WIRTSCHAFTSKAMMER ÖSTERREICH

Justizausschuss des
Österreichischen Nationalrats
z.H. Obfrau AbgzNR Mag. Michaela Steinacker
Parlament
1010 Wien

via E-Mail: ausschussbegutachtung.justizausschuss@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
17 BlgNR XXVI. GP 6.3.2018	Rp 662/18/AS/CG Dr. Artur Schuschnigg	4014	23.3.2018

Regierungsvorlage eines Bundesgesetzes, mit dem die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden (Strafprozessrechtsänderungsgesetz 2018)
Ausschussbegutachtung gem. § 40 GOG - Stellungnahme

Sehr geehrte Damen und Herren,

die Wirtschaftskammer Österreich begrüßt den Beschluss des Justizausschusses, die Regierungsvorlage eines Strafprozessrechtsänderungsgesetzes 2018 einer Ausschussbegutachtung zu unterziehen, und dankt für die Einladung, zu dieser schriftlich Stellung zu nehmen. Wir nehmen diese Einladung gerne an und führen aus, wie folgt:

Evident ist, dass Strafverfolgungsbehörden aufgrund fortschreitender technischer Entwicklungen immer wieder vor dem Problem stehen werden, die entsprechenden Ermittlungsmöglichkeiten seitens des Gesetzgebers angepasst zu erhalten. Da zudem 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.

Vieles ist zwar ansatzweise gut gemeint, doch scheint die technische Verwirklichung und Absicherung in den Kinderschuhen zu stecken, sodass eine missbräuchliche Datenverwendung nicht ganz ausgeschlossen werden kann. Auch in diesem Zusammenhang sollte man sich die Verwirklichung der angestrebten Punkte wohl überlegen, um nicht allfällig den Anschein einer überhasteten Anlassgesetzgebung erwecken.

Änderungen der Strafprozessordnung 1975

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:

Die Erläuterungen der Regierungsvorlage führen dazu aus:

Mit der vorgeschlagenen Änderung soll eine im Bereich des verwaltungsbehördlichen Finanzstrafverfahrens bereits durch das 2. Abgabenänderungsgesetz 2014, BGBl. I Nr. 105/2014, erfolgte und mit 30. Dezember 2014 in Kraft getretene Änderung (§ 99 Abs. 6 sechster Satz FinStrG) auch für den Bereich des gerichtlichen Strafverfahrens (und im Wege des § 195 Abs. 1 FinStrG) des Verfahrens wegen gerichtlich strafbarer Finanzvergehen nachvollzogen werden. **Durch die geltende Regelung des § 116 Abs. 6 zweiter Satz StPO erfüllen Kreditinstitute ihre gesetzliche Verpflichtung zur Herausgabe der Daten „in einem allgemein gebräuchlichen Dateiformat" auch durch Übermittlung von Dateien im PDF-Format. Die aus solchen PDF-Dateien nur ablesbaren – nicht aber strukturiert zu verarbeitenden – Informationen müssen sodann händisch in andere Dateiformate (Tabellenkalkulations- oder Datenbankprogramme) übertragen werden, um eine elektronische Auswertung vornehmen zu können. Damit ist gerade in der Praxis des strafprozessualen Ermittlungsverfahrens ein beträchtlicher Zeit- und Ressourcenaufwand verbunden.**[1] Um diesen Aufwand und damit auch Kosten zu verringern, potentielle Fehlerquellen bei der händischen Übertragung der Daten auszuschließen und eine verfahrensrechtlich nicht gebotene Differenzierung zum verwaltungsbehördlichen Finanzstrafverfahren zu beseitigen, soll § 116 Abs. 6 zweiter Satz StPO entsprechend § 99 Abs. 6 sechster Satz FinStrG geändert werden. Die Daten sollen künftig von Kredit- und Finanzinstituten auch im Bereich des gerichtlichen Strafverfahrens so zu übermitteln sein, dass diese auch elektronisch weiterverarbeitet werden können, beispielsweise in Form von Dateien gängiger Tabellenkalkulations- oder Datenbankprogramme (vgl. EBRV 360 BlgNr. 25. GP 24).

Die beabsichtigte Änderung könnte dahingehend ausgelegt werden, dass Kreditinstitute etwa auf Microfiche enthaltene Daten zunächst in Excel zu übertragen haben werden, bevor sie an die Ermittlungsbehörden weitergeleitet werden.

Inhaltlich wird dazu wie folgt Stellung bezogen:

- Der Halbsatz *„wenn zur Führung der Geschäftsverbindung automationsunterstützte Datenverarbeitung verwendet wird"* soll beibehalten werden, weil die in den Erläuterungen genannten Beweggründe die geplante Änderung nicht rechtfertigen.
- Es ist Kredit- und Finanzinstituten nicht zumutbar, archivierte Daten händisch in ein elektronisch auslesbares Format zu übertragen, wenn im Einzelfall Daten nicht in dieser Form vorliegen sollten.
- Subsidiär sollte zumindest in den Erläuterungen klargestellt werden, dass für derartige Tätigkeiten ein angemessener Kostenersatz gemäß § 111 Abs. 3 StPO zusteht.

---

[1] Hervorhebung durch den Stellungnehmenden.

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" gleichkommen. 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:

Allfällige Einrichtungen und Personaleinsatz, die über die individuellen betrieblichen Belange der einzelnen Betreiber hinausgehen, wären jedenfalls gesondert in Auftrag zu geben und zu vergüten.

Weiters wird betreffend Daten unbeteiligter Dritter auf die Judikatur zur Vorratsdatenspeicherung verwiesen.

Leider fehlt auch für die Anlassdatenspeicherung eine Regelung zum zwingend gebotenen Kostenersatz. Investitionskostenersatz für die Implementierung technischer Einrichtungen ist nur nach der Überwachungsverordnung möglich, die die Anlassdatenspeicherung nicht erfasst. Auch hier sei darauf verwiesen, dass die Betreiber seinerzeit bei der Implementierung der Vorratsdatenspeicherung 20% der Kosten selber tragen mussten und sie nunmehr nicht erneut belastet werden dürfen.

Daneben ist natürlich auch ein Ersatz der operativen Kosten vorzusehen, wie es für andere Maßnahmen die Überwachungskostenverordnung regelt. Auf diese sollte im Gesetz verwiesen werden und die Verordnung selbst entsprechend angepasst werden. Die vorzusehenden Beträge für die operative Arbeit der Anlassdatenspeicherung sind den Aufwänden der Betreiber anzupassen und wertgesichert zu benennen.

In den Erläuterungen sollte klargestellt werden, dass daraus, dass die Anbieter der Anlassdatenspeicherung unverzüglich zu entsprechen haben, keine andere Zeitigkeit folgt als aus der allgemein anerkannten Definition von unverzüglich im Sinne von ohne schuldhaftes Zögern. Dabei sind die gegebenen betrieblichen Abläufe zu berücksichtigen. Wie bisher (und aus der Umsetzung der Vorratsdatenspeicherung seinerzeit) ergeben sich daraus für die Betreiber keinerlei Verpflichtungen, ihre technischen Systeme zu ändern, zu erweitern oder organisatorische Abläufe umzustrukturieren. Dies gilt ebenso hinsichtlich der Verschaffung betrieblich gar nicht notwendiger Daten. Das war bisher Konsens zwischen Gesetzgeber/ Behörden und den Betreibern und sollte im besten einvernehmlichen Sinn bei der Anlassdatenspeicherung Eingang in die Erläuterungen finden.

Ad § 157 Abs. 1 Z 2:

§ 157 Abs. 1 Z 2 StPO knüpft bisher, was die prüfenden Berufe betrifft, an den sich aus der Definition der Wirtschaftstreuhandberufe in § 1 WTBG ableitbaren Begriff „Wirtschaftstreuhänder“ an. Revisoren nach dem Genossenschaftsrevisionsgesetz (GenRevG) und Sparkassenprüfer nach dem Sparkassengesetz (die Prüfer der Prüfungsstelle des Sparkassen-Prüfungsverbandes) sind im Gegensatz zu Wirtschaftsprüfern keine „Wirtschaftstreuhänder“ im Sinne des WTBG. Ihre Tätigkeit als Abschlussprüfer oder Bankprüfer entspricht jedoch vollständig der Tätigkeit der Wirtschaftsprüfer.

Sie unterliegen in dieser Tätigkeit derselben Verschwiegenheitspflicht gemäß § 275 UGB. Auch die spezifisch berufsrechtlichen Regelungen der Verschwiegenheitspflicht unterscheiden sich inhaltlich kaum (vgl. z.B. § 10 GenRevG einerseits und § 80 WTBG andererseits). Deshalb ist es sachlich nicht nachvollziehbar, dass in § 157 Abs. 1 Z 2 StPO nur Wirtschaftstreuhänder, nicht aber auch Revisoren und Sparkassenprüfer genannt sind. Die aktuelle Reform bietet die Gelegenheit, diese unverständliche Ungleichbehandlung zu beseitigen.

§ 157 Abs. 1 Z 2 StPO sollte vor diesem Hintergrund wie folgt geändert werden:

„2. Verteidiger, Rechtsanwälte, Patentanwälte, Verfahrensanwälte in Untersuchungsausschüssen des Nationalrats, Notare, ~~und~~ Wirtschaftstreuhänder, Revisoren im Sinne des Genossenschaftsrevisionsgesetz 1997, BGBl. I Nr. 127/1997, und Organmitglieder und Mitarbeiter des Prüfungsverbandes im Sinne des Sparkassengesetzes, BGBl. Nr. 64/1979, über das, was ihnen in dieser Eigenschaft bekannt geworden ist,“

ad § 514:

Anzumerken ist, dass die Frist zur Implementierung mit 1.6.2018 deutlich zu knapp bemessen ist. Hier sind frühestens zum 1.4.2019 die erforderlichen umfangreichen Implementierungsmaßnahmen realisierbar.

ad Änderungen des Telekommunikationsgesetzes 2003

Angemerkt wird, dass die Durchlaufstelle, die grundsätzlich in der Verordnung der Bundesministerin für Verkehr, Innovation und Technologie betreffend die Datensicherheit (Datensicherheitsverordnung TKG-DSVO) geregelt ist, auf § 94 Abs. 4 TKG und auf § 102c TKG basiert. Die Bestimmungen des § 102c sollen nun gestrichen werden. Es wäre allerdings sicherzustellen, dass dann § 94 Abs. 4 TKG als Grundlage ausreicht. Die Telekommunikationsanbieter brauchen und wollen auch weiter die Durchlaufstelle, um Beauskunftungen auch zur Anlassdatenspeicherung weiterhin durchführen zu können.

Wir bitten um Berücksichtigung unserer Anliegen.

Mit freundlichen Grüßen

KommR Dipl.-Ing. Dr. Richard Schenz
Vizepräsident

Mag. Anna Maria Hochhauser
Generalsekretärin