen. Eine solche Vernichtungsverpflichtung greift – mangels Erforderlichkeit der weiteren Verarbeitung in Form der Speicherung (§ 74 Abs. 1 StPO) – insbesondere, aber nicht nur für bereits rechtskräftig abgeschlossene Strafverfahren, Für die Verwahrung von Datenträgern, sofern sie nicht zurückgestellt werden können, ist das Gericht zuständig- Ergebnisse der Datenaufbereitung (§ 109 Z 2e StPO) hat bis zur Berichterstattung über die Auswertung der Daten (§ 115i StPO) die Kriminalpolizei, danach die Staatsanwaltschaft zu verwahren. Soweit dies aus rechtlichen oder tatsächlichen Gründen erforderlich ist, soll die Staatsanwaltschaft anordnen können, dass deren Verwahrung auch danach durch die Kriminalpolizei erfolgt.

Zum Rechtsschutz (§ 47a Abs. 4a und 7, § 115l StPO):

§ 115l StPO soll – im Gefüge der vorgeschlagenen Sonderbestimmungen – den vom VfGH genannten Gesichtspunkt der unabhängigen Aufsicht in einer eigenen Bestimmung umsetzen. Damit sollen die Befugnisse der bzw. des Rechtsschutzbeauftragten der Justiz ausgebaut werden, um an ihre bzw. seine langjährige und bewährte Tätigkeit in der Strafrechtspflege anzuknüpfen. Die unabhängige Aufsicht soll im Sinne des Erkenntnisses G 352/2021 des VfGH sicherstellen, dass diese *„überprüft, ob sich die Strafverfolgungsorgane bei der Auswertung der auf dem Datenträger gespeicherten Daten im Rahmen der gerichtlichen Bewilligung und gesetzlichen Vorgehensregeln bewegt haben sowie ob die Rechte der Betroffenen auf Schutz der Privatsphäre und Geheimhaltungsinteressen in verhältnismäßiger Weise im Prozess der Auswertung bzw. Verarbeitung der sichergestellten Datenträger gewahrt worden sind“* (vgl. Rn. 102).

Für den vorgeschlagenen Rechtsschutz durch den Rechtsschutzbeauftragten bzw. die Rechtsschutzbeauftragte der Justiz sind daher nicht nur Informations-, Auskunfts- und Akteneinsichtsrechte vorgesehen, sondern – zur Gewährleistung einer *„effektiven Maßnahme“* – auch (§ 91b Abs. 3 SPG nachgebildet) die Zurverfügungstellung der zu seiner bzw. ihrer Tätigkeit notwendigen Sach- und Personalressourcen. Der bzw. die Rechtsschutzbeauftragte benötigt zur wirkungsorientierten Aufgabenbewältigung, insb. zur Abwicklung der administrativen Tätigkeiten, personelle Unterstützung und eine angemessene Sachmittel- und Raumausstattung. Das Bundesministerium für Justiz hat ihm bzw. ihr daher einen Hilfsapparat aus den dem Bundesministerium für Justiz zur Verfügung stehenden Ressourcen beizugeben. Zur effektiven Ausgestaltung muss die Ausstattung auf Dauer so angelegt sein, dass Gewähr dafür gegeben ist, die vorgesehenen Aufgaben effektiv besorgen zu können (vgl. *Lienbacher*, BMI 107). Erforderlichenfalls sind die Personal- und Sachressourcen anzupassen. Abgesehen von der rechtlichen und politischen Verantwortung des Bundesministers bzw. der Bundesministerin für Justiz kann der bzw. die Rechtsschutzbeauftragte im Falle einer abweichenden Auffassung über den erforderlichen Umfang der Zurverfügungstellung eine Klage nach Art. 137 B-VG, die mit einer Feststellungsklage nach § 38 VfGG verbunden werden kann, beim VfGH einbringen (vgl. *Vogl*, Rechtsschutzbeauftragte 73 und zu den Ausführungen insgesamt *Thanner/Vogl*, SPG² § 91b Anm. 10).

Die Unabhängigkeit des bzw. der Rechtsschutzbeauftragten soll insbesondere auch dadurch sichergestellt werden, dass zur Erfüllung seiner bzw. ihrer Aufgaben nach § 23 Abs. 1a, § 115l, § 147, § 195 Abs. 2a und § 209b Abs. 6 StPO ausschließlich Personen bei ihr bzw. ihm tätig sind, die nicht auch für ein Gericht oder eine Staatsanwaltschaft tätig sind (somit keine Doppel- oder Mehrfachverwendungen von Richtern bzw. Richterinnen, oder Staatsanwälten bzw. Staatsanwältinnen oder Experten bzw. Expertinnen iSd § 2 Abs. 5a JBA-G). Neben juristischen Mitarbeiterinnen und Mitarbeitern wird dabei auch an technische Expertinnen bzw. Experten zu denken sein, die ihn bzw. sie etwa bei der Kontrolle unterstützen können, ob die Aufbereitung von Daten oder die Auswertung von Daten hinsichtlich eines Zeitraumes der gerichtlichen Entscheidung tatsächlich entspricht (**§ 47a Abs. 4a StPO**). Auch weiterhin sollen Zustellungen an den Rechtsschutzbeauftragten bzw. die Rechtsschutzbeauftragte im Wege der Geschäftsstelle des Obersten Gerichtshofes vorzunehmen sein; diese hat auch weiterhin die Kanzleigeschäfte des Rechtsschutzbeauftragten wahrzunehmen (§ 47a Abs. 5 StPO).

Der Jahresbericht des bzw. der Rechtsschutzbeauftragten über seine bzw. ihre Tätigkeit und Wahrnehmungen im Rahmen seiner bzw. ihrer Aufgabenerfüllung soll künftig auch die neue Ermittlungsmaßnahme umfassen (**§ 47a Abs. 7 StPO**).

Die inhaltliche Tätigkeit des bzw. der Rechtsschutzbeauftragten orientiert sich insbesondere an den bereits bestehenden, in gewissen Bereichen vergleichbaren Bestimmungen des § 147 StPO mit ergänzenden Anleihen an § 91c SPG und §§ 14 f. SNG.

§ 115l Abs. 1 StPO soll Anregungen aus dem Begutachtungsverfahren aufgreifend, zuerst die allgemeine, umfassende Kompetenz des bzw. der Rechtsschutzbeauftragten in allen Fällen einer Antragstellung nach § 115f StPO und im Anschluss in Bezug auf das besondere Ermächtigungsregime iZm Berufsgeheimnisträgern regeln. In Fällen einer Antragstellung nach § 115f StPO soll die

Staatsanwaltschaft daher den Rechtsschutzbeauftragten bzw. die Rechtsschutzbeauftragte unter Anschluss einer Ausfertigung des Antrages und der Bewilligung ehestmöglich zu informieren haben. Die Bestimmung orientiert sich an § 91c Abs. 1 SPG und § 14 Abs. 2 SNG, jedoch ohne die dort jeweils vorgesehene Pflicht zur Prüfung, weil im Gegensatz zu SPG und SNG bei der Beschlagnahme von Datenträgern und Daten, die zudem eine offene Ermittlungsmaßnahme darstellt, eine gerichtliche Bewilligung erforderlich ist, somit die Funktion des bzw. der Rechtsschutzbeauftragten eine andere als in den beiden anderen Materiengesetzen ist, bei denen keine gerichtliche Kontrolle zu diesem Zeitpunkt vorgesehen ist. Ein Tätigwerden des bzw. der Rechtsschutzbeauftragten in jedem Fall würde zudem aufgrund der Anzahl der Anwendungsfälle seine bzw. ihre Kapazitäten überlasten. Sehr wohl jedoch soll er bzw. sie auf diese Weise in die Lage versetzt werden, amtswegig tätig zu werden und unabhängige Kontrolle ausüben zu können. unter Anschluss einer Ausfertigung des Antrages und der Bewilligung ehestmöglich zu informieren haben. Die Bestimmung orientiert sich an § 91c Abs. 1 SPG und § 14 Abs. 2 SNG, jedoch ohne die dort jeweils vorgesehene Pflicht zur Prüfung, weil im Gegensatz zu SPG und SNG bei der Beschlagnahme von Datenträgern und Daten, die zudem eine offene Ermittlungsmaßnahme darstellt, eine gerichtliche Bewilligung erforderlich ist, somit die Funktion des bzw. der Rechtsschutzbeauftragten eine andere als in den beiden anderen Materiengesetzen ist, bei denen keine gerichtliche Kontrolle zu diesem Zeitpunkt vorgesehen ist. Ein Tätigwerden des bzw. der Rechtsschutzbeauftragten in jedem Fall würde zudem aufgrund der Anzahl der Anwendungsfälle seine bzw. ihre Kapazitäten überlasten. Sehr wohl jedoch soll er bzw. sie auf diese Weise in die Lage versetzt werden, amtswegig tätig zu werden und unabhängige Kontrolle ausüben zu können.

Ist jedoch eine Beschlagnahme von Datenträgern und Daten gegen eine Person gerichtet, die gemäß § 157 Abs. 1 Z 2 bis 4 StPO berechtigt ist, die Aussage zu verweigern, ist eine Ermächtigung des Rechtsschutzbeauftragten erforderlich. Die Bestimmung entspricht daher im Wesentlichen § 147 Abs. 2 und Abs. 3 StPO. Einer Anregung der österreichischen Bischofskonferenz und der Evangelischen Kirche in Österreich folgend soll dieses Erfordernis zum Schutz der geistlichen Amtsverschwiegenheit auch gelten, wenn eine Beschlagnahme von Datenträgern und Daten gegen eine Person gerichtet ist, deren Vernehmung als Zeuge bzw. Zeugin nach § 155 Abs. 1 Z 1 verboten ist.

Das muss aufgrund des Geheimhaltungsinteresses (§ 112a Abs 1 Z 1) und der Notwendigkeit einer Zustimmung einer ausländischen Sicherheitsbehörde oder Sicherheitsorganisation (§ 112a Abs 1 Z 2 StPO) sinngemäß gelten, wenn die Ermittlungsmaßnahme bei einer Behörde oder öffentlichen Dienststelle (§ 112a) durchgeführt werden soll

Die Prüfung des bzw. der Rechtsschutzbeauftragten nach **§ 115i Abs. 2 StPO** umfasst daher sowohl eine Rechtmäßigkeitskontrolle – zB die Frage, ob die geplante Ermittlung zu den angeführten Zwecken überhaupt zulässig ist – wie auch eine Ermessenskontrolle, zB hinsichtlich der Einschätzung der Verhältnismäßigkeit der Maßnahme in Hinblick auf die Dringlichkeit des Tatverdachts usw. Sollte nach seiner bzw. ihrer eine Eingriffsvoraussetzung nach der Beurteilung des Rechtsschutzbeauftragten fehlen, so hat er bzw. sie das Recht (aber auch die Pflicht), gegen die Bewilligung dieser Ermittlungsmaßnahme Beschwerde an das Oberlandesgericht (vgl. in Bezug auch die vergleichbare Bestimmung des § 147 StPO: *Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO § 147 Rz 4) und gegen deren Anordnung (vgl. zur Kritik an § 147 Abs. 3 StPO: ebenda Rz 6) Einspruch zu erheben. Dieses Recht erlischt mit dem Ablauf der Rechtsmittelfrist des bzw. der Beschuldigten.

§ 115i Abs. 2 und 3 StPO sehen – angelehnt an § 147 Abs. 3a StPO (vgl. auch § 15 Abs. 1 und 2 SNG) – vor, dass dem bzw. der Rechtsschutzbeauftragten jederzeit Gelegenheit zu geben ist, die Aufbereitung von Daten (§ 115h StPO) und die Auswertung von Daten (§ 115i StPO) zu überwachen und alle Räume zu betreten, in denen Originalsicherungen und Arbeitskopien, Datenträger und Ergebnisse der Datenaufbereitung aufbewahrt und die Aufbereitung von Daten vorgenommen wird; zu diesem Zweck stehen dem bzw. der Rechtsschutzbeauftragten auch Auskunfts- und Einsichtsrechte nach Abs. 3 zu, eine Amtsverschwiegenheit kann ihm gegenüber – auch durch Bedienstete des Bundesministeriums für Inneres und des Bundesministeriums für Finanzen – nicht geltend gemacht werden. Der bzw. die Rechtsschutzbeauftragte hat insbesondere darauf zu achten, dass bei der Aufbereitung von Daten (§ 115h StPO) und der Auswertung von Daten (§ 115i StPO) die Anordnung und die gerichtliche Bewilligung nicht überschritten werden.

Der Staatsanwaltschaft soll die Möglichkeit einer amtswegigen, zu begründenden Anregung eingeräumt werden, damit sie als Leiterin des Ermittlungsverfahrens nicht als Antragsteller aufzutreten hat (vgl. EBRV 25 BlgNR 22. GP 58 zu einer ähnlichen Konstellation in § 39 Abs. 3 StPO). Dies wird vor allem in clamorösen Fällen sowie in Verfahren gegen Berufsheimnisträger bzw. Berufsheimnisträgerinnen zweckmäßig sein, um Zweifel an der Rechtmäßigkeit des Vorgehens der Strafverfolgungsbehörden in allen Phasen der Durchführung dieser Ermittlungsmaßnahme bereits von Anfang durch eine effektive Kontrolle durch den Rechtsschutzbeauftragten bzw. die Rechtsschutzbeauftragte hintanhalten zu können.

Um die Rechtsposition und die Beteiligungsrechte der Verfahrensbeteiligten (weiter) zu stärken, soll ein entsprechendes Recht auf Anregung auf eine solche Prüfung neben der Staatsanwaltschaft auch dem bzw. der Beschuldigten und dem Opfer (§ 55 StPO) eingeräumt werden. Dies wird insbesondere eine Rolle spielen, wenn bei einem bzw. einer Verfahrensbeteiligten Zweifel an der Integrität der Daten, der Korrektheit des Umfangs des Ergebnisses der Datenaufbereitung oder einer den Vorgaben der gerichtlichen Bewilligung entsprechenden Auswertung der Daten vorliegt. Bedenken aus dem Begutachtungsverfahren aufgreifend, wonach das ursprünglich konzipierte ‚Antragsrecht‘ dem bisherigen System des Rechtsschutzbeauftragten zuwidergelaufen wäre (u.a. weil der Rechtsschutzbeauftragte nicht als Entscheidungsorgan konzipiert sei und unklare Konsequenzen bei Nichtentsprechung des Antrags bestünden), soll Beschuldigten und Opfern (lediglich) ein Anregungsrecht zustehen. Als Ausgleich dafür soll der bzw. die Rechtsschutzbeauftragte jedoch jedenfalls mitzuteilen haben, ob er bzw. sie einer solchen Anregung nachkommt; diese Mitteilung hat eine Begründung zu enthalten (s. dazu die Stellungnahme des Rechtsschutzbeauftragten der Justiz im Begutachtungsverfahren).

Die Prüfung des bzw. der Rechtsschutzbeauftragten nach § 115I Abs. 4 StPO umfasst daher sowohl eine Rechtmäßigkeitskontrolle – zB die Frage, ob die geplante Ermittlung zu den angeführten Zwecken überhaupt zulässig ist – wie auch eine Ermessenskontrolle, zB hinsichtlich der Einschätzung der Verhältnismäßigkeit der Maßnahme in Hinblick auf die Dringlichkeit des Tatverdachts usw. Sollte nach seiner bzw. ihrer eine Eingriffsvoraussetzung nach der Beurteilung des Rechtsschutzbeauftragten fehlen, so hat er bzw. sie das Recht (aber auch die Pflicht), gegen die Bewilligung dieser Ermittlungsmaßnahme Beschwerde an das Oberlandesgericht (vgl. in Bezug auch die vergleichbare Bestimmung des § 147 StPO: Reindl-Krauskopf in Fuchs/Ratz, WK StPO § 147 Rz 4) und Einspruch wegen Rechtsverletzung (§ 106 StPO) gegen deren Anordnung und Durchführung (vgl. ebenda Rz 6) zu erheben. Dieses Recht erlischt mit dem Ablauf der Rechtsmittelfrist bzw. Frist zur Erhebung des Rechtsbehelfs durch die bzw. den Beschuldigten.

§ 115I Abs. 5 StPO ist § 147 Abs. 4 StPO nachgebildet (vgl. auch § 5 Abs. 2 SNG), sodass auf die einschlägige Kommentierung verwiesen werden kann.

Zur Gewährleistung, dass der bzw. die Rechtsschutzbeauftragte die Kontrolltätigkeit tatsächlich umfänglich ausüben kann, soll auch ausdrücklich verankert werden, dass er bzw. sie diese auch nach Beendigung der Ermittlungsmaßnahme vornehmen kann und sich insbesondere auch nach Beendigung des Strafverfahrens von der ordnungsgemäßen Löschung sowohl der Originalsicherung, der Arbeitskopie als auch der Ergebnisse der Datenaufbereitung vergewissern kann (**§ 115I Abs. 6 StPO**). Diese Maßnahme stellt eine weitere Schutzmaßnahme (ergänzend – soweit hier relevant – speziell zu den Regelungen der besonderen Verwahrung der Originalsicherung und der Arbeitskopie) zu den der von der Ermittlungsmaßnahme Betroffenen dar, dass die Daten nicht weiterverwendet werden können: die verfahrensrelevanten Daten sind ohnedies zum Akt zu nehmen, der Rest soll jedoch mit Ende des Strafverfahrens nachweislich gelöscht werden.

Zu Z 58 (§ 157 Abs. 2 StPO):

Da die vorgeschlagene Ermittlungsmaßnahme nach §§ 115f ff. StPO die Bezeichnung ‚Beschlagnahme von Datenträgern und Daten‘ tragen soll, ist eine terminologische Anpassung in § 157 Abs. 2 StPO erforderlich.

Zu Z 72 (§ 367 bis § 369 StPO):

Zu § 367 und § 368 StPO:

§ 367 Abs. 1 StPO regelt in seiner geltenden Fassung zwei Fälle, nämlich einerseits den Fall der Ausfolgung von beschlagnahmten Gegenständen des (mutmaßlichen) Opfers an dieses nach Rechtskraft des Urteils und als Sonderfall die Ausfolgung vor Rechtskraft des Urteils mit Zustimmung des Beschuldigten; Abs. 2 leg. cit. hingegen umfasst die Ausfolgung nach Rechtskraft anhand der Kriterien des § 367 Abs. 2 Z 1 und Z 2 StPO. Auch bei der Ausfolgung von Gegenständen mit Zustimmung des Angeklagten (Sonderfall in Abs. 1) sind aber ebenfalls die Kriterien nach Abs. 2 relevant: So ist etwa eine Ausfolgung mit Zustimmung des Angeklagten auch dann nicht möglich, wenn der Gegenstand noch als Beweismittel nach Abs. 2 Z 1 StPO erforderlich ist (*Spenling in Fuchs/Ratz, WK StPO § 367 Rz 17*).

Wie bereits bei der Sicherstellung soll sich auch die Rückstellung an Opfer künftig sowohl auf Gegenstände als auch auf Vermögenswerte erstrecken. Zur besseren Verständlichkeit wird zudem vorgeschlagen, **§ 367 StPO** in zwei verschiedene Phasen zu teilen und in **Abs. 1** nur mehr den Fall der Ausfolgung nach Rechtskraft und **Abs. 2** nur den Fall der Ausfolgung vor Rechtskraft des Urteils zu regeln. Dem Opfer soll diesbezüglich auch weiterhin (vgl. aaO) ein Antragsrecht zukommen, die Ausfolgung aber auch von Amts wegen eingeleitet werden können. Wie bisher sind vor der Ausfolgung vor Rechtskraft die übrigen Beteiligten (vgl. § 210 Abs. 2 StPO) zu hören, wobei die Zustimmung des

Beschuldigten auch weiterhin im Rahmen der Anhörung eingeholt werden kann (vgl. derzeit § 367 Abs. 1 zweiter Satz StPO).

Kritik im Rahmen des Begutachtungsverfahrens aufgreifend, wonach infolge des Anhörungsrechts des Beschuldigten eine Aushändigung von Vermögenswerten in solchen Fällen nicht möglich sei, in denen die Täterinnen bzw. Täter langfristig nicht ausgeforscht werden können und dies in der Praxis oft zu unbefriedigenden Situationen führe, in denen trotz eindeutiger Zuordenbarkeit trotzdem keine Opferrestitution erfolgen könne, soll durch Aufnahme der an § 111 Abs. 4 StPO angelegten Wendung ‚soweit möglich‘ in § 367 Abs. 2 StPO klargestellt werden, dass sich das Anhörungsrecht nur auf bekannte und tatsächlich ausgeforschte Täterinnen bzw. Täter bezieht. Bei durchwegs unbekannten Täterinnen bzw. Tätern kann schließlich auch die Informationspflicht über eine erfolgte Sicherstellung (§ 111 Abs. 4 erster Satz StPO) nicht effektuert werden. Konsequenterweise soll auch ein Anhörungsrecht vor einer Rückstellung des Gegenstands oder Vermögenswerts an das Opfer die Rückstellung nicht auf unbestimmte Zeit blockieren können.

Im Falle der Rückstellung an das Opfer soll - im Einklang mit Art. 18 Abs. 4 der Richtlinie 2024/1260/EU (‚Hat ein Opfer Anspruch auf die Rückgabe von Vermögensgegenständen, die Gegenstand einer Einziehungsmaßnahme nach dieser Richtlinie sind oder werden könnten, so treffen die Mitgliedstaaten die erforderlichen Maßnahmen, um die betreffenden Vermögensgegenstände unter den in Artikel 15 der Richtlinie 2012/29/EU genannten Bedingungen an das Opfer zurückzugeben.‘) und unter Beachtung des dort genannten Art. 15 der RL 2012/29/EU (‚Die Mitgliedstaaten stellen sicher, dass die im Rahmen des Strafverfahrens beschlagnahmten Vermögenswerte, die für eine Rückgabe in Frage kommen, den Opfern aufgrund einer entsprechenden Entscheidung einer zuständigen Behörde unverzüglich zurückgegeben werden, es sei denn, die Vermögenswerte werden zum Zwecke des Strafverfahrens benötigt. Die Bedingungen oder Verfahrensvorschriften, nach denen die betreffenden Vermögenswerte den Opfern zurückgegeben werden, richten sich nach dem einzelstaatlichen Recht.‘) von einer Anhörung abgesehen werden können, wenn eine solche nicht möglich ist.

Die Beurteilung, wann eine Anhörung im Rahmen der Möglichkeiten ist, kann freilich nur im Einzelfall und anhand der individuellen Gegebenheiten beurteilt werden. Orientierung bieten die zu § 111 Abs. 4 StPO ergangene Judikatur und vergleichbare Fälle nach dem Maßstab des ‚besonderen Verfahrensaufwands‘ in § 133 Abs. 3 und § 139 Abs. 2 StPO hinsichtlich der dort normierten Ausforschungspflicht Betroffener, dem Äußerungsrecht in § 292 StPO oder dem Anhörungsrecht von Haftungsbeteiligten im vereinfachten selbstständigen Verfahren gemäß § 445a Abs. 1 StPO.

Die Zuständigkeit für die Entscheidung (§ 367 Abs. 2 StPO) soll unverändert im Ermittlungsverfahren der Staatsanwaltschaft und im Hauptverfahren dem erkennenden Gericht zukommen. Wird außerhalb der Hauptverhandlung über die Ausfolgung entschieden, soll klargestellt werden, dass die Entscheidung vom Vorsitzenden zu treffen ist.

Die Gründe, aus denen von einer Rückstellung eines Gegenstands oder Vermögenswerts abzusehen ist, sollen sprachlich präziser gefasst werden: Die Formulierung des **Abs. 2 Z 1** ist an § 115 Abs. 1 Z 1 StPO angelehnt. Der bislang kasuistisch formulierte **Abs. 2 Z 2 StPO** soll verschlankt und nur mehr auf ‚sonstige Umständen (§ 368)‘, die der Ausfolgung entgegenstehen, Bezug nehmen (s. dazu im Folgenden). Umfasst sollen davon jene Fälle sein, in denen das Opfer sein Recht an dem Gegenstand oder Vermögenswert nicht nachweisen kann, bestimmte Anhaltspunkte für dingliche Rechte Dritter daran vorliegen oder das Recht daran zwischen mehreren Opfern strittig ist.

Es wird überdies vorgeschlagen, die sich derzeit beim Vorgehen zur Abweisung eines Ausfolgungsantrags aus dem Grund des § 367 Abs. 2 Z 2 StPO überschneidenden Bestimmungen in § 367 Abs. 3 und in § 368 StPO zusammenzuziehen und § 367 Abs. 3 in einem neu gefassten § 368 StPO aufgehen zu lassen, der bisher ebenso das Vorgehen im Falle der Abweisung des Ausfolgungsantrags aus dem Grund des § 367 Abs. 2 Z 2 StPO regelte. Es soll dabei nicht verhehlt werden, dass damit in gewisser Weise eine Annäherung an die Systematik der Strafprozeßordnung 1873 hergestellt wird (§ 367 StPO bestand damals nur aus zwei Absätzen, § 368 StPO hat sich seitdem kaum verändert, sodass eine sprachliche Neugestaltung bereits aus diesem Grund naheliegt).

Zu Z 31 (§ 101 Abs 3 StPO), Z 32 (§ 102 Abs 3 StPO) und Z 33 (§ 105 Abs 3 StPO):

§ 38 Abs. 1 erster Satz GOG sieht vor, dass bei jedem für Strafsachen zuständigen Gerichtshof erster Instanz außerhalb der gerichtlichen Dienststunden jeweils ein Richter bzw. eine Richterin Rufbereitschaft zu leisten hat. Die Zuständigkeit des Rufbereitschaftsrichters bzw. der Rufbereitschaftsrichterin ist in erster Linie für außerhalb der gerichtlichen Dienststunden in Strafsachen anfallende unaufschiebbare und dringende Amtshandlungen gegeben (*Fellner/Nogratnig*, RStDG, GOG und StAG^{II5-02} § 38 GOG Rz 12). Die Rechtsprechung fordert dahingehend von der Staatsanwaltschaft, die Annahme einer solchen Dringlichkeit (samt Begründung) im Ermittlungsakt zu dokumentieren, widrigenfalls eine Entscheidung

durch den Rufbereitschaftsrichter bzw. die Rufbereitschaftsrichterin einen Verstoß gegen die Zuständigkeitsregeln der Geschäftsverteilung (Art. 87 Abs. 3 B-VG) darstellen kann (vgl. OLG Wien vom 3. Juli 2023, 31 Bs 113/23a und 31 Bs 114/23a). Im Fall einer gerichtlichen Bewilligung der beantragten Ermittlungsmaßnahme durch den Rufbereitschaftsrichter bzw. die Rufbereitschaftsrichterin erfolgt gleichermaßen eine (implizite) Feststellung der von der Staatsanwaltschaft getroffenen und dokumentierten Dringlichkeitsannahme sowie ihrer zugrundeliegenden Begründung. Hält der Rufbereitschaftsrichter bzw. die Rufbereitschaftsrichterin die Dringlichkeit nämlich nicht für gegeben, liegt solcherart auch keine Journaldringlichkeit vor, sodass die Entscheidung dem zuständigen Richter bzw. der zuständigen Richterin vorbehalten bleibt.

Zur Untermauerung dieser Dringlichkeitsannahme soll in § 102 Abs. 3 StPO die Anordnung der Staatsanwaltschaft an die Kriminalpolizei zur Durchführung einer vom Rufbereitschaftsrichter bzw. der Rufbereitschaftsrichterin bewilligten Zwangsmaßnahme mit dem Ablauf des auf die erfolgte Bewilligung folgenden übernächsten Werktages befristet werden. Sollte innerhalb dieser Frist keine Anordnung der Staatsanwaltschaft an die Kriminalpolizei erfolgen, tritt die erteilte Bewilligung außer Kraft. Im Fall einer fristgerechten Anordnung hat die Durchführung iSd eigentlichen kriminalpolizeilichen Vornahme der Zwangsmaßnahme wie auch bisher innerhalb der vom Gericht gesetzten Befristung zu erfolgen (vgl. dazu OLG Wien 21 Bs 32/22t).

Grundvoraussetzung für einen Übergang der Zuständigkeit zufolge Rufbereitschaft und Journaldienst ist schon zur gebotenen Verhinderung willkürlicher Auswahl des ‚zuständigen‘ Richters durch den Antragsteller die objektive und akute Dringlichkeit der anstehenden Amtshandlung, ohne die diese Form der ‚Notvertretung‘ bzw. der Abnahme nicht wirksam werden kann (Art. 87 Abs. 3 B-VG). Tätigwerden des durch die Geschäftsverteilung eingeteilten Rufbereitschafts- oder Journalrichters ohne entsprechenden Vertretungsfall begründet eine nicht gehörige Gerichtsbesetzung (vgl. *Fellner/Nogratnig*, RStDG, GOG und StAG II5.03 § 38 Rz 3/1 f. GOG (Stand 1.3.2024, rdb.at)).

Besteht innerhalb der zulässigen Inanspruchnahme der Rufbereitschaft iHa die beabsichtigte Durchführung einer Zwangsmaßnahme eine weitere (zusätzliche) Dringlichkeitsannahme, die es aus zeitlichen Gründen unabdingbar macht, dass der Kontakt zwischen der antragstellenden Staatsanwaltschaft und dem Rufbereitschaftsrichter bzw. der Rufbereitschaftsrichterin nicht schriftlich, sondern nur fernmündlich erfolgt, fehlt es derzeit zum Zweck hinreichender Nachvollziehbarkeit am Erfordernis einer entsprechenden Dokumentations- bzw. Begründungspflicht.

Eben jene bloß fernmündliche Kommunikation zwischen Staatsanwaltschaft und Gericht in Rufbereitschaft wurde seitens der Politik schon in der Vergangenheit als Problemfeld identifiziert: So trat der ehemalige Minister für Verfassung, Reformen, Deregulierung und Justiz Dr. Josef Moser bereits 2018 dafür ein, dass zwischen Staatsanwaltschaft und Rufbereitschaftsrichter bzw. Rufbereitschaftsrichterin außer bei absoluter Notwendigkeit nur mehr schriftlich und nicht mehr fernmündlich kommuniziert werden dürfe (Bericht des BVT-Untersuchungsausschusses 695 BlgNR XXVI. GP 181 mwN). Eine Empfehlung des BVT-Untersuchungsausschusses lautet dahingehend, sicherzustellen, dass die richterliche Entscheidung auf Basis ausreichender Informationsgrundlagen getroffen werden kann und die erforderliche Zeit für die Entscheidungsfindung zur Verfügung steht (aaO 288).

Durch die vorgeschlagene Regelung soll die Nachvollziehbarkeit des geforderten Vorliegens der für eine gerichtliche Entscheidung erforderlichen Informationsgrundlagen sichergestellt werden. Wie auch die Staatsanwaltschaft eine mündliche Vorausberichterstattung durch die Kriminalpolizei – ungeachtet der schriftlichen Nachreichung eines Anlassberichtes oder einer Dokumentation im nächstfolgenden Bericht – oder die vorläufige mündliche Übermittlung einer Anordnung oder Genehmigung an die Kriminalpolizei (§ 102 Abs. 1) in einem Amtsvermerk festzuhalten hat (*Vogl in Fuchs/Ratz*, WK StPO § 95 Rz 4), soll auch das Gericht den wesentlichen Inhalt des (mündlichen) Vorbringens der Staatsanwaltschaft samt den Gründen für die mündliche (Vorab-)Bewilligung einer Zwangsmaßnahme in einem Amtsvermerk festzuhalten haben. Die (schriftliche) Dokumentation dieser für das Verfahren bedeutsamen Vorgänge sichert nicht nur eine umfassende Nachvollziehbarkeit und Transparenz im (Ermittlungs-)Verfahren, sondern gewährleistet auch einen einheitlichen Wissenstand aller am Verfahren Beteiligten. Der Aktenvermerk ist dem Ermittlungsakt anzuschließen.

Zu Z 62 und Z 63 (§ 195 Abs. 2 StPO):

Mit dem Budgetbegleitgesetz 2009, BGBl. I Nr. 52/2009, wurde die Entscheidungskompetenz über Fortführungsanträge von den bis zu diesem Zeitpunkt dafür zuständigen Oberlandesgerichten auf die Landesgerichte übertragen. Gleichzeitig wurden die gerichtliche Überprüfungsmöglichkeit der Einstellungsentscheidung der Staatsanwaltschaft eingeschränkt und in § 195 Abs. 2 StPO formale Anforderungen an einen Fortführungsantrag festgelegt, bei deren Nichteinhaltung der Antrag gemäß § 196 Abs. 2 StPO zurückzuweisen ist.

§ 195 Abs. 2 dritter Satz StPO legt fest, dass der Antrag das Verfahren, dessen Fortführung begehrt wird, zu bezeichnen und die zur Beurteilung seiner fristgemäßen Einbringung notwendigen Angaben zu enthalten hat. Darunter ist insbesondere das Datum der Zustellung einer gemäß § 194 StPO erfolgten Verständigung (oder erweiterter Einstellungsbegründung) zu verstehen (*Nordmeyer in Fuchs/Ratz, WK StPO § 195 Rz 27*). Gemäß § 196 Abs. 2 erster Satz StPO hat das Gericht Anträge, die verspätet oder nicht von einer berechtigten Person eingebracht wurden, bereits rechtskräftig erledigt sind oder den Voraussetzungen des § 195 nicht entsprechen, als unzulässig zurückzuweisen und im Übrigen in der Sache zu entscheiden. Die Wendung ‚den Voraussetzungen des § 195 nicht entsprechen‘ wurde von Lehre und Rechtsprechung stets dahingehend verstanden, dass sie auch Angaben zur formalen Zulässigkeit, insbesondere zur fristgemäßen Einbringung, umfasst (*Nordmeyer in Fuchs/Ratz, WK StPO § 195 Rz 27* und § 196 Rz 4/1; *Tauschmann in Schmölzer/Mühlbacher, StPO² § 196 Rz 5*; *Hinterhofer/Oshidari, Strafverfahren Rz 7.1119*; *Steiner in Birklbauer/Haumer/Nimmervoll/Wess (Hrsg), stopp – Linzer Kommentar zur Strafprozessordnung (2020) zu § 195 Rz 59*). In seiner Entscheidung 11 Os 29/21f hat der OGH ausgesprochen, dass Anträge, die den – auch die genannten Angaben zur formalen Zulässigkeit umfassenden – Voraussetzungen des § 195 StPO nicht entsprechen, gemäß § 196 Abs. 2 erster Satz StPO sogar dann zurückzuweisen sind, wenn sie rechtzeitig eingebracht wurden. Demnach sei die (von *Nordmeyer in Fuchs/Ratz, WK StPO § 195 Rz 27*) in diesem Zusammenhang erwähnte, zu Gunsten des bzw. der Beschuldigten entwickelte Rechtsprechung zur – § 195 Abs. 2 dritter Satz StPO ähnlichen – Bestimmung des § 3 Abs. 1 letzter Satz GRBG (wonach die Unterlassung der Anführung des Tages, der für den Beginn der Beschwerdefrist maßgeblich ist, nicht zur Zurückweisung der Grundrechtsbeschwerde führt, wenn sich deren Rechtzeitigkeit aus den Akten ergibt [RIS-Justiz RS0114092]), auf das in §§ 195 f. StPO geregelte (gegen den Beschuldigten bzw. die Beschuldigte gerichtete) ‚Fortführungsrecht‘ nicht übertragbar, weil § 196 Abs. 2 erster Satz stopp – im Unterschied zum GRBG – die Zurückweisung des Fortführungsantrags für den Fall unterbliebener Angaben zur Rechtzeitigkeit ausdrücklich anordne (arg: ‚...hat das Gericht als unzulässig zurückzuweisen...‘; dazu auch Gw 14/17t = JSt-GP 2017/3, 253; *Steiner in Birklbauer/Haumer/Nimmervoll/Wess (Hrsg), stopp – Linzer Kommentar zur Strafprozessordnung (2020) § 195 Rz 59* [insb. FN 135]).

Demgegenüber hat der OGH in seiner jüngeren Entscheidung zu 12 Os 15/22f (12 Os 16/22b) gegenteilig entschieden und eine auf die vorstehende Argumentation gestützte Beschwerde der Generalprokuratur nach § 23 StPO mit dem Hinweis verworfen, dass ein Fortführungsantrag zwar nach § 195 Abs. 2 dritter Satz StPO die zur Beurteilung der fristgerechten Einbringung notwendigen Angaben enthalten müsse; wenn die Einhaltung der Fristen des § 195 Abs. 2 erster Satz StPO schon anhand der Aktenlage bestimmt werden könne, seien jedoch weitere Angaben dazu nicht ‚notwendig‘ und daher kein (unabdingbares) inhaltliches Zulässigkeitskriterium.

Zur Klarstellung (der 12. Senat hat die Entscheidung des 11. Senats lediglich mit der Beifügung ‚aM‘ versehen) und weil die StPO derart strenge formale Voraussetzungen für keine anderen Rechtsbehelfe oder Rechtsmittel vorsieht, die insbesondere für anwaltlich oft nicht vertretene Opfer eine große Hürde darstellen können, wird die Streichung der Wendung ‚und die zur Beurteilung seiner fristgemäßen Einbringung notwendigen Angaben zu enthalten‘ vorgeschlagen, womit dem Opferschutz und der Systematik der StPO entsprechend Rechnung getragen werden soll. Für die Prüfung der Rechtzeitigkeit des Antrags soll das Gericht auch weiterhin auf die in § 195 Abs. 2 erster Satz StPO normierten Fristen für die Einbringung des Fortführungsantrags abzustellen haben, wobei die Behörde in jenen Fällen, in denen sie Tatsache und Zeitpunkt der Zustellung einer Verständigung von der Einstellung (§ 194 Abs. 1 StPO) oder einer Einstellungsbegründung (§ 194 Abs. 2 zweiter Satz StPO) nicht nachweisen kann, die Folgen zu tragen hat (stRsp des VwGH: 2007/16/0207, 2007/16/0175, 2004/08/0087, 2001/13/0302), sodass die – für eine unterbliebene Verständigung vorgesehene – längere Frist von drei Monaten zur Anwendung kommt.

§ 195 Abs 2 dritter Satz StPO idgF sieht weiters vor, dass der Antrag (bei sonstiger Zurückweisung gemäß § 196 Abs 2) die Gründe des Abs 1 Z 1 und 2 einzeln und bestimmt zu bezeichnen hat. Darunter ist nichts anderes zu verstehen als eine über die Voraussetzungen bei Beschwerde oder Einspruch hinausgehende, dem Standard der Nichtigkeitsbeschwerde (vgl § 285 Abs 1 zweiter Satz) entsprechende Begründungspflicht (*Nordmeyer in Fuchs/Ratz, § 195 Rz 29*).

Da der Staatsanwaltschaft bei der Entscheidung über die Einstellung weites Ermessen zukommt und nur über den Antrag gemäß § 195 StPO gerichtliche Kontrolle erwirkt werden kann, sind die hohen formellen Hürden sachlich nicht nachvollziehbar. Es gibt keine anderen Rechtsmittel oder Rechtsbehelfe gegen Entscheidungen der Staatsanwaltschaft oder der Gerichte im Ermittlungsverfahren, deren Begründung dem Standard der – im Rechtsmittelverfahren zwingend die Beigebung einer Rechtsanwältin bzw eines Rechtsanwalts erfordernden (§ 61 Abs 1 Z 6 StPO) – Nichtigkeitsbeschwerde entsprechen muss. Zudem ist gegen die gerichtliche Entscheidung über den Antrag auf Fortführung kein Rechtsmittel zulässig.

Der Entfall nur der Wendung betreffend die Angaben zur Rechtzeitigkeit, nicht jedoch auch zur einzelnen und bestimmten Bezeichnung der Gründe (entsprechend dem Standard einer Nichtigkeitsbeschwerde) ist vor dem Hintergrund der intendierten Abschaffung formaler Hürden, die für keine anderen Rechtsmittel oder Rechtsbehelfe im Ermittlungsverfahren (ohne Anwaltszwang) vorgesehen sind, sachlich nicht rechtfertigbar.

Im Ergebnis darf das Gericht die Fortführung des Verfahrens auch weiterhin nur bei Vorliegen der in § 195 Abs 1 StPO idgF genannten und vom Opfer zumindest behaupteten Gründe anordnen, jedoch nicht gleich jeden nicht dem Standard einer Nichtigkeitsbeschwerde entsprechenden Fortführungsantrag zurückweisen.

Die Notwendigkeit der Ausführung eines diesem Standard entsprechenden Antrags auf Fortführung ist überdies im Hinblick auf die noch nicht einmal ansatzweise den Anforderungen an ein Urteil entsprechenden Einstellungsbegründungen der Staatsanwaltschaft (§ 194 Abs 2 StPO idgF) verfassungsrechtlich bedenklich.

Zu Z 64 (§ 196a Abs. 2 StPO):

Aufgrund der Zusammenführung von § 108 und § 108a StPO (vgl. Z 34) ist § 196a Abs. 2 StPO redaktionell anzupassen.

Zu Z 80 (§ 516 StPO):

Diese Bestimmung enthält Übergangsbestimmungen.

In Bezug auf die Neuregelung der Sicherstellung und der Einführung der neuen Ermittlungsmaßnahme der Beschlagnahme von Datenträgern und Daten sollen diese klarstellen, dass § 111 Abs. 2 StPO und §§ 115f bis 115l StPO in allen Ermittlungsverfahren Anwendung finden, die ab dem 1. Jänner 2025 beginnen (§ 1 Abs. 2 StPO). In bereits eingeleiteten Ermittlungsverfahren gelten diese Bestimmungen, wenn nach dem 1. Jänner 2025 die genannten Ermittlungsmaßnahme angeordnet wird. Bei Sicherstellungen nach § 111 Abs. 2 StPO ist der relevante Zeitpunkt die Anordnung (§ 102 StPO) der Ermittlungsmaßnahme, während bei der Beschlagnahme von Datenträgern und Daten nach § 115f Abs. 2 StPO der Zeitpunkt des Antrags auf gerichtliche Bewilligung der Anordnung maßgeblich ist. In allen anderen (laufenden) Verfahren sollen lediglich §§ 115h, 115i, 115j, 115k und 115l StPO sinngemäß Anwendung finden, sodass die Staatsanwaltschaft einen Antrag auf Beschlagnahme der bereits zuvor sichergestellten Daten zu stellen hat, um den Anforderungen des VfGH und des EuGH gerecht zu werden und eine unzulässige ‚Vorratsdatenspeicherung‘ durch Staatsanwaltschaft und Kriminalpolizei zu unterbinden. Die sinngemäße Anwendung der weiteren Bestimmungen bezieht sich ausschließlich auf die vorzunehmende neuerliche Antragstellung und allfällige gerichtliche Bewilligung. Damit soll insbesondere sichergestellt werden, dass Beteiligungsrechte von Beschuldigten und Opfern bei der Auswertung von Daten Berücksichtigung finden können. Zusätzlich soll auch in laufenden Verfahren die sichere Verwahrung von Datenträgern und Daten nach § 115k StPO gewährleistet werden. Durch die sinngemäße Geltung von § 115l StPO durch die bzw. den Rechtsschutzbeauftragten der Justiz soll insbesondere für Beschuldigte und Opfer auch in den bereits anhängigen Verfahren zusätzlicher Rechtsschutz gewährleistet werden. Eine rückwirkende (Verständigungs-)Pflicht nach § 115l Abs. 1 StPO der Staatsanwaltschaft an den bzw. die Rechtsschutzbeauftragten besteht nicht.

Zu Z 3 (§ 48a GOG):

Um der im letzten Regierungsprogramm verankerten Zielsetzung, die letztinstanzlichen rechtskräftigen Entscheidungen der Oberlandesgerichte in der Entscheidungsdokumentation Justiz zu veröffentlichen, zu entsprechen, hat das Bundesministerium für Justiz die für eine möglichst umfassende Veröffentlichung erforderlichen inhaltlichen und technischen Voraussetzungen geschaffen. Dem sich daraus ergebenden legislativen Anpassungsbedarf soll mit der hier vorgesehenen Änderung des § 48a GOG entsprochen und eine allgemeine Veröffentlichungspflicht der rechtskräftigen Entscheidungen der Oberlandesgerichte verankert werden, wobei sich die Veröffentlichung auf Entscheidungen im Volltext (§ 15 Abs. 1 Z 1 OGHG) beschränkt; Für die Erstellung von Rechtssätzen (§ 15 Abs. 1 Z 2 OGHG) besteht hingegen keine Verpflichtung, sie bleibt aber auch für Entscheidungen nach § 48a möglich. Die Ausnahmeregelung, wonach (hier) das erkennende Gericht bei der Beschlussfassung in Rechtssachen, in denen das Verfahren in allen Instanzen ohne Durchführung einer öffentlichen Verhandlung zu führen war, anordnen kann, dass die Entscheidung in der Datenbank nicht zu veröffentlichen ist, wenn sonst die Anonymität der Betroffenen nicht sichergestellt ist, ist durch den Verweis auf (auch) § 15 Abs. 2 OGHG sinngemäß anzuwenden. Durch Abs. 1 letzter Satz wird klargestellt, dass ausschließlich in ihrer Gesamtheit rechtskräftige Entscheidungen der Oberlandesgerichte zu veröffentlichen sind, also auch jene, in denen der Oberste Gerichtshof das Rechtsmittel ohne oder nur mit kurzer Begründung zurückgewiesen hat, nicht aber jene, in denen der Oberste Gerichtshof die Entscheidung abgeändert hat.

Aus Gründen der Transparenz, Rechtssicherheit und Waffengleichheit sollen auch alle rechtskräftigen letztinstanzlichen Entscheidungen der Landesgerichte als Rechtsmittelgerichte – soweit eine Befassung des OGH nicht mehr zulässig ist bzw zugelassen wird – in pseudonymisierter Form im Rechtsinformationssystem des Bundes zu veröffentlichen sein, um sie der Rechtswissenschaft sowie der Praxis zugänglich zu machen.

Eine Einschränkung dieser dem Grunde nach allgemeinen Veröffentlichungspflicht ist allerdings für die strafrechtlichen Ermittlungsverfahren mit Blick auf die im Strafverfahren geltenden besonderen grundrechtlichen Garantien, die bei der Abwägung, ob eine Entscheidung zu veröffentlichen ist oder nicht, gegen das Interesse an der Veröffentlichung abzuwägen sind, unabdingbar. Zu denken ist hier insbesondere an die Unschuldsvermutung und die Garantien des Art. 6 EMRK, aber auch an die Rechte der Opfer, die sich aus der Richtlinie Opferrechte ableiten. Die daraus resultierende Berücksichtigung von Beschuldigten- und Opferrechten wird in Abs. 2 explizit verankert. Darüber hinaus gilt es aber nicht zuletzt mit Blick auf die besonderen grundrechtlichen Garantien generell dafür Sorge zu tragen, dass Entscheidungen aus Ermittlungsverfahren erst nach deren rechtskräftiger Beendigung veröffentlicht werden. Das Bundesministerium für Justiz wird durch entsprechende technische und organisatorische Vorkehrungen sicherstellen, dass die für die Veröffentlichung zuständige Stelle rasch und einfach von der Beendigung des Ermittlungsverfahrens Kenntnis erlangen kann.

Die Pseudonymisierung und die anschließende Aufnahme in die Entscheidungsdokumentation Justiz erfolgen durch die Präsidentin oder dem Präsidenten des zuständigen Oberlandesgerichts im Rahmen der monokratischen Justizverwaltung. Dies soll nunmehr durch den Verweis auf § 42 GOG explizit klargestellt werden. Lediglich die in Abs. 3 unverändert vorgesehene Beurteilung, ob eine Entscheidung von einem allgemeinen, über den Einzelfall hinausgehenden Interesse ist, soll aus rechtsstaatlichen Erwägungen wie bisher der Rechtsprechung vorbehalten bleiben. Überdies ist entsprechenden Hinweisen aus der Praxis folgend im Interesse der Qualitätssicherung vorgesehen, dass sich das erkennende Gericht vorbehalten kann, die bereits pseudonymisierte Entscheidung vor der Aufnahme in die Entscheidungsdokumentation Justiz noch einmal vorgelegt zu erhalten, was sich insbesondere bei komplexen Sachverhaltskonstellationen als zweckmäßig erweisen kann. Wenn es das für erforderlich hält, kann das erkennende Gericht den pseudonymisierten Entwurf abändern oder einen (nachträglichen) Beschluss nach § 15 Abs. 2 OGHG fassen. Die finale Entscheidung über die Pseudonymisierung obliegt der monokratischen Justizverwaltung. Hiervon ausdrücklich unberührt bleibt § 15 Abs. 5 OGHG.

In Abs. 5 soll aus rechtsstaatlichen Erwägungen und im Interesse des Fair Trial (Art. 6 EMRK) vorgesehen werden, einer Ergänzung dahingehend, dass den Verfahrensbeteiligten alle rechtskräftigen Entscheidungen, auf die in gerichtlichen und staatsanwaltlichen Verfahren Bezug genommen wird, kostenlos zur Verfügung gestellt werden. Dafür ist im Wege der monokratischen Justizverwaltung durch die jeweils zuständige Justizverwaltungsstelle Sorge zu tragen.

Zu Artikel 4 (Änderung des Finanzstrafgesetzes)

Zu Z 1 (§ 57 Abs. 4, § 84 Abs. 5 und § 127 Abs. 1 FinStrG)

Die vorgeschlagene Änderung zielt darauf ab, den mitunter als diskriminierend empfundenen Begriff ‚stumm‘ in Anlehnung an die Terminologie des vorgeschlagenen § 61 Abs. 2 lit. a StPO auch im FinStrG durch den Begriff ‚hochgradig sprachbehindert‘ zu ersetzen.

Zu Z 2 (§ 201 FinStrG)

Der Verweis soll an die vorgeschlagene Änderung des § 108 StPO angepasst werden.

In § 53 FinStrG wird die Zuständigkeit zur Ahndung von Finanzvergehen zwischen Gericht und Finanzstrafbehörde abgegrenzt, wobei die originäre Gerichtszuständigkeit grundsätzlich von der Höhe des strafbestimmenden Wertbetrags abhängt. Da die Zuständigkeitsfrage zu Beginn der Ermittlungen oft noch zu klären ist, können verwaltungsbehördliche Finanzstrafverfahren in gerichtliche übergeleitet werden. Nach den EBRV 81 BlgNR XXIII. GP 14 trägt § 201 FinStrG in der geltenden Fassung diesem Umstand Rechnung, indem er den Zeitpunkt der ersten Berichterstattung an die Staatsanwaltschaft iSd § 100 Abs. 2 Z 3 erster Fall StPO als frühestmöglichen Zeitpunkt für die Einbringung eines Einstellungsantrags nach dem vorgeschlagenen § 108 Abs. 2 Z 2 StPO im Finanzstrafverfahren vorsieht.

Zu Z 4 und 5 (§ 228a, § 265 Abs. 6 FinStrG)

Der bestehende § 228a FinStrG verweist auf den durch den VfGH mit Erkenntnis vom 22.9.2022, G 90/2022, als verfassungswidrig aufgehobenen Abs. 2 des § 393a StPO. Dem Freigesprochenen gebührte demnach ein angemessener Teil des im Fall eines Freispruchs oder einer Einstellung nach § 393a Abs. 1 Z 1, 2 oder 3 StPO zustehenden Betrags. Aufgrund der Aufhebung des § 393a Abs. 2 StPO geht der Verweis des § 228a FinStrG nunmehr ins Leere. Angesichts dessen und des Umstandes, dass mit dem Bundesgesetz BGBl. I Nr. 96/2024 der Beitrag zu den Kosten der Verteidigung in den §§ 196a und

393a StPO neu geregelt wurde, erweist sich eine Anpassung der Ersatzregelung des bisherigen § 228a als erforderlich. Es soll sichergestellt werden, dass sowohl im Falle der Einstellung des Ermittlungsverfahrens wegen eines Finanzvergehens durch die Staatsanwaltschaft oder das Gericht als auch bei einer nicht verurteilenden Beendigung des gerichtlichen Finanz Strafverfahrens Ansprüche auf den Beitrag zu den Kosten der Verteidigung nach den Regelungen der StPO bestehen sollen. Die in § 265 Abs. 6 vorgeschlagene Anwendungsbestimmung entspricht § 516 Abs. 12 StPO in der Fassung des Bundesgesetzes BGBl. I Nr. 96/2024, um Wertungswidersprüche zu vermeiden.

Zu Artikel 6 (Änderung des Allgemeinen Verwaltungsverfahrensgesetzes 1991):

Zu Z 1 (§ 55a):

Mit der vorgeschlagenen Bestimmung soll – in Präzisierung der verfassungsgesetzlichen Amtshilferegelung des Art. 22 B-VG – eine gemäß § 76 Abs. 4 StPO erforderliche ausdrückliche gesetzliche Ermächtigung geschaffen werden, um den Behörden eine ordnungsgemäße Vollziehung zu ermöglichen (vgl. OGH 10.12.2019, 11 Os 76/19i). Diese wird sodann gemäß § 24 erster Satz des Verwaltungsstrafgesetzes 1991 – VStG, BGBl. Nr. 52/1991, § 17 und § 38 des Verwaltungsgerichtsverfahrensgesetzes – VwGGV, BGBl. I Nr. 33/2013, und § 62 Abs. 1 des Verwaltungsgerichtshofgesetzes 1985 – VwGG, BGBl. Nr. 10/1985, auch im Verwaltungsstrafverfahren (zB zur Vermeidung einer potenziellen Doppelbestrafung), im Verfahren der Verwaltungsgerichte und im Verfahren vor dem Verwaltungsgerichtshof anzuwenden sein.

In Abweichung von bisherigen Bestimmungen (siehe etwa § 158 Abs. 4d BAO), die eine Ermächtigung von Kriminalpolizei, Staatsanwaltschaften und Gerichten vorsehen, sollen gemäß dem ersten Satz die Behörden zur Stellung von Ersuchen an die zuvor genannten Organe und zur Verarbeitung der erhaltenen personenbezogenen Daten ermächtigt werden. Unter welchen Voraussetzungen Kriminalpolizei, Staatsanwaltschaften und Gerichte personenbezogene Daten übermitteln dürfen, ist nämlich schon Gegenstand des § 76 Abs. 4 StPO und auch in den Materialien zu dieser Bestimmung wird zum Ausdruck gebracht, dass eine Ermächtigung derjenigen Behörden, die die personenbezogenen Daten erhalten sollen, erforderlich ist (, [...] es künftig jedem Materiengesetzgeber zu ermöglichen, eine gesetzliche Ermächtigung zum Erhalt personenbezogener Daten aus einem Strafverfahren für bestimmte Behörden und Gerichte vorzusehen. In der einer solchen Ermächtigung korrespondierenden Bestimmung des § 76 Abs. 4 StPO als der erforderlichen Grundlage zur Zulässigkeit der Übermittlung von Daten aus einem Strafverfahren an die ersuchende Behörde bzw. das ersuchende Gericht [...]’ [970/A d.B. XXVI. GP, 39]; siehe auch *Lendl* in Fuchs/Ratz, WK StPO, § 76, Rz. 22/1 [Stand 15.3.2023, rdb.at]: ,wenn eine ausdrückliche gesetzliche Ermächtigung zum Erhalt bzw zur Verwendung der Daten vorliegt’).

Laut VfSlg. 19.801/2013 darf der Gesetzgeber die Verwendung von Ergebnissen über personenbezogene Daten, die in einem Strafverfahren rite erlangt wurden, in sonstigen (gerichtlichen oder verwaltungsbehördlichen) Verfahren nur insoweit vorsehen, als der Zweck der Datenverwendung in diesen Verfahren ein öffentliches Interesse oder das Interesse eines anderen verfolgt, welches das Interesse des Betroffenen an der Geheimhaltung (bzw. Löschung) der Daten übersteigt und das gelindeste Mittel zur Erreichung des Verfahrenszieles darstellt. Die vorgeschlagene Bestimmung trägt dem zunächst dadurch Rechnung, dass ein Ersuchen um Datenübermittlung nur gestellt werden kann, ,[s]oweit dies für die Durchführung des Ermittlungsverfahrens erforderlich und nicht unverhältnismäßig ist’.

Ob die Stellung eines Ersuchens ,erforderlich’ ist, ergibt sich aus den maßgeblichen Verwaltungsvorschriften. Eine nähere Determinierung kann allerdings in einem allgemeinen Verwaltungsverfahrensgesetz von vornherein nicht geleistet werden: ,Denn für Verfahrensvorschriften gibt es eigentlich keine ‘Vollziehung’ im technischen Sinne, da ja das Verfahren selbst nichts anderes ist als die Vollziehung materieller Normen’ (so bereits im Besonderen Teil der Erläuterungen zu 116 d.B. II. GP, 1; vgl. auch *Mayer*, Die Zuständigkeit der Verwaltungsbehörden im Vollstreckungsverfahren [1974] 91 f).

Zur Vornahme der grundrechtlich gebotenen Interessenabwägung werden ebenfalls die Verwaltungsvorschriften heranzuziehen sein. Die Prüfung durch die Behörde, ob die Datenübermittlung und -verarbeitung ,nicht unverhältnismäßig’ ist, kann allerdings schon mangels Kenntnis des konkreten Inhalts dieser Daten nur eine ex-ante-Prüfung sein. Gelangt die Behörde zum Ergebnis, dass die Unverhältnismäßigkeit zu bejahen ist, hat bereits die Stellung eines entsprechenden Ersuchens zu unterbleiben.

Zum zweiten Satz und dritten Satz vgl. *mutatis mutandis* die Vorbildbestimmung des § 76 Abs. 1 zweiter Satz StPO und *Lendl* in Fuchs/Ratz, WK StPO, § 76, Rz. 12 (Stand 15.3.2023, rdb.at) sowie ferner Art. 61 Abs. 3 DSGVO. Als Grundsatz gilt, dass das Ersuchen alle erforderlichen Angaben, einschließlich insbesondere des Zwecks der Datenverarbeitung, zu enthalten hat und, um Kriminalpolizei,

Staatsanwaltschaften und Gerichten die von ihnen gemäß § 76 Abs. 4 StPO (siehe insbesondere Z 1 und 2 leg. cit.) vorzunehmende Beurteilung zu ermöglichen, entsprechend zu begründen ist.

Die Bestimmungen des DSG bleiben unberührt und vollumfänglich anwendbar.

Zu Z 2 (§ 82 Abs. 25):

Inkrafttretensbestimmung.“

Der Budgetausschuss hat den gegenständlichen Initiativantrag erstmals in seiner Sitzung am 14. November 2024 in Verhandlung genommen. An der Debatte beteiligten sich außer dem Berichterstatter Abgeordneter Mag. Harald **Stefan** die Abgeordneten Dr. Elisabeth **Götze** und Dr. Stephanie **Krisper** sowie die Bundesministerin für Justiz Dr. Alma **Zadić**, LL.M.. Anschließend wurden die Verhandlungen vertagt.

Der Budgetausschuss hat den gegenständlichen Initiativantrag erneut in seiner Sitzung am 9. Dezember 2024 in Verhandlung genommen. An der Debatte beteiligten sich die Abgeordneten Mag. Agnes Sirkka **Prammer**, Mag. Harald **Stefan**, Mag. Selma **Yildirim**, Dr. Nikolaus **Scherak**, MA und Mag. Wolfgang **Gerstl** sowie der Bundesminister für Soziales, Gesundheit, Pflege und Konsumentenschutz Johannes **Rauch**.

Bei der Abstimmung fand der gegenständliche Initiativantrag keine Mehrheit (**für den Antrag:** F, **dagegen:** V, S, N, G).

Zur Berichterstatterin für den Nationalrat wurde Abgeordnete Mag. Agnes Sirkka **Prammer** gewählt.

Als Ergebnis seiner Beratungen stellt der Budgetausschuss somit den **Antrag**, der Nationalrat wolle diesen Bericht zur Kenntnis nehmen.

Wien, 2024 12 09

Mag. Agnes Sirkka Prammer

Berichterstattung

Gabriel Obernosterer

Obmann