BUNDESKANZLERAMT VERFASSUNGSDIENST

GZ ● BKA-601.598/0003-V/5/2017
ABTEILUNGSMAIL ● V@BKA.GV.AT
IHR ZEICHEN ●BMI-LR1340/0019-III/1/2017

An das
Bundesministerium für Inneres

Herrengasse 7
1010 Wien

Antwort bitte unter Anführung der GZ an die Abteilungsmail

Entwurf eines Bundesgesetzes, mit dem das Sicherheitspolizeigesetz, das Bundesstraßen-Mautgesetz 2002, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden;
Begutachtung; Stellungnahme

Zu dem mit der do. oz. Note übermittelten Gesetzesentwurf nimmt das Bundeskanzleramt-Verfassungsdienst wie folgt Stellung:

I. Allgemeines

Es wird darauf hingewiesen, dass die Übereinstimmung des im Entwurf vorliegenden Bundesgesetzes mit dem Recht der Europäischen Union vornehmlich vom do. Bundesministerium zu beurteilen ist.

II. Inhaltliche Bemerkungen

Zu Art. 1 (Änderung des Sicherheitspolizeigesetzes):

Zu Z 2 (§ 25 Abs. 1):

Ein Informationsaustausch soll nach dem vorgeschlagenen Gesetzestext zulässig sein, wenn es sich um Informationen handelt, die den Teilnehmern dem Grunde nach bekannt sind oder deren Weitergabe im wesentlichen Interesse Betroffener ist, und nicht besondere Gründe vorliegen, die dennoch für eine Geheimhaltung sprechen.

Die Erläuterungen sprechen von einer „Klarstellung, wie sich die Amtsverschwiegenheit zum Informationsaustausch im Sicherheitsforum verhält“. Die Amtsverschwiegenheit gilt nur für staatliche Organe; an den Sicherheitsforen sollen aber gerade auch Private teilnehmen. Auch der vorgeschlagene Gesetzestext scheint allgemein den Informationsaustauch im Sicherheitsforum zu regeln. Soll mit

der vorgeschlagenen Regelung hingegen – auch – die Amtsverschwiegenheit geregelt werden, sollte dies im Gesetzestext entsprechend (in Anlehnung an Art. 20 Abs. 3 B-VG) formuliert werden.

Des Weiteren sollte – zumindest in den Erläuterungen – das Verhältnis des § 25 Abs. 1 letzter Satz zum vorgeschlagenen § 56 Abs. 1 Z 9 geklärt werden: Insbesondere sollte klargestellt werden, dass die Ermächtigung zur Übermittlung personenbezogener Daten an die Teilnehmer eines Sicherheitsforums gemäß § 56 Abs. 1 Z 9 nur bei Vorliegen der in § 25 Abs. 1 letzter Satz festgelegten Voraussetzungen zulässig ist. In diesem Fall wäre zu überprüfen, warum es einen Vorrang der Ermächtigung zur Datenübermittlung gegenüber den Geheimhaltungsinteressen der Betroffenen geben soll.

Zu Z 3 und 12 (§ 53 Abs. 5 und § 91c Abs. 3):

1. Nach den Erläuterungen bezieht sich die Verwendungsermächtigung des § 53 Abs. 5 erster Satz auf Bild- und Tondaten, die den Sicherheitsbehörden „freiwillig“ von Rechtsträgern des öffentlichen oder privaten Bereichs übergeben werden. Die Beschränkung auf „freiwillig“ übergebene Daten fehlt im Gesetzestext und sollte ausdrücklich normiert werden.

Die §§ 50a ff DSG 2000 erfassen Tonaufnahmen nicht. Es stellt sich daher die Frage, auf Grund welcher Rechtsgrundlage Rechtsträger des privaten Bereichs überhaupt rechtmäßig Tondaten ermitteln dürfen.

2. Der vorgeschlagene § 53 Abs. 5 ermöglicht den Sicherheitsbehörden einen unmittelbaren Zugriff auf eine Vielzahl umfangreicher – auch privater – Videoüberwachungssysteme, die zusammen weite Teile des öffentlichen Raumes abdecken. Angesichts der besonderen Grundrechtssensibilität dieser Maßnahme ist besonderes Augenmerk auf ihre verhältnismäßige Ausgestaltung zu legen.

Im Vergleich zu den geltenden engen Voraussetzungen für Bildaufzeichnungen vom öffentlichen Raum durch die Sicherheitsbehörden (zB Überwachung von gefahrengeneigten Orten [„Hot Spots“] gemäß § 54 Abs. 6 SPG oder Mitfilmen bei Demonstrationen gemäß § 54 Abs. 5 SPG) sind die Voraussetzungen für die Zugriffsmöglichkeiten nach dem vorgeschlagenen § 53 Abs. 5 letzter Satz wesentlich gelockert. Insgesamt sollte daher geprüft werden, inwieweit es möglich ist, auf gesetzlicher Ebene absolute Grenzen hinsichtlich Dauer und Umfang der Zugriffsmöglichkeit festzulegen.

Fraglich ist, ob diese Zugriffsermächtigung unabhängig von den Voraussetzungen der Ermächtigung des ersten Satzes besteht; dies ist insbesondere deswegen von Bedeutung, weil lediglich die Ermächtigung nach dem ersten Satz eine Beschränkung auf den „Einzelfall“ vorsieht. Fraglich ist auch, weshalb § 53 Abs. 5 zweiter Satz eine besondere Achtung der Verhältnismäßigkeit nur für Datenverarbeitungen nach § 53 Abs. 5 erster Satz anordnet.

Gerade auch aufgrund der großen Zahl an (völlig unbeteiligten) Personen, die von dieser Maßnahme betroffen sind, bedarf es einer engen Zweckbegrenzung. Es ist fraglich, ob dies derzeit ausreichend gewährleistet ist, scheint doch beispielsweise der Zweck der Vorbeugung wahrscheinlicher gefährlicher Angriffe gegen das Vermögen ein äußerst weites Einsatzgebiet dieser Maßnahme zu eröffnen.

Der Begriff „öffentlicher Versorgungsauftrag“ sollte genauer erläutert werden; Gleiches gilt für den Begriff des „öffentlichen Raumes“, zumal damit offenbar auch Bereiche gemeint sind, die nicht ohne weiteres von jeder Person betreten werden können (dies legt zumindest die Erwähnung der Flughäfen in den Erläuterungen nahe). Klarstellungsbedürftig erscheint auch das Verbot der „Verwendung von Daten über nichtöffentliches Verhalten“. Nachdem die Maßnahme nur die Überwachung des öffentlichen Raumes erlaubt, stellt sich die Frage, welches erfasste Verhalten als „nichtöffentlich“ gilt.

Ferner sollten Datensicherheitsmaßnahmen für den Fall des Echtzeitstreamings angeordnet werden. Außerdem stellt sich die Frage, ob die Sicherheitsbehörden berechtigt sein sollen, die ihnen im Wege des Echtzeitstreamings zugänglichen Bilddaten zu speichern.

3. Nach geltendem Recht ist dem Rechtsschutzbeauftragten bei einer Überwachung von „Hot Spots“ oder öffentlichen Orten nach § 54 Abs. 6 und 7 SPG Gelegenheit zur Äußerung binnen dreier Tage zu geben; der Einsatz der Bild- und Tonaufzeichnungsgeräte darf erst nach Ablauf der Frist oder einer Äußerung des Rechtsschutzbeauftragten erfolgen (§ 91c Abs. 2). Hingegen soll nach dem vorgeschlagenen § 91c Abs. 3 bei einem Verlangen nach Zugang zu Bilddaten gem. § 53 Abs. 5 dritter Satz für einen Zeitraum von bis zu drei Tagen der Rechtsschutzbeauftragte lediglich zu verständigen sein. Dies sollte überprüft werden.

Zu Z 5 (§ 54 Abs. 4b):

Der geltende § 54 Abs. 4b lässt eine verdeckte automatisierte Kennzeichenerfassung ausschließlich für Zwecke der Fahndung zu und beschränkt diese Möglichkeit auf die Dauer eines Monats. Nach dem Entwurf sollen nicht nur das Kennzeichen sowie weitere Daten über das Fahrzeug, sondern auch Daten zur Identifizierung des Fahrzeuglenkers verarbeitet werden dürfen. Des Weiteren soll die Beschränkung auf einen Monat entfallen, womit eine unbefristete Überwachung möglich ist. Zudem sollen die Daten nicht mehr nur zur Fahndung, sondern auch zur Abwehr und Aufklärung bestimmter gefährlicher Angriffe bzw. zur Abwehr krimineller Verbindungen verarbeitet werden dürfen. Sämtliche erhobenen Daten sollen außerdem – unabhängig von einem konkreten Verdacht auf einen Zusammenhang mit einer strafbaren Handlung – für bis zu 48 Stunden gespeichert werden dürfen.

2. Auch wenn die Speicherdauer zeitlich beschränkt ist, weist diese anlasslose und umfassende Speicherung personenbezogener Daten aller Verkehrsteilnehmer deutliche Parallelen zu jenen Formen der Vorratsdatenspeicherung auf, die in der Vergangenheit vom EuGH (vgl. verb. Rs C-293/12 und C-594/12, Digital Rights, vom 8.4.2014; verb. Rs C-203/15 und C-698/15, Tele2 Sverige AB, vom 21.12.2016) sowie VfGH (VfSlg. 19.892/2014) als rechtswidrig erklärt wurden. Eine Vorratsdatenspeicherung ist nach der Judikatur nur unter engen Voraussetzungen zulässig: Sie muss der Bekämpfung schwerer Straftaten dienen, die Speicherung muss auf das absolut Notwendige beschränkt sein und sie bedarf der vorherigen Kontrolle durch eine unabhängige Behörde. Um die Verhältnismäßigkeit der Maßnahme zu wahren, sollte zudem klargestellt werden, dass nach der Erfassung der Daten zunächst ausschließlich das Kennzeichen mit der Fahndungsevidenz abgeglichen werden darf und nur im Trefferfall auch die restlichen Daten zu den genannten Zwecken verwendet werden dürfen.

Zu Z 6 (§ 56 Abs. 1 Z 9 und 10):

1. Es sollte – zumindest in den Erläuterungen – klargestellt werden, dass die Datenübermittlung für die Zwecke der Z 9 und 10 nur „im unbedingt erforderlichen Umfang“ erfolgen darf.

2. Die Erläuterungen stellen klar, dass eine Bekanntgabe personenbezogener Daten nach Z 9 nur im „Einzelfall“ erlaubt ist. Dies sollte auch im Normtext festgelegt werden. Siehe im Übrigen die Ausführungen zu Z 2 (§ 25 Abs. 1).

3. Die Kategorie der „Menschen, die an der Erfüllung von Aufgaben im öffentlichen Interesse mitwirken“, in Z 10 erscheint zu vage und sollte präzisiert werden. Der Kreis an Personen, an den die Sicherheitsbehörden personenbezogene Daten übermitteln dürfen, muss gesetzlich präzise determiniert werden. In diesem Zusammenhang wird auch darauf hingewiesen, dass die Erläuterungen von einer Weitergabe von Daten an „Einrichtungen oder Menschen“ sprechen und insofern vom Normtext abweichen.

Zu Z 7 (§ 57 Abs. 2a):

Es bedarf einer gesetzlichen Begrenzung der Zwecke, zu denen die nach § 57 Abs. 1 und 2 verarbeiteten Daten mit den übermittelten Daten verglichen werden dürfen. Verwiesen wird ferner auf die Anmerkungen im Zusammenhang mit dem vorgeschlagenen Art. 2 (Änderung des Bundesstraßen-Mautgesetzes 2002) und Art. 3 (Änderung der Straßenverkehrsordnung 1960).

Zu Z 8 (§ 58 Abs. 3):

Es sollte klargestellt werden, dass die übermittelten Daten jedenfalls nach spätestens 48 Stunden nach der Übermittlung zu löschen sind, unabhängig davon, ob sie nach § 57 Abs. 2a mit anderen Daten verglichen werden.

Zu Z 15 (§ 93a):

1. Die vorgeschlagene Regelung verpflichtet öffentliche und, soweit diesen ein öffentlicher Versorgungsauftrag zukommt, private Auftraggeber, die zulässigerweise den öffentlichen Raum überwachen, die örtliche zuständige Sicherheitsbehörde über die Verwendung von technischen Einrichtungen zur Bildverarbeitung zu informieren. Die Informationsverpflichtung dient nach den Erläuterungen dazu, den Sicherheitsbehörden „die Gelegenheit zu geben, eine auf den jeweiligen Einzelfall abstellende Prüfung zu ermöglichen“. Die Sicherheitsbehörde hat dabei zu prüfen, ob es aus Sicht der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit oder der Strafverfolgung erforderlich ist, die Daten über einen längeren Zeitraum zu speichern und bei Vorliegen entsprechender Gründe mit Bescheid eine zwei Wochen nicht überschreitende Aufbewahrungspflicht festzulegen.

2. Es ist unklar, ob die mit Bescheid festzulegende Aufbewahrungspflicht jeweils nur für konkrete Einzelfälle – also anlässlich bestimmter Ereignisse für einen konkreten (zwei Wochen nicht überschreitenden) Zeitraum – gelten soll, oder ob sie

unabhängig von bestimmten Ereignissen festgelegt werden kann, wodurch bestimmten Auftraggebern ganz generell eine Aufbewahrungspflicht von bis zu zwei Wochen auferlegt würde. Die Erläuterungen und der vorgeschlagene § 96 Abs. 10 legen Letzteres nahe. Es sollte daher eine entsprechende Klarstellung erfolgen.

3. Die Begriffsdivergenz zwischen § 53 Abs. 5 („Die Rechtsträger des öffentlichen oder des privaten Bereichs, sofern […]“) und § 93a („Öffentliche und private Auftraggeber, soweit […]“) sollte überprüft werden. Wenn in beiden Fällen der gleiche Kreis an Entitäten gemeint ist, sollte die Begrifflichkeit vereinheitlicht werden.

Zu Art.1, 2 und 3 (Änderung des Sicherheitspolizeigesetzes, des Bundestraßen-Mautgesetzes 2002 und der Straßenverkehrsordnung 1960):

Zu Art. 1 Z 7 bis 10, Art. 2 Z 1 und 2 und Art. 3 Z 1 und 2 (§ 57 Abs. 2a und 3, § 58 Abs. 3, § 59 Abs. 2 SPG, § 19a Abs. 1 und 1a BStMG und § 98a Abs. 1 und 2 StVO 1960):

1. Der vorgeschlagene § 57 Abs. 2a ermächtigt den Bundesminister für Inneres die – zulässigerweise – nach den § 57 Abs. 1 und 2 verarbeiteten Daten mit Daten zu vergleichen, die im Rahmen der automatischen Überwachung der ordnungsgemäßen Entrichtung der Maut gemäß § 19a BStMG („Digitale Vignette“) sowie im Rahmen der abschnittsbezogenen Geschwindigkeitsüberwachung gemäß § 98a StVO 1960 („Section Control“) ermittelt wurden. Korrespondierend dazu sehen die vorgeschlagenen § 19a Abs. 1a BStMG und § 98a Abs. 2 erster Satz StVO 1960 eine Übermittlung der entsprechenden Daten auf Ersuchen der Sicherheitsbehörden „für Zwecke des § 54b Abs. 4b SPG“ und der Strafrechtspflege vor.

2. Zunächst erscheint klarstellungsbedürftig, wie das „Ersuchen“ der Behörde rechtlich zu deuten ist, insbesondere, ob es sich dabei um einen Rechtsakt handeln soll, der eine Verpflichtung der ASFINAG zur Übermittlung begründet. Die Erläuterungen lassen dies offen, als sie bloß davon sprechen, dass die „ermittelten Daten zulässigerweise an die Sicherheitsbehörde übermittelt werden dürfen.“

3. Es ist unklar, was mit der Wendung „für Zwecke des § 54 Abs. 4b SPG“ gemeint ist, weil diese Bestimmung mehrere Verwendungszwecke regelt: Satz 1 die Fahndung, Satz 3 die Abwehr und Aufklärung gefährlicher Angriffe gegen näher genannte Schutzgüter und die Abwehr krimineller Verbindungen. Dies müsste konkretisiert werden.

4. Im Rahmen der „Digitalen Vignette“ bzw. der „Section Control“ ermittelte Daten sind gemäß § 19a Abs. 2 erster Satz BStMG bzw. § 98a Abs. 2 dritter Satz StVO 1960 unverzüglich und in nicht rückführbarer Weise zu löschen, wenn die Maut ordnungsgemäß entrichtet bzw. keine Geschwindigkeitsübertretung festgestellt wurde; eine Weiterverarbeitung ist nur für die spezifischen Zwecke der Verfolgung (iwS) von „Mautprellerei“ bzw. von Geschwindigkeitsübertretungen zulässig. Dies entspricht auch der Judikatur des Verfassungsgerichtshofes, der im Zusammenhang mit der „Section Control“ eine strenge Zweckbindung und Pflicht zur sofortigen Löschung verlangt (vgl. VfSlg. 18.146/2007). Bei den bestehenden Systemen der „Digitalen Vignette“ und der „Section Control“ ist – soweit bekannt – die Weiterverwendung jener Daten, denen kein Mautvergehen bzw. keine Geschwindigkeitsübertretung zugerechnet werden, derzeit schon technisch ausgeschlossen („privacy by design“). Diese Systeme kommen daher weitgehend ohne die Verarbeitung von personenbezogenen Daten aus, womit auch – iS einer grundrechtskonformen Ausgestaltung – gezielt die Entstehung von Bewegungsprofilen von Personen schon auf technischer Ebene ausgeschlossen ist.

Die vorgeschlagenen § 19a Abs. 1a BStMG und § 98a Abs. 2 erster Satz StVO 1960 ermächtigen nun zur Übermittlung aller erhobenen Daten an die Sicherheitsbehörden, somit auch jener Daten, die gemäß § 19a Abs. 2 erster Satz BStMG bzw. § 98a Abs. 2 dritter Satz StVO 1960 grundsätzlich unverzüglich zu löschen sind. Es ist auch – soweit ersichtlich – keine Einschränkung auf eine Übermittlung in konkreten Einzelfällen vorgesehen. Es ist daher nicht ausgeschlossen, dass auf ein entsprechendes Ersuchen die Daten aller Verkehrsteilnehmer übermittelt werden, um den Sicherheitsbehörden einen Abgleich mit ihrer Zentralen Informationssammlung zu ermöglichen.

Damit wird nicht nur die Zweckbindung der Weiterverwendung der im Rahmen der „Digitalen Vignette“ bzw. der „Section Control“ ermittelten Daten unterlaufen. Durch die in § 57 Abs. 2a SPG normierte Ermächtigung zum Abgleich von Daten der elektronischen Kennzeichenerfassung (§ 54 Abs. 4b SPG), der elektronischen Mautkontrolle (§ 19a BMStG) und der elektronischen Geschwindigkeitsüberwachung (§ 98a StVO 1960) wird die umfassende Erstellung von Bewegungsprofile ermöglicht. Das ist nach der Judikatur des Verfassungsgerichtshofes (vgl. VfSlg. 19.892/2014) nur unter engen Voraussetzungen – Vorliegen eines vergleichbar gewichtigen öffentlichen Interesses, das den Eingriff in das Recht auf

informationelle Selbstbestimmung rechtfertigt, im Einzelfall; Gebot der richterlichen Kontrolle – zulässig. Es erscheint zweifelhaft, ob die in § 19a Abs. 1a BStMG und in § 98a Abs. 2 StVO 1960 vorgesehenen Übermittlungszwecke (für Zwecke des § 54 Abs. 4b SPG und der Strafrechtspflege) diesen Anforderungen entsprechen.

Zu Art. 4 (Änderung des Telekommunikationsgesetzes 2003):

Zu Z 1 (§ 17 Abs. 1a):

1. Die vorgeschlagene Bestimmung bezieht sich auf „Verkehrsmanagementmaßnahmen im Sinn von Art. 3 der Verordnung (EU) 2015/2120“. Der Sinn dieser Regelung ist unklar:

Gemäß dem neuen Abs. 1a sollen „Anbieter von Internetzugangsdiensten“ (zur Definition siehe Art. 2 Z 1 und 2 der VO (EU) 2015/2120) „Verkehrsmanagementmaßnahmen“ (zur Bedeutung dieses Begriffes siehe insbesondere Art. 9ff der VO (EU) 2015/2120) anbieten können. Diese Möglichkeit wird jedoch bereits durch Art. 3 Abs. 3 zweiter UAbs. der zitierten VO eröffnet. Auch die diesbezüglichen Erläuterungen geben keinen Aufschluss darüber, welcher (darüber hinausgehende) Inhalt der neuen Bestimmung zukommen soll.

Darüber hinaus wird darauf hingewiesen, dass über angemessene (technische) Verkehrsmanagementmaßnahmen (Art. 3 Abs. 3 UAbs. 2 VO (EU) 2015/2120) hinausgehende Verkehrsmanagementmaßnahmen – wie das Blockieren oder Verlangsamen von bestimmten Inhalten, Anwendungen oder Diensten – von Anbietern von Internetzugangsdiensten nur angewendet werden dürfen, wenn dies im Unionsrecht oder in mit diesem im Einklang stehenden nationalen Recht (einschließlich Verfügungen von Gerichten oder Behörden) vorgesehen ist, aber auch dies nur, soweit und solange es erforderlich ist (vgl. Art. 3 Abs. 3 UAbs. 3 lit. a VO (EU) 2015/2120).

Auch aus den Ausführungen in den Erläuterungen, die lediglich auf eine „nicht zu rechtfertigende Benachteiligung österreichischer Accessprovider“ im Wettbewerb rekurrieren, ergibt sich nichts zur Zulässigkeit einer derartigen Verkehrsmanagementmaßnahme. Es sollte zumindest in den Erläuterungen dargelegt werden, an welche Maßnahmen hier beispielsweise gedacht ist, warum diese „Verkehrsmanagementmaßnahmen im Sinn von Art. 3 der Verordnung (EU) 2015/2120“ darstellen, und warum diese den strengen Anforderungen an die

Verhältnismäßigkeit genügen (vgl. die Erwägungsgründe 11 bis 13 VO (EU) 2015/2120).

2. Selbst wenn es sich in der Tat um „Verkehrsmanagementmaßnahmen im Sinn von Art. 3 VO (EU) 2015/2120“ handeln sollte, ist unklar, warum es Anbietern von Internetzugangsdiensten überlassen bleiben sollte, diese anzubieten, bzw. warum Kunden die Option haben sollten, diese nachzufragen und auszuwählen. Vielmehr ist davon auszugehen, dass bei konkret drohenden „strafrechtlich relevanten Handlungen“, die es zu vermeiden gilt, Verkehrsmanagementmaßnahmen – bei Erfüllung der Voraussetzungen des Art. 3 Abs. 3 UAbs. 3 lit. a VO (EU) 2015/2120 – verpflichtend zu setzen wären und nicht im Belieben des Anbieters oder des Kunden stehen können.

Zu Z 3 (§ 97 Abs. 1a):

1. Das Verhältnis zwischen dem bestehenden Abs. 1, der das Recht zur Datenermittlung und -verwendung regelt, und dem vorgeschlagenen Abs. 1a, der eine entsprechende Pflicht vorsieht, ist unklar und sollte präzisiert werden. Insbesondere sollte geprüft werden, ob in Abs. 1 ein eigenständiger Regelungsgehalt verbleibt oder ob sich die vorgeschlagene Pflicht mit der bisher bestehenden Befugnis deckt.

2. Nach dem vorgeschlagenen Normtext sind „die zur Identifizierung erforderlichen Stammdaten“ zu registrieren. Die Erläuterungen sprechen demgegenüber pauschal von der Registrierung der „Stammdaten (§ 92 Abs. 3 Z 3)“ und legen damit nahe, dass nicht nur gewisse, sondern sämtliche der in § 92 Abs. 3 Z 3 genannten Daten registriert werden müssen. Nachdem § 92 Abs. 3 Z 3 auch Daten nennt, die zur Identifizierung nicht erforderlich scheinen (zB. akademischer Grad, Bonität), sollte klargestellt werden, welche Daten registriert werden müssen, wobei darauf zu achten ist, dass das erforderliche Ausmaß nicht überschritten wird.

Zu Z 4 (§ 99 Abs. 1a bis 1f):

1. Die vorgeschlagenen Bestimmungen regeln die Modalitäten einer „Quick Freeze“-Verpflichtung auf Grund einer staatsanwaltschaftlichen Anordnung. Sie scheinen dabei nicht nur eine Ausnahme von der generellen Löschungsverpflichtung des § 99 Abs. 1 TKG sowie weitere Pflichten für Telekommunikationsanbieter zu normieren, sondern in erheblichem Ausmaß auch die Modalitäten strafprozessualer Ermittlungsmaßnahmen.

Entsprechende Regelungen wären systematisch richtig in der StPO und nicht im TKG zu verankern. Dies sollte – insbesondere auch unter dem Gesichtspunkt, dass auf Grund der (systemwidrigen) Verankerung im TKG zentrale Schutzbestimmungen der StPO, wie etwa die Kontrolle durch den Rechtsschutzbeauftragten nach § 147 StPO oder Beweisverwendungsverbote nach § 140 StPO, nicht zur Anwendung kommen und Rechtsschutzlücken entstehen – überprüft werden.

Darüber hinaus wird darauf hingewiesen, dass die vorgeschlagene Bestimmung die Modalitäten strafprozessualer Ermittlungsmaßnahmen nicht abschließend regelt: So bleibt etwa unklar, welche Voraussetzungen für die staatsanwaltschaftliche Anordnung bzw. für die gerichtliche Bewilligung vorliegen müssen. Es ist lediglich vorgesehen, dass für die Schwere der Straftaten, zu deren Ermittlung die entsprechenden Maßnahmen seitens der Staatsanwaltschaft angeordnet werden dürfen, § 135 Abs. 2 Z 2 bis 4 StPO maßgeblich ist. Die verwiesenen Bestimmungen der StPO enthalten neben der im Verfahren nach Abs. 1a und 1b zu beachtenden Strafdrohung allerdings eine Reihe weiterer Voraussetzungen, auf die sich der Verweis in den vorgeschlagenen Bestimmungen des TKG nicht bezieht („Straftaten, deren Schwere eine Anordnung nach § 135 Abs. 2 Z 2 bis 4 StPO rechtfertigt“). Es bleibt sohin unklar, aufgrund welcher Kriterien, abgesehen von der Strafdrohung, die staatsanwaltschaftliche Anordnung bzw. die gerichtliche Bewilligung zu ergehen hat.

2. Dem Grunde nach bestehen verfassungsrechtlich keine Bedenken gegen eine anlassbezogene Speicherung von Telekommunikationsdaten in Form eines „Quick freeze“-Modells. Freilich muss sich die Ausgestaltung dieses Modells im grundrechtlich vorgegebenen Rahmen bewegen, der in erster Linie durch § 1 DSG, Art. 8 EMRK und Art. 7 sowie 8 GRC festgelegt wird, wobei sich maßgebliche Leitlinien aus der Judikatur des EuGH und des VfGH ergeben (siehe insbesondere EuGH 8.4.2014, verb. Rs. C-293/12 und C-594/12, Digital Rights, EuGH 21.12.2016, verb. Rs. C-203/15 und C-698/15, Tele2 Sverige AB, und VfSlg. 19.892/2014).

Um den vom EuGH und VfGH aufgestellten Anforderungen zu entsprechen, sollten folgende Präzisierungen vorgenommen werden:

Unklar erscheint der Umfang der vom „Quick freeze“-Verfahren erfassten Daten: Obwohl § 99 prinzipiell nur die Verarbeitung von Verkehrsdaten regelt, legen die Erläuterungen nahe, dass sich das vorgeschlagene „Quick freeze“-Modell umfassend auf „Telekommunikationsdaten (Verkehrsdaten, Zugangsdaten und Standortdaten)“

beziehen soll. Es ist allerdings unerlässlich, dass bereits aus der gesetzlichen Grundlage eindeutig und präzise hervorgeht, welche Datenkategorien von der Ermittlungsmaßnahme überhaupt erfasst sind.

Fraglich ist weiters, worauf sich der Begriff der „Anfrage“ in § 99 Abs. 1c bezieht. § 99 Abs. 1b sieht lediglich eine „Auskunft“ aufgrund einer staatsanwaltschaftlichen Anordnung vor.

Auch der vorgeschlagene § 99 Abs. 1d erscheint unklar: Es sollte klargestellt werden, wer „Adressaten einer Anordnung nach Abs. 1a“ sind. Außerdem sind Umfang und Modalitäten der vorgesehenen Protokollierungspflicht präzisierungsbedürftig.

Klarstellungsbedürftig ist schließlich die Frage der Kostentragung.

3. Die Voraussetzungen für die Anordnung einer Speicherpflicht und für einen anschließenden Zugriff der Strafverfolgungsbehörden auf die gespeicherten Daten erscheinen zu niedrigschwellig und undifferenziert (vgl. dazu VfSlg. 19.892/2014, Rz 171 f). Während die Speicherpflicht zur „Ermittlung, Feststellung und Verfolgung“ von Straftaten angeordnet werden kann, „deren Schwere eine Anordnung nach § 135 Abs. 2 Z 2 bis 4 StPO rechtfertigt“, ist ein Zugriff zur „Aufklärung und Verfolgung“ ebendieser Straftaten zulässig. Aus dem Verweis folgt, dass diese Maßnahmen bereits in Bezug auf vorsätzlich begangene Straftaten eingesetzt werden können, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht sind. Auch mangels zusätzlicher gesetzlicher Determinanten ist daran zu zweifeln, ob diese Regelungen – wie vom EuGH gefordert – „in der Praxis geeignet [sind], den Umfang der Maßnahme und infolgedessen die betroffenen Personenkreise wirksam zu begrenzen“ (EuGH 21.12.2016, verb. Rs. C-203/15 und C-698/15, Tele2 Sverige AB, Rz 110).

Auch die vorgesehene Protokollierungspflicht erscheint insofern unzureichend, als schon die Anordnung einer Speicherverpflichtung einen Grundrechtseingriff darstellt (siehe VfSlg. 19.892/2014, Rz 160) und somit protokolliert werden sollte.

Im Übrigen fehlen umfassende Datensicherheitsmaßnahmen (vgl. § 102c zu Vorratsdaten) wie auch ein wirksamer Schutz vor Missbrauchsrisiken (siehe VfSlg. 19.892/2014, Rz 188 ff).

Auch ist fraglich, ob die Regelungen über die Löschung von Daten nach § 99 Abs. 1f in einer Weise bestimmt sind, die grundrechtlichen Vorgaben entspricht (vgl. VfSlg. 19.892/2014, Rz 195).

4. Des Weiteren ist unklar, was unter den Begriffen „Ermittlung, Feststellung und Verfolgung von Straftaten“ in Abs. 1a zu verstehen ist sowie aus welchem Grund in Abs. 1b demgegenüber die Begriffe „Aufklärung und Verfolgung von Straftaten“ verwendet werden. Dies insbesondere vor dem Hintergrund, dass diese Begriffe in den korrespondierenden Bestimmungen der StPO, an die die Abs. 1a und 1b anknüpfen, nicht verwendet werden. Dies sollte vereinheitlicht und präzisiert werden.

5. Abs. 1b sieht die Auskunft über eingefrorene Daten an die Staatsanwaltschaft aufgrund einer gerichtlich bewilligten staatsanwaltlichen Anordnung vor. Nach dem Wortlaut der Bestimmung enthält diese allerdings lediglich eine Ermächtigung („Eine Auskunft … ist … zulässig.“), jedoch keine Verpflichtung der Telekommunikationsdienstleister zur Herausgabe der angeforderten Daten. Eine solche lässt sich auch nicht auf § 90 Abs. 7 TKG stützen, weil von dieser Bestimmung nur Stammdaten umfasst sind. Berücksichtigt man den Umstand, dass im vorgeschlagenen § 97 Abs. 1a in Abweichung von § 97 Abs. 1 TKG eine ausdrückliche Verpflichtung normiert werden soll, so folgt aus der vorgeschlagenen Systematik, dass in § 99 Abs. 1b lediglich eine Ermächtigung statuiert wird. Diese auf Wortlaut und Systematik gestützte Schlussfolgerung steht allerdings im Widerspruch zum in den Erläuterungen dargelegten Anliegen, bei einer Erhärtung des Anfangsverdachts mit gerichtlicher Bewilligung auf diese Daten zugreifen zu können.

6. Die Formulierung des Abs. 1c legt nahe, dass nicht nur eine erfolgte Auskunft, sondern jedes Auskunftsbegehren protokolliert werden muss, wobei unklar ist, unter welchen Voraussetzungen eine „Anfrage“ oder eine gerichtlich bewilligte Anordnung der Staatsanwaltschaft seitens der Telekommunikationsbetreiber gegebenenfalls verweigert werden darf. Die Differenzierung zwischen Anfrage und Auskunft deutet darauf hin, dass nicht jeder „Anfrage“ entsprochen werden muss. Überdies ist das Verhältnis der zwei Sätze des Abs. 1c zueinander unklar: Da der zweite Satz sich spezifisch nur auf eine „Auskunft nach Abs. 1b“ bezieht, liegt der Schluss nahe, dass die im zweiten Satz genannten Protokollierungsdaten im Zusammenhang mit einer „Anfrage“ nicht zu protokollieren sind.

Es bleibt somit unklar, wann konkret eine Auskunft zu erteilen ist. Dies sollte, insbesondere vor dem Hintergrund der verwaltungsstrafrechtlich sanktionierten Protokollierungspflicht des vorgeschlagenen Abs. 1c, klargestellt werden.

Zu Z 5 (§ 109 Abs. 4 Z 9 bis 13):

Die vorgeschlagene Z 12 ist unklar:

Im ersten Teil der Z 12 könnte es aus Gründen der besseren Verständlichkeit lauten: „entgegen § 99 Abs. 1c einen Zugriff, eine Anfrage oder eine Auskunft nicht protokolliert …“.

Es ist unklar, worauf sich der zweite Halbsatz bezieht: Soll damit die Erteilung der notwendigen Auskünfte unter Missachtung der Protokollierungspflicht erfasst werden, könnte dies angesichts der vorgeschlagenen Umformulierung des ersten Halbsatzes entfallen. Soll damit anderes gemeint sein, sollte dies entsprechend präzisiert werden. Dabei wäre auch näher zu präzisieren, was unter „notwendigen“ Auskünften zu verstehen ist. Sollte ein Zuwiderhandeln gegen die Auskunftsverpflichtung des Abs. 1b geregelt werden, sollte diese systematisch besser in Z 10 oder eine eigene Ziffer aufgenommen werden.

III. Legistische und sprachliche Bemerkungen

Allgemeines:

Es sollte auf die korrekte Setzung geschützter Leerzeichen (zB nach „Art.“, „§“, „Abs.“, „Z“, „lit.“, „Nr.“ und „S.“ sowie in Ausdrücken wie „BGBl. I“) geachtet werden (vgl. Layout-RL 2.1.3).

Zu Art. 1 (Änderung des Sicherheitspolizeigesetzes):

Zu Z 11 (§ 84 Abs. 1):

In der Novellierungsanordnung sollte es aus Gründen der Übersichtlichkeit besser lauten: „In § 84 Abs. 1 wird im Schlussteil nach dem Zitat …“. Der letzte Halbsatz der Novellierungsanordnung sollte lauten: „…und werden folgende Z 7 und 8 eingefügt:“

Zu Z 12 (§ 91c):

Die den Gegenstand der Novellierung bildenden Wortfolgen (sowie die vor und nach diese Wortfolgen gesetzten Anführungszeichen) sind nicht in Kursivdruck wiederzugeben.

Zu Z 16 (§ 94 Abs. 42):

1. Die Inkrafttretensbestimmung für § 96 Abs. 10 (Z 17) fehlt.

2. Aus Gründen der Übersichtlichkeit sollte die Inkrafttretensbestimmung besser lauten: „§ 25 Abs. 1, § 53 Abs. 5, § 53a Abs. 6, § 54 Abs. 4b, § 56 Abs. 1, § 57 Abs. 2a und 3, § 58 Abs. 3, § 59 Abs. 2, § 84 Abs. 1, § 91c Abs. 1 und 3, § 92a Abs. 1 und 1a, § 93a samt Überschrift und § 96 Abs. 10 …“

Zu Art. 2 (Änderung des Bundestraßen-Mautgesetzes 2002):

Zu Z 1 (§ 19a Abs. 1):

Folgende Umformulierung wird angeregt: „Der Einsatz dieser technischen Einrichtungen ist der Sicherheitsbehörde sieben Tage vor seinem Beginn für die Zwecke des Abs. 1a mitzuteilen.“

Zu Art. 3 (Änderung der Straßenverkehrsordnung 1960):

Zum Einleitungssatz:

Die StVO 1960 wurde zuletzt durch das Bundesgesetz BGBl. I Nr. 68/2017 geändert.

Zu Z 2 (§ 98a Abs. 2):

Folgende Umformulierung des ersten Halbsatzes wird angeregt: „Die nach Abs. 1 ermittelten Daten ...“

Zu Z 3 (§ 103 Abs. 18):

Dem § 103 wurde bereits mit dem Bundesgesetz BGBl. I Nr. 68/2017 ein Abs. 18 angefügt. Richtigerweise sollte daher ein Abs. 19 angefügt werden.

Zu Art. 4 (Änderung des Telekommunikationsgesetzes 2003):

Zu Z 1 (§ 17 Abs. 1a):

1. § 17 Abs. 3 TKG bezieht sich auf „Mindestanforderungen an die Dienstequalität […], insbesondere um eine Verschlechterung der Dienste und eine Behinderung oder Verlangsamung des Datenverkehrs in den Netzen zu verhindern“; es sollte geprüft werden, ob die vorgeschlagene Bestimmung nicht systematisch besser als Abs. 3a eingefügt werden sollte.

2. Im Hinblick auf den in § 3 Abs. 3 TKG definierten und auch in § 17 Abs. 1 TKG verwendeten Terminus „Betreiber von öffentlichen Kommunikationsdiensten“ wird zur Erwägung gestellt, – je nach beabsichtigter Aussage – anstelle von „Anbieter von Internetzugangsdiensten“ (Diktion der EU-Verordnung) den Terminus des TKG zu verwenden.

3. Zur korrekten Zitierung gemeinschaftsrechtlicher Normen wird auf Rz 53 bis 55 des EU-Addendums hingewiesen. Danach ist der Titel der Norm unter Entfall der Bezeichnung des erlassenden Organs sowie unter Entfall des Datums zu zitieren; die Fundstellenangabe sollte dem Muster „ABl. Nr. L 257 vom 10.10.1996 S. 26“ folgen.

Zu Z 5 (§ 109 Abs. 4 Z 9 bis 13):

1. Auf das Schreibversehen in der Z 9 („ein“ statt „in“) wird hingewiesen.

2. Es ist unklar, worauf sich die Wendung „oder die notwendigen Auskünfte erteilt“ in der vorgeschlagenen Z 1 bezieht.

Zu Z 6 (§ 137 Abs. 9):

Aus Gründen der Übersichtlichkeit sollte die Inkrafttretensbestimmung besser lauten: „§ 17 Abs. 1a, § 92 Abs. 3 Z 3, § 97 Abs. 1a, § 99 Abs. 1a bis 1f sowie § 109 Abs. 4 …“

IV. Zu den Materialien

Zur Textgegenüberstellung:

Die Textgegenüberstellung sollte auf ihre Vollständigkeit überprüft werden. So fehlt etwa die Darstellung der Textunterschiede in § 91c Abs. 1 SPG und ist die Wiedergabe des geltenden § 92a Abs. 1 SPG unvollständig.

Diese Stellungnahme wird im Sinne der Entschließung des Nationalrates vom 6. Juli 1961 auch dem Präsidium des Nationalrates zur Kenntnis gebracht.

21. August 2017
Für den Bundesminister
für Kunst und Kultur, Verfassung und Medien:
HESSE

Elektronisch gefertigt

REPUBLIK ÖSTERREICH BUNDESKANZLERAMT AMTSSIGNATUR	Unterzeichner	serialNumber=1026761,CN=Bundeskanzleramt,C=AT
	Datum/Zeit	2017-08-21T10:56:17+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bka.gv.at/verifizierung
	Hinweis	Dieses Dokument wurde amtssigniert.