

Alice Sedmidubsky

21.08.2017

Alice Sedmidubsky nimmt zu dem Entwurf wie folgt Stellung:

Stellungnahme im Begutachtungsverfahren zum Ministerialentwurf des Innenministeriums, mit dem das Sicherheitspolizeigesetzes, das Bundesstraßen-Mautgesetzes 2002, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetzes 2003 geändert werden (326/ME)

Netzsperrern

Ich bin gegen eine Einführung von Netzsperrern in §17 Abs 1a TKG-E.

Diese Art der Zensur untergräbt das Grundrecht auf freie Meinungsäußerung und ist ein unverhältnismäßiges Mittel mit enormen Missbrauchspotential. Die Entscheidung, auf welche Inhalte zugegriffen werden kann oder ob mein Datenverkehr manipuliert wird, darf nicht ein Internetprovider treffen. Der Entwurf lässt es gänzlich ungeregelt, ob, wann, wie, warum oder wie lange welche Inhalte zensiert werden. Darüber hinaus ist das Sperren von Inhalten kein geeignetes Mittel, um Probleme mit Pornographie, gewaltverherrlichenden Darstellungen oder strafrechtlich relevanten Urheberrechtsverletzungen im Internet zu lösen.

Vorratsdatenspeicherung für Videoüberwachung

Ich bin gegen die Vernetzung von Videoüberwachung nach § 53 Abs. 5 SPG-E und gegen die Vorratsdatenspeicherung von Videoüberwachung für 2 Wochen mittels einfachem Bescheid nach § 93a SPG-E.

Ob Videoüberwachung überhaupt ein geeignetes Mittel ist, um Terroranschläge zu verhindern, muss bezweifelt werden. Schließlich wurde auch die gesamte Uferpromenade von Nizza mit Videokameras überwacht und der Anschlag dort konnte damit auch nicht verhindert werden. Großbritannien ist eines der am meisten überwachten Länder, trotzdem ist es

in letzter Zeit von Anschlägen geplagt. Im Gegenteil: Videokameras können Terroristen sogar als Ansporn dienen. Schließlich zielen sie mit ihren Gräueltaten ja auf größtmögliche Verstörung der Bevölkerung und somit auf größtmögliche Sichtbarkeit ab.

Im Jänner wurde bekannt, dass die LPD Wien 15 von 17 Überwachungskameras abbauen ließ, weil die Kosten zu hoch waren und der Nutzen für die Verbrechensbekämpfung nicht erkennbar war.

Autobahnüberwachung

Ich bin gegen die Videoüberwachung im Straßenverkehr und die aus § 54 Abs. 4b SPG-E und §19a Abs. 1a BStMG-E resultierende Erfassung und Verarbeitung des Lenkers, des Kennzeichens, der Marke, des Typs und der Farbe des Fahrzeuges durch Sicherheitsbehörden.

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 von 2007 [1] vereinbar und ist auch im Lichte der Rechtsprechung des EuGH im Fall Watson/Tele 2 Sverige sehr zweifelhaft.

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. Wie angeführt steht die nun vorgeschlagene Normierung einer Vorratsdatenspeicherung des gesamten Straßenverkehrs zur Prävention und Verfolgung jeglicher Kriminalität aus meiner 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 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 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 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 durch die Übermittlung von Daten der ASFINAG auch zur Verfolgung minderschwerer Kriminalität und zur Abwehr gefährlicher Angriffe zu einer deutlichen Ausweitung des Eingriffs.

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

Abschaffung von anonymen SIM-Karten

Ich bin gegen die verpflichtende Registrierung der Käufer von Prepaid-Wertkarten nach § 97 Abs. 1a TKG-E.

Kriminelle können diese Maßnahme leicht mit ausländischen SIM-Karten oder gratis verfügbaren, anonymen Messaging-Diensten umgehen. Für die Mehrzahl der Nutzerinnen und Nutzer in Österreich fällt jedoch eine weitere Möglichkeit weg, anonym zu kommunizieren. Damit werden 4,5 Millionen Nutzerinnen und Nutzer unter Generalverdacht gestellt. Der äußerst zweifelhafte Nutzen für die Bekämpfung von Kriminalität steht einem Eingriff in das Recht aller Österreicherinnen und Österreicher, frei und unbeobachtet zu kommunizieren, gegenüber. Das lässt diese Maßnahme nicht verhältnismäßig erscheinen.

Eine Studie der Interessensvertretung der Telekomindustrie [2] 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 sogar wieder abgeschafft, da die Verbrechensrate sogar stieg und es nur zu einem Schwarzmarkt für SIM-

Karten führte. Tschechien, Neuseeland, Kanada, Rumänien, Großbritannien und die EU-Kommission [3] haben die Maßnahme analysiert und sich aufgrund der fehlenden Belege dagegen entschieden. Nach den Terroranschlägen in London 2005 hat sogar eine eigene Kommission von Sicherheitsbehörden [4] diese Maßnahme geprüft und weil es keine Belege für die Nützlichkeit für die Sicherheit gab, von einer Einführung abgeraten.

Des Weiteren wird durch diese Maßnahme die aufblühende Szene der günstigen virtuellen Mobilfunkbetreiber geschwächt und somit der Wettbewerb. Wenige dieser Diskonter besitzen aktuell die Infrastruktur, beim Kauf einer SIM-Karte die Identität ihrer Käufer zu überprüfen.

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

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

[3] http://www.europarl.europa.eu/RegData/questions/reponses_qe/2012/006014/P7_RE%282012%29006014_EN.doc

[4] <https://www.theyworkforyou.com/wrans/?id=2007-07-16b.4.3&s=%22pay+as+you+go%22+mobile+phones>