

Sg. Damen und Herren,

ich erlaube mir als Geschäftsführer auch namens meiner Unternehmensgruppe (kapper.net) im Zusammenhang mit der öffentlichen Konsultation des Bundesministeriums für Inneres zum Entwurf eines Bundesgesetzes, mit dem das Sicherheitspolizeigesetz, das Bundesstraßen-Mautgesetz 2002, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden wie folgt Stellung zu nehmen:

- a) Netzsperrern – in welcher Geschwindigkeit aus „Verkehrsmanagement“ eine handfeste Netzsperrung und in weiterer Folge ein Internet-Blackout werden können, zeigen uns bereits zahlreiche Länder in den letzten Jahren. Das Internet ist ein Hort der Innovation und die UNO hat bereits erklärt, dass die Sustainable Development Goals (SDGs) damit befördert werden können. Es sollte vielmehr das Prinzip „Löschen statt Sperren“ für illegale Inhalte hochgehalten werden. Banken schaffen es weltweit illegale sog. „Phishing“ Websites binnen weniger Stunden zu sperren. Dieselbe Durchsetzungskraft sollte auch für andere illegale Inhalte erzeugt werden, dann wäre die Idee von Netzsperrern nicht notwendig.
- b) Kundenwunsch nach Inhaltsveränderung – sollten beispielsweise Eltern für Ihre Kinder einen Jugenschutzfilter für den Internetzugang ihrer Kinder aktivieren wollen, dann soll das dem Kunden möglich sein, ebenso könnte für Blinde beispielsweise ein Textkonverter mit Vorlesefunktion ein Angebot sein, diese Möglichkeiten sollte der Gesetzgeber einräumen, allerdings nicht zum Staatszensur werden und den Bürgerinnen und Bürgern vorschreiben, wer, was im Internet zu sehen bekommt und was ihm oder ihr lieber nicht zeigen.
- c) SIM-Karten-Registrierung – dem Gesetzgeber ist wohl bewusst, dass selbst England mit umfassender Terrorerfahrung auf diese Registrierung wegen schlichter Sinnlosigkeit verzichtet. Neben der inhaltlichen Nutzenkritik gibt es aber auch technische Faktoren: Das Internet der Dinge wird besonders auf Mobilfunk und damit SIM-Karten basierend zahlreiche mobile Geräte verbinden. Diese Angebote gibt es auch bereits zB „Amazon Kindle mit Whispernet“, aber auch integrierte SIM und Mobilfunkzugänge in Kassensysteme, Notfallrufsystem uvm. Eine derartige Maßnahme würde also nicht nur die Verkaufsstellen von Supermärkten für SIM-Karten behindern, vielmehr wäre die Entwicklung neuer mobiler Hardware mit Internetverbindung massiv behindert, da für jedes Gerät eine umfassende Personenregistrierung notwendig wäre, obwohl diese im Fall zB einer Notrufsäule völlig absurd wäre und für zB Crows-Sensoren gänzlich kontraproduktiv, besonders wenn Daten dieser Sensoren gezielt anonymisiert erfasst werden sollen.
- d) Vorratsdatenspeicherung 2.0 – „Quick Freeze“ der EuGH hat zu den Verfahren der vergangenen Vorratsdatenspeicherung (VDS), welche bekanntlich aufgehoben wurde, bereits festgestellt: VDS ist nur zur Bekämpfung schwerer Kriminalität zulässig, dennoch werden bereits Strafrahmen ab 6 Monaten zum Einsatz der VDS2.0 im Entwurf als zulässig gesehen, diesen Widerspruch zum EuGH sollte der Gesetzgeber jedenfalls reparieren und auf tatsächlich schwere Delikte verweisen.
Der EuGH hat ebenfalls erkannt, dass die Speicherung der Daten auf das notwendigste beschränkt sein muss. Der neue „Quick-Freeze“ sorgt aber dafür, dass der Speicherzeitraum gegenüber der VDS1.0 sich mehr als verdoppelt, sechs Monate sollten – wie auch schon im alten Gesetz das absolute Maximum der Speicherdauer sein.
Nebstbei sollen auch noch die EDV-Systeme die all das bewerkstelligen sollen bis 1.1.2018 fertig sein, die Frist ist daher für die Umsetzung jedenfalls bis 1.7.2018 auszuweiten und eine Klarstellung bezüglich der zu speichernden Daten zu treffen. Ebenfalls wäre wie bereits in der VDS1.0 ein entsprechender Kostenersatz für die Provider vorzusehen.
- e) Löschverpflichtungsausnahme – etwas komplizierter wäre es vielleicht noch gegangen, aber verkürzt wird dem Provider freigestellt ob er Daten löscht oder nicht und auch noch welche Daten das sein könnten. Allenfalls wäre auch noch eine kreative Interpretation möglich und der Gesetzgeber meint eigentlich eine Speicherverpflichtung aller Daten. Einerseits wäre es absurd nun plötzlich Daten speichern zu müssen, welche bisher nicht einmal vorhanden waren und andererseits möge der Gesetzgeber bitte Klarheit schaffen: was soll wie lange

gespeichert werden, dieser Teil des Entwurfs kommt einem schlechten Scherz gleich: Entweder man muss speichern oder nicht, die Version „Du kannst mal nicht löschen, aber wir wollen dann sicher die Daten haben“ ist eine unklare Anweisung, welche in der Providerbranche für deutliche Verwirrung sorgen wird. Damit das alles noch spannend bleibt, packt man eine Strafanandrohung oben drauf, weil der Provider soll ja richtig raten, was der Gesetzgeber hier von ihm will, sonst gibt's Strafen.

- f) Private „Hilfssheriffs“ – die Idee, dass hoheitliche Aufgaben nun auch von „Teilnehmern von Sicherheitsforen“ ausgeführt werden können grenzt an einen Aprilscherz. Hier sollen persönliche Daten nun an Private übermittelt werden, welche etwa schon im Vorfeld von Veranstaltungen die Übermittlung dieser Daten verlangen könnten. Das neue DSG klärt ganz eindeutig im 3. Hauptstück, dass solche Daten nur an Behörden und Stellen mit entsprechenden Hoheitsbefugnissen übermittelt werden können. Kurz gefragt: Möchten Sie, dass der freundliche Hilfssheriff von Nebenan mal schnell Ihre Internetdaten abgreift um Sie dann über Ihre Verhalten im Internet zu belehren? In diesem Sinne – das ist ernsthafter Blödsinn.

Danke im Voraus
Harald Kapper, CEO
KAPPER NETWORK-COMMUNICATIONS GmbH
A-1090 Wien, Alserbachstrasse 11