BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 52
Dezember 2022

zum

Referentenentwurf des Bundesministeriums der Justiz eines Gesetzes zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der StPO

vom 25.10.2022

Mitglieder des Ausschusses Datenschutzrecht

RA Klaus Brisch, LL.M.
RA Michael Dreßler
RAin Simone Eckert
RA Prof. Dr. Armin Herb, (Vorsitzender)
RAin Simone Kolb
RA Jörg Martin Mathis
RA Dr. Hendrik Schöttle
RA Prof. Dr. Ralph Wagner, LL.M.
RA André Haug, Vizepräsident BRAK
RA Sebastian Aurich, LL.M., BRAK

Mitglieder des Ausschusses Strafprozessrecht

Rechtsanwalt Dr. Matthias Dann
Rechtsanwalt Prof. Dr. Michael Gubitz
Rechtsanwältin Dr. Vera Hofmann (Berichterstatterin)
Rechtsanwalt Prof. Dr. Christoph Knauer (Vorsitzender)
Rechtsanwalt Dr. jur. Andreas Minkoff
Rechtsanwalt Maximilian Müller
Rechtsanwalt Jürgen Pauly
Rechtsanwältin Anette Scharfenberg
Rechtsanwältin Dr. Alexandra Schmitz
Rechtsanwältin Stefanie Schott
Rechtsanwalt Prof. Dr. Gerson Trüg
Rechtsanwältin Ulrike Paul, Vizepräsidentin Bundesrechtsanwaltskammer
Rechtsanwältin Eva Melina Buchmann, Bundesrechtsanwaltskammer

Verteiler: Bundesministerium des Innern und für Heimat
Bundesministerium der Justiz
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Landesdatenschutzbeauftragte
Rechtsausschuss des Deutschen Bundestages
Innenausschuss des Deutschen Bundestages
Arbeitskreise Recht der Bundestagsfraktionen
Landesjustizminister/Justizsenatoren der Länder
Rechtsanwaltskammern
Bundesnotarkammer
Bundessteuerberaterkammer
Bundesverband der Freien Berufe
Deutscher Anwaltverein
Deutscher Juristinnenbund
Deutscher Notarverein
Deutscher Richterbund
Neue Richtervereinigung e. V.
Patentanwaltskammer
Deutscher Steuerberaterverband e. V.
Wirtschaftsprüferkammer
Gesellschaft für Datenschutz und Datensicherheit e. V.
Berufsverband der Datenschutzbeauftragten Deutschlands e. V.
Deutsche Vereinigung für Datenschutz e. V.
Bitkom e. V.
davit – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e. V.
eco – Verband der Internetwirtschaft e. V.
VAUNET – Verband Privater Medien e. V.
Stiftung Datenschutz
Datenschutzberater
Computer und Recht
Redaktionen der NJW, ZAP, AnwBl, DRiZ, FamRZ, FAZ, Süddeutsche Zeitung, Die Welt,
taz, Handelsblatt, dpa, Spiegel, Focus, Deubner Verlag Online Recht, Beck aktuell, Jurion Expertenbriefing, Juris Nachrichten, LexisNexis Rechtsnews, Otto Schmidt Verlag

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Gegenstand

Das Bundesministerium der Justiz hat am 25.10.2022 einen Referentenentwurf eines Gesetzes zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der StPO in das Bundeskabinett eingebracht. Angesichts der mit diesem Regelungsvorhaben potenziell verbunden Auswirkungen auf die anwaltliche Tätigkeit und den Zugang aller Bürgerinnen und Bürger zum Recht nimmt die Bundesrechtsanwaltskammer (BRAK) bereits in diesem inoffiziellen Entwurfsstadium wie folgt Stellung und behält sich etwaig erforderlich werdende Ergänzungen ausdrücklich vor.

Zusammenfassende Bewertung

Jede Speicherung und Erhebung von Verkehrsdaten ist mit mannigfaltigen Risiken für die Rechte und Freiheiten der Kommunikationsteilnehmer[1] verbunden. Dies gilt insbesondere, wenn es sich dabei um Berufsgeheimnisträger handelt.

Die Bundesrechtsanwaltskammer (BRAK) begrüßt vor diesem Hintergrund den mit dem Referentenwurf verfolgten Ansatz einer in ihren Anforderungen und ihrem Umfang vergleichsweise maßvollen Regelung der Sicherung und des Zugriffs auf Verkehrsdaten. Begrüßenswert ist auch, dass auf anlass- und unterschiedslose Datensicherungen auf Vorrat – insbesondere auch mit Blick auf IP-Adressen – verzichtet wird. Zustimmungswürdig ist mit Einschränkungen auch die vorgeschlagene Beibehaltung des § 160a StPO, der nach zutreffender Einschätzung der Entwurfsautoren auf die nun eingeführten Regelungen zur Erhebung und Sicherung der Daten anwendbar ist und diesbezüglich einen gewissen – jedoch nicht ausreichenden – Schutz der anwaltlichen Verschwiegenheit und so mittelbar auch des Zugangs zum Recht bietet.

Indes kann auch der nun vorgelegte Regelungsentwurf die eingangs erwähnten Risiken – namentlich in Bezug auf Mandatskontakte – nicht vollständig ausräumen. Er begegnet überdies trotz aller Einschränkungen grundsätzlichen Bedenken mit Blick auf die Grundsätze der Erforderlichkeit und Angemessenheit.

Insbesondere im Interesse eines umfassenden Mandatsgeheimnisschutzes sollte daher auch von der nun vorgelegten Lösung Abstand genommen und auf die vorgeschlagenen Erhebungs- und Sicherungsbefugnisse verzichtet werden.

Zumindest muss eine weitergehende Risikominimierung durch folgende Maßnahmen erfolgen:

1) **Beibehaltung des derzeitigen § 100g Abs. 4 StPO**

2) **Ergänzung des derzeitigen § 100g Abs. 4 StPO um Vorgaben zur Aussonderung von Daten zu Berufsgeheimnisträgern**

[1] Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die im Folgenden willkürlich gewählte weibliche oder männliche Form schließt alle Geschlechter gleichberechtigt ein.

3) **Beibehaltung der gegenwärtig in §§ 176 – 181 TKG vorgesehenen Datenschutz- und Datensicherheitsvorschriften**

4) **Eingrenzende Definition des Verkehrsdatenbegriffs in § 100b Abs. 1 StPO-E**

5) **Klarstellung in § 100g Abs. 5 StPO-E, dass keine zusätzlichen Datenerhebungen durch Telekommunikationsanbieter angeordnet werden können**

Keinesfalls darf den – etwa aus dem Bundesministerium des Innern und für Heimat zu vernehmenden – Forderungen nach einer anlass- und unterschiedslosen Vorratsspeicherung von IP-Adressen und gegebenenfalls weitere Datenkategorien nachgegeben werden, da hiermit erhebliche zusätzliche Risiken für das Mandatsgeheimnis und weitere (Grund-)Rechte verbunden wären.

Die BRAK bittet um frühzeitige Einbindung in die Konzeption eines Verfahrens zur Aussonderung zu Berufsgeheimnisträgerdaten.

Inhalt

Stellungnahme

Der vorgelegte Referentenentwurf enthält im Vergleich zur derzeit vorgesehenen Vorratsdatenspeicherung eine Reihe begrüßenswerter Elemente. Angesichts seiner nach wie vor erheblichen Eingriffstiefe – insbesondere mit Blick auf das Mandatsgeheimnis – sind diese jedoch nicht ausreichend, um die skizzierten Datensicherungen und -erhebungen zu rechtfertigen. Daher sollte auf diese verzichtet werden. Alternativ bedürfte es zumindest einer Reihe zusätzlicher Sicherungsmaßnahmen und Eingriffsbegrenzungen.

1. Eingriffstiefe

Zwar würden durch den skizzierten Verzicht auf massenhafte Vorratsdatenspeicherungen im Vergleich zur derzeitigen gesetzlichen Regelung die Risiken für die davon potentiell Betroffenen gesenkt. Dies darf aber nicht darüber hinwegtäuschen, dass die nun vorgelegten Erhebungs- und Sicherungsbefugnisse immer noch eine erhebliche Eingriffstiefe für die davon betroffenen und überwiegend tatunbeteiligten Personen bergen. Diese reicht von der Möglichkeit der Offenbarung einer Kontaktaufnahme zu einer Rechtsanwältin bis hin zur – nach wie vor nicht ausgeschlossenen – Möglichkeit einer Profilbildung oder eines sonstigen Datenmissbrauchs (siehe im Einzelnen auch unten unter 1., 3.1 und 4.1). Dies gilt insbesondere mit Blick auf die in § 100g Abs. 5 StPO-E vorgesehene Sicherungsanordnung, die nach der Entwurfsbegründung einen bewusst weiten Kreis von Personen mit Bezug zum Opfer oder Tatort erfassen soll (S. 31 des Entwurfs). Für tatunbeteiligte Mitbetroffene macht es im Ergebnis keinen Unterschied, ob deren Daten aufgrund einer nun vorgesehenen Sicherungsanordnung oder der derzeit gültigen Regelung zur Vorratsdatenspeicherung gespeichert bzw. abgerufen werden. Ihr Kommunikationsverhalten kann dann gleichermaßen über bis zu 3 Monate (§ 101a Abs. 1a Nr. 1 StPO-E) ausgewertet und Kontaktaufnahmen etwa zu einer Rechtsanwaltskanzlei, einer Seelsorgeeinrichtung, einer Redaktion, einer Abtreibungsklinik, einer politischen Vereinigung oder einer dem privaten Kernbereich zuzuordnenden Freizeiteinrichtung offenbart werden. Die Sicherung bzw. der Abruf der Daten kann standort- oder ereignisgebunden erfolgen – etwa, weil, wie wohl häufig gegeben, im Umfeld eines Bahnhofs, Flughafens oder einer Großveranstaltung ein Anfangsverdacht[2] bezüglich einer Straftat von erheblicher Bedeutung erkannt wird. Dies führt dazu, dass jedenfalls in derartigen Bereichen alle Bürgerinnen und Bürger mit Einblicken in ihr Kommunikationsverhalten rechnen müssen. Insoweit ist also auch das vom Bundesverfassungsgericht beanstandete Gefühl des Überwachtwerdens (BVerfGE 65, 1 – Volkszählung; 107, 299 – Fernmeldegeheimnis, 115, 320 – Rasterfahndung II) keinesfalls hinreichend beseitigt. Angesichts der erheblichen Anzahl von Personen, die derartige Orte und Veranstaltungen tagtäglich und oft auch regelmäßig frequentieren, wird man den Umfang dieser Beeinträchtigungen auch weiterhin als massenhaft und andauernd bezeichnen müssen. Wer an einem entsprechenden Ort oder auf derartigen Veranstaltungen arbeitet, wird rund um die Uhr mit entsprechender Datensicherung rechnen müssen und damit dem Gefühl des Überwachtwerdens im Sinne der genannten Bundesverfassungsgerichtsendscheidungen in besonderem Maße unterliegen. Aufgrund des in § 100g Abs. 1 StPO-E vorgesehenen Verweises auf den umfangreicheren Straftatenkatalog des § 100a Abs. 2 StPO stiege für tatunbeteiligte Mitbetroffene sogar die Gefahr, dass ihre Verkehrsdaten eingesehen werden. Ferner wären von der vorgeschlagenen Sicherungsanordnung potentiell mehr Datenkategorien erfasst als dies nach der derzeitigen Vorratsdatenspeicherregelung der Fall ist (siehe unten 4.1). Verletzungen des Mandatsgeheimnisses werden ebenfalls mitnichten ausgeschlossen (siehe unten 3.1).

[2] Die in § 100g Abs. 5 StPO-E genannten Voraussetzungen entsprechen einem solchen – so auch Kiparski, *Die Vorgaben des EuGH zur Vorratsdatenspeicherung und ihre Umsetzung im jüngsten Referentenentwurf,* Computer und Recht 11/2022, S. 715, 721

2. Erforderlichkeit und Angemessenheit

Auch wenn der mit dem Entwurf verfolgte Quick-Freeze-Ansatz in der Entscheidung *Spacenet* und *Telekom Deutschland* des EuGH eine grundsätzliche Anerkennung gefunden hat, muss, auch nach dem Wortlaut des EuGH-Urteils selbst, jede Maßnahme auf das absolut Notwendige und Angemessene reduziert bleiben (vgl. EuGH-Urteil vom 20.09.2022, 20. September 2022 – C-793/19 und C-794/19 Rn. 67). Diese Grenzen werden mit dem vorliegenden Entwurf im Allgemeinen und insbesondere mit Blick auf Beeinträchtigungen des Mandatsgeheimnisses überschritten. Letztere scheinen vom EuGH mit Blick auf seine in den Entscheidungen *Spacenet und Telekom* sowie *La Quadrature du Net* aufgestellten Zulässigkeitsmaßstäbe (noch) nicht berücksichtigt worden zu sein, werden sie darin doch nicht einmal erwähnt. Bei gehöriger Berücksichtigung auch dieser Beeinträchtigungen ist indes ein (noch) strengerer Zulässigkeitsmaßstab anzulegen.

Die Erforderlichkeit der vorgeschlagenen Maßnahmen erscheint auch vor dem Hintergrund zweifelhaft, dass, wie die Entwurfsverfasser zutreffend einräumen, in der Vergangenheit ohne die vorgeschlagenen Instrumente bereits über 90-prozentige Aufklärungsraten zu verzeichnen waren. Jedenfalls von einer Ausweitung der Datensicherungen – etwa in Richtung der vom Bundesinnenministerium geforderten Vorratsdatenspeicherung von IP-Adressen – muss daher dringend abgesehen werden.

3. Schutz der anwaltlichen Verschwiegenheit

Die anwaltliche Verschwiegenheit ist eine Grundvoraussetzung für die Inanspruchnahme rechtsanwaltlicher Beratung und des Zugangs zum Recht und damit ein Grundpfeiler eines jeden Rechtsstaats. Sie unterfällt dem Schutz der europäischen wie nationalen Rechtsstaatsgarantien aus Art. 47 Abs. 1 Satz 2 GRCh, Art. 6 Abs. 1 Satz 1, Abs. 3 lit. c EMRK sowie Art. 20 Abs. 2 GG, Art. 103 Abs. 1 GG. Zugleich ist sie im Kontext anwaltlicher Beratung Voraussetzung für die Verwirklichung europäischer wie nationaler Grundrechte aus Art. 6 Abs. 1 Satz 1, Abs. 3 lit. c EMRK, Art. 47 Abs. 1, 2 Satz 2 GRCh, Art. 20 Abs. 3, Art. 103 Abs. 1 GG, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK, Art. 7 GRCh, Art. 12 Abs. 1 GG. Sie dient in erster Linie dem Schutz der Mandantschaft und ihres Zugangs zum Recht. Rechtsuchende müssen sich darauf verlassen können, dass ihre Kontaktaufnahme zu bzw. ihre Kommunikation mit einem Rechtsanwalt oder einer Rechtsanwältin niemandem offenbart wird. Anderenfalls werden sie in vielen Fällen von einer rechtlichen Beratung Abstand nehmen und in ihrer adäquaten Rechtsausübung beschränkt sein. In diesen Fällen wird zugleich die Anwaltschaft in ihrer Berufsausübungsfreiheit beeinträchtigt. Das Erfordernis entsprechender Schutzmaßnahmen auch und gerade im Rahmen von Überwachungsmaßnahmen wurde mehrfach verfassungsgerichtlich bestätigt. Die Entwurfsbegründung erkennt diesen Schutzbedarf ausdrücklich an und verweist zutreffend drauf, dass § 160a StPO insoweit einen gewissen Schutz biete (S. 27). Ausreichend ist dieser Schutz jedoch aus den nachstehenden Gründen nicht.

3.1 Schutz des Mandatsgeheimnisses praktisch nur begrenzt zu erreichen

Ungeachtet der rechtlichen Ausgestaltung wird ein Schutz von Mandatskontakten bereits aus praktischen Gründen nicht in hinreichendem Maße gewährleistet werden können.

3.1.1 Aussonderungen von Mandatskontakten schwierig

So stellt sich mit Blick auf § 160a Abs. 1 StPO ebenso wie im Rahmen des derzeit noch für die Vorratsdatenspeicherung geltenden § 100g Abs. 4 StPO das Problem, dass diese ihre Schutzwirkung nur insoweit entfalten könnten als überhaupt ersichtlich ist, dass Berufsgeheimnisträger bzw.

Mandatskommunikationen betroffen sind.[3] Dies ist aber nur in der überschaubaren Anzahl der Fälle gegeben, in denen bereits einer der betroffenen Kommunikationsteilnehmer als Berufsgeheimnisträger bekannt ist. Insbesondere in den vielen zu erwartenden Fällen, in denen Tatbeteiligte bzw. deren Kontaktpersonen durch die Anordnung überhaupt erst ermittelt werden sollen und daher noch gar nicht klar ist, welche und wessen Daten erhoben bzw. gesichert werden sollen, wird der Schutz des § 160a Abs. 1 StPO daher genauso selten greifen wie der des derzeitigen § 100g Abs. 4 StPO. Hinzu kommt, dass Ermittlungsbehörden regelmäßig nicht alle Anschluss- bzw. Verbindungsinformationen von Berufsgeheimnisträgern kennen werden, weshalb diese nicht aussortiert werden können.

Aber auch in Fällen, in denen Ermittlungsbehörden Anschlussinformationen von Berufsgeheimnisträgern bekannt sind und solche aussortiert werden, werden sich Verletzungen des Mandatsgeheimnisses nicht gänzlich vermeiden lassen.

So können Berufsgeheimnisträger aus technischen oder organisatorischen Gründen gezwungen sein, kurzfristig andere Anschlüsse oder ein VPN zu benutzten. Dies gilt insbesondere bei eiligen Rechtsangelegenheiten. Derart genutzte Anschlüsse werden sich nicht aussortieren lassen.

3.1.2 Verbleibende Erhebung der Kontaktaufnahme

Vor allem aber wird sich ein Aussortieren der Berufsgeheimnisträger-Anschlüsse in den seltensten Fällen so gestalten lassen, dass dabei auch die zentrale und kritische Information, dass ein Mandant bzw. eine Mandantin überhaupt Kontakt zu einer Kanzlei aufgenommen hat, nicht erfasst wird. Es wird insoweit also ganz überwiegend lediglich das Verwendungsverbot des § 160a Abs. 1 Satz 1 Variante 2 StPO greifen können. Damit ist aber dem Sinn und Zweck des Mandatsgeheimnisses, dass sich die Mandantschaft nämlich darauf verlassen kann, dass bereits der Umstand an sich und ggf. auch die Häufigkeit der Kontaktaufnahme zur Kanzlei unerkannt bleiben, nicht mehr gedient. Durch § 160a Abs. 1 Satz 1 Variante 2 StPO können nur noch die Folgen der Offenbarung – in sehr begrenztem Umfang – gemildert werden. Die rechtsstaatliche Funktion des Mandatsgeheimnisses wird dadurch indes nicht mehr sichergestellt (siehe zu diesem Aspekt ausführlich: BRAK-Stellungnahme 32/2015 unter B.I.2.).

3.1.3 Änderungsbedarf zum Schutz des Mandatsgeheimnisses

Zum Schutz des Mandatsgeheimnisses ist daher Nachstehendes geboten.

3.1.3.1 Verzicht auf die Verkehrsdatenerhebung

Der vorgelegte Entwurf kann aus den skizzierten praktischen Gründen – auch in abgewandelter Form – keinen umfassenden Schutz des Mandatsgeheimnisses gewährleisten. Dies wäre vielmehr nur durch einen Verzicht auf die skizzierte Datensicherung bzw. -erhebung zu erreichen, zu welchem die BRAK daher primär aufruft.

3.1.3.2 Hilfsweise: Absenkung des Erhebungs- bzw. Sicherungsumfangs und flankierende Schutzmaßnahmen

Soweit sich ein solcher Verzicht – etwa aufgrund der Festlegungen des Koalitionsvertrages – politisch nicht durchsetzen lässt, sollten zumindest der Umfang der Datensicherungen bzw. -erhebungen weitestmöglich reduziert und damit verbundene Risiken durch weitere horizontale Schutzmechanismen (siehe unten unter 4.) gemindert werden. Ferner sollten weitergehende Sicherungsmaßnahmen speziell

[3] vgl. auch Kiparski, Die Vorgaben des EuGH zur Vorratsdatenspeicherung und ihre Umsetzung im jüngsten Referentenentwurf, Computer und Recht 11/2022, S. 715, 721

zum Schutz des Mandatsgeheimnisses und gegebenenfalls anderer Berufsgeheimnisse eingeführt werden (siehe dazu sogleich unter 3.2 und 3.3).

3.2 Vermeidung der mit einer Streichung des derzeitigen § 100g Abs. 4 StPO verbundenen Risiken für den Schutz des Mandatsgeheimnisses und weiterer Vertraulichkeitstatbestände

In seiner gegenwärtigen Fassung enthält § 100g Abs. 4 StPO eine Spezialvorschrift zum Schutz von Zeugnisverweigerungsberechtigten und namentlich von Berufsgeheimnisträgern. Diese wird nach der Entwurfsbegründung (S. 27) angesichts des für die nun eingeführten Datenerhebungs- bzw. Sicherungsbefugnisse ebenfalls einschlägigen § 160a Abs. 1 Satz 1 StPO für entbehrlich erachtet und soll daher gestrichen werden. Dies sollte aus den nachstehenden Gründen nicht erfolgen.

3.2.1 Entfallende Appellfunktion und fehlende Klarstellung

In der Entwurfsbegründung (S. 27) wird zutreffend ausgeführt, dass § 160a StPO „auch für das neue Ermittlungsinstrument der Sicherungsanordnung“ gelte. Bemerkenswert ist in diesem Zusammenhang, dass in der restlichen Entwurfsbegründung gleichwohl konsequent nur noch von der „Erhebung“ der Daten bzw. einem „grundsätzlichen Erhebungsverbot“ die Rede ist. Möglicherweise sind die Autoren insoweit ihrer eigenen Konsolidierung zum Opfer gefallen und haben die zunächst selbst erkannte Anwendbarkeit des § 160a StPO auf den neuen Sachverhalt aus den Augen verloren. Mit Blick auf künftige Rechtsanwender sollte daher bereits in § 100g StPO jeder Zweifel ausgeräumt und unmissverständlich hervorgehoben werden, dass (im Mindesten) der in § 160a StPO postulierte Schutzmaßstab bereits auf der Ebene der Datensicherung zu beachten ist. Auch aus diesem Grund sollte der derzeitige § 100g Abs. 4 StPO mit einigen Änderungen (siehe dazu sogleich unter 3.2.2 und 3.3) beibehalten werden.

3.2.2 Regelungsvorschlag

§ 100g Abs. 4 StPO sollte daher im Grundsatz in folgender Abwandlung beibehalten werden:

> *„Die Erhebung und Sicherung von Verkehrsdaten nach ….“ (im Folgenden unverändert bzw. wie unter 3.3 vorgeschlagen).*

3.3 Konkrete Verpflichtung zur (Bemühung um) Aussortierung von Berufsgeheimnisträgerdaten erforderlich

Es muss sichergestellt werden, dass alle Möglichkeiten einer frühzeitigen Aussonderung von Berufsgeheimnisträgerdaten ausgeschöpft werden. Zugleich muss das Risiko, dass in diesem Zuge Kenntnis von einer Kontaktaufnahme zu einem Rechtsanwalt oder einer Rechtsanwältin genommen wird, minimiert werden. Dem Prinzip der Nichterhebung bzw. -sicherung ist dabei der Vorzug vor einem Verwertungsverbot einzuräumen.

Soweit die Sicherung bzw. Erhebung von Berufsgeheimnisträgerdaten aus technischen Gründen nicht zu vermeiden ist, muss zum Zwecke der Aussonderung ein frühzeitiger Abgleich der potentiell zu erhebenden Daten mit den von den berufsständischen Kammern veröffentlichten Kommunikationsdaten und Anschlussinformationen der Berufsträger sowie gegebenenfalls weiteren von Berufsgeheimnisträgern angegebenen Telekommunikationsdaten vorgesehen werden. Dieser muss so erfolgen, dass die Kontaktaufnahme zu einem Berufsgeheimnisträger weder positiv (z. B. „Rechtsanwältin Maximiliane Musterfrau“) sowie nach Möglichkeit auch nicht negativ („z. B. darf nicht angezeigt werden) zu erkennen ist, also zumindest den ermittelnden Personen nicht angezeigt wird.

Die BRAK steht für Gespräche über die Ausgestaltung des automatischen Abgleichs mit den im Bundesweiten Amtlichen Anwaltsverzeichnis (BRAV) veröffentlichten Daten jederzeit zur Verfügung und bittet um eine frühzeitige Einbindung in dessen Konzeption. Ebenfalls darin einzubinden sein werden die gemäß § 100g StPO zur Erhebung, Anordnung bzw. Sicherung befugten bzw. potentiell verpflichteten Stellen (z. B. Ermittlungs- und Telekommunikationsbehörden).

Es muss gewährleistet sein, dass für die diesbezüglichen Datenverarbeitungen hinreichende gesetzliche Grundlagen zur Verfügung stehen. So bedarf es möglicherweise, je nach konkreter Ausgestaltung, parallel zur Anordnung des Datenabgleichs entsprechender Abruf- bzw. Übermittlungsbefugnisse seitens der Kammern bzw. Ermittlungsbehörden. Nach Ansicht der BRAK wären Datenabrufe durch bzw. Datenübermittlungen an die Ermittlungsbehörden bereits auf der Grundlage des derzeitigen § 31 Abs. 2 BRAO hinreichend legitimiert. Sofern man den Anwendungsbereich des § 31 Abs. 2 Satz 1 BRAO indes für auf den Rechtsverkehr im eigentlichen Sinne beschränkt erachtete („sonstige am Rechtsverkehr Beteiligte“), wäre eine ergänzende Befugnis erforderlich.

Regelungsvorschlag:

Die grundlegende Festlegung eines solchen Aussonderungsprozesses könnte in § 100g Abs. 4 StPO vor dem derzeitigen Satz 2 sowie in § 175 TKG erfolgen. Gegebenenfalls weitergehend datenschutzrechtlich erforderliche Rechtsgrundlagen könnten daneben in den Berufsordnungen der Berufsgeheimnisträger – im Falle der Anwaltschaft etwa in § 31 Abs. 2 BRAO – implementiert werden. Die technischen Einzelheiten des Abgleichs sollten zweckmäßigerweise einer Verordnung des Bundesministeriums der Justiz vorbehalten bleiben.

4. Risikominimierung durch allgemeine Reduzierung des Erhebungs- bzw. Sicherungsumfangs und Sicherungsmechanismen

Da ein vollständiger Schutz des Mandatsgeheimnisses aus praktischen Gründen nicht zu erzielen ist (siehe dazu oben unter 3.1.), muss das Risiko der Offenbarung von Mandatsinformationen und namentlich von Kontaktaufnahmen zu Rechtsanwältinnen bzw. Rechtsanwälten durch horizontal wirkende Maßnahmen zur Reduzierung von Vertraulichkeitseingriffen gemindert und deren Eingriffsintensität abgemildert werden. Dies ist auch zum Schutz anderer (Grund-)Rechtspositionen wie etwa der informationellen Selbstbestimmung geboten. Nicht zuletzt kann nur auf diese Weise den verfassungs- und primärrechtlichen Grundsätzen der Erforderlichkeit bzw. Angemessenheit genügt werden (siehe oben unter 2.).

Folgende Änderungen sollten in diesem Sinne vorgenommen werden:

4.1 Umfang der Sicherungsanordnung: Engere Definition und expliziter Ausschluss zusätzlicher Erhebungen erforderlich

Der Entwurf verzichtet auf eine Auflistung der von einer Sicherungsanordnung umfassten Daten. Begründet wird dies damit, dass die möglichen zu speichernden Verkehrsdaten durch die Verweisung in § 100g Abs. 1 Satz 1 StPO-E in §§ 9 und 12 des TTDSG und § 2a Abs. 1 des BDBOS-Gesetzes abschließend definiert seien (S. 36).

Dabei wird außer Acht gelassen, dass dies zu einer potentiell weiteren Definition des Verkehrsdatenbegriffs und unter Umständen zu umfangreicheren Datenspeicherungen führt als derzeit gemäß § 176 TKG für die Vorratsdatenspeicherung vorgesehen. Denn in §§ 9 und 12 TTDSG wird lediglich die Verwendung einiger Verkehrsdaten geregelt, die dort maßgebliche Definition demgegenüber findet sich in

§ 3 Nr. 70 TKG.[4] Danach wären alle Daten erfasst, deren Erhebung, Verarbeitung oder Nutzung für die Erbringung eines Telekommunikationsdienstes erforderlich ist. Es sollte klargestellt werden, dass nur im Anwendungsbereich der genannten Vorschriften verarbeitete Verkehrsdaten erfasst sein sollen oder eine dem bisherigen § 176 TKG entsprechende Auflistung erfolgen.

Ungeachtet der Frage, ob die in Absatz 1 gewählte Definition für normenklar und angemessen erachtet wird, sollte klargestellt werden, dass eine Sicherungsanordnung nur solche Daten erfassen kann, die von den Telekommunikationsanbietern ohnehin erhoben werden und dass demgegenüber keine Sicherung zusätzlicher Daten angeordnet werden kann.

> **Regelungsvorschlag:** § 100g Abs. 1 und 5 StPO-E sollte wie folgt ergänzt werden:
>
> *„(1) Verkehrsdaten, **die gemäß** (§§ 9 und 12 des Telekommunikation-Telemedien-Datenschutz-Gesetzes ~~und~~ **oder** § 2a Absatz 1 des BDBOS-Gesetzes **verarbeitet werden**),~~,~~ **sowohl** des Beschuldigten sowie von Personen, bei denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt, dürfen erhoben werden, wenn…*
>
> ***…***
>
> *…*
>
> *(5) Auch ohne das Wissen des Betroffenen darf angeordnet werden, dass die in § 175 Absatz1 Satz 1 des Telekommunikationsgesetzes bezeichneten Anbieter öffentlich zugänglicher Telekommunikationsdienste die bei der Nutzung des Dienstes bereits erzeugten oder verarbeiteten sowie künftig anfallenden **und vom Anbieter im ordnungsgemäßen Geschäftsgang ohnehin gemäß §§ 9 und 12 TTDSG bzw. § 2a Absatz 1 des BDBOS-Gesetzes zu erhebenden** Verkehrsdaten unverzüglich zu sichern haben (Sicherungsanordnung), wenn zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass eine in Absatz 1 bezeichnete Straftat begangen worden ist, und soweit die Verkehrsdaten für die Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Beschuldigten von Bedeutung sein können. Die Erhebung der nach Satz 1 gesicherten Daten erfolgt nach den Absätzen 1 und 3.“*
>
> (Hinzufügungen hervorgehoben)

4.2 Sicherungsmechanismen: Beibehaltung der §§ 176-181 TKG erforderlich

Angesichts der nach wie vor teils erheblichen und über bloß geschäftliche Datenverarbeitungen hinausgehenden Eingriffstiefe sollten die derzeit in den §§ 176-181 TKG vorgesehenen Datenschutz- und Datensicherheitsvorschriften entgegen der im Entwurf (S. 36) geäußerten Einschätzung im Wesentlichen beibehalten bzw. in das TTDSG überführt werden.

* * *

[4] So auch Kiparski, *Die Vorgaben des EuGH zur Vorratsdatenspeicherung und ihre Umsetzung im jüngsten Referentenentwurf,* Computer und Recht 11/2022, S. 715, 729