WIRTSCHAFTSKAMMER ÖSTERREICH

Wiedner Hauptstraße 63 | Postfach 195
1045 Wien
T +43 (0)5 90 900-4273 | F +43 (0)5 90 900-243
E rp@wko.at
W https://news.wko.at/rp

Herrn
SC Dr. Mathias Vogl
Bundesministerium für Inneres
Herrengasse 7
1010 Wien

per E-Mail: bmi-III-1@bmi.gv.at

cc: begutachtungsverfahren@parlament.gv.at

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen, Sachbearbeiter	Durchwahl	Datum
BMI-LR1340/0019-III/1/2017	Rp 1685/17/TK/SL	4273	17.8.2017

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

Sehr geehrter Herr Sektionschef,

die Wirtschaftskammer Österreich bedankt sich für die Übermittlung des Entwurfes eines Bundesgesetzes, mit dem das Sicherheitspolizeigesetz, das Bundesstraßen-Mautgesetz 2002, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden (fortan kurz: Entwurf) und nimmt hiezu wie folgt Stellung:

A. Allgemeines

Wir begrüßen grundsätzlich Maßnahmen zur Stärkung der Sicherheit und zur Bekämpfung der Kriminalität. Die durch die neuen Maßnahmen und Ermittlungsmethoden geschaffenen Eingriffsmöglichkeiten müssen jedoch klar und unstrittig determiniert, verhältnismäßig und grundrechtskonform ausgestaltet sein.

Bei einigen im Entwurf vorgesehen Maßnahmen scheint dies zumindest zweifelhaft. So ist es insbesondere bei der Herausgabepflicht von vorhandenem Videomaterial, der Übermittlung der Kennzeichendaten durch die ASFINAG (betrifft alle Autobesitzer in Österreich) und der Registrierung von Prepaid-Wertkarten höchst fraglich, ob die vorgesehen Maßnahmen verhältnismäßig sind und nicht übermäßig in verfassungsrechtlich gewährleistete Grundrechte (Recht auf persönliche Freiheit, Grundrecht auf Datenschutz) eingreifen.

B. Zu den Änderungen des Sicherheitspolizeigesetzes

Die vorgesehenen Änderungen im SPG führen zu einer erheblichen Ausdehnung der Zugriffsbefugnisse der Sicherheitsbehörden auf Videomaterial. Ob derartige Maßnahmen ein geeignetes und verhältnismäßiges Mittel sind, um das Ziel der Verhinderung einer Gefährdung der öffentlichen Sicherheit und insbesondere der Verübung terroristischer Anschläge zu erreichen, scheint zweifelhaft.

Zu § 53 Abs 5

Die Datenspeicherung von Bildmaterial mittels elektronischer Überwachungsanlagen durch private Rechtsträger unterliegt den einschlägigen Bestimmungen des Datenschutzgesetzes und wird im Wege der erforderlichen Registrierung von der Datenschutzbehörde überprüft. Es ist darauf hinzuweisen, dass die Datenspeicherung durch private Rechtsträger grundsätzlich anderen Zwecken dient als denen der (eine Aufgabe der Hoheitsverwaltung darstellenden) Strafverfolgung. Die beabsichtigte Gesetzesänderung könnte dazu führen, dass es zu unterschiedlichen Speicherfristen je nach Speicherzweck bei ein und derselben Überwachungsanlage kommt.

Die letzten beiden Sätze des § 53 Abs 5 lauten: „Ab dem Zeitpunkt der Kenntnis von einem solchen Verlangen darf der verpflichtete Rechtsträger die verlangten Bilddaten nicht löschen. Nicht zulässig ist die Verwendung von Daten über nicht öffentliches Verhalten." In den Erl wird hinsichtlich des Löschungsverbotes auf die Regelung bei Auskunftsverlangen nach dem DSG 2000 (§ 26 Abs 7 DSG 2000) verwiesen. Diese Regelung legt allerdings fest, dass „ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen ... der Auftraggeber über den Auskunftswerber innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde gem § 31 an die Datenschutzbehörde bis zum rechtskräftigen Abschluss des Verfahrens nicht vernichten" darf. In der gegenständlichen Regelung findet sich jedoch keine zeitliche Begrenzung für das Löschungsverbot. Unklar scheint weiters, was unter „nicht öffentlichem Verhalten" zu verstehen ist. Diesbezüglich geben auch die Erl keinen Aufschluss.

Hinsichtlich des Zugriffs auf die Daten bzw. deren Weitergabe ist Folgendes festzuhalten: Das Risiko einer Verletzung des Grundrechtes auf Datenschutz trägt der jeweilige Betreiber einer Videoüberwachung. Wenn daher der Sicherheitsbehörde ohne Vorliegen der Voraussetzungen Daten nach § 53 Abs 5 iVm § 53 Abs 1 übermittelt werden, treffen allfällige Rechtsfolgen (Verwaltungsstrafen; zivilrechtliche Ansprüche) zunächst den Betreiber der Videoüberwachung. Problematisch ist jedoch, dass die Voraussetzungen der „unverzüglichen" Datenweitergabe im Entwurf nicht näher erläutert werden. Die Gesetzesbestimmung ist unbestimmt. Das SPG ordnet lediglich eine „unverzügliche" Weitergabe an. Um Rechtssicherheit zu gewährleisten, müssten die Parameter, welche inhaltliche Qualität das „Verlangen" der Sicherheitsbehörde haben muss, dargelegt werden. Dies insbesondere auch vor jenem Hintergrund, dass das „nicht unverzügliche Nachkommen" der Verpflichtung zur Gewährung des Zugangs gem § 84 Abs 1 Z 7 mit Verwaltungsstrafe bedroht wird.

Zielsetzung der Gewährung des Zugangs zu Videodaten ist - zumindest nach den Erl - die Möglichkeit, im Fall der Notwendigkeit eines Echtzeitstreamings unverzüglich Zugang zu den gerade erst anfallenden Bilddaten zu gewähren. Dies widerspricht klar und eindeutig den bisherigen Bescheiden der Datenschutzbehörde, die auf Basis des geltenden DSG ergangen sind. Die Datenschutzbehörde hat allergrößten Wert daraufgelegt, dass Videodaten eben nicht unverschlüsselt gespeichert werden können, und dass nur in ganz bestimmten und genau definierten Abläufen diese Bilddaten auch wieder entschlüsselt werden. So ist jedoch zB bei den Wiener Linien das gesamte System der Videoüberwachung auf dieser Basis errichtet und konzipiert. Die Rechtsgrundlage wird sich diesbezüglich auch durch das Datenschutzanpassungsgesetz 2018 materiell nicht ändern. Die Bereitstellung eines unverschlüsselten Zugangs zu einer derartig großen Menge von Videodaten widerspricht daher völlig den bisherigen Prinzipien der Datenschutzbehörde.

Weiters ist die „Gewährung" eines Systemzugangs im vorliegenden Entwurf in keiner Weise definiert. In der Praxis würde dies umfangreiche bauliche und technische Vorkehrungen (technische Verbindung, Software, Räumlichkeiten etc.) erfordern, die mit massiven Kostenbelastungen verbunden wären. Der Gesetzestext liefert keinerlei Hinweise in welcher Form diese Eigentumsbeschränkungen erfolgen sollen. Auch über die Kostentragung sprechen sich weder Gesetzestext noch Erl aus. Die Kosten dafür

müssten jedenfalls von der einschreitenden Behörde getragen werden. Es ist fraglich ob die Gewährung des Zugangs aufgrund der notwendigen Maßnahmen eine unverhältnismäßige Beschränkung des Rechts auf Eigentum darstellt.

Insgesamt erachten wir es daher aus den genannten Gründen als äußerst kritisch, wenn den Sicherheitsbehörden derartig weitreichender Zugang zu Videodaten eingeräumt werden soll. Dabei stellt sich mitunter auch bereits die Frage der technischen Machbarkeit.

Zu § 92a

Kritisch zu hinterfragen ist der Ausbau der Kostenersatzpflicht im § 92a SPG bei mutwillig verursachten Polizeieinsätzen. Hier könnte es zu Abgrenzungsschwierigkeiten kommen. Der Ausbau der Kostenersatzpflicht sollte nicht dazu führen, dass allenfalls erforderliche Notmeldungen aus Angst vor einem allfälligen Kostenersatz nicht mehr im erforderlichen Ausmaß vorgenommen werden. Allenfalls sollte die Formulierung dahingehend geändert werden, dass „vorsätzlich" durch „absichtlich" ersetzt werden. Ein bedingter Vorsatz sollte in einer solchen Situation noch nicht kostenpflichtig sein.

Zu § 93 a

Der Entwurf birgt insbesondere für Verkehrsunternehmen zwei massive Verschärfungen in der - wichtigen und erwünschten - Zusammenarbeit mit den Sicherheitsbehörden.

Zunächst hätten die betroffenen Unternehmen die Sicherheitsbehörden über die Verwendung von technischen Einrichtungen zur Bildverarbeitung zu informieren. Weder aus den Erl noch aus dem Text ergibt sich, wie dies zu erfolgen hat und ob dies für die Einrichtung eines Systems oder für jede einzelne Kamera gilt. Meldeverpflichtungen von privaten Unternehmen sind, da sie weitere bürokratische Maßnahmen darstellen, grundsätzlich abzulehnen. Bewilligte Überwachungen scheinen ohnehin bei der Datenschutzbehörde auf.

In weiterer Folge sieht der Entwurf in § 93a letzter Satz vor, dass „im Einzelfall" aus Gründen der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit eine bis zu zwei Wochen dauernde Aufbewahrungsverpflichtung (offensichtlich der aufgezeichneten Bilder, wenngleich dies aus der Formulierung nicht eindeutig ersichtlich ist) mittels Bescheid festzulegen ist.

Diesbezüglich kann es zu Widersprüchen mit Auflagenbescheiden, die im Zuge der Registrierung der jeweiligen Videoüberwachung erlassen wurden, kommen. So wurde zB für die Videoüberwachungsanlagen der Wiener Linien eine wesentlich kürzere Aufbewahrungsdauer mittels rechtskräftigen Bescheides von der Datenschutzbehörde festgelegt.

Weiters unklar ist, ob sich der Einzelfall auf den Einzelfall der Bilder einer Kamera richtet, oder aber ob das System eines Unternehmens an sich Gegenstand eines solchen Einzelfalls sein kann. Die Erl treffen dazu leider keine Aussagen. Es muss wohl eine besondere Gefährdungslage vorliegen und kann nicht bloß mit der „normalen" großstädtischen Gefährdungslage argumentiert werden.

Es gibt auch schwerwiegende technische Argumente gegen eine derart lange Aufbewahrungsdauer. Die derzeit zB bei den Wiener Linien verwendeten Speichermedien (insbesondere in den Fahrzeugen) können maximal die von der Datenschutzbehörde als Höchstgrenze verfügten Zeiträume aufzeichnen. Bei den Speichermedien, die dies theoretisch könnten, führt dies zu einer Versiebenfachung des vorrätig zu haltenden Datenvolumens. Bis dato wurde im Rahmen der Verbrechensbekämpfung in der laufend

sehr guten Kooperation mit den Sicherheitsbehörden kein Defizit und keine Notwendigkeit der Ausdehnung der Speicherdauer artikuliert. Es stellt sich daher die Frage, ob die Investitionen, die ja schließlich die Verkehrsunternehmen tragen müssten, in Relation zum tatsächlichen Nutzen stehen - uns erscheint dies zumindest zweifelhaft.

Zu § 54 Abs 4b SPG, § 19a BStMG, 98a Abs 2 StVO

Neben Autokennzeichen sollen fortan auch zusätzliche Informationen wie Automarke, -type, -farbe und Informationen über den Fahrzeuglenker für Fahndungszwecke gespeichert werden dürfen. Die ermittelten Daten sind der Sicherheitsbehörde auf Ersuchen für bestimmte Zwecke zu übermitteln. Fraglich ist ob diese Maßnahme verhältnismäßig ist, da hier sämtliche Autofahrer unter Generalverdacht gestellt werden und zahllose Datensätze über Kfz, Lenker und Halter auf der jeweils überwachten Strecke übermittelt werden. Gerade im Vergleich mit § 98a Abs 2 Satz 2 u 3 StVO wird klar, welche Abkehr von der bisherigen Datenschutz, -verarbeitungs- und -nutzungspolitik dies bedeutet.

Die Einführung bzw. Ausweitung der Kennzeichenerkennung durch Videoüberwachungseinrichtungen (insbesondere durch die ASFINAG) sowie die Verpflichtung zur Übermittlung der Daten an die Sicherheitsbehörden schafft die technische Basis für die Einführung flächendeckender Section-Control-Systeme am gesamten Autobahnen- und Schnellstraßennetz. Die Einführung einer solchen Maßnahme müsste gesondert und vollständig hinsichtlich ihrer Wirkungsdimensionen - und nicht als Teil eines Sicherheitspakets - erörtert werden.

C. Zu den Änderungen des Telekommunikationsgesetzes

Maßnahmen zur Unterstützung der Strafrechtspflege und zur Wahrung der öffentlichen Sicherheit stehen im Interesse der Allgemeinheit. Dementsprechend hat der Verfassungsgerichtshof in seinem Erkenntnis vom 27.02.2003 zur GZ 37/02 ua (VfSlg 16.808) die Überwälzung aller Kosten für die Bereitstellung von Überwachungseinrichtungen durch den Ausschluss eines Kostenersatzes an die Telekommunikationsbetreiber für verfassungswidrig erklärt. Grund ist die Verletzung des Verhältnismäßigkeitsgrundsatzes, wenn die Kosten alleine dem Betreiber überwälzt werden.

Die Regelung des § 94 Abs. 1 TKG, die den Kostenersatz regelt und laut Erl diese Entscheidung dezidiert umsetzt, stellt laut ihrem Wortlaut auf die Kosten ab, die er aufwenden muss, um die erforderlichen Funktionen der gem § 94 Abs. 3 und 4 TKG erlassenen Verordnungen in seinen Anlagen einzurichten.

Das Erkenntnis des Verfassungsgerichtshofes hat Gültigkeit für alle Implementierungen zur Bereitstellung von Einrichtungen, die der Umsetzung öffentlicher Interessen gelten.

Wenn der Gesetzgeber diese außerhalb der Verordnungen nach § 94 Abs. 3 und 4 TKG anordnet, hat er zugleich gesondert klarzustellen, dass den Betreibern die entstehenden Kosten in überwiegendem Maße zu ersetzen sind. Das fehlt im vorliegenden Gesetzesentwurf und ist entsprechend zu ergänzen, ansonsten die geplanten Bestimmungen im Lichte der zitierten Entscheidung verfassungswidrig wären.

Zu § 17a TKG

Wir begrüßen ausdrücklich diese Bestimmung als ein wesentlicher Baustein zur präventiven Verhinderung strafrechtlich relevanter Handlungen.

Österreichische Telekomanbieter sind bereits als Accessprovider gegenüber reinen Diensteanbietern benachteiligt. Darüber hinaus wendet die RTR im europaweiten Vergleich eine sehr enge Auslegung der Netzneutralitätsregeln an. Viele etablierte und von den Kunden erwartete Services zum Kinder- und Jugendschutz sowie Dienstleistungen zum Schutz von Daten oder gegen Viren und Hacking sind jedoch Gegenstand kritischer Überprüfungen und könnten in der aktuellen Form nicht mehr weiter angeboten werden. Dies wäre eine einseitige Belastung der Accessprovider, aber auch der Kunden als Nutzer dieser Services.

Die Klarstellung, dass es sich bei Verkehrsmanagementmaßnahmen zur Verhinderung dieses Verhaltens nicht um Verstöße gegen Artikel 3 der Verordnung (EU) 2015/2120 handelt (Netzneutralität), bringt den Betreibern ein erhöhtes Maß an Rechtssicherheit.
Allerdings erscheint es aus Sicht der Rechteinhaber in diesem Zusammenhang wünschenswert, wenn neben den vorgeschlagenen Formulierungen - zumindest in den Erl - auch eine Klarstellung aufgenommen wird, dass das Setzen von entsprechenden Maßnahmen im Falle von Urheberrechtsverletzungen nicht der Netzneutralitätsverordnung (TSM-VO 2015/2120) widerspricht.

Die Netzneutralitätsverordnung kennt eine Einschränkung auf „strafrechtlich relevante Urheberrechtsverletzungen" - wie dies in § 17 Abs 1a formuliert wurde - nicht, sie dürfte auch mit den Vorgaben von Art 8 Abs 3 TSM-VO nicht konform gehen.

Um Unklarheiten und damit Interpretationsproblemen vorzubeugen, sollten außerdem noch zu folgende Fragen Klarstellungen erfolgen:

- Sind als Anbieter von Internetzugangsdiensten ausschließlich Accessprovider zu verstehen?
- Was wird derzeit in einem exemplarischen Sinne unter „Verkehrsmanagementmaßnahmen" verstanden (eventuell unter Verweis auf die entsprechenden EU-Vorgaben)?
- Eingriffe ins Urheberrecht sind - mit Ausnahme der erlaubten Nutzung zum eigenen Gebrauch - grundsätzlich strafrechtlich relevant. Daher stellt sich die Frage der Erforderlichkeit einer expliziten Unterscheidung in § 17.

Zu § 97 Abs 1a

Wiewohl das Bestreben, die Sicherheit im Staat zu erhöhen, begrüßt wird, und auch der Vorstoß zur Einführung einer verpflichtenden Registrierung der Daten von Käufern im Zusammenhang mit dem Erwerb von Prepaid-Wertkarten in diesem Kontext auf den ersten Blick nachvollziehbar ist, erscheint uns die vorgeschlagene Maßnahme aus unterschiedlichen Überlegungen zur Erreichung dieses Zieles nicht geeignet und hinsichtlich des mit ihrer Durchführung verbundenen Aufwandes unverhältnismäßig.

Zunächst führt eine umfangreiche Studie der GSM Association (internationale Standardisierungvereinigung von Mobilfunkbetreibern) detailliert aus, dass es in verschiedenen Ländern nach Einführung einer Registrierungspflicht für Prepaid-Wertkarten keine Veränderungen bei der Aufklärungsquote gegeben hat. Aus diesem Grund hat sich eine Reihe von Staaten mit dem Thema intensiv auseinandergesetzt - und sich letztlich gegen eine Einführung einer solchen Verpflichtung entschieden (zB UK, RO, CZ). Das Fehlen empirisch gesicherter Belege für die Wirksamkeit einer Registrierungspflicht für die genannten Zwecke stellt aus unserer Sicht ein zentrales Argument gegen die Einführung einer entsprechenden Verpflichtung dar.

Dessen ungeachtet erscheint bei Einführung einer Registrierungspflicht auch das Entstehen eines Schwarzmarktes für SIM-Karten als durchaus realistisches Szenario. Daneben würde wohl auch die Nachfrage nach ausländischen Wertkarten steigen. Außerdem erscheint auch eine Anmeldung mit gefälschten Dokumenten möglich. All das würde dem proklamierten Ziel klar entgegenwirken.

Darüber hinaus stellt die vorgeschlagene Maßnahme in mehrfacher Hinsicht einen intensiven Eingriff in die Geschäftsprozesse der betroffenen Unternehmen dar:

Mit der Erhebung der Identität und der erforderlichen Stammdaten jedes Vertragspartners wäre ein erheblicher zusätzlicher Zeitaufwand im Rahmen des Kassiervorgangs verbunden. Die übrigen wartenden Kunden hätten für das Anwachsen der Warteschlange wohl kaum Verständnis. Zusätzliche Infrastrukturkosten seien der Vollständigkeit halber ebenso erwähnt.

Dieser administrative Aufwand steht in keinem Verhältnis zu den erzielbaren Einnahmen des Unternehmers, und zahlreiche Anbieter würden im Lichte dieses enormen Bürokratieaufwandes mit einem deutlichen Umsatzrückgang oder mit Umsatzverschiebungen zu rechnen haben, so dass sie letztlich wohl zwangsläufig auf den Verkauf von Prepaid-Karten verzichten würden.

Insgesamt stehen die durch die Einführung einer Registrierungspflicht für Prepaid Wertkarten zu erwartenden Verbesserungen für die öffentliche Sicherheit und in der Kriminalitätsbekämpfung in keinem sinnvollen Verhältnis zu den schwerwiegenden Nachteilen, die die geplante Verpflichtung für Gewerbetreibende mit sich bringen würde.

Auch aus Nutzersicht wären erhebliche Grundrechtseingriffe mit dieser Registrierungspflicht verbunden, vor allem das Recht, anonym Kommunikationsnetze und -dienstleistungen zu nutzen.

Außerdem sei noch auf die Regulierungsziele in § 1 TKG hingewiesen. Genannt seien dabei insbesondere die "Förderung des Wettbewerbes im Bereich der elektronischen Kommunikation die Versorgung der Bevölkerung und der Wirtschaft mit zuverlässigen, preiswerten, hochwertigen und innovativen Kommunikationsdienstleistungen" und die „Sicherstellung größtmöglicher Vorteile in Bezug auf Auswahl, Preis und Qualität für alle Nutzer". Zur Erreichung dieser Ziele wurden MVNO-Angebote ermöglicht. Sie wären nach der Einführung einer Registrierungsplicht für Prepaid-Wertkarten womöglich gefährdet.

Schließlich ist auch unklar, wer für falsche Angaben (etwa im Falle gefälschter Ausweise) haftet und welches Risiko für den Händler bei Verlust der Daten durch technische Defekte bestehen würde.

Unbeschadet der vorangegangenen Überlegungen, aufgrund derer wir die Registrierung von Prepaid Wertkarten ablehnen, sei noch angemerkt, dass eine Registrierung vor Freischaltung eine eher handhabbare Lösung darstellen würde als eine Registrierung bei Vertragsschluss. Dabei werden nur solche Daten sinnvoll erhebbar sein, die sich durch einen amtlichen Lichtbildausweis nachweisen lassen (Vor- und Familienname sowie Geburtsdatum). Ohne die Gewährung eines angemessenen Kostenersatzes für die betroffenen Unternehmen (die Reglung erfolgt klar im öffentlichen Interesse) wäre die Einführung einer verpflichtenden Registrierung von Wertkarten jedenfalls nicht vorstellbar.

Zu § 99

Mit § 99 wird das sog Quick Freeze Verfahren eingeführt. Der Vollständigkeit halber sei bereits an dieser Stelle angemerkt, dass ein klarer Hinweis darauf, dass diese Maßnahme tatsächlich zur Verhinderung oder Aufklärung von schweren Verbrechen oder Terroranschlägen beitragen kann, derzeit noch aussteht.

Im Arbeitsprogramm der Bundesregierung fand sich hier noch eine Pflicht, fälschlicherweise überwachte Personen beim Abschluss der Maßnahme über ihre Überwachung zu informieren. Diese Verpflichtung findet sich nicht im Entwurf, stattdessen kann der Betroffene offenbar lediglich ein Auskunftsbegehren nach Datenschutzrecht stellen, was in keiner Weise ein Ersatz wäre.

Auf Anordnung der Staatsanwaltschaft soll ein Telekombetreiber künftig wieder „auf Vorrat" Daten für bis zu ein Jahr speichern müssen. Somit kann diese Überwachungsmaßnahme eingesetzt werden, noch bevor ein Gericht zugestimmt hat, da der Entwurf nach § 99 Abs. 1b TKG-E erst bei der Beauskunftung der Daten, aber nicht bei der Speicherung auf Vorrat eine gerichtliche Bewilligung vorsieht. Jedoch wird bereits durch die Speicherung, in Grundrechte eingegriffen, nicht erst durch die Beauskunftung.

Die vorgeschlagene Gesetzesbestimmung an sich ist unbestimmt. Es ist daher klarzustellen, welche Parameter die Anordnung im konkreten Fall haben muss, andernfalls ist eine Implementierung nicht möglich. Eine Speicherung auf Basis von Zellen, Sektoren oder Adressen führt zu erheblichen Implementierungsaufwänden, insbesondere, wenn davon Großveranstaltungen umfasst werden sollen.

Im vorliegenden Entwurf ist bei der sog. „Quick-Freeze" Datenspeicherung nicht ersichtlich, wie sich der Zeitrahmen von 12 Monaten bemisst. Durch staatsanwaltschaftliche Anordnung wird die Löschungsverpflichtung ausgesetzt. Unklar ist, ob sich der Zeitrahmen von 12 Monaten auf die anfallenden Daten ab der Anordnung bezieht, oder auf die bis zur Anordnung angefallenen Daten. Die vorgesehene Regelung bringt daher nicht nur eine Speicherung von Daten auf Vorrat für 12 Monate, sondern für bis zu 18 Monate mit sich. Zum Zeitpunkt der staatsanwaltschaftlichen Anordnung bereits angefallene und gespeicherte Daten dürfen dann ebenfalls nicht gelöscht werden. Es ist eine Klarstellung dahingehend wünschenswert, auf welchen Zeitpunkt sich die Aussetzung der Löschungsverpflichtung durch staatsanwaltschaftliche Anordnung bezieht. Alternativ wird vorgeschlagen, dass sich der Zeitrahmen auf maximal 6 Monate vor staatsanwaltschaftlicher Anordnung und maximal 6 Monate nach staatsanwaltschaftlicher Anordnung bezieht.

Weiters verweisen wir betreffend die Speicherung auf Basis von Zellen und Sektoren auf die Rechtsprechung des EuGH zur Vorratsdatenspeicherung, dass gespeicherte Daten auf das absolut Notwendigste beschränkt werden müssen. Auch betreffend die Dauer der neuen Vorratsdatenspeicherung und den Umfang der zu speichernden Verkehrsdaten weisen wir auf die Rechtsprechung des EuGH zur Beschränkung der Speicherung auf das absolut Notwendigste hin.

Die im Entwurf gewählte Systematik, dass eine Löschungsverpflichtung aufgehoben wird und die Speicherverpflichtung über die Strafbestimmungen in § 109 TKG eingeführt werden, ist irreführend. Dementsprechend muss in der Bestimmung des § 99 TKG einerseits die Speicherverpflichtung festgelegt und andererseits der Widerspruch zur Löschungsverpflichtung aufgelöst werden.

Es sind durch den Regelungsentwurf nicht nur betriebsnotwendige Daten umfasst, sondern alle Verkehrsdaten, an denen die Löschungsverpflichtung des § 99 TKG umgesetzt wird.

Die Verpflichtung des § 99 Abs 1d TKG führt zu Rechtsunsicherheit. Einerseits verpflichten die Gerichtsbeschlüsse die Betreiber zur Geheimhaltung angeordneter Überwachungsmaßnahmen, andererseits bestehen Auskunftspflichten nach dem geltenden Datenschutzgesetz (DSG 2000) und in weiterer Folge nach der Datenschutzgrundverordnung (DSGVO).

Es ist Aufgabe des Gesetzgebers für Rechtssicherheit zu sorgen und klar zu stellen, ob Betreiber im Zuge ihrer datenschutzrechtlichen Auskunftspflichten über die Speicherung von Daten auf Grund staatsanwaltschaftlicher Anordnung nach § 99 TKG trotz einer etwaigen Geheimhaltungsverpflichtung in Beschlüssen nachkommen müssen oder nicht. Die vorliegende Bestimmung des § 99 Abs 1d TKG ist unbestimmt.

Die im Entwurf vorgesehene Weitergabe von Daten bedarf einer im Gesetz zwingend vorzusehenden Vorabkontrolle durch ein unabhängiges Gericht und sollte keinesfalls auf einfache Anordnung durch die Sicherheitsbehörde erfolgen. Hier ist jedenfalls vorab eine Kontrolle der unbedingten Notwendigkeit

der Erfassung der Daten erforderlich. Eine versteckte „Vorratsdatenspeicherung“ sollte keinesfalls möglich sein.

Die bereits zu § 97 Abs 1a angestellten Überlegungen zum Kostenersatz gelten auch für diese Bestimmung. Derzeit sieht der Gesetzesentwurf weder einen Kostenersatz für die Investitionen noch für die konkrete Mitwirkung an einzelnen Aufträgen vor - das ist entsprechend dem oben zitierten Erkenntnis des Verfassungsgerichtshofes (VfSlg 16.808) verfassungswidrig. Ergänzend zu den eingangs gemachten Ausführungen zur Pflicht zum Kostenersatz sei darauf hingewiesen, dass die Umstellung der Server und des hinterlegten Löschrhythmus Personalkosten in noch nicht abschätzbarer Höhe mit sich bringen wird. Weiter könnten je nach zu bestimmendem Zeitraum auch sonstige Hard- und Softwarekosten mit zu deckenden Investitionskosten anfallen. Unbedingt zusätzlich vorzusehen ist ein Kostenersatz für die tatsächliche Speicherung auf Anordnung der Staatsanwaltschaft. Im Ergebnis fordern wir aufgrund der erneuten Umstellung (es gab schon vergebliche Investitionen im Rahmen der Vorratsdatenspeicherung) einen zur Gänze deckenden Kostenersatz, weil der Aufwand auf Seiten der Betreiber ausschließlich im Interesse der öffentlichen Sicherheit und Strafrechtspflege liegt.

Zu § 137 Abs 9 (Übergangsbestimmungen)

Die Bereitstellung technischer Einrichtungen und die Implementierungsdauer richtet sich nach dem Zeitpunkt des Inkrafttretens. Diese Regelungen bedeuten eine grundlegende Umstrukturierung der betroffenen technischen und organisatorischen Prozesse. Es sind umfangreiche technische und organisatorische Änderungen sowie massive Investitionen bei jedem Betreiber, sowohl bei klassischen Telekommunikationsbetreibern als auch bei MVNOs zu tätigen.

Weiters richtet sich die erforderliche Umsetzungsdauer nach der Belastung der Unternehmensressourcen durch den Geschäftsbetrieb, auch das variiert je nach Zeitpunkt des Geschäftsjahres.

Hinzu kommen externe Einflüsse durch andere Gesetzes- und Regulierungsvorgaben, Maßnahmen zur Umsetzung der Verordnung (EU) 531/2012 („Roaming-Verordnung“) oder der Datenschutz-Grundverordnung, die die technischen Implementierungsressourcen von Betreibern an ihre Grenzen bringen.

Die im vorliegenden Gesetzesentwurf vorgesehene Umsetzung zum 01.01.2018 ist nicht machbar. Eine nachhaltige und funktionierende Implementierung bedarf eines Umsetzungszeitraumes von 12 Monaten ab Inkrafttreten der geplanten Bestimmungen.

Wir ersuchen um Berücksichtigung unserer Überlegungen und verbleiben

mit freundlichen Grüßen

KommR DI Dr. Richard Schenz
Vizepräsident

Mag. Anna Maria Hochhauser
Generalsekretärin