WIEN / 18. August 2017

STELLUNGNAHME

Zum Ministerialentwurf betreffend Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Bundesstraßen-Mautgesetz 2002, die Straßenverkehrs-ordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden

Für epicenter.works
Angelika Adensamer
Alexander Czadilek
Thomas Lohninger
Christof Tschohl

EPICENTER .WORKS
for digital rights

Stellungnahme im Begutachtungsverfahren zum Entwurf eines Bundesgesetzes, mit dem das Sicherheitspolizeigesetz, das Bundesstraßen-Mautgesetz 2002, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden (XXV. GP 326/ME)

EPICENTER.WORKS NIMMT ZUM VORLIEGENDEN GESETZESENTWURF WIE FOLGT STELLUNG

Vorwort und Kurzfassung

Mit den geplanten Änderungen im SPG, dem BStMG und der StVO soll eine flächendeckende Videoüberwachung des öffentlichen Raums, eine umfassende (Kfz-)Kennzeichenerfassung, eine neue Form der Vorratsdatenspeicherung, die Abschaffung der Anonymität der Kommunikation sowie Netzsperren durch private Unternehmen in Österreich eingeführt werden. Begründet werden diese weiteren 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.

Erst kürzlich hat einer der international renommiertesten Experten zum Thema Überwachung, Bill Binney, ehemaliger technischer Direktor der NSA, bei einer Pressekonferenz zum Überwachungspaket in Wien bestätigt[1], 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 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!

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

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. Nur ein Beleg: Frankreich befindet sich seit den 1960er Jahren im Ausnahmezustand. – Und was hat das gebracht? 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.
- SPG und StPO: Die Schwellen für Grundrechtseingriffe werden sukzessive herabgesetzt.
- Insgesamt soll eine Fülle an (weiteren) Bestimmungen mit grundrechtlich äußerst bedenklichen Tendenzen Einzug in den österreichischen Rechtsbestand halten. Es ergibt sich zunehmend das Bild, dass Österreich quasi „scheibchenweise" zum Polizei- und Überwachungsstaat mutiert. Selbst wenn die derzeit handelnden politischen Entscheidungsträger dies größtenteils gar nicht beabsichtigen, sind die vorgeschlagenen gesetzlichen Regelungen eine rechtsstaatliche Zeitbombe.
- Es entstehen **enorme finanzielle Kosten** für eingriffsintensive Maßnahmen, die die **Sicherheit** erwiesenermaßen **nicht erhöhen**.

Inhaltsverzeichnis

Sicherheitsforen: Zu Artikel 1 Änderung des Sicherheitspolizeigesetzes

Zu Ziffer 2 und 11 (§§ 25 Abs. 1 und 84 Abs. 1 Z8):

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. Dabei soll insbesondere auch ein Informationsaustausch personenbezogener Daten ermöglicht werden (§ 56 Abs 1 Z 9 SPG-E). Auch an Personen, die Sicherheitsbehörden gem § 26 SPG in der Streitschlichtung unterstützen, sollen in Zukunft personenbezogene Daten übermittelt werden können. Wer diese Daten trotz Verpflichtung, sie vertraulich zu behandeln, widerrechtlich weitergibt, muss eine Strafe von bis zu 500 € zahlen. Notwendig wäre jedenfalls, in die Bestimmung mitaufzunehmen, dass sich Teilnehmerinnen und Teilnehmer von Sicherheitsforen einer datenschutzrechtlichen wie sicherheitspolizeirechtlichen Belehrung unterziehen müssen. Damit soll sichergestellt werden, dass ihnen bewusst wird, dass die Daten- und Informationsübermittlung an sie in die Grundrechte von Dritten eingreift. Schließlich muss den Teilnehmerinnen und Teilnehmern klar sein, dass sie keine polizeilichen Befugnisse haben.

Grundsätzlich ist es im Sinne des guten Funktionierens der Polizeiarbeit, dass die Sicherheitsbehörden mit der Bevölkerung – auf Augenhöhe – zusammenarbeiten. Es geht aus dem Entwurf aber nicht hervor, wer, wie und wann von den Sicherheitsforen erfährt, bzw. zu einer Teilnahme eingeladen wird. Es könnten also informelle Hierarchien zwischen Bürgerinnen und Bürgern, die der Polizei näher stehen und nun auch einen formalisierten Kommunikationskanal zu dieser bekommen, und den Bevölkerungsgruppen entstehen, 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.

In den Erläuterungen 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 und eine gelungene Integration 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: Zu Artikel 1 Änderung des Sicherheitspolizeigesetzes

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[2] der automatisierten Videoüberwachung und der damit verbundenen negativen Auswirkungen[3] einer flächendeckenden Überwachung auf Individuen und Gesellschaft sollen nun, nur ein Jahr nach Inkrafttreten des Polizeilichen Staatsschutzgesetzes (PStSG) weitere Überwachungsmaßnahmen Teil des österreichischen Rechtsbestandes werden.

zu Ziffer 3 (§ 53 Abs. 5):

Mit der Änderung dieser Bestimmung wird sowohl eine Herausgabepflicht von Videomaterial (Bilddaten) für Rechtsträger des öffentlichen und privaten Bereichs, sofern diesen ein öffentlicher Versorgungsauftrag zukommt, als auch der direkte Zugang zu diesem Bildmaterial (Echtzeit-Streaming) normiert. Die aktuell gültige Regelung erfährt eine umfassende Erweiterung, da die Bilddaten nach bisheriger Rechtslage nur verwendet werden durften, 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). Die freiwillige Herausgabe von Videomaterial und die Verwendung dieser Daten soll für alle in § 53 Abs. 1 SPG genannten Zwecke weiterhin möglich bleiben. Die Verwendung von Bilddaten, die aufgrund der Herausgabepflicht ermittelt wurden, soll auf in § 53 Abs. 5 taxativ aufgezählte Zwecke beschränkt werden. 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 Bilddaten erfolgt insoweit, als diese nun auch schon zur Vorbeugung wahrscheinlicher Angriffe zulässig ist. Sowohl die "Vorbeugung" als auch die "Wahrscheinlichkeit" sind äußerst unbestimmte Gesetzesbegriffe, die einen Eingriff in das Recht auf Datenschutz als auch auf das Recht auf Privatsphäre für die Sicherheitsbehörden sehr einfach möglich machen. Im Gegensatz zur Voraussetzung des konkreten Verdachts lässt sich der Eingriff somit mit jeder einfachen Einschätzung einer Ermittlungsbeamtin oder eines Beamten, es könnte eine Gefahr bestehen, deren Wahrscheinlichkeit erforscht werden soll, 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.

2 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.

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

Auch der Wegfall des Verweises auf § 54 Abs. 3, durch den die Verwendung personenbezogener Bilddaten bisher nur zulässig war, wenn die Abwehr gefährlicher Angriffe oder krimineller Verbindungen ansonsten erheblich erschwert wäre, macht deutlich, dass die Schwellen für Grundrechtseingriffe sukzessive herabgesetzt werden.

Zu bezweifeln ist, ob 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 furchtbaren 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 (Verletzung des Grundrechts auf Datenschutz gem. § 1 DSG, des Rechts auf Achtung des Privatlebens gem. Art. 8 EMRK).

Im Entwurf wird eine Echtzeitüberwachung 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.

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[4] waren. Die Regelung widerspricht somit dem grundrechtlichen Determinierungsgebot.

Zum mangelnden Rechtsschutz siehe unten zu Ziffer 12.

zu Ziffer 4 (§ 53a Abs. 6):

Eine Verlängerung der Speicherfrist von Daten zu Verdächtigen einer mit mindestens dreijähriger Freiheitsstrafe bedrohten, vorsätzlichen gerichtlich strafbaren Handlung ist vertretbar. Allerdings bedarf es einer klaren Regelung der Praxis der sicherheitsbehördlichen Datenabfragen. Bloße Dienstanweisungen sind nicht ausreichend, um Missbrauch zu verhindern (siehe oben zu Ziffer 3).

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

zu Ziffer 12 (§ 91c Abs. 1 und 3):

Betreiberinnen und Betreiber von Videoüberwachungsanlagen sind verpflichtet, den Sicherheitsbehörden Bilddaten auf deren Verlangen herauszugeben. Hierzu reicht die bloße Verständigung des Rechtsschutzbeauftragten (RSB), eine Genehmigung durch diesen ist jedoch nicht erforderlich. 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, die im Übrigen von Bundesminister Wolfgang Sobotka schon jetzt gefordert werden, 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. Insofern ist völlig unverständlich, dass der RSB einer Echtzeitüberwachung erst zustimmen muss, wenn diese länger als drei Tage andauert.

zu Ziffer 15 (§ 93a):

Die Sicherheitsbehörden können mittels eines einfachen Bescheids eine zweiwöchige Vorratsdatenspeicherung der gesamten Videoüberwachung eines öffentlichen oder privaten Rechtsträgers, dem ein öffentlicher Versorgungsauftrag zukommt, anordnen. Diese Bestimmung steht nicht im Einklang mit der Rechtsprechung des EuGH[5] und des VfGH[6] zur Vorratsdatenspeicherung (dort: von Kommunikationsdaten). 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 zwei Wochen gespeichert werden können, werden viele Menschen ihr Verhalten ändern. Sie werden ihre Meinung nicht mehr frei 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[7] 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

5 EuGH Digital Rights Ireland verbundene RS C-293/12 und C-594/12.
6 VfGH G 47/12 ua.
7 EuGH Watson/Tele2 Sverige verbundene RS C-20315 und C-698/15.

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 verwendet werden. Der betroffene Personenkreis ist nach dem vorliegenden Entwurf aber keineswegs abgrenzt 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.

zu Ziffer 17 (§ 96 Abs. 10):

Die durch eine unabhängige Behörde und aufgrund einer datenschutzrechtlichen Prüfung der Datenverarbeitungsanlage (Videoüberwachungsanlage) festgelegte Aufbewahrungsdauer von Bilddaten ist nicht mit einer (zweiwöchigen) Aufbewahrungsverpflichtung durch Bescheid der Sicherheitsbehörde zu vergleichen. Durch letztere wird nämlich nicht nur der Zweck der Datenverwendung konterkariert, sondern auch gegen das Prinzip der Datenminimierung und der Datensparsamkeit verstoßen. Eine bloße Verständigung der Datenschutzbehörde ändert daran nichts.

Kennzeichenerfassung: Zu Artikel 1 - Änderung des SPG, Artikel 2 - Änderung des BStMG und Artikel 3 - Änderung der StVO

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[8] vereinbar und ist auch im Lichte der jüngsten Rechtsprechung des EuGH im Fall Watson/Tele 2 Sverige sehr zweifelhaft.

Seit Kurzem dürfen auf allen österreichischen Straßen von jedem Fahrzeug die Lenkerinnen bzw. Lenker des Fahrzeugs, das Kennzeichen, die Marke, der Typ und die Farbe von der ASFINAG erfasst werden (BStMG). Nach dem vorliegenden Entwurf können die von den Sicherheitsbehörden selbst ermittelten oder auf deren Ersuchen von der ASFINAG übermittelten Daten in Verdachtsfällen bis zu fünf Jahren gespeichert werden (§ 53a Abs. 6 SPG-E). Daten, die nicht zur Verfolgung von Straftaten erforderlich sind, müssen erst nach 48 Stunden gelöscht werden 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.

Zu Artikel 1 Ziffer 5 - Änderung des SPG (§ 54 Abs. 4b), Artikel 2 Ziffer 1 und 2 - Änderung des BStMG (§§ 19a Abs. 1 und 1a) und Artikel 3 Ziffer 1 und 2- Änderung der StVO (§§ 98a Abs. 1 und 2):

Sind die von den Sicherheitsbehörden selbst ermittelten oder an diese übermittelten Daten nicht zur weiteren Verfolgung gerichtlich strafbarer Handlungen erforderlich, sind sie erst nach 48 Stunden zu löschen. Die Inanspruchnahme sämtlicher Kennzeichenerfassungsgeräte der ASFINAG (§§ 19 Abs. 1 BStMG und 19 Abs. 1 StVO) erhöht die Streubreite des Grundrechtseingriffs deutlich. Die 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. Die Bestimmung enthält zwar gewisse Einschränkungen hinsichtlich der Kategorien der zu speichernden

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

Daten, der Kreis der betroffenen Personen wird aber - im Widerspruch zu der eben zitierten Rsp des EuGH - *nicht* auf das absolut Notwendige beschränkt.

Weder § 19a Abs. 1a BStMG noch § 98a Abs. 1a StVO ist hinsichtlich des Verfahrens der Datenübermittlung durch die ASFINAG klar und präzise, als schon das bloße "Ersuchen" der Sicherheitsbehörde ausreichen soll, die Daten an diese zu übermitteln und von ihr verwendet zu werden. Es sind keine Maßnahmen ersichtlich, um die gespeicherten Daten vor Missbrauchsrisiken zu schützen, insbesondere gibt es keine Ermächtigung zu einer Durchführungsverordnung, die organisatorische und technische Maßnahmen normiert, um Missbrauch hintanzuhalten. 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 verletzt auch ganz neu geschaffene Prinzipien aus dem Sekundärrecht der EU.

Zudem ist nicht geregelt, für welchen Zeitraum die Übermittlung zulässig sein soll. Dies kommt einer Generalermächtigung gleich und steht nicht mit dem grundrechtlichen Determinierungsgebot in Einklang. Zuletzt hat auch der EuGH[9] in seinem Gutachten zum Abkommen der EU mit Kanada über die Speicherung und Übermittlung von Fluggastdaten festgestellt, dass hinsichtlich der Erforderlichkeit der Eingriffe die gesetzlichen Bestimmungen auf das absolut Notwendige beschränkt sowie klar und präzise sein müssen.

In den Erläuterungen zum PStSG[10] wurde der Grundrechtseingriff (Ermittlung von Kennzeichendaten durch die Staatsschutzbehörden) auch damit gerechtfertigt, dass ein Abgleich von KfZ-Kennzeichen[11] nur aufgrund des SPG und nur für Zwecke der Fahndung und nur durch Abgleich mit der Datenbank gemäß § 47 KFG zulässig ist. Nun kommt es zu einer deutlichen Erweiterung des Eingriffs durch die Übermittlung von Daten der ASFINAG auch zur Verfolgung minderschwerer Kriminalität und zur Abwehr gefährlicher Angriffe.

Die genannten Bestimmungen im Gesetzentwurf widersprechen somit europäischer höchstgerichtlicher Judikatur und sind nicht mit der Bundesverfassung in Einklang zu bringen.

Netzsperren: Zu Artikel 4 Änderung des TKG zu Ziffer 1 (§17 Abs. 1a TKG-E)

Durch die Regelung („können Verkehrsmanagementmaßnahmen [...] anbieten“) ist es einzig und allein dem Internetanbieter überlassen, ob, wann, wie und wie lange Angebote im Internet gesperrt werden. Da es hier um Sperren im Zusammenhang mit strafrechtlich relevanten Handlungen geht, kommt dies einer Privatisierung von Rechtsprechung und Rechtsdurchsetzung im Internet gleich. Weil diese Sperren nicht gesetzlich vorgeschrieben sind, sondern Teil der freiwilligen Produktgestaltung des Internetanbieters, könnten Internetprodukte mit mehr oder weniger gesperrten Websites auch unterschiedliche Preise bekommen. Es gäbe mit dieser Bestimmung keine Verpflichtung für

9 Gutachten des EuGH zum Abkommen zwischen Kanada und der Europäischen Union über die Übermittlung von Fluggastdatensätzen vom 26. Juli 2017.

10 AB 988 XXV. GP, S. 7.

11 § 11 Abs. 1 Z 4 PStSG idF BGBl. I 5/2016.

Internetanbieter, noch ein Produkt mit vollständigem, ungefiltertem Internet anzubieten oder dieses nicht als das teuerste Produkt zu vermarkten.

Durch die Formulierung „wie etwa“ wird klar, dass Netzsperren nicht auf die aufgezählten Deliktgruppen beschränkt sind. Netzsperren könnten zur Vermeidung aller strafrechtlich relevanter Handlungen herangezogen werden, wie zum Beispiel Diffamierung (§297 StGB) oder Herabwürdigung des Staates und seiner Symbole (§248 StGB).

Diese Art der Netzsperren untergräbt das Grundrecht auf freie Meinungsäußerung und Informationsfreiheit, insbesondere weil die Entscheidung, Inhalte zu sperren, von privaten Unternehmen getroffen wird. Zudem wurde keinerlei Möglichkeit vorgesehen, die Rechtmäßigkeit der Sperre überprüfen zu lassen. Somit sind Netzsperren ein unverhältnismäßiges Mittel mit enormen Missbrauchspotential. Die Entscheidung, ob Datenverkehr manipuliert wird und auf welche Inhalte zugegriffen werden kann, darf ein privates Unternehmen nicht nach eigenem Ermessen treffen. Dies würde die EU-Verordnung zur Netzneutralität ins Gegenteil verkehren.

Es ist sehr fragwürdig, ob der Entwurf des Bundesministers für Inneres mit der EU-Verordnung zur Netzneutralität vereinbar ist. Zwar erlaubt die Verordnung Internetzugangsanbietern, Netzsperren durchzuführen, um nationales Recht, EU-Recht oder Gerichtsurteile umzusetzen. Das gilt aber nur "soweit und solange es erforderlich ist" (Art. 3 Abs. 3 UnterAbs. 3 der Verordnung (EU) 2120/2015). Österreich könnte Internetanbieter also dazu verpflichten, Netzsperren für spezifische Inhalte einzuführen, darf Internetanbietern jedoch keine Produkte erlauben, die die EU-Verordnung explizit verbietet. Eine einseitige Änderung der EU-Netzneutralitätsbestimmungen, die Österreich mit dem vorgeschlagenen § 17 Abs. 1a TKG zu erwirken versucht, widerspricht den Grundprinzipien des EU-Binnenmarkts und wäre unionsrechtswidrig. Diese Rechtsauffassung findet sich auch in der Stellungnahme der UPC Austria GmbH[12].

Die Netzsperren sollen laut dem Entwurf der „Vermeidung von strafrechtlich relevanten Handlungen“ dienen. Die Prüfung, ob eine Handlung strafrechtliche Relevanz besitzt, obliegt jedoch nicht dem Internetprovider, sondern den ordentlichen Gerichten. Es widerspricht dem Prinzip der Rechtsstaatlichkeit, diese Prüfung an private Unternehmen auszulagern. Darüber hinaus sind die meisten Internetprovider klassische KMU und beschäftigen keine Juristen.

Für betroffene Inhaltsanbieter und Nutzer sind keinerlei Rechtsschutz oder Beschwerdemöglichkeiten vorgesehen. Wenn eine Website fälschlicherweise gesperrt wird, sind deren Anbieter und Nutzer komplett auf den guten Willen des Internetanbieters angewiesen, um die Sperre wieder aufzuheben. Durch die fehlende gerichtliche Prüfung der strafrechtlichen Relevanz gibt es auch keine Berufungsmöglichkeit, jedoch ein Stigma der (kolportierten) Illegalität des Angebots. Dies widerspricht dem Rechtsstaatsprinzip.

Da die Sperrung einzelner Inhalte auf Basis der Einschätzung des Internetanbieters vorgenommen wird und auch im Rahmen seiner Produktgestaltung die Filter beliebigen Kunden angeboten werden kann, etabliert sich der Internetanbieter als Anlaufpunkt für andere gesellschaftliche Gruppen, die ein Interesse an der Erschwerung des Zugangs zu gewissen Inhalten haben. Interessenvertretungen der Urheberrechteverwerter, Elternvertreter, Strafverfolgungsbehörden oder religiöse Gruppen könnten Druck auf Internetanbieter ausüben oder ihnen Geschäftsbeziehungen anbieten, um Art und Ausmaß der gesperrten Inhalte im Internet zu beeinflussen. Da es sich dabei um private Absprachen handelt, ist eine nachträgliche staatliche oder gerichtliche Kontrolle fast ausgeschlossen.

12 Siehe https://parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_28797/index.shtml

Das Sperren von Inhalten ist kein geeignetes Mittel, um Probleme mit Pornographie, gewaltverherrlichenden Darstellungen oder strafrechtlich relevanten Urheberrechtsverletzungen im Internet zu lösen. Der gesellschaftliche Nutzen dieser Maßnahme ist deshalb stark zu bezweifeln. In den Erläuterungen wird nicht einmal der Versuch unternommen, die Notwendigkeit oder Nützlichkeit der Maßnahme darzustellen.

Die Erläuterungen sprechen von einer derzeitigen Diskriminierung der Internetanbieter gegenüber „Serviceprovidern" (Anbieter von Viren- oder Jugendschutzfiltern). Diese Diskriminierung ist jedoch nicht nachvollziehbar, da Internetanbieter nicht daran gehindert werden, clientseitige Viren- oder Jugendschutzfilter anzubieten; die Entscheidung für eine Filterung liegt dann schließlich bei den Nutzern. Bei der vorgeschlagenen Ausnahme handelt es sich um Sperrmaßnahmen im Netz, die nicht mit Sperrmaßnahmen am Client zu vergleichen sind. Vielmehr entsteht eine Wettbewerbsverzerrung, da Internetanbieter nicht allen Anbietern von Viren- und Jugendschutzfiltern die Möglichkeit der netzseitigen Integration ihrer Sperren geben, sondern exklusive Partnerschaften mit einzelnen Anbietern eingehen. Netzseitige Sperren können darüber hinaus leicht umgangen werden (bspw. beim Wechsel von WLAN auf das Mobilfunknetz).

Zu dieser Maßnahme gab es im Vorfeld keine öffentliche Debatte oder Ankündigung im Arbeitsprogramm der Regierung 2017/18. Das erstaunt insbesondere, da seit Monaten eine Arbeitsgruppe zum Thema Urheberrechtsfilter im Justizministerium tagt, deren Ergebnisse in keiner Weise im vorliegenden Entwurf berücksichtigt worden sind.

Quick Freeze: Zu Artikel 4 Änderung des TKG zu Ziffer 4 (§ 99 Abs. 1a-1f TKG-E)

Mit § 99 Abs. 1a bis 1f TKG-E findet sich im Entwurf ein Teil einer auf Fälle staatsanwaltschaftlicher Anordnungen beschränkten Form der Vorratsdatenspeicherung von Verkehrsdaten, was als „Quick Freeze" bezeichnet werden kann. Wie der EuGH in zwei Grundsatzurteilen[13] festgestellt hat, bedeutet eine solche Speicherung einen Eingriff in die in Art. 7 und Art. 8 GRC verankerten Grundrechte der betroffenen Personen, der von großem Ausmaß und als besonders schwerwiegend anzusehen ist.

epicenter.works lehnt Quick Freeze nicht grundsätzlich ab, sofern diese Maßnahme auf Fälle schwerer Kriminalität beschränkt und für deren Bekämpfung geeignet und erforderlich ist, der Zugriff auf die aufgrund dieser Maßnahme gespeicherten Daten nur mit richterlicher Bewilligung zulässig ist, und Personen, die von dieser Maßnahme betroffen sind, zu einem späteren Zeitpunkt davon in Kenntnis gesetzt werden müssen. Dem vorliegenden Vorschlag fehlen jedoch solche organisatorischen Maßnahmen und Garantien und er ist auch insofern unvollständig, als nur eine Ausnahme der Löschungsverpflichtung und entsprechende Durchführungsbestimmungen normiert werden.

Die Bestimmung des § 99 Abs. 1a TKG-E geht von einer „staatsanwaltschaftlichen Anordnung gemäß den Bestimmungen der StPO" aus. Die Befugnis zur Ausstellung einer solchen Anordnung ist jedoch in der StPO nicht enthalten, weder nach geltender Rechtslage noch nach dem vorliegenden Entwurf. Die Regelung ist insofern unklar, als es sich auch um "gemäß den Bestimmungen der StPO bezeichneten Daten" handeln könnte, die die StA durch die Anordnung einfrieren kann. Einerseits sprechen sprachliche und grammatikalische Gründe gegen diese Interpretation, andererseits würde diese Lesart

13 EuGH 8.4.2014, C-293/12, Digital Rights Ireland, Rz. 37; EuGH 21.12.2016, C-203/15 Tele2 Sverige, Rz. 60.

nicht dem grundrechtlichen Determinierungsgebot entsprechen, da eine pauschale Verweisung auf jegliche Datenkategorien, die die StPO kennt, viel zu unbestimmt wäre An dieser Stelle sei wiedereinmal auf des Denksporterkenntnis des VfGH (VfSlg 16.381) verwiesen, in dem das Gebot der Normenklarheit mehrfach und durchaus pointiert zum Ausdruck gebracht wird.

Nach der Judikatur des EuGH ist Vorratsdatenspeicherung nur zur Bekämpfung schwerer Straftaten zulässig.[14] Allerdings findet sich eine Definition des Begriffs der schweren Straftaten weder in der Judikatur des EuGH noch in der österreichischen Rechtsordnung. Der vorliegende Entwurf verweist auf § 135 Abs. 2 Z 2 bis 4 StPO, sodass eine Anordnung zur Vorratsdatenspeicherung bereits zur Ermittlung, Feststellung und Verfolgung von Straftaten, die mit einer Freiheitsstrafe von mehr als einem Jahr, bei Zustimmung des Inhabers sogar von mehr als sechs Monaten, bedroht sind, zulässig ist. Diese Schwelle ist am unteren Ende der möglichen Strafrahmen des StGB angesiedelt und somit im Hinblick auf die Vorgaben des EuGH jedenfalls zu niedrig angesetzt, sodass auch Delikte umfasst sind, die in Relation zu anderen Strafdelikten nicht als schwere Straftaten einzustufen sind. Der Entwurf genügt daher in diesem Punkt den Vorgaben der zitierten EuGH-Judikatur nicht.

Wie der EuGH ebenfalls festhält, ist jeder Eingriff in die genannten Grundrechte auch auf das absolut Notwendige zu beschränken.[15] Eine solche Beschränkung liegt aber bei der vorgeschlagenen Regelung in mehrerlei Hinsicht nicht vor. Die Befugnis zur Ausstellung einer staatsanwaltschaftlichen Anordnung, die derzeit – wie oben ausgeführt – nicht vorgesehen ist, ist mit Kriterien zu versehen, die dazu führen müssen, dass solche Anordnungen stets auf das Notwendige beschränkt sind, d.h. „stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Diese Voraussetzungen müssen insbesondere in der Praxis geeignet sein, den Umfang der Maßnahme und infolgedessen die betroffenen Personenkreise wirksam zu begrenzen.“[16] Die Regelung muss sich somit auf „objektive Anknüpfungspunkte stützen, die es ermöglichen, Personenkreise zu erfassen, deren Daten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten sichtbar zu machen, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern.“[17] Aus der Formulierung, dass die Speicherung auch zur „Ermittlung“ und sogar Feststellung“ von Straftaten zulässig sein soll, kann geschlossen werden, dass für eine Anordnung noch keine Straftat und kein konkreter Verdächtiger vorliegen muss. Damit ist einer ausufernden Anwendung der geplanten Regelung über das notwendige Maß hinaus Tür und Tor geöffnet. Insbesondere könnten beispielsweise die Speicherung der Verkehrsdaten aller Personen im Umkreis einer Demonstration im Vorhinein angeordnet werden, mit dem Argument, dass es dabei zu Straftaten kommen könnte, was tatsächlich bei keiner Demonstration im Vorhinein ausgeschlossen werden kann (z.B. schwere Sachbeschädigungen). Schließlich ist zu hinterfragen, ob auch die Speicherdauer von 12 Monaten über das Notwendige hinausgeht, zumal der Gesetzgeber in der – vom VfGH aufgehobenen – Regelung zur Vorratsdatenspeicherung in Österreich offenbar nicht mehr als 6 Monate für notwendig hielt.

Zu begründen sind diese Forderungen nach einer Beschränkung der Maßnahme unter anderem auch damit, dass die Auskunft über den Inhaber einer IP-Adresse der Inhaltsüberwachung viel näher ist als der Überwachung von Metadaten. Typischerweise sind hier die Inhalte den Behörden bereits bekannt, oder überhaupt im Internet frei verfügbar, jedoch anonym. Mittels Auskunft über Inhaberin oder Inhaber einer IP-Adresse werden die Inhalte ihrem Urheber, oder vielmehr einem Anschlussinhaber,

14 EuGH 8.4.2014, C-293/12, Digital Rights Ireland, Rz. 60; EuGH 21.12.2016, C-203/15 Tele2 Sverige, Rz. 102.
15 EuGH 21.12.2016, C-203/15 Tele2 Sverige, Rz. 108.
16 EuGH 21.12.2016, C-203/15 Tele2 Sverige, Rz. 110.
17 EuGH 21.12.2016, C-203/15 Tele2 Sverige, Rz. 111.

zugeordnet. Die Information, welche IP-Adresse welcher Teilnehmerin bzw. Teilnehmer zu einem bestimmten Zeitpunkt zugeordnet war, stellt dazu den „missing link" dar.[18] Diese Information kann grundsätzlich gemäß § 76a Abs. 2 StPO auf Anordnung der Staatsanwaltschaft ohne die Notwendigkeit einer gerichtlichen Bewilligung beauskunftet werden. § 99 Abs. 1b TKG-E geht dem offenbar in Bezug auf Daten, die durch eine Anordnung nach § 99 Abs. 1a TKG-E von der Löschungsverpflichtung ausgenommen werden, als spätere und speziellere Norm vor und knüpft die Auskunft über diese Daten stets an das Vorliegen einer gerichtlichen Bewilligung. Das Verhältnis der beiden Normen § 76a Abs. 2 StPO und § 99 Abs. 1b TKG-E sollte jedoch ausdrücklich klargestellt werden. An dieser Stelle ist zu bemerken, dass die bestehende Regelung des § 76a Abs. 2 StPO, die eine Ausforschung des Anschlussinhabers ohne richterliche Genehmigung zulässt, aus grundrechtlicher Sicht stark zu kritisieren ist – wie gesagt steht diese Auskunft einer Inhaltsüberwachung näher als einer Verkehrsdatenauskunft, weil der Inhalt immer vorher bekannt ist.

Zu präzisieren ist die Bestimmung des § 99 Abs. 1a TKG-E auch dahingehend, ob sie sich nur auf Daten bezieht, die ab dem in der Anordnung genannten Zeitpunkt anfallen, oder auch auf Daten, die zu diesem als gemäß § 99 Abs. 2 TKG zulässigerweise gespeicherte Verkehrsdaten bereits vorliegen. Dabei ist zu beachten, dass sich in letzterem Fall eine 12 Monate übersteigende Gesamtspeicherdauer solcher Daten ergeben kann, wobei – wie oben ausgeführt – bereits die Erforderlichkeit einer zwölfmonatigen Speicherung zu hinterfragen ist, und erst recht eine noch längere. Nachdem schon die staatsanwaltliche Anordnung zum Quick Freeze nicht explizit in der StPO geregelt ist, ist auch § 137 Abs. 2 nicht anzuwenden (Anordnung der Ermittlungsmaßnahme für einen vergangenen Zeitraum, der zur Erreichung ihres Zwecks voraussichtlich erforderlich ist).

Im Gesamtkontext des vorliegenden Entwurfs ist in der Folge auch § 109 Abs. 4 Z 9 TKG-E zu kritisieren, da diese Bestimmung ein Verhalten sanktioniert, das keinen Verstoß gegen eine gesetzliche Verpflichtung darstellt, da kein Verbot der Löschung normiert ist, sondern in § 99 Abs. 1a TKG-E ausdrücklich nur eine Ausnahme von der Löschungsverpflichtung.

Im Arbeitsprogramm der Regierung fand sich in Bezug auf Quick Freeze noch eine Pflicht, fälschlicherweise überwachte Personen beim Abschluss der Maßnahme über ihre Überwachung zu informieren. Diese Verpflichtung findet sich jedoch im vorliegenden Entwurf nicht mehr. epicenter.works fordert in jedem Fall eine Benachrichtigung der von einer solchen Speicheranordnung betroffen Personen, zu einem Zeitpunkt, zu dem dadurch Ermittlungen nicht mehr gefährdet werden können oder sich herausgestellt hat, dass die Speicherung eine tatsächlich unbeteiligte Person betroffen hat, und jedenfalls dann, wenn eine richterliche Bewilligung nach § 99 Abs. 1b TKG-E zur Auskunft über die Daten nicht erteilt wird. Eine solche Pflicht zur Information von Betroffenen ist durch Art 6 EMRK geboten: Betroffene haben das Recht, zu erfahren, dass sie Ziel von Ermittlungsmaßnahmen waren, nicht zuletzt, da ihnen das erst ermöglicht, Rechtsmittel zu ergreifen.

Darüber hinaus ist eine solche Informationspflicht vor allem eine wirksame Maßnahme gegen das oben angesprochene Ausufern der Anwendung von Quick Freeze. Ohne eine solche Informationspflicht besteht die Gefahr, dass diese Maßnahme über das absolut Notwendige hinaus in Richtung einer allgemeinen Vorratsdatenspeicherung ausufert, indem unzählige Personen von einer solchen staatsanwaltschaftlichen Anordnung erfasst werden. Nur wenn jede Anordnung letztlich den Betroffenen bekannt und damit ein wirksamer Rechtsschutz überhaupt erst möglich wird, ist sichergestellt, dass bei ihrer Ausfertigung sorgsam geprüft wird, ob sie tatsächlich notwendig ist.

18 Vgl. Tschohl, Die Anonymität im Internet – Umsetzung der Vorratsdatenspeicher-RL im österreichischen Telekom-, Strafprozess- und Sicherheitspolizeirecht in Jaksch-Ratajczak/Stadler, Aktuelle Rechtsfragen der Internetnutzung, Band 2, Facultas, Wien 2011.

Schließlich bleibt die Frage, ob eine Vorratsdatenspeicherung zur Bekämpfung schwerer Straftaten überhaupt geeignet und erforderlich ist. Eine entsprechende Evaluierung von EDRi (European Digital Rights)[19] zeigt, dass die Vorratsdatenspeicherung viel kostet, aber wirkungslos ist. Aus den Ländern, die Vorratsdatenspeicherung einsetzen oder eingesetzt haben, sind keine Beispiele bekannt, dass diese zur Verhinderung oder Aufklärung von schweren Straftaten oder Terroranschlägen beigetragen hätte. Die Erläuterungen bleiben eine Erklärung schuldig, warum im Gegensatz dazu Quick Freeze, eine beschränkte Form der Vorratsdatenspeicherung, wirksam sein soll, wobei diese Beschränkungen – wie dargelegt – grundrechtlich geboten sind aber zur vorgeschlagenen Regelung völlig fehlen.

zu Ziffer 2 (§ 92 Abs. 3 lit g - „Exkurs“ § 76a Abs. 1)

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. Um Willkür und Missbrauch hintanzuhalten, ist es dringend geboten, diese Bestimmung mit geeigneten organisatorischen Sicherheitsmaßnahmen zu versehen, sodass einzelne Beamtinnen oder Beamte nicht mehr alleine eine Auskunft erwirken kann.

Diese Erweiterung der Ermittlungsmaßnahme darf nicht unterschätzt werden. Zusammen mit dem Stammdatum “Namen” und einem Bild(datum) (das z.B. aufgrund § 53 Abs. 5 SPG-E verarbeitet wurde) lassen sich mit Open Source Intelligent Tools (OSINT) umfassende Persönlichkeitsprofile erstellen (eine Stammdatenauskunft ist nach der StPO, dem SPG und dem PStSG auch ohne richterliche Genehmigung möglich). Der Einsatz solcher Software, durch die jegliche, frei im Internet verfügbare Information verarbeitet werden kann, ist gem. § 10 Abs. 5 PStSG[20] und § 53 Abs. 4 SPG zulässig – obgleich dieser Umstand grundrechtlich ebenso höchst bedenklich ist, weil diese Rechtsgrundlagen keinerlei Determinierung des zulässigen technologischen Rahmens vorsehen, gleichzeitig aber ein beachtliches Angebot für solche Software am Markt existiert. Im Prinzip handelt es sich um hochspezialisierte Suchmaschinentools, die speziell auf nachrichtendienstliche und/oder polizeiliche Ermittlungsfragen maßgeschneidert sind und systematisch auf der Basis bestimmter Algorithmen alle im Internet zugänglichen Daten durchsuchen, um daraus Informationen zu gewinnen. Die Funktionen der öffentlich verfügbaren Suchmaschinen und sozialen Netzwerke werden dabei regelmäßig automatisiert mitgenutzt. Zugekaufte Software von Unternehmen wie HackingTools oder Celebrite können mitunter aber mehr als in Österreich rechtlich zulässig ist, allerdings werden die Behörden keinen Einblick in den proprietären Code bekommen, um dies überprüfen zu können. Zu befürchten ist, dass den Herstellern einfach vertraut wird und die Ergebnisse mit der Begründung, dass der generelle Einsatz solcher Tools zulässig ist, verwendet werden. Insbesondere problematisch ist, dass der Einsatz solcher Programme von der Rasterfahndung (§ 141 StPO) nicht zu unterscheiden ist, die im Anwendungsbereich von SPG und PStSG jedoch unzulässig ist. Die Erweiterung der Stammdaten um den Begriff "Geburtsdatum" und deren Beauskunftung ohne richterliche Genehmigung ermöglichen somit die Erstellung von umfassenden Persönlichkeitsprofilen, die einen besonders schweren Grundrechtseingriff darstellen.

19 https://edri.org/data-retention-shadow-report/

20 Diese Bestimmung wird derzeit im Zuge der Anfechtung des PStSG vom VfGH geprüft (G 223/16).

Abschaffung von anonymen SIM-Karten: Zu Artikel 4 Änderung des TKG zu Ziffer 3 (§ 97 Abs. 1 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[21] fand keine Belege dafür, dass die Registrierung von SIM-Karten zu einer verbesserten Verbrechensaufklärung führt oder gegen Terrorismus hilft. Mexiko hat das Verbot 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[22] als auch 2013[23] 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[24] 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.“[25] 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 Messaging-Dienste wie „Wire“, die Kommunikation komplett unabhängig von der Telefonnummer ermöglichen. 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[26].

21 https://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf
22 http://www.europarl.europa.eu/RegData/questions/reponses_qe/2012/006014/P7_RE%282012%29006014_EN.doc
23 http://www.europarl.europa.eu/RegData/questions/reponses_qe/2012/006014/P7_RE%282012%29006014_EN.doc
24 https://www.theyworkforyou.com/wrans/?id=2007-07-16b.4.3&s=%22pay+as+you+go%22+mobile+phones
25 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Oeffentl-Mobilfunknetze.pdf?__blob=publicationFile&v=1
26 https://netzpolitik.org/2017/interaktive-karte-registrierungspflicht-fuer-prepaid-sim-karten-in-europa-weit-verbreitet/

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[27]. Der äußerst zweifelhafte Nutzen für die Bekämpfung von Kriminalität steht also einem Eingriff in das Recht aller Österreicherinnen und Österreicher gegenüber, frei und unbeobachtet zu kommunizieren. Das lässt diese Maßnahme nicht verhältnismäßig erscheinen.

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,[28] 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 Ermittler gelangen.[29]

27 http://diepresse.com/home/techscience/technews/5152191/Sobotka-fordert-Ende-der-anonymen-PrepaidSIMKarten
28 http://derstandard.at/2000051861142/Die-Registrierungspflicht-fuer-Prepaid-Simkarten-wirft-Fragen-auf
29 http://consumer.ncc.gov.ng/Archive/publication/pub/SIM.pdf