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

Parlamentsdirektion
Innenausschuss

per E-Mail:
Stellungnahmen.Innenausschuss@parlament.gv.at

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen, Sachbearbeiter	Durchwahl	Datum
GZ. 13260.0060/1-L1.3/2018	Rp 1685/17/TK/MH	4273	26.3.2018

Regierungsvorlage eines Bundesgesetzes, mit dem das Sicherheitspolizeigesetz, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden - Ausschussbegutachtung gem. § 40 GOG - Stellungnahme

Sehr geehrte Damen und Herren,

die Wirtschaftskammer Österreich begrüßt den Beschluss des Innenausschusses, die Regierungsvorlage eines Bundesgesetzes, mit dem das Sicherheitspolizeigesetz, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden einer Ausschussbegutachtung zu unterziehen. Wir danken für die Übermittlung des Entwurfes und nehmen 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 beim Zugriff der Behörden auf Video- und Tondaten und dem Ausbau der Kennzeichenerkennungssysteme (betrifft alle Autobesitzer in Österreich) fraglich, ob die vorgesehenen 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 SPG

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.

Nicht zulässig ist die Verarbeitung von Daten über nichtöffentliches Verhalten. Unklar erscheint in diesem Zusammenhang, was unter „nicht öffentlichem Verhalten" zu verstehen ist. Diesbezüglich geben auch die Erl keinen Aufschluss.

Fraglich erscheint weiters die Auslegung der Formulierung „...Rechtsträger des öffentlichen oder privaten Bereichs, sofern letzteren ein öffentlicher Versorgungsauftrag zukommt...". In den Erl werden als Beispiele die ASFINAG, Bahnhöfe, Flughäfen und öffentliche Verkehrsbetriebe genannt. Ein genauer Betroffenenkreis ergibt sich aus den Erl jedoch nicht. Eine Definition, welche Tätigkeiten als öffentlicher Versorgungsauftrag zu sehen sind, wäre daher wünschenswert.

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 SPG

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 wird. Ein bedingter Vorsatz sollte in einer solchen Situation noch nicht kostenpflichtig sein.

Zu § 93 a SPG

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 vier 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, 98a Abs 1 und 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 und 3 StVO wird klar, welche Abkehr von der bisherigen Datenschutz-, -verarbeitungs- und -nutzungspolitik dies bedeutet.

§ 98a StVO schafft eine Rechtsgrundlage, um die im Rahmen der Section Control ermittelten Daten mit den Fahndungsevidenzen für die Zwecke des § 54 Abs 4b SPG abzugleichen. Die in § 98a StVO vorgesehene Meldung und auf Anforderung der Landespolizeidirektionen zu erfolgende Weitergabe der im Rahmen der Section Control ermittelten Daten wird kritisch gesehen. Ein solcher Eingriff sollte, wenn überhaupt, nur mit gerichtlichem Auftrag zulässig sein. Die Dauer der Überwachung und der Speicherung sowie die zulässigen Zwecke sollten jedenfalls detaillierter und restriktiver geregelt werden.

Die Ausweitung der Kennzeichenerkennung sowie die Verpflichtung zur Übermittlung der Daten an die Landespolizeidirektion darf nicht zur Schaffung einer technischen Basis für die Einführung flächendeckender Section-Control-Systeme am gesamten Autobahnen- und Schnellstraßennetz führen. 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

§ 97 Abs 1a TKG

Ungeachtet der Frage, inwiefern eine Registrierungspflicht für Wertkarten eine Verbesserung der Aufklärung von Verbrechen oder der Abwehr von Gefahren herbeizuführen vermag, ist zu begrüßen, dass gegenüber der im Juli 2017 konsultierten Fassung der genannten Bestimmung eine Verbesserung in der Textierung vorgenommen wurde. Konkret ist positiv anzumerken, dass nunmehr für den relevanten Zeitpunkt der Erhebung der zu registrierenden Kundendaten nicht mehr auf den Vertragsschluss abgestellt wird, sondern die Erhebung auch nachgelagert erfolgen kann und somit nicht allein am Point of Sale erfolgen muss. Das ist eine wesentliche Voraussetzung für den Vertrieb von Wertkarten.

Freilich ist bei den noch näher im Verordnungswege zu bestimmenden Identifizierungsverfahren jedenfalls eine möglichst große Bandbreite von am Markt erhältlichen Systemen und Verfahren zuzulassen (zB auch e-Mandat, Bank-Ident). Vor allem müssen auch Verfahren ermöglicht werden, die eine zuverlässige Registrierung bzw Authentifizierung außerhalb von Verkaufsstellen für Wertkarten zulassen (zB Online-Registrierung). Nur dadurch kann sichergestellt werden, dass wichtige Vertriebswege für Handy-Wertkarten (zB Supermärkte und Trafiken) nicht verschwinden.

Im Einzelnen ist zur neuen Bestimmung des § 97 Abs 1a TKG anzumerken, dass die Pflicht zur Erfassung der Wohnanschrift problematisch ist. Diese ist nicht auf den allgemein als Identifikationsdokument anerkannten Ausweisen vermerkt und müsste daher auf anderen Wegen geprüft werden, was den Telekommunikationsanbietern jedoch nicht zuzumuten ist. Allerdings ist dieses Datum für die Identifizierung des Teilnehmers auch nicht relevant, sodass davon abgegangen werden kann, ohne das Regelungsziel der Bestimmung zu konterkarieren. Mit dem künftig verbindlich zu erfassenden Datum

des Geburtstages hat man in Kombination mit dem Namen die zur Identifikation der Person erforderlichen Daten. Schließlich haben die Ermittlungsbehörden sicheren Zugang zu den Meldedaten.

Weiters sei darauf hingewiesen, dass bei der Erfassung von Daten aus Dokumenten in nicht-lateinischer Schrift diese Übertragung und Zuordnung nicht mit der gebotenen (und strafbewehrten) Qualität sichergestellt werden kann. Hierzu sollte es Ausnahmen geben, zumindest bei der Einbeziehung der Identifizierungspflicht in die Verwaltungsstraftatbestände. Gleiches gilt generell bei ausländischen Dokumenten, da hier die Betreiber nicht verlässlich wissen, welche Dokumente welchen Grad an Richtigkeit und Aktualität haben.

Von der Nachregistrierung bei bestehenden Postpaid-Kunden sollte abgesehen werden: Hier haben die Betreiber schon aus Gründen einer gesicherten Forderungseintreibung dafür Sorge getragen, dass der vorhandene Datenbestand ggf. eine gerichtliche Rechtsdurchsetzung ermöglicht. Daher sind diese Daten hinreichend für eine Identifizierung geeignet. Sollte dennoch eine Nachregistrierung erforderlich sein, so ist hier aufgrund umfangreicher Maßnahmen und Eingriffe in die Systeme der Betreiber eine Umsetzungsfrist von mindestens 18 Monaten erforderlich. Im Falle einer Nachregistrierung von bereits ausgegebenen aktiven Wertkarten, sollte an den nächstfolgenden Vorgang der Aufladung des Guthabens angeknüpft werden. Die gesetzlich vorgesehene Frist per 1. Jänner 2019, ab der Registrierungen jedenfalls verpflichtend sein sollen, ist bei bereits ausgegebenen Wertkarten nicht einhaltbar, da diese noch bis zu 12 Monate gültig sein können und erst daran anschließend eine Aufladung erforderlich wird, um deren Gültigkeit aufrecht zu erhalten.

Weiters würde dies sicher auch die Implementierungskosten senken, die von der öffentlichen Hand zu tragen sind, was seit einer Entscheidung des Verfassungsgerichtshofs aus 2003 (VfGH v. 27.2.2003, Az. G37/02) außer Frage steht - aber sich leider dennoch nicht im Entwurf findet. Um unnötige nachgelagerte Diskussion oder gar Rechtsstreitigkeiten zu vermeiden, muss zeitgleich mit den Änderungen im TKG auch der Kostenersatz geregelt sein. Es sei ergänzend darauf hingewiesen, dass die Registrierung von Wertkarten allein im Interesse der Sicherheits- und Ermittlungsbehörden liegt, weshalb nur ein 100%iger Kostenersatz angemessen ist (die Betreiber sind erst vor nicht allzu langer Zeit auf 20% der Investitionskosten für die Vorratsdatenspeicherung sitzen geblieben).

Schließlich sollte die Verordnung unbedingt mit den Betreibern (der Fachverband Telekom-Rundfunk bietet an, hierfür eine Plattform zu organisieren) diskutiert werden, wie es sich seinerzeit bei der Einführung der Vorratsdatenspeicherung bewährt hat, und sie sollte so rasch wie möglich erlassen werden. Es wird dann nämlich erst die nötige Rechtssicherheit gegeben sein, sodass Investitionen in die Erfassungssysteme getätigt werden, diese evaluiert und getestet werden können. Dazu wird ein Zeitraum von mindestens einem Jahr zwischen Erlass der Verordnung und Inkrafttreten der Identifizierungspflicht erforderlich sein.

Wir ersuchen um Berücksichtigung unserer Überlegungen und verbleiben

mit freundlichen Grüßen

KommR DI Dr. Richard Schenz
Vizepräsident

Mag. Anna Maria Hochhauser
Generalsekretärin