WIEN / 21. März 2018

STELLUNGNAHME

Zum Ministerialentwurf betreffend Bundesgesetz, mit dem das Sicherheitspolizeigesetz, die Straßenverkehrs-ordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden (Sicherheitspolizeigesetz, Straßenverkehrsordnung 1960 u.a., Änderung – 15 d.B. XXVI. GP)

Für epicenter.works

Mag.[a] Angelika Adensamer, MSc
Mag. Alexander Czadilek
Alina Hanel, BA
Thomas Lohninger, BA
Ing. Dr. Christof Tschohl

EPICENTER .WORKS
for digital rights

Stellungnahme im Begutachtungsverfahren[1] zum Entwurf eines Bundesgesetzes, mit dem das Sicherheitspolizeigesetz, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden (15 d.B. XXVI. GP)

EPICENTER.WORKS NIMMT ZUM VORLIEGENDEN GESETZESENTWURF WIE FOLGT STELLUNG

VORWORT UND KURZFASSUNG

Mit den geplanten Änderungen im vorliegenden Entwurf soll eine flächendeckende Videoüberwachung des öffentlichen Raums und eine umfassende (Kfz-)Kennzeichenerfassung auf Österreichs Straßen eingeführt werden. Die Anonymität der Kommunikation im Mobilfunknetz soll durch eine Registrierungspflicht von SIM-Karten massiv eingeschränkt werden. Alle drei Maßnahmen haben eine enorme Streubreite in der gesamten Bevölkerung. Diese Formen der Überwachung greifen direkt in die Privatsphäre von allen Autofahrerinnen und Autofahrern, allen Fahrgästen der videoüberwachten öffentlichen Verkehrsmitteln und den Nutzerinnen und Nutzern der über 4,5 Millionen Wertkarten in Österreich ein. Der vorliegende Entwurf beinhaltet deshalb drei neue Formen der anlasslosen Massenüberwachung und wird von uns als unverhältnismäßig und grundrechtswidrig abgelehnt.

Begründet werden diese Einschränkungen der Grund- und Freiheitsrechte aller in Österreich lebenden Menschen mit der Notwendigkeit dieser Maßnahmen für die Aufrechterhaltung der öffentlichen Ordnung und Sicherheit und insbesondere mit dem Schutz vor terroristischen Angriffen. Diese Notwendigkeit der Maßnahmen wird zwar medial vom Bundesminister für Inneres immer wieder betont und hervorgehoben, allerdings wurden bislang keinerlei Belege vorgelegt, dass diese Maßnahmen tatsächlich die Erhöhung der allgemeinen Sicherheit bewirken würden. In den Erläuterungen zu den Gesetzesentwürfen wird nicht einmal der Versuch unternommen, die Notwendigkeit der Maßnahmen zu begründen. Es wurde keine Evaluation der Sicherheitslage in Österreich oder der Auswirkungen auf diese durch die Einführung der neuen Überwachungsmaßnahmen durchgeführt.

Im August 2017 hat einer der international renommiertesten Experten zum Thema Überwachung, Bill Binney, ehemaliger technischer Direktor der NSA, bei einer Pressekonferenz zum Überwachungspaket in Wien bestätigt[2], dass es keinen Beleg dafür gibt, dass das massenweise Sammeln und Auswerten von Daten tatsächlich für mehr Sicherheit sorgt. Allerdings gebe es sehr viele Belege dafür, dass zu viele Daten der Verbrechensprävention aufgrund der Schwierigkeit, die Datenflut zu analysieren, sogar hinderlich sind.

epicenter.works warnt eindringlich vor der Einführung gesetzlicher Bestimmungen mit polizeistaatlichen Tendenzen und fordert die Bundesregierung auf, den vorliegenden überschießenden Gesetzesentwurf zurückzuziehen. Neuerlich soll den Sicherheitsbehörden ein ganzes Bündel mächtiger Instrumente in die Hand gegeben werden, obwohl sachlich aufgrund der

1 https://parlament.gv.at/PAKT/VHG/XXVI/AUA/AUA_00004/index.shtml

2 Der Falter 33/17. Siehe: https://epicenter.works/medienspiegel/648.

Vorschläge, der Erläuterungen und der politischen Begleitaussagen nicht nachvollziehbar ist, warum diese Instrumente notwendig sind und die bisherigen Möglichkeiten nicht ausreichen. Neben dieser allgemeinen Kritik verorten wir zahlreiche Grundrechtswidrigkeiten in den einzelnen Bestimmungen, die nicht in Einklang mit der österreichischen Verfassung stehen.

Der Gesetzgeber ist dafür verantwortlich, grundrechtskonforme Gesetze zu erlassen – der Verfassungsgerichtshof kann nur das letzte Mittel sein, um grundrechtswidrige Gesetze wieder aufzuheben. Das darf aber nicht zur Regel werden!

Zudem geht es in der Debatte um (Massen-)Überwachung **nicht** um eine Balance zwischen Freiheit und Sicherheit. „Freiheit" und „Sicherheit" sind keine kommunizierenden Gefäße oder Werte, die einander gegenüberstehen. Das bedeutet, dass ein „Mehr" an Freiheit keinesfalls zwingend die Sicherheit gefährdet. Vor allem aber bedeutet es, dass die Einschränkung bürgerlicher Freiheiten umgekehrt keineswegs zwingend zu mehr Sicherheit führt. **Weniger Freiheit bedeutet zunächst einmal nur eines: weniger Freiheit.**

Die Kritik bezieht sich konkret auf folgende Punkte:

- Eine Überwachungsgesamtrechnung wurde nicht durchgeführt.
- Eine Wirkungsfolgenabschätzung bzgl. der Auswirkungen auf Grundrechte und Gesellschaft fehlt im Begutachtungsentwurf.
- Die Schwellen für Grundrechtseingriffe werden sukzessive herabgesetzt.
- Insgesamt soll eine Fülle an neuen Überwachungsbefugnissen mit grundrechtlich äußerst bedenklichen Tendenzen Einzug in den österreichischen Rechtsbestand halten. Es ergibt sich zunehmend das Bild, dass Österreich in einen Polizei- und Überwachungsstaat umgebaut wird.
- Es entstehen **enorme finanzielle Kosten** für eingriffsintensive Maßnahmen, deren **Beitrag zur Erhöhung der Sicherheit nicht erwiesen** ist.

Inhaltsverzeichnis

SICHERHEITSFOREN

Zu Artikel 1 Ziffer 2 (§ 25 Abs. 1 SPG-E):

Mit dem vorliegenden Entwurf sollen sogenannte „Sicherheitsforen" eingeführt werden. Verschiedene Personen aus der Bevölkerung sollen die Sicherheitsbehörden u.a. bei der Vorbeugung gefährlicher Angriffe gegen Leben, Gesundheit und Vermögen unterstützen.

Begrüßenswert ist, dass der Entwurf nicht mehr vorsieht, dass personenbezogene Daten an „Sicherheitspartnerinnen" und „Sicherheitspartner" weitergegeben werden. Der Entwurf sieht jedoch weiterhin sogenannte „Sicherheitsforen" vor, ohne wesentliche Aspekte zu regeln:

Es geht aus dem Entwurf weiterhin nicht hervor, wer, wie und wann von den Sicherheitsforen erfährt, bzw. zu einer Teilnahme eingeladen wird, bzw. ob diese „Sicherheitsforen" öffentlich zugänglich sind. Es könnten also **informelle Hierarchien** zwischen den der Polizei näher stehenden Bevölkerungsgruppen entstehen, und denen, die sich von den Sicherheitsbehörden weniger repräsentiert fühlen. Insofern ist in den Sicherheitsforen auf eine Wahrung von Diversität zu achten und darauf, dass die Teilnahme an diesen offen und transparent erfolgt.

Problematisch ist weiters der unreflektierte Bezug auf ein sogenanntes „subjektives Sicherheitsgefühl". Die Gefahr, dass es aufgrund von vorhandenen Vorurteilen in der österreichischen Gesellschaft zu vermehrtem **„racial profiling"** kommt, ist gegeben. Beispielsweise schreibt DerStandard.at am 09.08.17 zu diesem Thema: „Das unbekannte schwarze Fahrzeug in Mank war tagelang Thema im Onlineforum der kleinen Stadt im niederösterreichischen Mostviertel. Das Auto mit zuagrastem

Kennzeichen war immer dann unterwegs, wenn normale Bürger schon oder noch schlafen. Sehr verdächtig! Die Manker Polizeiinspektion nahm die Hinweise ernst und sich der Sache an. Nach einer Observierung gaben die Beamten Entwarnung: Es war nur ein neuer Zeitungszusteller, der spätnachts seine Arbeit erledigte."[3] Die Hinweise von Bürgerinnen und Bürge auf ein ausländisches Kennzeichen scheinen hier wesentliche Grundlage für eine polizeiliche Untersuchung gewesen zu sein. Zur Stärkung des subjektiven Sicherheitsgefühls wäre es notwendig, Antirassismusschulungen mit den „Sicherheitspartnerinnen" und „Sicherheitspartnern" durchzuführen, denn wie der Begriff „subjektives Sicherheitsgefühl" bereits selbst erklärt, geht es dabei nicht um die Abwehr einer realen Gefahr.

In den Erläuterungen (S. 1) ist von einem Beispiel die Rede, in dem durch das Reparieren einer defekten Parkbeleuchtung gefährlichen Angriffen vorgebeugt würde. Diese Ansichtsweise scheint sich auf die – sozialwissenschaftlich umstrittene – **Broken Windows Theorie** zu stützen. Es ist nicht nachvollziehbar, dass ein „Sicherheitsforum" sich zur Vorbeugung gefährlicher Angriffe um Parkbeleuchtungen kümmern sollte, für die es doch ohnehin klare Zuständigkeiten gibt, anstatt sich tatsächlichen sozialen Problemen anzunehmen. Radikalisierung und Rassismus sind viel grundlegendere Ursachen für Straftaten als eine funktionsunfähige Parkbeleuchtung.

Eine bessere Vernetzung mit Communities als vertrauensbildende Maßnahme und zur frühzeitigen Erkennung radikaler Tendenzen wäre wünschenswert. Hinreichende Sozialmaßnahmen stellen unserer Ansicht nach die beste Art der Präventionsarbeit gegen Radikalisierungstendenzen dar. Der vorliegende Entwurf erweckt jedoch den Eindruck, dass es bei der Kooperation mit den Sicherheitsbehörden nicht unbedingt um diese durchaus sinnvollen Sozialmaßnahmen geht.

VIDEOÜBERWACHUNG

Eine Evaluation der Sicherheitslage in Österreich oder der Auswirkungen groß angelegter Videoüberwachung im öffentlichen Raum wurde bislang nie durchgeführt. Vielmehr wird die Notwendigkeit der Maßnahmen ohne jegliche wissenschaftliche Auseinandersetzung mit der Thematik einfach postuliert. **Trotz nicht nachgewiesener Effektivität**[4] der automatisierten Videoüberwachung und der damit verbundenen negativen Auswirkungen[5] einer flächendeckenden Überwachung auf Individuen und Gesellschaft sollen nun, nicht lange nach dem Inkrafttreten des Polizeilichen Staatsschutzgesetzes (PStSG), weitere Überwachungsmaßnahmen Teil des österreichischen Rechtsbestandes werden.

Zu Artikel 1 Ziffer 3 (§ 53 Abs. 5 SPG-E):

Mit der Änderung dieser Bestimmung wird sowohl eine Herausgabepflicht von Videomaterial (Bild- und Tondaten) für Rechtsträger des öffentlichen und privaten Bereichs, sofern diesen ein öffentlicher Versorgungsauftrag zukommt, als auch der direkte Zugang zu diesem Bild- und Tonmaterial (Echtzeit-Streaming) normiert.

3 Der Standard: Bürgerpolizei. Dein Nachbar, der Freund und Helfer. Online: https://www.derstandard.at/2000062427685/Buerger-Polizei-Dein-Nachbar-der-Freund-und-Helfer. Aufgerufen am: 19.03.2018.

4 Vgl. Kees, Benjamin J., Algorithmisches Panopticon - Identifikation gesellschaftlicher Probleme automatisierter Videoüberwachung sowie Rothmann, Zur Evaluation der sicherheitstechnischen Eignung von Videoüberwachung, juridikum 4/2012, 483ff mit weiteren Nachweisen.

5 Vgl. Wright, David, and Reinhard Kreissl (eds.) Surveillance in Europe, Routledge 2015.

Weiters wird die Möglichkeit, rechtmäßig verarbeitete Bild- und Tondaten, die von öffentlichen oder privaten Rechtsträger freiwillig an die Sicherheitsbehörde übermittelt wurden, zu verwenden, erheblich erweitert.
Die aktuell gültige Regelung erfährt eine umfassende Erweiterung, obwohl keine objektiven Mängel am derzeitigen System benannt werden können. Die Daten durften nach bisheriger Rechtslage nur verwendet werden, wenn die jeweiligen Rechtsträger das Material freiwillig zur Verfügung stellten. Ein zwangsweiser Zugriff ist bislang nur unter den strengen Voraussetzungen der StPO im Rahmen der Sicherstellung zulässig (die Sicherstellung muss aus Beweisgründen erforderlich sein und es muss eine Anordnung der Staatsanwaltschaft vorliegen).
Neu in dem vorgelegten Entwurf ist, dass nun **auch Tonaufnahmen** von der Behörde verarbeitet werden dürfen sollen. Nach den Erläuterungen wird diese Neuerung vorgeschlagen, damit nun auch Handyaufnahmen verarbeitet werden können[6]. Es besteht die Gefahr, dass dies eine **Anregung** darstellt, gegen § 120 StGB (Missbrauch von Tonaufnahmen und Abhörgeräten) zu verstoßen. Zu beachten ist nämlich, dass auch die Weitergabe von Tonbandaufnahmen an die Polizei strafrechtlich relevant sein kann.

Zur freiwilligen Herausgabe gem. § 53 Abs. 5 Satz 1 und 2 SPG-E:

Bisher durften die personenbezogenen Bild- und Tondaten, die freiwillig durch öffentliche und private Rechtsträger an die Sicherheitsbehörden übermittelt wurden nur für die Zwecke des § 54 Abs. 3 SPG verwendet werden.
Es war bisher nicht zulässig die Daten zur Vorbeugung von minderschwerer Kriminalität[7] zu verwenden, sondern nur bei schweren Verbrechen. Die Daten dürfen nun zusätzlich auch beispielsweise für die Zwecke der *„Gefahrenforschung"*, zur Vorbeugung *„wahrscheinlicher gefährlicher Angriffe"* oder auch nur zur Aufrechterhaltung der öffentlichen Ordnung bei bestimmten Ereignissen durch die Sicherheitsbehörden verarbeitet werden.
Dies ist eine bedenkliche Ausweitung der Verarbeitungszwecke von Bild- und Tonmaterial. Typischerweise geht es hierbei um Videoaufnahmen von öffentlich zugänglichen Orten, auf denen häufig eine Vielzahl von Personen abgebildet sind, die auch von der Datenverarbeitung betroffen sind, obwohl sie in keiner Weise etwas mit einem gefährlichen Angriff zu tun haben. **Damit wird der Grundrechtseingriff in Privatsphäre der Bevölkerung massiv ausgeweitet.**
Die Novelle scheint davon auszugehen, dass die freiwillige zur Verfügungsstellung von privaten und öffentlichen Rechtsträgern der von ihnen Aufgezeichneten Bild- und Tondaten einer Zustimmung der abgebildeten Personen gleich zuhalten ist. Dem ist nicht so.

Zur Herausgabeverpflichtung gem. § 53 Abs. 5 Satz 3 bis 5 SPG-E

Die Herausgabepflicht soll nur aus den in § 53 Abs. 5 Satz 3 SPG-E genannten taxativen Gründen bestehen. Damit wird allerdings **nur scheinbar eine Einschränkung** normiert, denn hier werden Zwecke zum Schutz von praktisch allen Individualrechtsgütern, die das österreichische Strafgesetzbuch kennt, genannt. Der Anwendungsbereich der Bestimmung ist somit äußerst weit gefasst und kennt praktisch keine Differenzierung. Eine Erweiterung bezüglich der Verwendung aller ermittelten Bild- und Tondaten erfolgt insoweit, als diese nun auch schon zur *„Vorbeugung*

6 Vgl. Erläuterungen. Online: https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00015/imfname_681955.pdf. S. 2.
7 Vgl. Keplinger, Rudolf / Pühringer Lisa, Sicherheitspolizeigesetz – Praxiskommentar, 16. Auflage, 2016, proLibris.at, S. 206.

wahrscheinlicher gefährlicher Angriffe" zulässig ist. Sowohl die *„Vorbeugung"* als auch die *„Wahrscheinlichkeit"* sind äußerst interpretationsbedürftige und weite Gesetzesbegriffe, die einen **Eingriff in das Recht auf Datenschutz als auch auf das Recht auf Privatsphäre für die Sicherheitsbehörden sehr einfach möglich machen**[8]. Im Gegensatz zur Voraussetzung des konkreten Verdachts lässt sich der Eingriff somit mit jeder einfachen Einschätzung einer Ermittlungsbeamtin oder -beamten, es könnte eine Gefahr bestehen, begründen. Problematisch ist jedenfalls, dass die Befugnisse nach diesem Bundesgesetz, und somit **Grundrechtseingriffe, bereits weit im Vorfeld einer strafbaren Handlung** ausgelöst werden und die Zahl an Betroffenen eine **extrem hohe Streubreite** aufweist. Daher ist die hier normierte Maßnahme eine Befugnis zur Massenüberwachung.

Zu bezweifeln ist, dass die geplante Maßnahme überhaupt geeignet ist, das Ziel der Aufrechterhaltung der öffentlichen Ruhe und Ordnung sowie der Aufrechterhaltung der Sicherheit der Bevölkerung, zu erreichen. Wie die terroristischen Anschläge der vergangenen Jahre in London, Paris oder Berlin gezeigt haben, konnten auch die CCTV-Systeme dieser Städte **keinen Anschlag verhindern**. Eine flächendeckende Überwachung des öffentlichen Raums und damit einer Unzahl unbescholtener Menschen ist auch **nicht das gelindeste Mittel**, um das erklärte und legitime Ziel zu erreichen. Eine erhöhte Polizeipräsenz durch besser geschultes Personal an bestimmten hoch frequentierten und verkehrstechnisch wichtigen Punkten wäre zur Verhinderung krimineller Handlungen nicht nur effektiver, sondern würde bei der Bevölkerung zudem in geringerem Maße das abstrakte Gefühl verursachen, ständig überwacht und kontrolliert zu werden. Stattdessen würde das subjektive Sicherheitsgefühl der Menschen erhöht. Schon die mangelnde Geeignetheit und Erforderlichkeit der Maßnahme lassen diese als nicht verhältnismäßig und somit als grundrechtswidrig erscheinen[9] .

Eine Schnittstelle zu den Videoüberwachungsanlagen der betroffenen Rechtsträger stellt zudem ein enormes Sicherheitsrisiko dar, da über diese auch kriminelle Angreifer Zugang zu den Systemen sowohl der Betreiber, als auch der Sicherheitsbehörden erlangen können. Im schlimmsten Fall könnten die Videoüberwachungsanlagen dazu genutzt werden, terroristische Anschläge zu koordinieren oder effektiver durchzuführen. Es gibt weder eine Ermächtigung zu einer Durchführungsverordnung, in der die technischen Details festgelegt werden, noch irgendwelche organisatorischen und technischen Maßnahmen um Missbrauch beim Datenzugriff hintan zu halten. Dass solche dringend notwendig sind, zeigt nicht zuletzt die bestehende Praxis bei Datenabfragen durch BeamtInnen der Sicherheitsbehörden, die kürzlich auch Thema einer parlamentarischen Anfrage[10] waren. **Die Regelung widerspricht somit dem Grundrecht auf Datenschutz.**

Im Entwurf wird auch eine **Echtzeitüberwachung**[11] der Menschen im öffentlichen Raum normiert (der Begriff „Zugang" umfasst sowohl den Fernzugriff auf Echtzeitdaten als auch den lokalen Zugang zu Videoanlagen der Betreiber), es bleibt aber völlig unklar, wie die technische Umsetzung aussehen soll. Dieser Punkt wird in den Erläuterungen nicht einmal ansatzweise thematisiert. Dabei hat die konkrete technische Umsetzung entscheidende Bedeutung für die Beurteilung der Schwere des Grundrechtseingriffs. Diesbezüglich verweisen wir auf die **enormen Mehrkosten** auf seiten der Betreiber wie ASFINAG, ÖBB oder Wiener Linien, sollten diese ihre bestehenden dezentralen und teils

8 Diesbezüglich verweisen wir auf unsere Stellungnahmen zum Polizeilichen Staatsschutzgesetz: https://epicenter.works/documents?field_tags_tid=5

9 Verletzung des Grundrechts auf Datenschutz gem. § 1 DSG, des Rechts auf Achtung des Privatlebens gem. Art. 8 EMRK.

10 https://www.parlament.gv.at/PAKT/VHG/XXV/J/J_11061/index.shtml.

11 Vgl. Erläuterungen S. 2, „Echtzeitstreaming".

datenschutzfreundlichen Videoüberwachungsanlagen umrüsten müssen. Ein Echtzeitstreaming ist zum Beispiel im Falle einer dezentral gespeicherten Wagonüberwachung technisch nicht möglich.

Eine Schnittstelle zu den Videoüberwachungsanlagen der betroffenen Rechtsträger stellt zudem ein enormes Sicherheitsrisiko dar, da über diese auch kriminelle Angreifer Zugang zu den Systemen sowohl der Betreiber, als auch der Sicherheitsbehörden erlangen können. Im schlimmsten Fall könnten die Videoüberwachungsanlagen dazu genutzt werden, terroristische Anschläge zu koordinieren oder effektiver durchzuführen. Es gibt weder eine Ermächtigung zu einer Durchführungsverordnung, in der die technischen Details festgelegt werden, noch irgendwelche organisatorischen und technischen Maßnahmen um Missbrauch beim Datenzugriff hintan zu halten. Dass solche dringend notwendig sind, zeigt nicht zuletzt die bestehende Praxis bei Datenabfragen durch BeamtInnen der Sicherheitsbehörden, die kürzlich auch Thema einer parlamentarischen Anfrage[12] waren. Die Regelung widerspricht somit dem Grundrecht auf Datenschutz.

In den Materialien wird zwar behauptet, es gäbe einen **Rechtsschutz** durch den oder die Rechtsschutzbeauftragte für Betroffene[13] gem. § 91c Abs. 1 SPG-E, durch die geplante Einführung der Wortfolge „erster Satz" im entsprechendem Paragraphen wird der Rechtsschutz aber auf die Fälle der freiwilligen Herausgabe beschränkt. Die Erläuterungen stehen demnach im Widerspruch zu der vorgeschlagenen Novelle. **Es ist gerade keine Rechtsschutzeinrichtung vorgesehen, die im Falle, dass ein Rechtsträger verpflichtet wird, Videomaterial herauszugeben, die Interessen der Betroffenen wahrt.** Aber auch die Pflicht, den Rechtsschutzbeauftragten oder die Rechtsschutzbeauftragte im Nachhinein zu informieren – wie es in § 91c SPG grundsätzlich vorgesehen ist – würde keinen hinreichenden Rechtsschutz darstellen. Auch der nicht vorhandene Rechtsschutz macht die Bestimmung im Ergebnis verfassungswidrig (ausführlicher zum mangelnden Rechtsschutz siehe unten zu Ziffer 12).

Weiters wird durch die vorgesehene Bestimmung das **Recht auf Eigentum gem. Art. 1 1. ZP. EMRK** verletzt. § 53 Abs. 5 normiert auch die Verpflichtung der Rechtsträger, die aufgenommenen Daten zu speichern oder Echtzeitstreaming zur Verfügung zu stellen. Das bedeutet, dass manche Rechtsträger u.U. zusätzliche technische Vorrichtungen anschaffen müssen, um das zu ermöglichen. Die Speicherpflicht beginnt mit dem Zeitpunkt, in dem von dem Herausgabeverlangen Kenntnis erlangt wird. Das bedeutet, dass private und öffentliche Rechtsträger dazu gezwungen sind, sich bereits im Vorfeld eines Herausgabeverlangens um besagte technische Mittel zu kümmern. Das ist jedenfalls eine **unverhältnismäßig** hohe Belastung. Weiters ist es **gleichheitswidrig**, zu verbieten, dass Videos gelöscht werden können, wohingegen es weiterhin jederzeit möglich sein soll, gar keine Videoaufzeichnungen durchzuführen.

Zusätzlich verschärft wird diese Problematik dadurch, dass nicht hinreichend klargestellt ist, welche privaten Rechtsträger die Herausgabepflicht trifft. Das Gesetz stellt auf einen „öffentlichen Versorgungsauftrag" ab. Wer darunter fällt, ist unklar. Aus diesem Grund **v**erstößt der Entwurf außerdem gegen das Bestimmtheitsgebot**.**

Die Bestimmung knüpft außerdem an der „rechtmäßigen Verarbeitung" von Bild- und Tonaufnahmen an. Es ist allerdings unklar, ob dies bedeutet, dass die Sicherheitsbehörden selbst bevor sie diese Befugnis in Anspruch nehmen, verpflichtet sind, zu prüfen, ob die ursprüngliche Datenverarbeitung überhaupt rechtmäßig erfolgt ist.

12 https://www.parlament.gv.at/PAKT/VHG/XXV/J/J_11061/index.shtml.

13 Vgl. Erläuterungen, S. 2.

Rechtsschutz

Zu Artikel 1 Ziffer 12 (§ 91c Abs. 1 SPG-E)

Betreiberinnen und Betreiber von Videoüberwachungsanlagen sind verpflichtet, den Sicherheitsbehörden Bild- und Tondaten auf deren Verlangen herauszugeben. Hierzu ist nicht einmal die bloße Verständigung des Rechtsschutzbeauftragten (RSB) vorgesehen. Im Gegenteil – sie wird explizit ausgeschlossen. Dass der ohnehin schon unzureichende Rechtsschutz ausgeschlossen wird, wird nicht begründet und verletzt offensichtlich Art. 8 Abs. 3 GRC und Art. 13 in Verbindung mit Art. 8 EMRK.

Weiters stellt die Einfügung der Wortfolge „erster Satz" in den § 91c SPG-E eine **Umgehung der Verfassungsbestimmung § 91a Abs. 3 SPG**, wonach die Rechte des Rechtsschutzbeauftragten, die ihm gem. § 91c SPG zu kommen, nur mit einem erhöhten Präsenz- und Konsensquorum im Nationalrat eingeschränkt werden dürfen. Eine teleologische Interpretation der Bestimmung lässt zweifellos darauf schließen, dass somit auch neu hinzukommende Überwachungsbefugnisse, die mit den bestehenden in Zusammenhang stehen, der Kontrolle des Rechtsschutzbeauftragten zu unterstellen sind.

Aufgrund der Streubreite (unzählige Menschen sind von der Maßnahme betroffen) und der Intensität des Eingriffs, ist ein solch **mangelndes Rechtsschutzsystem** gänzlich abzulehnen. Insbesondere im Hinblick auf die immer ausgefeilteren technischen Möglichkeiten der Videoüberwachung wie „motion tracking" oder „face recognition", ist es nicht hinnehmbar, dass der RSB, der den kommissarischen Rechtsschutz für Betroffene ausüben soll, die von der Maßnahme keine Kenntnis erlangen, den Grundrechtseingriff vorab nicht genehmigen muss.

Im Klartext bedeutet diese Möglichkeit angesichts der gegenwärtigen technologischen Entwicklungen, dass jede Person anhand eines Referenz-Bildes in Echtzeit innerhalb eines flächendeckenden öffentlichen und privaten Videonetzwerks gefunden werden kann – wer freilich bewusst nicht gefunden werden will, wie insbesondere professionelle Kriminelle, wird viel eher einen Weg finden, sich trotzdem zu verbergen; übrig bleiben wie zumeist völlig normale Menschen, die der totalen Überwachung (und all den Möglichkeiten, sie zu missbrauchen) ausgeliefert sind.

Speicherverpflichtung

Zu Artikel 1 Ziffer 14 (§ 93a SPG-E)

Die Sicherheitsbehörden können mittels eines einfachen Bescheids eine vierwöchige Vorratsdatenspeicherung aller Daten aus der Videoüberwachung eines öffentlichen oder privaten Rechtsträgers, dem ein öffentlicher Versorgungsauftrag zukommt, anordnen. Diese Bestimmung steht nicht im Einklang mit der **Rechtsprechung des EuGH[14] und des VfGH[15] zur Vorratsdatenspeicherung.** Durch die Maßnahme wird nicht nur in Art. 8 EMRK bzw. in Art. 7 (Achtung des Privat- und Familienlebens) und in Art. 8 (Schutz personenbezogener Daten) der EU-Grundrechtecharta (GRC) eingegriffen, sondern auch in Art. 11 GRC (Freiheit der Meinungsäußerung und Informationsfreiheit). **Durch das Wissen, dass öffentlicher Raum nicht nur überwacht, sondern die Bilddaten auch jederzeit und überall für vier Wochen gespeichert werden können, werden viele Menschen ihr Verhalten ändern.** Sie werden ihre Meinung nicht mehr frei

14 EuGH Digital Rights Ireland verbundene RS C-293/12 und C-594/12.

15 VfGH G 47/12 ua.

äußern, wie es in einer Demokratie selbstverständlich ist, wenn sie etwa bestimmte Kleidungsstücke, die Ausdruck einer gewissen Lebensweise oder Meinung sind, nicht mehr tragen oder werden nicht mehr an Versammlungen teilnehmen, weil sie bei der Anreise und der Teilnahme überwacht werden. In Watson/Tele 2 Sverige[16] hält der EuGH ausdrücklich fest, dass dieses in Art. 11 der Charta gewährleistete Grundrecht eine der wesentlichen Grundlagen einer demokratischen und pluralistischen Gesellschaft darstellt, die zu den Werten gehört, auf die sich die Union nach Art. 2 EUV gründet.

Nach ständiger Rechtsprechung des EuGHs und insbesondere nach dem zitierten Urteil muss eine nationale Regelung, die zur Bekämpfung schwerer (!) Straftaten eine gezielte Vorratsspeicherung ermöglicht, hinsichtlich der Kategorien von zu speichernden Daten, der betroffenen Personen und der vorgesehenen Dauer der **Speicherung auf das absolut Notwendige beschränkt** sein. Zudem muss eine solche Regelung klar und präzise sein und Garantien enthalten, um die gespeicherten Daten vor Missbrauchsrisiken zu schützen. § 93a SPG-E widerspricht klar all diesen Punkten, **insbesondere dürfen die Vorratsdaten sogar zur Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit und zur Verfolgung jeglicher, also auch minderschwerer Kriminalität oder auch zur Überwachung einer Versammlung verwendet werden**. Der betroffene Personenkreis ist nach dem vorliegenden Entwurf keineswegs abgegrenzt und organisatorische und technische Maßnahmen, die vor Missbrauchsrisiken schützen, sind nicht normiert.

Durch die Maßnahme wird auch die Möglichkeit der **Erstellung von umfassenden Bewegungs- und Persönlichkeitsprofilen geschaffen, die äußerst sensible Daten darstellen** und einen besonders intensiven Grundrechtseingriff bedeuten.

Dass eine dermaßen **eingriffsintensive Maßnahme dem Rechtsschutzbeauftragten (RSB) weder zur Kenntnis gebracht werden muss, noch dieser die Maßnahme genehmigen muss,** ist nicht hinzunehmen. Daran ändert auch die Möglichkeit nichts, gegen den Bescheid Beschwerde bei den Verwaltungsgerichten einlegen zu können. Der RSB hat kommissarisch die Interessen der Betroffenen des Grundrechtseingriffs (die überwachten Menschen) wahrzunehmen, wohingegen die Adressaten des Bescheids (Betreiberinnen und Betreiber der Videoüberwachungsanlagen) in einer Beschwerde nur ihre eigenen Interessen wahrnehmen können. Daher verletzt die vorgeschlagene Fassung des § 93a SPG-E Art. 8 Abs. 2 GRC und Art. 8 iVm Art. 13 EMRK.

Die Rechtsträger werden mit dem vorliegenden Entwurf verpflichtet, die Sicherheitsbehörden über die Verwendung von Videoaufzeichnungen an öffentlichen Orten zu informieren und unter Umständen die betreffenden Daten zu speichern. Das führt zu einigen Problemen: Zum einen sind nicht alle technischen Einrichtungen dazu gedacht, Videoaufzeichnungen zu speichern. Die bloße Möglichkeit, dass die Sicherheitsbehörde eine Aufbewahrungspflicht festlegt, bedeutet einen Eingriff in das Recht auf Eigentum, da auch die freie Verwendung von Eigentum von diesem Grundrecht garantiert wird. Auch bedeutet die Bestimmung, dass für manche Rechtsträger hohe Kosten für die Anschaffung von Speicherkapazitäten, bzw. Umgestaltung der technischen Einrichtungen anfallen können. Auch das ist ein Eingriff in das Recht auf Eigentum gem. Art. 1 1. ZP EMRK. Normen, die eine bestimmte Benutzung/Verwendung von Eigentum vorschreiben, sind grundsätzlich zulässig. Zulässig sind aber nur Beschränkungen/Auflagen, die die konkreten Gefahren der Nutzung verhindern sollen. Eine Einschränkung, die darauf hinauslauft, Equipment nicht nur im Notfall den Sicherheitsbehörden zur Verfügung zu stellen, ist jedoch unzulässig. (Zu weiteren Bedenken siehe auch Ziffer 3.)

16 EuGH Watson/Tele2 Sverige verbundene RS C-20315 und C-698/15.

KFZ-DATENVERARBEITUNG

Zu Artikel 1 Ziffer 5 - § 54 Abs. 4b SPG-E und zu Artikel 2 Ziffer 1 und 2 § 98a Abs. 1 und 2 StVO-E:

Die vorgeschlagenen Änderungen des § 54 Abs. 4b SPG-E bedeuten eine erhebliche Ausweitung der Überwachungsmöglichkeiten der Sicherheitsbehörden und eine Erweiterung des legalen Verwendungszweckes der erhobenen Daten, die abzulehnen ist. Zur Verarbeitung von Kfz-Daten sollen, laut den Erläuterungen zur Wirkungsfolgenabschätzung[17] zehn stationäre und zwanzig mobile Kennzeichenerkennungsgeräte angeschafft werden.

Nach dieser Bestimmung soll künftig nicht nur – wie bisher – die Erfassung des Kennzeichens möglich sein, sondern auch alle weiteren, in irgendeiner Weise in Betracht kommenden Daten. Demonstrativ werden jedoch ohnehin weitgehend alle in Frage kommende Daten (Typ, Marke, Farbe des Fahrzeuges, Lenkerin/Lenker) genannt, weshalb auch eine Streichung des Wortes „insbesondere" zu keiner befriedigenden Einschränkung führen würde.

Diese Daten sollen – ebenfalls wie bisher – für Zwecke der Fahndung verarbeitet werden. Der Verweis auf § 24 SPG, wo die Fahndung formal geregelt ist, entfällt, daher **ist zu befürchten, dass der Begriff „Fahndung" nunmehr extensiv ausgelegt wird** und dahingehend interpretiert werden könnte, dass die Daten nicht nur beim Vorliegen der (im Verhältnis zu anderen SPG-Bestimmungen) konkreten Voraussetzungen des § 24 SPG verarbeitet werden dürfen, sondern bei der bloßen Möglichkeit, dass die Daten für Fahndungszwecke verwendet werden könnten.

Weiters sollen die Daten nun neuerdings auch für Zwecke der Abwehr und Aufklärung gefährlicher Angriffe sowie zur Abwehr krimineller Verbindungen verarbeitet werden dürfen. Diese Begriffe gehören zu den sehr weit gefassten des SPGs, da sie sich auf quasi alle vorsätzlich zu begehenden Offizialdelikte beziehen und auch schon bevor eine strafbare Handlung tatsächlich gesetzt wurde, relevant sind. **Die Novelle würde es künftig beispielsweise ermöglichen, Daten von Fahrzeugen, die zur Anreise zu einem Fußballspiel gedacht sind, zu verarbeiten, nur weil die Behörde von Auseinandersetzungen zwischen Fans ausgeht.**

Zur Verfolgung dieser Zwecke erachtet der Entwurf eine unterschiedslose Erfassung und Speicherung der Daten jedes Kfzs für erforderlich. Diese Daten sollen **grundsätzlich zwei Wochen gespeichert werden.** Für Zwecke der Strafverfolgung kann sie gegebenenfalls verlängert werden. Dass die Speicherfrist grundsätzlich zwei Wochen beträgt, ergibt sich aus § 54 Abs. 4b letzter Satz und aus den Erläuterungen.

Diese Maßnahme stellt einen schweren Grundrechtseingriff dar, insbesondere weil die Möglichkeit einer umfassenden Erstellung von Bewegungs- und Persönlichkeitsprofilen geschaffen wird, die höchst sensible Daten darstellen. Zudem steht die nun vorgeschlagene Normierung einer **Vorratsdatenspeicherung des gesamten Straßenverkehrs** zur Prävention und Verfolgung jeglicher Kriminalität aus unserer Sicht im **Widerspruch zur Rechtsprechung des EuGH** (Digital Rights Ireland und Watson/Tele 2 Sverige), nach der eine Vorratsdatenspeicherung unter anderem nur zur Bekämpfung schwerer oder organisierter Kriminalität zulässig sein kann. Im Gegensatz dazu soll nun die Verfolgung minderschwerer Kriminalität sowie die Abwehr gefährlicher Angriffe aufgrund der ermittelten Daten ermöglicht werden. Auch der Kreis der betroffenen Personen wird – im

17 https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00015/imfname_681954.pdf, S. 1.

Widerspruch zu der eben zitierten Rechtssprechung des EuGH – **nicht** auf das absolut Notwendige beschränkt.

Trotz der Gefahr, dass ganze Bewegungsprofile erstellt werden könnten, sind keine Maßnahmen ersichtlich, die die gespeicherten Daten vor Missbrauch schützen sollen. Damit wird das Prinzip „privacy by design" (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen) nach Art. 19 und 20 der „Polizei-Datenschutz"-Richtlinie (EU) 2016/680 im vorliegenden Vorschlag vollkommen ignoriert. Die Verpflichtungen decken sich mit jenen des Art. 24 Abs. 1 und 2 und Art. 25 Abs. 1 und 2 Datenschutz-Grundverordnung (DSGVO). Der vorliegende Entwurf ist daher nicht nur grundrechtswidrig, sondern auch unionsrechtswidrig.

Es können außerdem nunmehr die gesamten Videodaten, von Radargeräten dafür verwendet werden und auch diese können dann zwei Wochen gespeichert werden (vgl. § 98a STVO-E).

Die vorgeschlagenen Änderungen der §§ 57 und 58 SPG-E sind unklar und verstoßen daher gegen das Bestimmtheitsgebot gem. Art. 18 B-VG. Es bleibt zunächst offen, ob die gem. § 98a STVO-E übermittelten Daten in das EKIS, also in ein zentrales Informationsregister eingespeist werden dürfen oder nicht. Über diesen Umweg könnten die ermittelten Daten wiederum **für alle Zwecke, unter anderem auch für das Asyl- und Fremdenwesen, von den Sicherheitsbehörden** benutzt werden und sogar **an andere Behörden übermittelt** werden. Da es sich bei dem Gesetz um einen Grundrechtseingriff handelt, ist der Gesetzgeber verpflichtet, dieses in erhöhtem Maße zu determinieren.

Mit dieser Ausweitung der Videoüberwachung im Straßenverkehr werden alle Autofahrerinnen und Autofahrer unter Generalverdacht gestellt. **Diese Form der Vorratsdatenspeicherung ist nicht mit dem VfGH-Erkenntnis zur Section Control aus dem Jahr 2007[18] vereinbar** und ist auch im Lichte der jüngsten Rechtsprechung des EuGH im Fall Watson/Tele 2 Sverige sehr zweifelhaft. Damit entsteht eine neue Form der **anlasslosen Massenüberwachung** und alle Autofahrerinnen bzw. Autofahrer werden unter Generalverdacht gestellt. Aus grundrechtlicher Perspektive ist dieser Schritt in Richtung einer kompletten Überwachung aller Kennzeichen sehr problematisch. Der VfGH hat 2007 in seiner Entscheidung zur Section Control festgestellt, dass eine Überwachung von Autofahrerinnen und Autofahrern nur auf bestimmten, besonders gefährlichen und per Verordnung festgelegten Strecken zulässig ist. Zudem dürfen laut VfGH nur Kennzeichendaten gespeichert und an die Behörden übermittelt werden, wenn die erfassten Fahrzeuge zu schnell unterwegs oder bereits zur Fahndung ausgeschrieben sind. Diese Form der Vorratsdatenspeicherung ist aus unserer Sicht nicht mit der jüngsten höchstgerichtlichen Rechtsprechung vereinbar.

Geburtsdaten unter der Stammdatenauskunft

Zu Artikel 3 Ziffer 1 (§ 92 Abs. 3 lit g TKG-E – „Exkurs" § 76a Abs. 1 StPO)

In § 92 Abs. 3 TKG soll der Definition der Stammdaten das „Geburtsdatum" hinzugefügt werden. Das mag grundsätzlich verständlich erscheinen, ist jedoch in Zusammenschau mit der bestehenden Rechtslage nach § 76a Abs. 1 StPO zu kritisieren, der die Auskunft über Stammdaten sehr einfach und ohne Absicherung durch organisatorische Maßnahmen auch den kriminalpolizeilichen Behörden unmittelbar ermöglicht. Eine richterliche Bewilligung ist dafür nicht notwendig. Um Willkür und Missbrauch hintanzuhalten, ist es dringend geboten, diese Bestimmung mit geeigneten

18 https://www.vfgh.gv.at/downloads/VfGH_G_147-148-06_ua_-_section_control.pdf.

organisatorischen Sicherheitsmaßnahmen zu versehen, sodass einzelne Beamtinnen oder Beamte nicht mehr alleine eine Auskunft erwirken können.

Speicherfristverlängerung

Zu Ziffer 4 (§ 53a Abs. 6 SPG-E)

Die Speicherfrist von Daten gem. § 53a Abs. 2 Z 1 SPG soll von 3 auf 5 Jahre verlängert werden. Diese Verschärfung betrifft Daten von Verdächtigen, d.h. nicht verurteilten Personen. Die Auflistung der Daten umfasst eine lange Reihe personenbezogener Daten des Verdächtigen, sowie personenbezogene Daten Dritter (wie etwa der Name der Eltern gem. § 53a Abs. 2 lit d SPG). Die Verarbeitung von sensiblen Daten ist explizit zulässig und einige Daten, wie etwa Daten die gem. § 53a Abs. 2 lit k SPG („Beruf/Qualifikation/Beschäftigung/Lebensverhältnisse") gespeichert werden, können sehr extensiv ausgelegt werden.

Anzunehmen ist, dass die Speicherung in vielen Fällen ohnehin länger ist, da bei jedem neuen Eintrag die Frist von vorne zu laufen beginnt.

Gespeichert werden können diese Daten von Verdächtigen, für

- die Abwehr krimineller Verbindungen oder
- die Abwehr von gefährlichen Angriffen sowie
- zur Vorbeugung gefährlicher Angriffe, wenn nach Art des Angriffes eine wiederholte Begehung wahrscheinlich ist.

Die Erläuterungen begründen die Notwendigkeit dieses Eingriffes in die Privats- und Persönlichkeitsrechte von Verdächtigen lediglich in Hinblick auf Ermittlungstätigkeiten gegen organisierte Kriminalität. In dieser Hinsicht erscheint eine fünfjährige Speicherfrist jedoch unverhältnismäßig, da es sich wohlgemerkt um Daten von Personen handelt, die irgendwann einmal verdächtig waren (d.h. nicht rechtskräftig verurteilt wurden) und nur in Ausnahmefällen mit Ermittlungserfolgen zu rechnen ist. Es sind auch keine Begründungspflichten von seiten der Behörde vorgesehen.

Es wird nicht erläutert, warum eine derart lange Speicherungen zur Abwehr oder Vorbeugung gefährlicher Angriffe notwendig sei. Schon allein durch das Unterlassen der Interessenabwägung verletzt der Gesetzgeber Art. 8 EMRK und Art. 8 GRC und § 1 DSG. Weiters bedarf es einer klaren Regelung der Praxis der sicherheitsbehördlichen Datenabfragen. Bloße Dienstanweisungen sind nicht ausreichend, um Missbrauch zu verhindern.

ABSCHAFFUNG VON ANONYMEN SIM-KARTEN

zu Artikel 3 Ziffer 2 (§ 97 Abs. 1 TKG-E) und Ziffer 3 (§ 109 Abs. 3 TKG-E)

Die Nützlichkeit einer Registrierungspflicht für anonyme SIM-Karten muss angesichts internationaler Erfahrungen stark bezweifelt werden. Eine Studie des weltweit größten Verbands der Telekommunikationsindustrie[19] fand keine Belege dafür, dass die Registrierung von SIM-Karten zu einer verbesserten Verbrechensaufklärung führt oder gegen Terrorismus hilft. Mexiko hat das Verbot

19 https://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf

anonymer SIM-Karten wieder abgeschafft, da die Verbrechensrate sogar angestiegen ist und sie nur zu einem Schwarzmarkt für SIM-Karten geführt hat. Tschechien, Neuseeland, Kanada und Rumänien haben die Maßnahme analysiert und sich aufgrund der fehlenden Belege dagegen entschieden. Die EU-Kommission hat eine Registrierungspflicht für SIM-Karten sowohl 2012[20] als auch 2013[21] geprüft und konnte keinen Beleg für ihre Wirksamkeit für die Strafverfolgung feststellen. Nach den Terroranschlägen in London 2005 hat sogar eine eigene Kommission von Sicherheitsbehörden[22] diese Maßnahme evaluiert. Sie kam zu dem Schluss, dass es keine Belege für die Nützlichkeit einer Registrierungspflicht gibt und hat von einer Einführung abgeraten. Bis heute wurde in Großbritannien keine Registrierungspflicht für SIM-Karten eingeführt.

Diesem zweifelhaften Nutzen für die Verhinderung oder Aufklärung schwerer Straftaten steht ein großer Kollateralschaden für besonders schützenswerte Personengruppen gegenüber. Vor allem im Bereich des investigativen Journalismus ist die Verwendung anonymer SIM-Karten ein weit verbreiteter Schutzmechanismus für die eigene Anonymität und das Berufsgeheimnis. Insbesondere Menschen, die unter großem persönlichen Risiko auf Missstände in ihrem Umfeld hinweisen, besitzen oft nicht die technischen Vorkenntnisse, um sich über verschlüsselte Messengerdienste zu schützen. Diese Personen greifen häufig auf anonyme Wertkarten als einfachstes Mittel für ihre anonyme Kommunikation mit Journalisten und Behörden zurück. Das deutsche Bundesamt für Sicherheit in der Informationstechnik empfiehlt etwa den „Erwerb von Prepaid-SIM-Karten ohne Ausweisprüfung [...] zur Vermeidung der Identifikation beim Mobilfunkbetreiber" und ergänzt „Im Geschäftsumfeld kann diese Maßnahme ergänzend für Mobilfunkteilnehmer mit erhöhtem Schutzbedarf durchgeführt werden."[23] Durch die Einführung einer Registrierungspflicht für anonyme Wertkarten wird vielen schützenswerten Personengruppen ein Weg der sicheren Kommunikation versperrt.

Mit einem Mindestmaß an krimineller Energie kann die vorgeschlagene Registrierungspflicht leicht umgangen werden. Die einfachste Möglichkeit stellen ausländische SIM-Karten oder kostenlose anonyme Messengerdienste wie „Wire", die Kommunikation komplett unabhängig von der Telefonnummer ermöglichen, dar. Die Mehrzahl der EU-Mitgliedsstaaten, die seit 15. Juni 2017 durch die neuen Roaming-Regelungen noch attraktiver wurden, haben derzeit keine Registrierungspflicht für SIM-Karten und die Erfahrungen aus jenen Ländern mit einschlägigen Gesetzen zeigen drastische Lücken im Registrierungsprozess[24].

Für die Mehrzahl der Nutzerinnen und Nutzer in Österreich fällt durch diese Maßnahme eine weitere Möglichkeit weg, anonym zu kommunizieren. Damit werden 4,5 Millionen Nutzerinnen und Nutzer, die aktuell anonyme Prepaid SIM-Karten nutzen, unter Generalverdacht gestellt[25]. Der äußerst zweifelhafte Nutzen für die Bekämpfung von Kriminalität steht also einem Eingriff in das Recht vieler

20 http://www.europarl.europa.eu/RegData/questions/reponses_qe/2012/006014/P7_RE%282012%29006014_EN.doc
21 http://www.europarl.europa.eu/RegData/questions/reponses_qe/2012/006014/P7_RE%282012%29006014_EN.doc
22 https://www.theyworkforyou.com/wrans/?id=2007-07-16b.4.3&s=%22pay+as+you+go%22+mobile+phones
23 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Oeffentl-Mobilfunknetze.pdf?__blob=publicationFile&v=1
24 https://netzpolitik.org/2017/interaktive-karte-registrierungspflicht-fuer-prepaid-sim-karten-in-europa-weit-verbreitet/.
25 http://diepresse.com/home/techscience/technews/5152191/Sobotka-fordert-Ende-der-anonymen-PrepaidSIMKarten.

Menschen gegenüber, frei und unbeobachtet zu kommunizieren. Daher ist die Maßnahme unverhältnismäßig.

Des Weiteren wird durch diese Maßnahme der wachsende Markt der günstigen virtuellen Mobilfunkbetreiber (MVNOs) geschwächt und somit der Wettbewerb zwischen Mobilfunkanbietern und das niedrige Preisniveau für Mobilfunkverträge in Österreich gefährdet. Wenige dieser Discounter besitzen aktuell die Infrastruktur, beim Kauf einer SIM-Karte die Identität ihrer Käufer zu überprüfen. Discounter wie „Hot" haben bereits Bedenken angemeldet und verweisen auf Zahlen aus Italien und Spanien,[26] wonach eine Einführung der Registrierungspflicht keinen Kriminalitätsrückgang zur Folge hatte und man aufgrund dieser Überlegung bisher von einer Einführung von SIM-Karten-Registrierung in Österreich absehen sollte. Durch die Weitergabe von gebrauchten Telefonen und SIM-Karten können auch Probleme für die Strafverfolgung entstehen und falsche Personen ins Fadenkreuz der Ermittlerinnen und Ermittler gelangen.[27]

Weiters ist es nicht nachvollziehbar, warum der Entwurf den akademischen Grad natürlicher Personen (§ 92 Abs. 3 Z 3 lit. b TKG) überhaupt als notwendiges Identifizierungsmerkmal ansieht.

ZUSAMMENFASSUNG UND EMPFEHLUNGEN

Sicherheitsforen

- Sozialmaßnahmen und Präventionsmaßnahmen gegen Radikalisierungstendenzen wären wirkungsvoller als sogenannte „Sicherheitsforen" durch die die Gefahr entsteht, dass informelle Hierarchien zwischen BürgerInnen entstehen.

Videoüberwachung

- Es ist stark zu bezweifeln, dass umfassende Videoüberwachung im öffentlichen Raum geeignet ist, Straftaten vorzubeugen.
- Durch flächendeckende Überwachung im öffentlichen Raum ist es möglich, umfassende Bewegungs- und Persönlichkeitsprofile zu erstellen, wodurch intensiv in Grundrechte eingegriffen wird.
- Überwachung des öffentlichen Raums betrifft eine große Anzahl an Personen und stellt daher eine Maßnahme zur Massenüberwachung dar.
- Die Speicherverpflichtung verletzt das Recht auf Eigentum gem. Art. 1 1. ZP. EMRK
- Der Rechtsschutzbeauftragte ist unbedingt auch mit der Kontrolle der Videoüberwachung und der Verwendung daraus entstandenen Materials zu betrauen.
- Die Speicherung von Videomaterial muss auf das absolut Notwendige beschränkt werden

26 http://derstandard.at/2000051861142/Die-Registrierungspflicht-fuer-Prepaid-Simkarten-wirft-Fragen-auf.

27 http://consumer.ncc.gov.ng/Archive/publication/pub/SIM.pdf.

- Die Daten aus der Videoüberwachung sollen schon zur Aufrechterhaltung der öffentlichen Ruhe und Ordnung verwendet werden, die Voraussetzungen für die Datenverarbeitung sind also äußerst gering.

Kfz-Kennzeichen

- Die Speicherung von Kfz-Daten für zwei Wochen widerspricht der EuGH Rechtsprechung zur Vorratsdatenspeicherung.
- Von der Speicherung von Kfz-Daten wird ein großer Kreis an Personen betroffen sein, sie ist daher als Maßnahme zur Massenüberwachung zu werten.
- Schon die Möglichkeit, dass die Daten für Fahndungszwecke verwendet werden könnten, soll für die Speicherung ausreichen.
- Die Speicherung von Kfz-Daten ermöglicht das Erstellen von umfassenden Bewegungsprofilen und greift damit in etliche Grundrechte ein.

Abschaffung anonymer SIM-Karten

- Dass die Registrierung von SIM-Karten zur besseren Aufklärung bzw. Prävention von Straftaten beiträgt, ist nicht erwiesen.
- Vielen Menschen, die auf anonyme Kommunikation angewiesen sind, z.B. um die eigene Sicherheit zu schützen, wird diese Möglichkeit genommen

Sonstiges

- Dass nun die Auskunft von Behörden über Stammdaten auch Geburtsdaten beinhalten soll, ist überschießend und wird nicht von geeigneten organisatorischen Sicherheitsmaßnahmen begleitet.
- Die Speicherfristverlängerung von 3 auf 5 Jahre ist unverhältnismäßig und damit eine Verletzung von Art. 8 EMRK, Art. 8 GRC und § 1 DSG.