



Ausschussdrucksache 21(6)122f
vom 6. Oktober 2026, 10:25 Uhr

Schriftliche Stellungnahme
des Sachverständigen Prof. Eike Richter

Öffentliche Anhörung

zu dem Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und
Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren
BT-Drucksachen 21/6581, 21/7154

Hochschule der Akademie der Polizei Hamburg, Carl-Cohn-Straße 39,
22297 Hamburg

An den
Ausschuss für Recht und Verbraucherschutz
im Deutschen Bundestag
Platz der Republik 1
11011 Berlin

Prof. Eike Richter

Professur für Öffentliches Recht,
insbesondere Recht der Digitalisierung
und IT-Sicherheitsrecht
Hochschule der Akademie
der Polizei Hamburg
Carl-Cohn-Straße 39, 22297 Hamburg
Tel.: +49 (0)40/4286-24432
eike.richter@ak.polizei.hamburg.de

Stellungnahme zum Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren (Drucksache 21/6581)

Sehr geehrter Herr Vorsitzender, sehr geehrte Damen und Herren Abgeordnete,

ich danke für die Gelegenheit zur Stellungnahme zum genannten Gesetzentwurf.

Ich konzentriere mich in meiner schriftlichen Stellungnahme auf vier Themenbereiche des vorgelegten Gesetzentwurfs.¹ Zunächst wird auf den Schutz der Berufsgeheimnisträger im Zusammenhang mit der Erhebung von Verkehrsdaten (Artikel 1 Nr. 2 des Gesetzentwurfs – § 100g StPO-E²) eingegangen (dazu A). Im Anschluss nehme ich zur Einführung einer Sicherungsanordnung und hier zur Frage eines Richtervorbehalts (Artikel 1 Nr. 2 und 4 des Gesetzentwurfs – § 100g Abs. 7 und § 101a Abs. 1 S. 1 Nr. 3 Buchst. a StPO-E) Stellung (dazu B). Im Anschluss befasse ich mich mit der Erwägung, das Instrument der Sicherungsanordnung auch den Verfassungsschutzbehörden zu eröffnen (Artikel 6 Nr. 2 des Gesetzentwurfs – § 176 Abs. 1 TKG-E; dazu C). Sodann prüfe ich die Neuregelung der Funkzellenabfrage in § 100g Abs. 4 StPO-E (dazu D). Schließlich unterbreite

¹ Ich danke meinem wiss. Mitarbeiter Ass. iur. Markus Matthias Göppert für die Unterstützung bei der Erstellung dieser Stellungnahme.

² Um in der Stellungnahme Vorschriften des vorliegenden Gesetzentwurfs von geltenden Vorschriften unterscheiden zu können, sind erstere mit einem „-E“ in der Gesetzesbezeichnung ergänzt (z.B. § 100g StPO-E). Seitenzahlen ohne Quellenangaben beziehen sich auf den Gesetzentwurf der Bundesregierung (Drucksache 21/6581).

ich auf dieser Grundlage Formulierungshilfen zur Ergänzung des vorgelegten Gesetzentwurfs, die den dargelegten Erwägungen Rechnung tragen (dazu E). Im Rahmen der Anhörung gehe ich gerne auf einzelne Punkte und weitere Themen des Gesetzentwurfs ein.

Die Ergebnisse zu den vier genannten Themen lassen sich vorab wie folgt **zusammenfassen**:

1. Die im Vergleich zur geltenden Rechtslage im Gesetzentwurf vorgesehene **Absenkung des Schutzniveaus von Berufsgeheimnisträgern, insbesondere von Medienangehörigen**, verletzt keine verfassungs- und menschenrechtlichen Grenzen. Sie trägt jedoch Art. 4 Abs. 3 S. 2 Buchst. b der Verordnung (EU) 2024/1083 (EMFA) nicht hinreichend Rechnung. Denn die vorgeschlagene Regelung für die Sicherungsanordnung sieht jedenfalls für Medienangehörige keine ausdrückliche Ausnahmeregelung oder zumindest einen Vorbehalt der vorherigen Zustimmung einer Justizbehörde oder eines unabhängigen und unparteiischen Entscheidungsgremiums verbunden mit einer entsprechenden Benachrichtigungspflicht vor (dazu A).

2. Die vorgeschlagene **Regelung zur Sicherungsanordnung** verletzt nicht verfassungsrechtliche Grenzen. Sie ist jedoch in Hinblick auf die Richtlinie 2002/58/EG bedenklich, soweit sie keinen Richtervorbehalt vorsieht und sie bei Straftaten nach § 100g Abs. 2 StPO-E nicht nur der Identifizierung anhand von IP-Adressen dient (dazu B).

3. Die vom Bundesrat vorgeschlagene **Öffnung der Sicherungsanordnung für die Verfassungsschutzbehörden** begegnet in der vorgelegten Fassung verfassungs- und unionsrechtlichen Bedenken. Die Verweisung auf § 174 Abs. 3 Nr. 5 TKG begrenzt die Sicherung nicht hinreichend auf die nach dem jeweiligen Eingriffsgewicht zulässigen Anlässe und Zwecke (dazu C).

4. Die Neuregelung der **Funkzellenabfrage** in § 100g Abs. 4 StPO-E dürfte nicht gegen höherrangiges Recht verstoßen (dazu D).

Soweit der Gesetzentwurf höherrangiges Recht nicht verletzt, sollte der Gesetzgeber in den ihm durch die Verfassung eingeräumten Gestaltungsspielräumen exekutive Eingriffsbefugnisse, richterliche Kontrolle und mediale Beobachtung auch mit dem verstärkten Blick darauf ausbalancieren, dass Eingriffsbefugnisse der StPO auch künftigen Re-

gierungen und den ihnen unterstellten Behörden sowohl in Bund und in Ländern zur Verfügung stehen. Für die Resilienz des demokratischen Rechtsstaats kommt es auch darauf an, die Gewalten in ihren Mächtigkeiten und in ihren Verschränkungen auch so auszutarieren, dass sich exekutivische Befugnisse auch dann nicht ohne Weiteres gegen die freiheitliche demokratische Grundordnung wenden lassen, wenn Stellen über sie verfügen, die sich dieser nicht mehr verpflichtet fühlen (vgl. EGMR (Plenum), Klass u.a./Deutschland, Nr. 5029/71, § 49 f. u. 56).

A. Schutz der Berufsgeheimnisträger, insbesondere von Medienangehörigen, im Zusammenhang mit der Erhebung von Verkehrsdaten

Nach dem bislang geltenden § 100g Abs. 4 S. 1 u. 2 StPO ist es unzulässig, auf Vorrat gespeicherte Verkehrsdaten zu erheben und ggf. zu verwerten, wenn sich die Erhebung bzw. Verwertung gegen Geistliche, Verteidiger, Rechtsanwälte, Medienangehörige und andere Berufsgeheimnisträger nach § 53 Abs. 1 S. 1 Nr. 1 bis 5 StPO richtet und voraussichtlich Erkenntnisse erbringen würde, über die diese Personen das Zeugnis verweigern dürften.

Der vorgelegte Gesetzentwurf streicht dieses Erhebungs- und Verwertungsverbot zum Schutz von Berufsgeheimnisträgern. Er verweist dazu kompensierend auf § 160a StPO (BT-Drs. 21/6581, S. 35), der gestufte Ermittlungseinschränkungen vorsieht. Während Abs. 1 für bestimmte Berufsgeheimnisträger ein vollständiges Erhebungs- und Verwertungsverbot statuiert, senkt Abs. 2 den Schutz anderer Berufsgeheimnisträger, nämlich insbesondere Medienangehöriger nach § 53 Abs. 1 S. 1 Nr. 5 StPO, nur insoweit ab, als deren Zeugnisverweigerungsrecht bei der Prüfung der Verhältnismäßigkeit besonders zu berücksichtigen und die Maßnahme, soweit geboten, zu unterlassen oder zu beschränken ist. Dieser gestufte bzw. eingeschränkte Schutz von Berufsgeheimnisträgern soll auch für die Sicherungsanordnung gelten, die mit dem vorgelegten Gesetzentwurf (§ 100g Abs. 7 StPO-E) eingeführt werden soll. Insbesondere soll eine Sicherungsanordnung, die Medienangehörige betrifft, nicht unzulässig sein (BT-Drs. 21/6581, S. 8).

Diese im Gesetzentwurf vorgesehene Absenkung des Schutzniveaus verletzt zwar nicht verfassungs- und menschenrechtliche Grenzen (dazu I). Sie trägt jedoch Art. 4 Abs. 3 S. 2 Buchst. b EMFA nicht hinreichend Rechnung, weil § 100g Abs. 7 in Verbindung mit § 101a Abs. 1 S. 1 Nr. 3 Buchst. a StPO-E für die Sicherungsanordnung für Medienangehörige keine ausdrückliche Ausnahmeregelung oder zumindest einen Vorbehalt der vorherigen Zustimmung einer Justizbehörde oder eines unabhängigen und unparteiischen Entscheidungsgremiums verbunden mit einer entsprechenden Benachrichtigungspflicht vorsieht (dazu II).

I. Die Streichung des bisherigen § 100g Abs. 4 StPO durch Artikel 1 Nr. 2 des Gesetzentwurfs verletzt keine verfassungs- und menschenrechtlichen Grenzen. Insbesondere die grundgesetzliche Pressefreiheit gem. Art. 5 Abs. 1 S. 2 GG verlangt nicht, Medienangehörige in den absoluten Schutz des § 160a Abs. 1 StPO einzubeziehen (vgl. BVerfGE 129, 208, Rn. 267 f.). Auch die nach Art. 10 EMRK erforderliche unabhängige Prüfung muss in dringenden Fällen jedenfalls vor Zugriff und Verwendung erfolgen (hierzu EGMR (GK), *Sanoma Uitgevers B.V./Niederlande*, Nr. 38224/03, § 91); zugegriffen wird erst bei der Erhebung der gesicherten Daten nach § 100g Abs. 7 S. 2 StPO-E (BT-Drs. 21/6581, S. 8).

II. § 100g Abs. 7 in Verbindung mit § 101a Abs. 1 S. 1 Nr. 3 Buchst. a StPO-E trägt jedoch Art. 4 Abs. 3 S. 2 Buchst. b der Verordnung (EU) 2024/1083 (EMFA) nicht hinreichend Rechnung, weil die vorgelegte Regelung für die Sicherungsanordnung für Medienangehörige keine ausdrückliche Ausnahmeregelung (dazu 1) oder zumindest einen Vorbehalt der vorherigen Zustimmung einer Justizbehörde oder eines unabhängigen und unparteiischen Entscheidungsgremiums verbunden mit einer entsprechenden Benachrichtigungspflicht vorsieht (dazu 2).

1. Nach Art. 4 Abs. 3 S. 2 Buchst. b EMFA dürfen Mediendiensteanbieter und ihr redaktionelles Personal nicht untersucht oder überwacht werden, um Informationen zu erhalten, die mit journalistischen Quellen oder vertraulicher Kommunikation im Zusammenhang stehen oder diese identifizieren können; dasselbe gilt für Personen, die aufgrund ihrer regelmäßigen oder beruflichen Beziehung zu ihnen über solche Informationen verfügen könnten. Dazu sollen auch Personen gehören, die mit Medienangehörigen in enger Beziehung dauerhaft in einem gemeinsamen Haushalt leben (EMFA, Erwägungsgrund

20 S. 2) und die § 53 Abs. 1 S. 1 Nr. 5 StPO als nicht-berufsmäßig Mitwirkende nicht erfasst. Eine Sicherungsanordnung ergeht nach § 100g Abs. 7 S. 1 StPO-E zum Zweck einer etwaigen Erhebung (BT-Drs. 21/6581, S. 8) und kann sich, soweit die Erhebung es erlaubt, auch auf künftig anfallende Daten erstrecken (BT-Drs. 21/6581, S. 39). Die Verordnung harmonisiert die Begriffe der Untersuchung und der Überwachung zwar nicht (EMFA, Erwägungsgrund 22 S. 5); Art. 4 Abs. 3 S. 2 Buchst. b EMFA dürfte eine Sicherung aber jedenfalls dann erfassen, wenn sie Informationen über journalistische Quellen erbringen soll, denn sie bereitet die Erhebung von Verkehrsdaten vor, die bislang unbekannte Quellen aufdecken können (siehe dazu auch BVerfGE 107, 299, Rn. 108). Dafür spricht, dass die Verordnung Mindeststandards für Zwangsmaßnahmen einführt, mit denen Mitgliedstaaten an solche Informationen gelangen wollen (EMFA, Erwägungsgrund 23 S. 5). Der Vereinbarkeit mit Art. 4 Abs. 3 S. 2 Buchst. b der Verordnung (EU) 2024/1083 (EMFA) würde Rechnung getragen, soweit der vorgelegte Entwurf um Ausnahmen von der Sicherungsanordnung für Medienangehörige ergänzt würde.

2. Die EMFA statuiert zwar kein absolutes Verbot von Überwachungsmaßnahmen. Ausnahmen bedürfen aber nach Art. 4 Abs. 4 Buchst. d EMFA der vorherigen Zustimmung einer Justizbehörde oder eines unabhängigen und unparteiischen Entscheidungsgremiums, in hinreichend gerechtfertigten und dringenden Ausnahmefällen der unverzüglichen nachträglichen Genehmigung. Ein Staatsanwalt kommt nur „im Rahmen einer justiziellen Tätigkeit“ und nur als Stelle in Betracht, die unabhängig und unparteiisch beurteilen kann (EMFA, Erwägungsgrund 21 S. 3); diese Fähigkeit spricht der EuGH der Staatsanwaltschaft für die Kontrolle des Zugangs zu Vorratsdaten ab, solange sie das Ermittlungsverfahren leitet (EuGH, C-140/20, Rn. 108 f.).

Der vorgelegte Gesetzentwurf sieht indes keinen Vorbehalt einer vorherigen Zustimmung, insbesondere eines Gerichts, vor (BT-Drs. 21/6581, S. 46). Zwar wird auf den Vorrang des Europäischen Medienfreiheitsgesetzes hingewiesen (BT-Drs. 21/6581, S. 35), aber keine zustimmende Stelle bestimmt. Hinzu kommt, dass § 101a Abs. 4 S. 1 StPO-E keine Benachrichtigung der betroffenen Personen von der Sicherungsanordnung vorsieht (BT-Drs. 21/6581, S. 49) und § 176 Abs. 3 TKG-E die Anbieter zum Schweigen verpflichtet (BT-Drs. 21/6581, S. 16). Da es sich bei der Sicherungsanordnung um eine Überwachungsmaßnahme handelt, die ohne Wissen der Betroffenen durchgeführt wird,

bleibt somit unklar, wie die Betroffenen ihre in der EMFA garantierten Rechte wahrnehmen können sollen. Für die Verarbeitung im Zusammenhang mit Überwachungsmaßnahmen nach Art. 4 Abs. 3 S. 2 Buchst. b EMFA gilt nach Art. 4 Abs. 7 EMFA die JI-Richtlinie (EU 2016/680) einschließlich des Rechts der betroffenen Personen auf Information. Art. 4 Abs. 8 UAbs. 1 EMFA verlangt bei Verstößen gegen die Absätze 3 und 7 ein Recht auf wirksamen Rechtsschutz, das grundsätzlich die rechtzeitige Information über Überwachungsmaßnahmen voraussetzt, die ohne Wissen der Betroffenen durchgeführt wurden (EMFA, Erwägungsgrund 22 S. 1).

3. Die dargelegten Defizite – fehlende Bestimmung der zustimmenden Stelle und Unklarheiten beim Rechtsschutz – sind keine Frage der politischen Zweckmäßigkeit, sondern entfalten rechtliche Relevanz. Die der StPO in der Anwendung vorgehenden (BT-Drs. 21/6581, S. 35) Gewährleistungen der EMFA setzen in diesen beiden Punkten nationale Regelungen voraus (vgl. Art. 4 Abs. 4 Buchst. d und Erwägungsgrund 21 S. 3 EMFA), die aber nicht vorliegen. Auch unmittelbar geltende Verordnungen (Art. 288 Abs. 2 S. 2 AEUV) wie die EMFA können zu ihrer Durchführung Maßnahmen der Mitgliedstaaten erfordern (EuGH, C-403/98, Rn. 26), zu denen sie dann Art. 291 Abs. 1 AEUV verpflichtet. Solange sie fehlen, folgt aus dem Vorrang der EMFA ein Verbot. Eine Anordnung der Staatsanwaltschaft nach § 101a Abs. 1 S. 1 Nr. 3 Buchst. a StPO-E wäre mangels Zustimmung nach Art. 4 Abs. 3 S. 2 Buchst. b EMFA unzulässig, auch wenn sie die Voraussetzungen des § 100g Abs. 7 S. 1 StPO-E erfüllte. Der EuGH hat es als Verstoß gegen die Pflichten aus EWG-Vertrag und der jeweiligen Verordnung gewertet, wenn ein Mitgliedstaat an einem Gesetzeswortlaut festhält, der von unmittelbar geltendem Gemeinschaftsrecht abweicht, weil es die Normadressaten über ihre Möglichkeiten, sich auf das Gemeinschaftsrecht zu berufen, im Ungewissen lässt (EuGH, 167/73, Rn. 41 f. und 48). Auch die Information der Betroffenen regelt die EMFA nicht selbst. Nach Art. 4 Abs. 7 EMFA ist es den Mitgliedstaaten zwar zu den in Art. 13 Abs. 3 Buchst. a bis e JI-Richtlinie genannten Zwecken erlaubt, die Unterrichtung aufzuschieben, einzuschränken oder zu unterlassen. Der geltend gemachte Aufwand der Strafverfolgungsbehörden (BT-Drs. 21/6581, S. 49) gehört allerdings nicht zu diesen Zwecken.

4. Schließlich sollte insbesondere der Schutz journalistischer Quellen und Informanten nicht zu gering gewichtet werden (vgl. BVerfGE 107, 299, Rn. 107), so dass die Behebung der genannten Defizite nicht nur rechtlich geboten, sondern auch zweckmäßig erscheint. Unklare Schutzvorkehrungen können Informanten aus Sorge vor ihrer Identifizierung von einer Kontaktaufnahme abhalten und Journalisten von Recherchen zu Missständen insbesondere in Behörden abschrecken. Klare Regelungen zur unabhängigen Kontrolle und zum Rechtsschutz sind deshalb sachgerecht, um das Vertrauen in die Vertraulichkeit journalistischer Kontakte zu erhalten, auf das die Medien bei der Aufdeckung von Missständen angewiesen sind (vgl. BVerfGE 107, 299, Rn. 103, 107 und 127).

B. Zur Notwendigkeit eines Richtervorbehalts für die Sicherungsanordnung

§ 100g Abs. 7 S. 1 StPO-E des vorgelegten Gesetzentwurfs verlangt für eine Sicherungsanordnung in Hinblick auf die Eingriffs- bzw. Ermittlungsschwelle, dass zureichende tatsächliche Anhaltspunkte für eine Straftat vorliegen, die die Erhebung nach den Absätzen 1 bis 4 rechtfertigen würde (BT-Drs. 21/6581, S. 8). Anlass der Sicherung kann nach § 100g Abs. 7 S. 1 Nr. 1 in Verbindung mit Abs. 2 StPO-E auch eine mittels Telekommunikation begangene Straftat sein (BT-Drs. 21/6581, S. 40), die keine erhebliche Bedeutung haben muss (BT-Drs. 21/6581, S. 36). Verfahrensbezogen setzt § 101a Abs. 1 S. 1 Nr. 3 Buchst. a StPO-E voraus, dass die Staatsanwaltschaft die Sicherung anordnet. Bei Gefahr im Verzug darf die Anordnung auch durch ihre Ermittlungspersonen erfolgen. Das Gericht muss dagegen erst eingebunden werden, wenn die Sicherung verlängert werden soll (BT-Drs. 21/6581, S. 10). Eine nachträgliche gerichtliche Bestätigung der Erstanordnung und eine Benachrichtigung der Betroffenen von der Sicherung sind hingegen nicht vorgesehen (s. BT-Drs. 21/6581, S. 46 u. 49).

Die so vorgeschlagene Regelung verletzt zwar nicht verfassungsrechtliche Grenzen (dazu I). Sie ist jedoch in Hinblick auf die Richtlinie 2002/58/EG bedenklich, soweit sie keinen Richtervorbehalt vorsieht (dazu II) und soweit sie bei Straftaten nach § 100g Abs. 2 StPO-E nicht nur der Identifizierung anhand von IP-Adressen dient (dazu III).

I. Die Anordnung, Verkehrsdaten zu speichern, greift in Art. 10 Abs. 1 GG ein (BVerfGE 125, 260, Rn. 190). Das BVerfG hat für die Abfrage und Übermittlung vorsorglich gespeicherter Verkehrsdaten grundsätzlich einen Richtervorbehalt verlangt (BVerfGE 125, 260, Rn. 247). Bei der Speicherung verbleiben die Daten allerdings zunächst beim Anbieter und stehen dem Staat nicht unmittelbar zur Verfügung (BVerfGE 125, 260, Rn. 214). Auch nach § 176 Abs. 2 Nr. 2 und 3 TKG-E des vorgelegten Gesetzentwurfs bleiben die gesicherten Daten, selbst wenn sie erst künftig anfallen, beim Anbieter, bis die anordnende Stelle ihre Übermittlung verlangt (BT-Drs. 21/6581, S. 16 u. 39). Daher dürfte es dem verfassungsgerichtlichen Maßstab genügen, wenn der vorgelegte Gesetzentwurf einen Richtervorbehalt nur für die Erhebung der gesicherten Daten vorsieht (BT-Drs. 21/6581, S. 10). Eine noch weitergehende Vorabkontrolle durch eine unabhängige Instanz kann nach dem BVerfG zwar bei Ermittlungsmaßnahmen geboten sein, die einen schwerwiegenden Grundrechtseingriff bewirken (vgl. BVerfGE 125, 260, Rn. 248); gemessen an diesem Maßstab erscheint der Eingriff durch die Sicherung jedoch nicht hinreichend gewichtig, weil die Strafverfolgungsbehörden die Daten noch nicht herausverlangen können (vgl. auch BT-Drs. 21/6581, S. 46).

II. Soweit § 101a Abs. 1 S. 1 Nr. 3 Buchst. a StPO-E keinen Richtervorbehalt vorsieht, wirft dies jedoch im Hinblick auf die Richtlinie 2002/58/EG europarechtliche Bedenken auf. Nach Art. 15 Abs. 1 S. 2 der Richtlinie 2002/58/EG können die Mitgliedstaaten u.a. zu Strafverfolgungszwecken in ihren Rechtsvorschriften vorsehen, dass Daten während einer begrenzten Zeit aufbewahrt werden. Für die umgehende Sicherung von beim Anbieter vorhandenen Verkehrs- und Standortdaten verlangt der EuGH eine behördliche Entscheidung, die einer wirksamen gerichtlichen Kontrolle unterliegt (EuGH, C-511/18 u.a., Rn. 163). Ob nach dem vorgelegten Entwurf eine solche wirksame gerichtliche Kontrolle gewährleistet ist, erscheint zweifelhaft. Denn die Sicherung erfolgt ohne Wissen des Betroffenen (BT-Drs. 21/6581, S. 49), so dass der Rechtsbehelf nach § 98 Abs. 2 S. 2 StPO analog regelmäßig leerläuft. Eine gerichtliche Befassung ist erst vorgesehen, wenn die Sicherung verlängert oder die gesicherten Daten erhoben werden sollen (vgl. BT-Drs. 21/6581, S. 10). Um dennoch der vom EuGH verlangten wirksamen gerichtlichen Kontrolle gerecht zu werden, dürfte ein Richtervorbehalt notwendig sein. Für den Zugang zu Verkehrsdaten verlangt der EuGH eine vorherige unabhängige Kontrolle, in hinreichend

begründeten Eilfällen eine kurzfristige Kontrolle, weil eine spätere Kontrolle nicht verhindern könne, dass ein über das absolut Notwendige hinausgehender Zugang genehmigt wird (EuGH, C-140/20, Rn. 110). Für die Sicherung, die ebenfalls die Grenzen des absolut Notwendigen einhalten muss (EuGH, C-140/20, Rn. 87), gilt das entsprechend. Eine spätere Kontrolle kann nicht mehr verhindern, dass Daten über die Grenzen des Notwendigen hinaus vorgehalten werden. Insbesondere eine Benachrichtigung würde nur nachträglichen Rechtsschutz nach § 101 Abs. 7 S. 2 StPO eröffnen, der jedoch in seiner Wirkung nicht eine vorherige Kontrolle ersetzen dürfte (EuGH, C-140/20, Rn. 112). Insbesondere bei Funkzellendaten, die regelmäßig eine große Zahl Unbeteiligter betreffen und daher eine hohe Streubreite aufweisen (BT-Drs. 21/6581, S. 38), kommt eingriffsverschärfend hinzu, dass eine (nachträgliche) Benachrichtigung viele Betroffene nicht erreichen dürfte, zumal Unbeteiligte nach § 101 Abs. 4 S. 4 StPO in Verbindung mit § 101a Abs. 4 S. 2 StPO-E nicht benachrichtigt werden müssen, wenn sie nur unerheblich betroffen wurden und anzunehmen ist, dass sie kein Interesse daran haben (s. dazu auch BVerfGE 125, 260, Rn. 245). Nachforschungen zu ihrer Identität nach § 101 Abs. 4 S. 5 StPO sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität, des Aufwands und der daraus folgenden Beeinträchtigungen geboten ist.

Die Befürchtung eines Zeitverzugs (BT-Drs. 21/6581, S. 46) dürfte unbegründet sein, wenn der Richtervorbehalt nach dem Vorbild des § 163f Abs. 3 S. 1 und 2 StPO mit einer Eilkompetenz der Staatsanwaltschaft und Ermittlungspersonen kombiniert wird. Auch dürfte der Aufwand überschaubar bleiben (s. hierzu BT-Drs. 21/6581, S. 27). Ohne Richtervorbehalt läge das Instrument der Sicherungsanordnung im Wesentlichen in der Hand der Staatsanwaltschaft und damit auch bei der insoweit weisungsbefugten Landesjustizverwaltung (vgl. §§ 146, 147 Nr. 2 GVG).

III. Art. 15 Abs. 1 der Richtlinie 2002/58/EG erlaubt eine Aufbewahrung bzw. Sicherung u.a. zur Ermittlung und Verfolgung von Straftaten oder aus Anlass des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen. Nach ihrem Wortlaut stellt die Vorschrift zwar keine besonderen qualitativen Anforderungen an die Straftaten. Der EuGH sieht indes eine umgehende Sicherung wegen des mit ihr einhergehenden Eingriffsgewichts nur bei schwerer Kriminalität als gerechtfertigt an (EuGH, C-793/19 und C-794/19, Rn. 116). Insoweit ist es bedenklich, dass § 100g Abs. 7 iVm Abs. 2 StPO-E auch

dann eine Sicherung zulässt, wenn kein Verdacht hinsichtlich einer Straftat von auch im Einzelfall erheblicher Bedeutung besteht, zumal sich die Sicherung auch auf Verkehrsdaten (z.B. bei einem E-Mail-Anbieter die Kennungen der Kommunikationspartner und die Zeitpunkte von Empfang und Versand, BT-Drs. 21/6581, S. 39) beziehen darf und nur Standortdaten ausgenommen sind. Für die Vorratsspeicherung von IP-Adressen hat der EuGH dagegen die Bekämpfung von Straftaten im Allgemeinen als möglichen Rechtfertigungsgrund anerkannt (EuGH, C-470/21, Rn. 82); beim identifizierenden Zugang berücksichtigt er auch die „Gefahr der systemischen Straflosigkeit“ (EuGH, C-470/21, Rn. 119). Dazu müsse allerdings gewährleistet sein, dass die IP-Adresse auch nur zur Identifizierung genutzt werde und nicht mit anderen Verkehrs- oder Standortdaten zu genauen Schlüssen auf das Privatleben verknüpft werden könne (EuGH, C-470/21, Rn. 82 u. 101). Damit steht es nicht im Einklang, soweit § 100g Abs. 7 StPO-E in den Fällen des § 100g Abs. 2 StPO-E auch die Sicherung solcher Verkehrsdaten erlaubt, die genaue Schlüsse auf das Privatleben ermöglichen. Die Gesetzesbegründung weist selbst darauf hin, dass solche Daten regelmäßig sensibler sind als Daten, die nur die Identifizierung eines Anschlussinhabers ermöglichen (vgl. BT-Drs. 21/6581, S. 56).

C. Eröffnung einer Sicherungsanordnung auch für Verfassungsschutzbehörden

Nach § 176 Abs. 1 S. 1 TKG-E ist vorgesehen, dass Anbieter Verkehrsdaten zur Erfüllung von Sicherungsanordnungen nach StPO, BKAG und BPolG verarbeiten und so gesicherte Daten nach Satz 2 unter den Voraussetzungen des § 175 TKG-E beauskunften dürfen (BT-Drs. 21/6581, S. 16). Der Bundesrat bittet, diese „erste Tür“ im Sinne des Doppeltürmodells des BVerfG (s. BVerfGE 155, 119, Rn. 93) auch für alle in § 174 Abs. 3 TKG genannten Sicherheitsbehörden, insbesondere die Verfassungsschutzbehörden und die Nachrichtendienste, zu öffnen (BT-Drs. 21/6581, S. 70). Die „zweite Tür“ in den Verfassungsschutz- und Nachrichtendienstgesetzen vorausgesetzt (BT-Drs. 21/6581, S. 71) stünde die Sicherungsanordnung damit auch diesen Behörden zur Verfügung. Dabei sollen nach der Vorstellung des Bundesrats für die Speicherung der zu sichernden Daten die Eingriffsschwellen des § 174 Abs. 3 TKG maßgeblich sein. Davon zu unterscheiden

ist der weitergehende Vorschlag unter Nummer 3 der Bundesratsstellungnahme: Dort sollen die Bindung an § 175 TKG-E gestrichen und für die im vorgeschlagenen § 176 Abs. 1 S. 4 TKG-E in Bezug genommene Sicherung eine Anordnung der Behördenleitung oder ihrer Vertretung für höchstens drei Monate sowie eine richterliche Verlängerung um höchstens drei Monate vorgesehen werden (BT-Drs. 21/6581, S. 73). Die Bundesregierung lehnt die Öffnung für die Verfassungsschutzbehörden ab (BT-Drs. 21/7154, S. 1 f.).

Die vorgeschlagene Erstreckung der Sicherungsanordnung auf die Verfassungsschutzbehörden bedeutet eine Vorverlagerung dieses Instruments in das Vorfeld der Gefahrenabwehr und Strafverfolgung. Sie begegnet Bedenken in Hinblick auf die Verhältnismäßigkeit (dazu I) und das Unionsrecht (dazu II) und ist daher abzulehnen.

I. Nach der vom Bundesrat vorgeschlagenen Regelung (BR-Drs. 263/26 (Beschluss), S. 4) sollen Anbieter Verkehrsdaten „unter den in § 174 Absatz 3 genannten Voraussetzungen“ verarbeiten dürfen, soweit dies zur Erfüllung der Sicherungsanordnung einer dort genannten Behörde erforderlich ist. Diese Verweisung ist in Hinblick auf Art. 10 Abs. 1 GG bedenklich. Denn die Sicherung bedeutet auch dann einen Eingriff in das Fernmeldegeheimnis, wenn die Daten zunächst beim Anbieter bleiben (BVerfGE 125, 260, Rn. 190, 193). Mit der vorgesehenen Verweisung auf das TKG würde der Bundesgesetzgeber zwar seine Pflicht wahrnehmen, bereits im Bundesgesetz die tatbestandliche Eingriffsschwelle festzulegen und dies nicht den Ländern zu überlassen (BVerfGE 155, 119, Rn. 130 u. 134). Die Verweisung auf § 174 Absatz 3 TKG ist allerdings als Eingriffsschwelle für Verkehrsdaten materiell zu niedrig und vermag daher den Eingriff nicht nach Art. 10 Abs. 2 Satz 1 GG zu rechtfertigen. Denn § 174 Abs. 3 Nr. 5 TKG verlangt nur, dass die Sicherung aufgrund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist, um bestimmte Bestrebungen oder Tätigkeiten aufzuklären. Diese Schwelle hat das BVerfG zwar grundsätzlich als tragfähig angesehen, allerdings nur für mindergewichtige Eingriffe, die – wie etwa die allgemeine Bestandsdatenauskunft – nicht tief in die Privatsphäre eingreifen (vgl. BVerfGE 155, 119, Rn. 150 f.). Verkehrsdaten kommt hingegen eine höhere Persönlichkeitsrelevanz zu (vgl. BVerfGE 155, 119, Rn. 168).

Die Eingriffsschwelle des § 174 Abs. 3 Nr. 5 TKG dürfte das Eingriffsgewicht, das mit der vorgesehenen Regelung einhergeht, nicht mehr tragen. Zwar ist das Eingriffsgewicht bei der Zuordnung dynamischer IP-Adressen abgemildert, da die Behörden keine Kenntnis

der Verkehrsdaten erhalten und sich aus den Auskünften keine Bewegungsprofile erstellen lassen (BVerfGE 155, 119, Rn. 169). Nach dem vorgelegten Gesetzentwurf sollen dagegen auch gesicherte Verkehrsdaten an die berechnete Stelle beauftragt werden und dabei sowohl vorhandene als auch künftig anfallende Daten sowie auch Standortdaten umfassen (BT-Drs. 21/6581, S. 39 u. 55). Aus solchen Daten dürften sich nach dem Abruf Bewegungsprofile erstellen lassen, was für eine gesteigerte Beobachtungsbedürftigkeit spricht (vgl. BVerfGE 162, 1, Rn. 190, 324, 328 u. 331), auch wenn es vorliegend zunächst nur um die Sicherung der Daten geht.

Die Rechtfertigungslücke dürfte auch nicht durch eine spätere Auskunft geschlossen werden. § 176 Abs. 1 Satz 2 TKG-E bindet diese Auskunft an § 175 TKG-E, dessen Absatz 3 Nr. 7 für die Verfassungsschutzbehörden der Länder ebenfalls nur die niedrige Schwelle verlangt (BT-Drs. 21/6581, S. 16); der eigenständige Vorschlag unter Nummer 3 der Bundesratsstellungnahme will diese Bindung sogar streichen (BT-Drs. 21/6581, S. 73). Gerade von diesen Verwendungsregeln hängt aber ab, ob die Speicherung zulässig ist (BVerfGE 155, 119, Rn. 131). Für das Bundesamt für Verfassungsschutz verweist § 175 Abs. 3 Nr. 6 TKG-E dagegen auf § 8a Abs. 1 Satz 1 Nr. 4 BVerfSchG (BT-Drs. 21/6581, S. 15), wonach Tatsachen vorliegen müssen, die die Annahme schwerwiegender Gefahren für die Schutzgüter des § 3 Abs. 1 BVerfSchG stützen.

II. Die vom Bundesrat vorgeschlagene Erstreckung auf die Verfassungsschutzbehörden dürfte zudem gegen Art. 15 Abs. 1 Satz 1 und 2 RL 2002/58/EG i.V.m. Art. 7, 8, 11 und 52 Abs. 1 GRCh verstoßen, weil sie Sicherungen auch zu Zwecken erlauben würde, die das Unionsrecht nicht anerkennt.

Die Richtlinie erfasst auch mitgliedstaatliche Regelungen, nach denen Anbietern zur Wahrung der nationalen Sicherheit vorgeschrieben werden kann, Verkehrs- und Standortdaten an Nachrichtendienste zu übermitteln (EuGH, Urteil vom 6. Oktober 2020, C-623/17, Privacy International, ECLI:EU:C:2020:790, Rn. 49) oder zu speichern (EuGH, Urteil vom 6. Oktober 2020, C-511/18 u. a., La Quadrature du Net, ECLI:EU:C:2020:791, Rn. 104). Insoweit müssen die Mitgliedstaaten den Zweck einer umgehenden Sicherung gesetzlich angeben, der sich auf die Bekämpfung schwerer Kriminalität oder den Schutz der nationalen Sicherheit beziehen muss (EuGH, C-511/18 u. a., Rn. 164). Der Bekämpf-

fung schwerer Kriminalität stellt der EuGH die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit gleich (EuGH, C-140/20, Rn. 67, 91). Zur nationalen Sicherheit zählt er die Verhütung und Repression von Tätigkeiten, die geeignet sind, die tragenden Strukturen eines Landes in schwerwiegender Weise zu destabilisieren (EuGH, C-511/18 u. a., Rn. 135).

Die vom Bundesrat in Bezug genommene Eingriffsschwelle des § 174 Abs. 3 Nr. 5 Buchst. a TKG stellt lediglich auf Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 BVerfSchG ab, ohne eine besondere Schwere zu verlangen. Verfassungsfeindliche Bestrebungen müssen zwar aktiv auf die Beeinträchtigung eines Elements der freiheitlichen demokratischen Grundordnung abzielen und objektiv geeignet sein, über kurz oder lang politische Wirkungen zu entfalten, aber nicht kämpferisch-aggressiv oder illegal vorgehen (BVerfGE 162, 1, Rn. 185 f.). Für die gleichlautende Schwelle des § 174 Abs. 5 Nr. 5 Buchst. a TKG hat das BVerwG angenommen, dass sie sich nicht ohne Weiteres auf die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit stützen lässt und über den Schutz der nationalen Sicherheit hinausgeht (BVerwG, Urteil vom 14. August 2023, 6 C 6.22, Rn. 44). Nach § 174 Abs. 3 Nr. 5 Buchst. b TKG genügt außerdem die Aufklärung von Bestrebungen oder Tätigkeiten, die ein landesgesetzlich begründeter Beobachtungsauftrag erfasst, insbesondere solcher der organisierten Kriminalität. Kriminalität, auch besonders schwere, kann einer Bedrohung der nationalen Sicherheit aber nicht gleichgesetzt werden (EuGH, C-140/20, Rn. 63). Schwere Kriminalität oder eine schwere Bedrohung der öffentlichen Sicherheit verlangt die Norm nicht. Eine unionsrechtskonforme Auslegung scheidet aus, weil präzise Eingriffsvoraussetzungen Sache des Gesetzgebers sind (BVerwG, 6 C 6.22, Rn. 45). § 176 TKG-E wäre in der vorgeschlagenen Fassung daher für Sicherungen der Verfassungsschutzbehörden insgesamt nicht anwendbar, wie es das BVerwG für die bisherige Speicherpflicht festgestellt hat (BVerwG, 6 C 6.22, Rn. 46; BT-Drs. 21/6581, S. 34).

D. Vereinbarkeit der Funkzellenabfrage nach § 100g Abs. 4 StPO-E mit höherrangigem Recht

Das geltende Recht setzt als Einschreiteschwelle für eine Funkzellenabfrage u.a. einen Verdacht voraus. Dabei bezieht sich dieser Verdacht nach § 100g Abs. 3 Satz 1 Nr. 1 iVm Abs. 1 Satz 1 Nr. 1 StPO auf den ersten Blick auf eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 bezeichnete Straftat. Die höchstrichterliche Rechtsprechung hat diese Voraussetzung enger ausgelegt und entschieden, dass nicht jede Straftat von auch im Einzelfall erheblicher Bedeutung ausreicht, sondern der Verdacht sich auf eine besonders schwere Straftat iSd § 100g Abs. 2 StPO richten muss. Sie beruft sich u.a. darauf, dass sich die Verweisung in Abs. 3 Satz 1 Nr. 1 auch auf Abs. 1 Satz 3 und hierüber auf Abs. 2 beziehe. Zudem würden mit einer Funkzellenabfrage retrograde Standortdaten erhoben werden (BGH, Beschl. v. 10.1.2024, 2 StR 171/23, Rn. 16).

Der vorgelegte Gesetzentwurf versperrt dieser engführenden Auslegung durch die Rechtsprechung den Weg (vgl. BT-Drs. 21/6581, S. 37), indem in § 100g Abs. 4 StPO-E die Funkzellenabfrage nun „unter den Voraussetzungen von Absatz 3“ als zulässig erklärt wird. In Abs. 3 des Entwurfs werden über Abs. 1 S.1 Nr. 1 des Entwurfs eindeutig nur Straftaten von auch im Einzelfall erheblicher Bedeutung in Bezug genommen. Selbstverständlich ist der Gesetzgeber frei, Gesetze zu ändern und so der Rechtsprechung die Grundlage für eingeschlagene Gesetzesauslegungen zu nehmen. Im Fall der vorliegenden Neuregelung der Funkzellenabfrage in § 100g Abs. 4 StPO-E geht damit allerdings die Absenkung der Einschreiteschwelle einher, die sich an höherrangigem Recht, also vor allem an Unionsrecht (dazu I) und Verfassungsrecht (dazu II) messen lassen muss. § 100g Abs. 4 StPO-E dürfte allerdings diese Grenzen des höherrangigen Rechts nicht verletzen.

I. § 100g Abs. 4 StPO-E wahrt insbesondere die unionsrechtliche Grenze des Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58/EG in Verbindung mit Art. 7, 8, 11 und 52 Abs. 1 GRCh. Danach können die Mitgliedstaaten Rechtsvorschriften u.a. zur Erhebung von Verkehrs- und Standortdaten erlassen, sofern die Erhebung dieser Daten u.a. für die nationale Sicherheit (d.h. die Sicherheit des Staates) oder die Ermittlung, Feststellung und Verfolgung von Straftaten notwendig, angemessen und verhältnismäßig ist. Geht es jedoch um

Verkehrs- oder Standortdaten, die geeignet sind, Informationen über die Kommunikationen eines Nutzers eines elektronischen Kommunikationsmittels oder über den Standort der von ihm verwendeten Endgeräte zu liefern, aus denen genaue Schlüsse auf das Privatleben der betroffenen Personen gezogen werden können, hat der EuGH die Einschreiteschwelle höher gelegt: Es muss dann um die Verfolgung schwerer Kriminalität gehen (EuGH, Urt. v. 2.3.2021, C-746/18, Rn. 35). Denn es handele sich dann um einen schwerwiegenden Eingriff – und zwar unabhängig von der Länge des Zeitraums und der Datenmenge (EuGH, C-746/18, Rn. 39).

1. Für die Vereinbarkeit der vorgelegten Neuregelung in § 100g Abs. 4 StPO-E mit dieser unionsrechtlichen Grenze ist somit zunächst entscheidend, ob aus den Telekommunikationsverbindungsdaten, die durch eine Abfrage einer bestimmten, räumlich bezeichneten Funkzelle in einem bestimmten Zeitraum erhoben werden, Rückschlüsse auf das Privatleben der betroffenen Personen möglich sind. Die vorliegende Gesetzesbegründung verneint dies: Die Funkzellenabfrage erlaube nur den Rückschluss, dass ein Anschluss zu einem bestimmten Zeitpunkt in einer bestimmten Funkzelle mit dem Mobilfunknetz verbunden war (BT-Drs. 21/6581, S. 38). Der BGH hält die Erstellung von (partiellen) Bewegungsprofilen hingegen für möglich (BGH, Beschl. v. 10.1.2024, 2 StR 171/23, Rn. 26). Werden etwa bei mehreren räumlich und zeitlich aufeinander bezogenen Funkzellenabfragen dieselben Gerätekennungen festgestellt, lässt sich daraus eine Abfolge von Aufenthalten des betreffenden Mobilgeräts rekonstruieren (vgl. BGH, Beschl. v. 10.1.2024 – 2 StR 171/23, juris Rn. 25 f.). Wiederkehrende Aufenthalte im Bereich einer bestimmten Wohnung können je nach räumlicher Genauigkeit und Kontext beispielsweise auf regelmäßige private Besuche hindeuten und damit Rückschlüsse auf soziale Beziehungen ermöglichen (zur Aussagekraft solcher Daten vgl. auch EuGH, Urt. v. 2.3.2021 – C-746/18, Rn. 36).

2. Wenn somit nicht ausgeschlossen werden kann, dass Rückschlüsse auf das Privatleben möglich sind, dann stellt sich die Frage, ob der vorgelegte § 100g Abs. 4 StPO-E den Anforderungen des EuGH an die dargelegte Einschreiteschwelle gerecht wird. Zwar dürften Straftaten der „schweren Kriminalität“ in vielen Fällen auch „Straftaten von auch im Einzelfall erheblicher Bedeutung“ (z.B. Terrorismus) sein. Dennoch dürften beide Begriffe

nicht deckungsgleich sein. Der EuGH hat anlässlich der Überprüfung einer ihm vorgelegten mitgliedstaatlichen Regelung eine abstrakte Schwelle von mindestens drei Jahren Höchstfreiheitsstrafe als grundsätzlich zulässig erklärt, allerdings betont, dass die Mitgliedstaaten festlegen, was eine schwere Straftat ist (EuGH, Ur. v. 30.4.2024, C-178/22, Rn. 46, 54-56). Er hat auch hervorgehoben, dass die Definition nicht so gewählt werden darf, dass der Zugang zu den Daten zur Regel wird (EuGH, C-178/22, Rn. 55). Ohne damit einen abschließenden Katalog benennen zu wollen, hat der EuGH beispielsweise vorsätzliche Tötung, Vergewaltigung, Menschenhandel sowie sexuelle Ausbeutung von Kindern und Kinderpornografie als Kriminalität mit hohem Schweregrad genannt (EuGH, C-817/19, Rn. 149). Ob aus dieser Warte der Begriff „Straftaten von auch im Einzelfall erheblicher Bedeutung“ nicht zu weit ist, erscheint zumindest zweifelhaft. Weiter hat der EuGH hervorgehoben, dass der Zugang grundsätzlich nur zu Daten von Personen gewährt werden darf, die an der Straftat beteiligt sind (EuGH, C-746/18, Rn. 50). Dies spricht für eine räumlich und zeitlich eng begrenzte Funkzellenabfrage. Dem trägt der vorliegende Entwurf mit § 101a Abs. 1 Satz 1 Nr. 1 Buchst. b StPO-E Rechnung. Schließlich muss das kontrollierende Gericht den Zugang zu den Daten verweigern können, wenn die Tat offensichtlich nicht zur schweren Kriminalität gehört (EuGH, C-178/22, Rn. 60). Dies gewährleistet der vorliegende Entwurf: Nach § 101a Abs. 1 Satz 1 Nr. 1 StPO-E in Verbindung mit § 100e Abs. 1 Satz 1 StPO ordnet das Gericht an und muss seine Erwägungen zur Erforderlichkeit und Angemessenheit nach § 101a Abs. 2 StPO-E einzelfallbezogen darlegen, sodass es Abfragen bei offensichtlich nicht schweren Taten ablehnen kann.

II. Am Maßstab des Art. 10 Abs. 1 GG übernimmt die Vorschrift die Schwelle, die das BVerfG für die Erhebung von Verbindungsdaten unter anderem verlangt, nämlich eine Straftat von erheblicher Bedeutung und einen konkreten Tatverdacht (BVerfGE 107, 299, Rn. 75), wobei die Straftat auch im konkreten Fall erhebliche Bedeutung haben muss (BVerfGE 107, 299, Rn. 76). Der hohen Streubreite, die die Begründung selbst einräumt, begegnet der Entwurf mit der Subsidiaritätsklausel (BT-Drs. 21/6581, S. 38).

E. Formulierungshilfen

Zur Behebung der unter A und B dargelegten Defizite werden folgende Formulierungshilfen angeboten:

I (zu oben A): In Artikel 1 Nummer 4 wird in § 101a Absatz 4 nach Satz 1 der folgende Satz eingefügt:

„Würde eine Sicherungsanordnung nach § 100g Absatz 7 voraussichtlich Erkenntnisse erbringen, die mit journalistischen Quellen oder vertraulicher Kommunikation im Zusammenhang stehen oder diese identifizieren können, und richtet sie sich gegen eine in Artikel 4 Absatz 3 Satz 2 Buchstabe b der Verordnung (EU) 2024/1083 genannte Person, so ist diese Person von der Sicherungsanordnung zu benachrichtigen.“

In der Liste „EU-Rechtsakte“ wird der bisher nicht nummerierte Eintrag zur Nummer 1. Dieser Nummer 1 wird die folgende Nummer 2 angefügt:

„2. Verordnung (EU) 2024/1083 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Schaffung eines gemeinsamen Rahmens für Mediendienste im Binnenmarkt und zur Änderung der Richtlinie 2010/13/EU (Europäisches Medienfreiheitsgesetz) (ABl. L, 2024/1083, 17.4.2024)“

Begründung: Der Satz setzt Art. 4 Abs. 8 UAbs. 1 EMFA in Verbindung mit Abs. 7 um und übernimmt den Personenkreis und die geschützten Informationen aus Art. 4 Abs. 3 S. 2 Buchst. b EMFA, weil Mediendiensteanbieter nach Art. 2 Nr. 2 EMFA anders als die in § 53 Abs. 1 S. 1 Nr. 5 StPO genannten Personen auch juristische Personen sein können; zurückgestellt wird die Benachrichtigung nach § 101 Abs. 5 S. 1 StPO, der nach dem bisherigen Satz 2 entsprechend gilt. Nach demselben Satz gilt außerdem § 101 Abs. 7 S. 2 bis 4 StPO entsprechend, dessen besonderen nachträglichen Rechtsschutz die Entwurfsbegründung für die Sicherungsanordnung mangels Benachrichtigungspflicht verneint (BT-Drs. 21/6581, S. 49). Das Vollzitat der Verordnung steht in der Liste „EU-Rechtsakte“, die bei mehreren Rechtsakten nummeriert wird (Handbuch der Rechtsförmlichkeit, 4. Aufl., Rn. 195 und 197).

II (zu oben A und B): In Artikel 1 Nummer 4 wird in § 101a Absatz 1 Satz 1 Nummer 3 der Buchstabe a wie folgt gefasst:

„a) abweichend von § 100e Absatz 1 Satz 2 und 3 die Maßnahme bei Gefahr im Verzug auch durch die Staatsanwaltschaft und ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) angeordnet werden kann, die gerichtliche Entscheidung in diesem Fall unverzüglich nachzuholen ist, die Anordnung der Staatsanwaltschaft oder ihrer Ermittlungspersonen außer Kraft tritt, soweit sie nicht binnen drei Werktagen von dem Gericht bestätigt wird, und § 100e Absatz 1 Satz 5 nur für eine einmalige Verlängerung gilt,“

III (zu oben B): In Artikel 1 Nummer 4 wird dem § 101a Absatz 1 der folgende Satz angefügt:

„Soweit eine Sicherungsanordnung nach § 100g Absatz 7 außer Kraft tritt oder aufgehoben wird oder die Maßnahme nach Satz 1 in Verbindung mit § 100e Absatz 5 Satz 1 zu beenden ist, unterrichtet die Staatsanwaltschaft die Verpflichteten hierüber unverzüglich.“

IV (zu oben B): In Artikel 6 Nummer 2 wird in § 176 Absatz 2 Nummer 4 der Buchstabe b durch den folgenden Buchstaben b ersetzt:

„b) im Übrigen nach Ablauf der in der Sicherungsanordnung genannten Frist oder, soweit die Sicherung vorher endet, nach Eingang der Unterrichtung hierüber.“

Begründung: Die Änderung setzt das Erfordernis einer wirksamen gerichtlichen Kontrolle jeder Sicherungsanordnung um (EuGH, C-511/18 u. a., Rn. 163). Die Pflicht, die gerichtliche Entscheidung unverzüglich nachzuholen, ist § 101a Abs. 1 S. 2 Nr. 1 StPO-E nachgebildet (BT-Drs. 21/6581, S. 10) und genügt dem Erfordernis einer kurzfristigen Kontrolle in Eilfällen (EuGH, C-140/20, Rn. 110) sowie Art. 4 Abs. 4 Buchst. d EMFA. Weil § 176 Abs. 2 Nr. 4 Buchst. b TKG-E die Löschung nur an den Fristablauf knüpft (BT-Drs. 21/6581, S. 16), sichern die Änderungen unter III und IV bei Sicherungsanordnungen nach § 100g Abs. 7 StPO-E die Löschung, soweit die Sicherung früher endet, etwa weil sie nach § 101a Abs. 1 S. 1 StPO-E in Verbindung mit § 100e

Abs. 5 S. 1 StPO zu beenden ist (BT-Drs. 21/6581, S. 10); die Speicherdauer ist auf das absolut Notwendige zu beschränken (EuGH, C-511/18 u. a., Rn. 164).

V (zu oben B): In Artikel 1 Nummer 2 wird dem § 100g Absatz 7 der folgende Satz angefügt:

„Würde die Straftat nach Satz 1 Nummer 1 nur eine Erhebung nach Absatz 2 rechtfertigen, darf die Sicherungsanordnung nur Daten erfassen, die für eine Identifizierung des Anschlussinhabers anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse erforderlich sind; diese Daten dürfen nur zu diesem Zweck erhoben und verwendet werden.“

Begründung: Der Satz lehnt sich an § 177 Abs. 1 S. 1 Nr. 2 TKG-E an (BT-Drs. 21/6581, S. 17) und bindet die gesicherten Daten an die Identifizierung (EuGH, C-470/21, Rn. 101). Bei mittels Telekommunikation begangenen Straftaten, für welche die Begründung einen Bedarf sieht (BT-Drs. 21/6581, S. 40), bleibt so die Identifizierung anhand von IP-Adressen möglich.

Prof. Eike Richter