Stellungnahme zu 192/ME

Sehr geehrte Damen und Herren!

> *Der Einzelne und seine freie Persönlichkeitsentfaltung sind nicht nur auf die öffentliche, sondern auch auf die vertrauliche Kommunikation in der Gemeinschaft angewiesen; die Freiheit als Anspruch des Individuums*
> *und als Zustand einer Gesellschaft wird bestimmt von der Qualität der Informationsbeziehungen.*
>
> *VfGH 27.06.2014, G47/2012, https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Vfgh&Dokumentnummer=JFR_20140627_12G00047_01*

Wir möchten Ihnen sehr herzlich für das Vergnügen danken, das wir bei der Lektüre des Entwurfes für ein “Bundesgesetz, mit dem die Strafprozessordnung 1975 und das Staatsanwaltschaftsgesetz geändert werden” hatten und begrüßen ausdrücklich, dass Sie offensichtlich keinerlei Ambitionen haben, tatsächlich ein ernstgemeintes Gesetz zur Einführung eines "Bundestrojaners" auf den Weg zu bringen. Wir möchten Sie allerdings darauf hinweisen, dass möglicherweise nicht alle Menschen diese Form von Humor verstehen und gutheißen. Und den Text kurz nach den Anschlägen in Brüssel zu veröffentlichen, kann durchaus auch als Verhöhnung der Opfer aufgefasst werden.

Im Folgenden möchten wir nun aber auf die Punkte eingehen, die uns am besten gefallen haben.

- Im neuen § 134 Abs. 4a wird die "Installation eines Überwachungsprogramms im Computersystem ohne Kenntnis des Inhabers eines solchen Systems oder sonstiger Verfügungsbefugter" vorgesehen. In den Erläuterungen wird dazu ausgeführt, dass "ausschließlich eine Installation durch physischen Zugriff auf das Computersystem, nicht jedoch eine remote-Installation der Überwachungssoftware zulässig" sei. Nö, im Gesetzestext steht das freilich nicht, im Gegenteil impliziert § 134a Abs. 2 eher, dass es sich bei Remote-Installation um den Regelfall handelt, ein physischer Zugriff auf das Computersystem nur vorgesehen ist, "soweit dies zur Druchführung der Ermittlungsmaßnahme unumgänglich ist". Aber hey, marketingtechnisch klingt "keine Remote-Installation" gleich viel besser.

- Von Computersystemen wird, so die Erläuterungen, unter anderem deshalb gesprochen, weil "die Kommunikation der Attentäter von Paris im November 2015 nicht auf dem Wege der Kommunikation über Kurznachrichten oder Sprachtelefonie, sondern vielmehr internetbasiert über Spielekonsolen erfolgte". Nein, es gibt keine Beweise dafür. Aber hey, so what. Es klingt gut. (vgl. http://mashable.com/2015/11/16/isis-playstation-paris-attacks/#I4q3KXI1D5qH)

- Die vorgesehene Formulierung des § 134a Abs. 1 spricht von einer "Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, [...], wenn der Eingriff in das Computersystem notwendig ist, um die Überwachung und Aufzeichnung von Nachrichten in unverschlüsselter Form zu ermöglichen". Dass im Jahr 2016 so gut wie jede Verbindung, damit also auch die übermittelten Nachrichten, verschlüsselt sind, und diese Form der Überwachung damit sinnlos ist, muss man ja nicht dazusagen.

- Dabei ist die Definition von "Nachricht" ja unheimlich kreativ. Eine Nachricht umfasst laut Erläuterungen den "Gedankeninhalt der Mitteilung", außerdem "auch sonstige Daten", mithin also eh alles. Insbesondere auch "Protokolldateien der für diese Übertragung verwendeten Programme (z. B. Chat-Logs) als auch die Möglichkeit der Identifizierung der Kommunikationspartner jener Person, gegen die sich die Überwachung richtet". Das ist dann natürlich "keinesfalls eine Durchsuchung des Computersystems nach weiteren Daten zur Identifizierung einer Person oder sonstiger im Computersystem gespeicherter oder verarbeiteter Daten im Sinne einer „Online-Durchsuchung“", deshalb "ist nicht die Gesamtheit der für eine Online-Durchsuchung als notwendig angedachten Sicherungsmaßnahmen erforderlich". Zwinkersmiley.

- Nach § 137 Abs. 3 soll es möglich sein, die Überwachung für einen vergangenen Zeitraum anordnen zu lassen. Eine tolle Vorgehensweise. Erst mal überwachen, dann fragen, ob es legal war.

- In den Erläuterungen zu Z 12-16 wird festgehalten, "dass das Überwachungsprogramm nicht durch ein eventuell zwischenzeitig erfolgtes BackUp des Geräts nach einer Datenwiederherstellung aus diesem BackUp wieder aktiviert" werden darf und zu diesem Zweck "das Überwachungsprogramm mit einem Funktionszeitraum zu versehen" sei. Hoffen wir nur, dass niemand auf die abwegige Idee kommt, das Datum auf seinem Computer ein paar Jahre in die Zukunft zu drehen, um etwaige Überwachungsprogramme zu deaktivieren.

- Das Gesetz geht nicht auf die Rechte von Dritten ein, die ein Computersystem mitbenutzen und damit von der Überwachung ebenso betroffen sind. Bloß nicht zu viele Gedanken machen.

- Die Gefahr, dass die Überwachungssoftware entdeckt wird, ist sehr hoch, verursacht sie einen nicht unbeträchtlichen Datenverkehr. Und wenn das geschieht, können natürlich bewusst falsche Spuren gelegt werden. Klingt zunächst nicht besonders toll, aber: So wird den ÜberwacherInnen nicht so schnell langweilig.

- Zuletzt steht natürlich zu hoffen, dass niemand so paranoid ist und einen Virenscanner und eine Firewall auf dem zu überwachenden Computersystem installiert, und die Überwachungssoftware damit an der Kommunikation mit der Außenwelt hindert oder gar komplett löscht. Schließlich ist davon auszugehen, dass jeder Virenscanner ein solches Programm aufgrund offensichtlicher Sicherheitsrisiken als Bedrohung einstufen würde.

Wir möchten Ihnen nochmals für das Vergnügen danken, das wir mit Ihrer Gesetzesvorlage hatten. Abschließend möchten wir im Sinne einer freien und sicheren Gesellschaft unsere Hoffnung festhalten, dass es niemals zu einem ernsthaften Vorstoß zur Einführung eines solchen Bundestrojaners kommen wird. Falls dennoch einmal ein solcher Gesetzesvorschlag zur Begutachtung gebracht wird, sind wir natürlich gerne bereit, uns ernsthaft und auch etwas ausführlicher mit diesem aus rechtlicher, technischer und moralischer Sicht zu befassen.

Mit freundlichen Grüßen

Klaus-Uwe Mitterer

Badaisprecher