

Dr. Christoph Mayr

05.08.2017

Dr. Christoph Mayr 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

Eine Einführung von Netzsperrern in § 17 Abs 1a TKG-E ist nicht anzuraten.

Eine solche Zensur untergräbt das Grundrecht auf freie Meinungsäußerung und ist kein geeignetes und außerdem ein völlig unverhältnismäßiges Mittel mit enormem Missbrauchspotential. Eine Zensur ist bereits aus grundsätzlichen Erwägungen abzulehnen, weil sie einer freien Meinungsäußerung diametral zuwiderläuft.

Vorratsdatenspeicherung für Videoüberwachung

Eine Vernetzung von Videoüberwachung nach § 53 Abs. 5 SPG-E und eine Vorratsdatenspeicherung von Videoüberwachung für 2 Wochen mittels einfachen Bescheids nach § 93a SPG-E ist nicht anzuraten.

Videoüberwachung ist an sich bereits kein geeignetes Mittel, um etwa Terroranschläge zu verhindern. Videokameras können Terroristen vielmehr sogar als Ansporn dienen. Schließlich zielen diese ja auf größtmögliche Sichtbarkeit und Aufmerksamkeit 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.

Ein Zugriff der Behörden auf (private) Überwachungskameras ohne gerichtliche Anordnung im Einzelfall ist jedenfalls verfassungswidrig.

Autobahnüberwachung

Eine 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 ist nicht anzuraten.

Mit dieser verfassungswidrigen 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.

Quick freeze

Eine Neuauflage einer verfassungswidrigen Vorratsdatenspeicherung in Form von Quick Freeze nach § 99 Abs. 1a bis 1f TKG-E ist nicht anzuraten.

Auf Anordnung der Staatsanwaltschaft soll ein Telekombetreiber künftig wieder Vorratsdaten für bis zu ein Jahr speichern müssen. Somit kann diese Überwachungsmaßnahme von der politisch abhängigen, weisungsgebundenen Staatsanwaltschaft eingesetzt werden, noch bevor ein unabhängiges, mit den für den Rechtsstaat unabdingbaren richterlichen Privilegien (Unabhängigkeit, grundsätzliche Unabsetzbarkeit, Unversetzbarkeit) ausgestattetes Gericht zugestimmt hat, da der Entwurf nach § 99 Abs. 1b TKG-E erst bei der Beauskunftung der Daten, aber nicht bei der Speicherung auf Vorrat eine gerichtliche Bewilligung vorsieht. Jedoch wird bereits durch die Speicherung massiv und in verfassungswidriger Weise in Grundrechte eingegriffen.

(Eine entsprechende Evaluierung von EDRI (European Digital Rights) [2] zeigt überdies, dass eine solche Maßnahme viel kostet, aber wirkungslos ist und keinesfalls zur Verhinderung von Straftaten beiträgt.)

Abschaffung von anonymen SIM-Karten

Eine verpflichtende Registrierung der Käufer von Prepaid-Wertkarten nach § 97 Abs. 1a TKG-E ist nicht anzuraten.

Damit würden 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 [3] 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 [4] 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 [5] 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://edri.org/data-retention-shadow-report/>

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

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

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