WIRTSCHAFTSKAMMER ÖSTERREICH

Bundesministerium für Justiz
Museumstraße 7
1070 Wien

via E-Mail: team.s@bmj.gv.at
cc: begutachtungsverfahren@parlament.gv.at

Wiedner Hauptstraße 63 | Postfach 195
1045 Wien
T +43 (0)5 90 900-4282 | F +43 (0)5 90 900-243
E rp@wko.at
W https://news.wko.at/rp

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen, Sachbearbeiter	Durchwahl	Datum
BMJ-S578.031/0008-IV 3/2017 10.7.2017	Rp 662/17/AS/CG Dr. Artur Schuschnigg	4014	11.8.2017

Ministerialentwurf eines Bundesgesetzes, mit dem die Strafprozessordnung1975 geändert wird (Strafprozessrechtsänderungsgesetz 2017) - Stellungnahme

Sehr geehrte Damen und Herren,

wir danken für die Übermittlung des gegenständlichen Ministerialentwurfs und nehmen zu diesem, wie folgt, Stellung:

Evident ist, dass Strafverfolgungsbehörden aufgrund der fortschreitenden technischen Entwicklungen immer wieder vor dem Problem stehen werden, die entsprechenden Ermittlungsmöglichkeiten seitens des Gesetzgebers angepasst zu erhalten. Da allerdings kriminelles Verhalten via internetbasierter Technologien auch der Wirtschaft schwere Schäden verursachen, ist nach Ansicht der Wirtschaftskammerorganisation den vom Gesetzgeber geplanten Maßnahmen zur Abwehr derartiger Schäden und Verfolgung derartiger Straftaten grundsätzlich zuzustimmen. Solche Eingriffsmöglichkeiten müssen allerdings klar und unstrittig determiniert, maßvoll, in einem adäquaten Verhältnis zur vermuteten Straftat und grundrechtskonform ausgestaltet sein.

Dies kann etwa auch dadurch erfolgen, dass bestimmte Maßnahmen ausschließlich nach gerichtlicher Bewilligung auf gesetzlicher Basis im Einzelfall ergriffen werden dürfen, etwa hinsichtlich eines Eingriffs in das Hausrecht oder einer Entnahme von Geräten aus der Kleidung oder aus anderen Gegenständen, wie z. B. Aktenkoffer, um die für die Überwachung notwendigen Programme auf Computersysteme installieren zu können. Nur unter diesen Voraussetzungen wäre auch eine Überwachung von Nachrichten und eine akustische Überwachung von Personen in Fahrzeugen zuzulassen.

ad § 76a Abs. 1:

Wir begrüßen die Neuregelung zur Bekanntgabe des PUK-Codes. Die bisherige Lösung über die Sicherstellung nach § 110 StPO war aufgrund der Tatsache, dass die gesamte Verdachts- und Beweislage zur Kenntnis gebracht werden musste ernsten Bedenken ausgesetzt. Da mit dem PUK-Code ein Zugriff auf in die § 76a Abs. 2 StPO angeführte Daten möglich ist, ist die vorgeschlagene Einordnung in der StPO systematisch richtig (Anordnung der Staatsanwaltschaft für die Bekanntgabe des PUK Codes; ein Ersuchen kriminalpolizeilicher Behörden genügt nicht). Anzumerken ist, dass eine klare Regelung zum Kostenersatz zu finden ist.

ad § 116 Abs. 6:

§ 116 Abs. 6 soll dahingehend geändert bzw. erweitert werden, dass Kredit- oder Finanzinstitute Daten künftig nicht mehr nur in einem allgemein gebräuchlichen Dateiformat (z. B. PDF-Format) zu übermitteln haben, sondern auch in strukturierter Form, sodass die Daten elektronisch weiterverarbeitet werden können.

Grundsätzlich besteht gegen die Änderung kein Einwand, solange die Änderung nicht dazu führt, dass Kredit- und Finanzinstitute künftig verpflichtet sind, ihre technischen Systeme auf ein von der Behörde vorgegebenes Format umzustellen und damit verbunden ein entsprechender Kosten- bzw. Ressourcenaufwand bei den Kredit- und Finanzinstituten einhergeht. Die geplante Änderung sollte nicht zu einem Mehraufwand für Kredit- oder Finanzinstitute führen, nur damit sich die Behörde einen Zeit- und Ressourcenaufwand erspart.

ad § 134 Z 3:

Kritisch sehen wir die Etablierung eines eigenen Nachrichtenbegriffs. Der bisherige Verweis auf den Nachrichtenbegriff des § 92 Abs. 3 Z 7 TKG stellte ein einheitliches Begriffsverständnis sicher. Der neue Begriff soll nun erweitert verstanden werden und alle Nachrichten und Informationen, die über ein Kommunikationsnetz oder einen Dienst der Informationsgesellschaft gesendet, übermittelt oder empfangen werden, erfassen. Über Kommunikationsnetze werden in diesem weiten Sinn so gut wie ausschließlich Informationen übermittelt, weshalb durch diesen neuen Begriff „Überwachung von Nachrichten" eine Überwachung des gesamten Datenverkehrs umfasst ist. Es wird versucht, diese überschießende Extension durch die Definition der technischen Schnittstellen im Rahmen der Überwachungsverordnung verfassungskonform zu reduzieren. Dies erscheint jedoch aufgrund der Weite und Intensität des Grundrechtseingriffs keine geeignete Maßnahme zu sein (auch, da es sich dabei bloß um eine Verordnung handelt).

§ 135 Abs. 2a:

Der IMSI-Catcher hat derart ausgestaltet zu sein, dass dessen Einsatz die Netzintegrität und Netzsicherheit des Betriebes nicht beeinträchtigt.

ad § 135a:

Digitalisierung erfasst sämtliche Lebensbereiche und Geschäftsfelder. Voraussetzung für das erfolgreiche Gelingen ist ein hohes Niveau an IT- und Datensicherheit. Nur so kann der Digitalstandort Österreich gestärkt werden. Aus diesem Grunde werden Bedenken an dieser Bestimmung geäußert.

Die vorgesehene neue Ermittlungsbefugnis des § 135a StPO soll es beispielsweise erlauben, ohne Zustimmung des Inhabers ein Programm zur Überwachung verschlüsselter Nachrichten auf einem Computersystem zu installieren. Die Notwendigkeit einer Anpassung der Überwachungsmöglichkeiten an neue Technologien ist zwar nachvollziehbar, kann jedoch auch eine Gefahr für die Datensicherheit darstellen.

Nutzer vertrauen darauf, dass ihre Daten in den von ihnen genutzten Diensten vor fremden Zugriffen sicher sind. Dieses Vertrauen basiert auf der intensiven Arbeit, die die IT-Branche über Jahre in die Etablierung von Sicherheitsstandards, wie einer effektiven Verschlüsselung der Daten, investiert hat. Ein Hauptaugenmerk liegt dabei darauf, fortwährend nach vorhandenen Sicherheitslücken in den Systemen zu suchen und diese mittels Updates zu schließen. Zur unbemerkten Ferninstallation der vorgesehenen Überwachungssoftware werden jedoch gerade solche „backdoors" ausgenutzt. Um eine effektive Umsetzung der Ermittlungsmaßnahme zu garantieren, müssten solche Sicherheitslücken demnach offengehalten werden, anstatt sie dem jeweiligen Unternehmen zu melden. Die Auswirkungen solch bewusst nicht geschlossener „backdoors" haben sich zuletzt anhand krimineller Cyber-Attacken mittels Ransomware („WannaCry" bzw. „Petrwrap") gezeigt, die vor kurzem enormen Schaden für die Wirtschaft verursacht haben. Die vorgeschlagenen Ermittlungsmaßnahmen untergraben damit auch das Vertrauen in österreichische Unternehmen und in den Wirtschaftsstandort Österreich, der bislang aufgrund der hohen Datenschutz- und Sicherheitsstandards geschätzt wird.

In den Erläuterungen wird wiederholt betont, § 135a solle lediglich der Ausleitung von Kommunikationsdaten während des aufrechten Kommunikationsvorgangs dienen und keinesfalls einer „Online-Durchsuchung" gleichkommt. Aus technischer Sicht dürfte ein solch „chirurgischer Eingriff" nicht umsetzbar ist. Auch in den Erläuterungen wird die technische Umsetzbarkeit lediglich festgestellt ohne diese tatsächlich näher zu beschreiben. Der Grund hierfür liegt darin, dass für die Installation, den Betrieb und das Verstecken einer solchen Überwachungssoftware umfangreiche Zugriffsrechte auf dem Zielsystem benötigt werden. Hierdurch würden jedoch zahlreiche weitere Funktionalitäten erlaubt werden, inklusive des Durchsuchens, Manipulierens und Erstellens von Dateien. Eine technische Einschränkung der Software, um dies gänzlich zu unterbinden, ist nicht möglich. Darüber hinaus wären auch Backups in einer Cloud erfasst, was wiederum einer de facto Online-Durchsuchung gleichkommt. Diese Risiken wurden bereits von einer interministeriellen Arbeitsgruppe zur „Online-Durchsuchung" im Jahr 2008 thematisiert und konnten bislang nicht ausgeräumt werden.

Verstärkt wird das Sicherheitsrisiko weiters dadurch, dass die Novelle eine exzessive Ausdehnung des Begriffs „Nachricht" vorsieht, durch welchen in Hinkunft nicht nur menschliche Gedankeninhalte, sondern auch Kommunikation im technischen Sinn erfasst werden soll. In Kombination mit der weiten Definition von „Computersystem" würde damit auch die Kommunikation zwischen Geräten im „Internet der Dinge" miteingeschlossen werden, wodurch auch auf diesen Geräten entsprechende „backdoors" notwendig wären und die potentiellen Missbrauchsmöglichkeiten noch weiter ansteigen.

Die dadurch notwendige Kooperation des Staats mit Dienstleistern, die Sicherheitslücken am Markt anbieten, erscheint hochgradig bedenklich. Auch unter dem Gesichtspunkt des Schutzes der öffentlichen Sicherheit wäre die Förderung eines „Markts für Sicherheitslücken" nicht zu rechtfertigen, der sowohl von Kriminellen als auch von fremden Geheimdiensten sowie autokratischen Regimes zur Verfolgung von Dissidenten oder Industriespionage genutzt werden kann. Insbesondere kann nicht gewährleistet werden, dass die entsprechenden „backdoors" ausschließlich dem anfragenden Staat mitgeteilt werden, wodurch das Missbrauchspotential noch weiter erhöht wird und zudem die Investitionen sowohl vom Staat als auch von Unternehmen in die Bemühungen um Cybersicherheit konterkariert werden.

Aus technischer Sicht ist weiters kritisch zu sehen, dass ein Gesetz beschlossen werden soll, dessen rechtmäßige technische Umsetzungsmöglichkeit in der Praxis erst im Anschluss bis 2019 geprüft wird. Um ein unausgegorenes Lösungsmodell zu verhindern, das Sicherheitsstandards und Grundrechte gleichermaßen gefährdet, muss diese Bestimmung zur Überwachung verschlüsselter Kommunikationsdienste nochmals ausdrücklich hinsichtlich der konkreten technischen Umsetzung von unabhängigen technischen Experten geprüft und für unbedenklich deklariert werden.

Die Materialien verdeutlichen nicht, dass ein Überwachungsprogramm nur zulässig ist, wenn es sowohl das Computersystem, in dem es installiert wurde, als auch dritte Computersysteme weder dauerhaft schädigt noch beeinträchtigt. Nach der Beendigung der Ermittlungsmaßnahme ist das Programm zu entfernen, es lediglich funktionsunfähig zu machen, ist aus Sicherheitsgründen unzureichend.

ad § 138 Abs. 2:

Zu dieser Änderung ist anzumerken, dass eine Verpflichtung der Betreiber zur unverzüglichen Auskunft über Daten einer Nachrichtenübermittlung bestehen soll. Sollten dadurch Bereitschaftsdienste bei den betroffenen Unternehmen erforderlich werden, die bisher nicht oder nicht in dem künftig notwendigen Umfang eingerichtet sind, so ist ein Kostenersatz dafür vorzusehen.

Hingewiesen sei daher auf das Erkenntnis des VfGH vom 27.2.2003, G37/02 ua, V42/02 ua, (VfSlg 16.808), in dem das Höchstgericht die Überwälzung aller Kosten für die Bereitstellung von Überwachungseinrichtungen durch Ablehnung eines Kostenersatzes an die Telekommunikationsbetreiber für verfassungswidrig erklärt. Dieses Erkenntnis des VfGH hat Gültigkeit für alle Implementierungen zur Bereitstellung von Einrichtungen, die der Umsetzung öffentlicher Interessen gelten, sodass folglich eine Bestimmung (wie gegenständliche, wenn sie so verstanden werden muss, dass Dienste einzurichten oder zu erweitern sind) ohne Kostenersatzregelung verfassungswidrig sein dürfte.

Auch wenn dies nur mittelbar mit dem gegenständlichen Entwurf zu tun hat: Im BMI-Teil des sog. Sicherheitspakets (326/ME BlgNR XXV. GP) soll in § 17 TKG ein neuer Abs. 1a eingefügt werden. Wir gehen davon aus, dass im dortigen Zusammenhang unter „strafrechtlich relevante Handlungen" jene gemeint sind, bei denen der objektive Tatbestand erfüllt ist. Die Erläuterungen schweigen zu diesem Punkt. Wir merken dies hier an, da es sich um justizrelevanten Aspekt handelt, zum Entwurf des Bundesministeriums für Inneres wird eine gesonderte Stellungnahme unsererseits ergehen.

Wir bitten um Berücksichtigung unserer Anliegen.

Mit freundlichen Grüßen

KommR Dipl.-Ing. Dr. Richard Schenz
Vizepräsident

Mag. Anna Maria Hochhauser
Generalsekretärin