OESTERREICHISCHE COMPUTER GESELLSCHAFT ®
AUSTRIAN COMPUTER SOCIETY

An das
Bundesministerium für Inneres
Herrengasse 7
1010 Wien

per E-Mail:
bmi-III-1@bmi.gv.at
begutachtungsverfahren@parlament.gv.at

Wien, am 21. August 2017

Stellungnahme der OCG zum Ministerialentwurf eines Bundesgesetzes, mit dem das Sicherheitspolizeigesetz, das Bundesstraßen-Mautgesetz 2002, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden – 326/ME

Die OCG erlaubt sich zunächst, sich selbst vorzustellen:

Die **Österreichische Computer Gesellschaft (OCG)** ist ein gemeinnütziger Verein, der 1975 zur Förderung der Informatik und der Kommunikationstechnologie unter Berücksichtigung ihrer Wechselwirkungen mit Mensch und Gesellschaft gegründet wurde. Die OCG hat rund 1.400 Mitglieder und versteht sich als Plattform, um Gesellschaft, Wissenschaft und Wirtschaft im Sinne der Förderung der Informatik zu vernetzen. Um IT-Kompetenz zu fördern und zu zertifizieren, bietet die OCG verschiedene Produkte und Leistungen an, u.a. seit 1997 als nationale Zertifizierungsstelle den ECDL (den Europäischen Computerführerschein).

Neben dem IT-Ausbildungsschwerpunkt liegt ein großer Fokus im IT-Security- und im Datenschutz-Bereich: Die OCG betreibt eine akkreditierte Zertifizierungsstelle für die ISO/IEC 27001-Norm, dem Standard für die Zertifizierung von Informationssicherheits-Managementsystemen (ISMS). Der Verein bietet darüber hinaus in rund 25 Arbeitskreisen (wie dem Forum Privacy, dem Forum e|Government und den Arbeitskreisen IT-Security sowie Rechtsinformatik) **ExpertInnen aus Wissenschaft, Wirtschaft, Verwaltung und Zivilgesellschaft** die Möglichkeit zum Austausch von Forschungsergebnissen, Best Practices sowie zum kritischen Diskurs.

Die OCG nimmt zum vorliegenden Entwurf wie folgt Stellung:

Zunächst ist anzumerken, dass bereits der **Zeitpunkt der Begutachtung** eines derart sensiblen Entwurfs im Hochsommer höchst bedenklich ist, da dadurch ein kollaboratives Verfassen und Abstimmen einer Stellungnahme erheblich erschwert wird, insbesondere innerhalb einer verhältnismäßig großen und gegliederten Organisation, deren Fachexpertinnen und Fachexperten sich ehrenamtlich beteiligen. Die OCG hat sich daher entschieden, eine verhältnismäßig kurze Stellungnahme abzugeben, die vor allem an technischen Aspekten anknüpft und leider nicht alle kritikwürdigen Punkte abdecken

kann. **Aus dem Umstand, dass die OCG nicht zu allen vorgeschlagenen Maßnahmen Stellung nimmt, ist daher nicht zu schließen, dass sie die übrigen Maßnahmen befürwortet.**

Grundsätzlich ist zu den vorliegenden Plänen der Bundesministerien für Justiz und für Inneres Folgendes zu sagen: Die OCG beobachtet mit Sorge eine **fortlaufende Ausweitung staatlicher Überwachungsbefugnisse**, deren Nutzen für die Kriminalitätsbekämpfung und Aufrechterhaltung der öffentlichen Sicherheit viel zu häufig fragwürdig bleibt. Eine Begründung der Erforderlichkeit und Eignung der Maßnahmen auf Basis einer **wissenschaftlichen Auseinandersetzung** mit der Sicherheitslage in Österreich und den zu erwartenden Auswirkungen der vorgeschlagenen Maßnahmen liegt nicht vor. Es bedarf daher dringend einer evidenzbasierten Sicherheitspolitik auf Basis einer **Überwachungsgesamtrechnung**[1] zur Evaluierung der Wirksamkeit und der Folgen bestehender und geplanter Überwachungsgesetze. Die OCG ist gerne bereit, sich insbesondere mit technischer Expertise an einem solchen Prozess zu beteiligen.

Zu Netzsperren (§ 17 Abs. 1a TKG-E):

Mit der vorgeschlagenen Bestimmung des § 17 Abs. 1a TKG-E soll es Anbietern von Internetzugangsdiensten gestattet werden, „Verkehrsmanagementmaßnahmen im Sinn von Art. 3 der Verordnung (EU) 2015/2120 zur Vermeidung von strafrechtlich relevanten Handlungen, wie etwa Datenbeschädigung durch Viren, Computerkriminalität, Verbreitung von pornografischen oder gewaltverherrlichenden Darstellungen im Sinn der Jugendschutzgesetze an Minderjährige oder strafrechtlich relevante Urheberrechtsverletzungen, anzubieten." Es handelt sich dabei um nichts weniger als Eingriffe aufseiten der Zugangsprovider, um zu diskriminieren, welche Daten von und zu ihren Kunden durchgeleitet werden und welche nicht, und somit um **Eingriffe in die Netzneutralität**.

Diese Regelung zu Netzsperren kam **völlig überraschend** in den Entwurf zur Änderung des TKG und war zuvor nicht von der Bundesregierung angekündigt worden, sodass bisher so gut **wie keine öffentliche Diskussion** dazu stattfinden konnte. Auch die Erläuterungen lassen jede sachliche Begründung für die Einführung dieser Maßnahme vermissen. Dabei ist der gesellschaftliche Nutzen von Netzsperren generell dringend zu hinterfragen, da das Sperren des Zugangs am grundsätzlichen Vorhandensein bedenklicher Inhalte nichts ändert.

Die OCG vertritt die Auffassung, dass die Bekämpfung strafrechtlich relevanter Handlungen eine staatliche Aufgabe ist. Sie lehnt daher eine Regelung ab, die es Privaten bloß freistellt, Maßnahmen zur Vermeidung von strafrechtlich relevanten Handlungen zu treffen, aber zugleich eine entsprechende Verpflichtung nicht für nötig erachtet. Durch diese **Auslagerung einer staatlichen Aufgabe an Private** ergibt sich auch ein erhebliches Rechtsschutzproblem im Fall von ungerechtfertigterweise erfolgten Sperren, zu denen es in der Praxis unweigerlich kommen würde.

Zudem erscheint die Regelung **mit dem Unionsrecht nicht vereinbar**. Art. 3 Abs. 3 lit. a der Verordnung (EU) 2015/2120 gestattet es zwar, Verkehrsmanagementmaßnahmen zu treffen, um „mit dem Unionsrecht im Einklang stehenden nationalen Rechtsvorschriften" zu entsprechen, dies trifft aber auf den

[1] Wie das deutsche Bundesverfassungsgericht (BVerfG) ausgesprochen hat (BvR 256/08 u.a. vom 2.3.2010, Rz. 218), kann eine staatliche Überwachungsmaßnahme bzw. deren Verhältnismäßigkeit nur in Zusammenschau mit anderen, bereits bestehenden Befugnissen beurteilt werden. Für eine solche Zusammenschau und Gesamtevaluierung hat sich der Begriff Überwachungsgesamtrechnung etabliert.

Vorschlag schon allein deshalb nicht zu, weil er keine Verpflichtung zu Verkehrsmanagementmaßnahmen vorsieht, sondern diese bloß gestattet. Die vorgeschlagenen Maßnahmen dienen auch nicht bloß der Wahrung der „Integrität und Sicherheit des Netzes“ (lit. b leg. cit.).

Die Bestimmung ist überdies völlig offen gestaltet, unter anderem durch die Formulierung „wie etwa“, und eröffnet den Anbietern daher **unüberschaubare Möglichkeiten, in die Netzneutralität einzugreifen** und solche Eingriffe auch in der Produktgestaltung kommerziell zu verwerten. Auch bleibt **offen, wie die Maßnahmen technisch umgesetzt werden**. Aus technischer Sicht ist dazu anzumerken, dass DNS-Sperren besonders leicht umgangen werden können und IP-Sperren einerseits ebenfalls umgangen werden können und andererseits auch Kollateralschäden verursachen können, indem sie auch Inhalte unbeteiligter Dritter treffen können, die unter derselben IP-Adresse abrufbar sind.

Wie dargelegt, handelt es sich bei dieser Maßnahme um nichts weniger als **einen Freibrief für Zugangsprovider zur Zensur der durchgeleiteten Inhalte**. Die OCG lehnt eine solche – wie gezeigt wohl auch unionsrechtswidrige – Maßnahme daher ab, schon allein deshalb, weil offenbar auch von den Urhebern des Entwurfs kein Bedarf gesehen wird, eine solche Zensur verpflichtend vorzusehen. Unabhängig davon sieht auch die OCG keinen Bedarf zu einer solchen Verpflichtung.

Zur Identifizierungspflicht beim Kauf von SIM-Karten (§ 97 Abs. 1a TKG-E):

Die OCG spricht sich gegen die Einführung einer Identifizierungspflicht beim Kauf von SIM-Karten aus. Es handelt sich dabei um eine weitere Maßnahme, die **mit fraglichem Nutzen die Freiheit aller einschränkt**. Insbesondere für Personen, die unter hohem persönlichen Risiko Missstände in ihrem Umfeld aufzeigen, sowie für den investigativen Journalismus ist die Möglichkeit zur anonymen Kommunikation mittels anonymer SIM-Karten essenziell, auch weil dafür keinerlei technische Kenntnisse erforderlich sind.

Dem steht gegenüber, dass die vorgeschlagene **Maßnahme voraussichtlich nicht wirksam** sein wird. Alleine in Österreich existieren derzeit Millionen von anonymen SIM-Karten. Da eine nachträgliche Identifizierung von deren Inhabern nicht vorgesehen ist, wird die Maßnahme höchstens zu einem lebhaften Sekundärmarkt dieser unregistrierten SIM-Karten führen. Kriminelle können so leicht an diese SIM-Karten herankommen, sofern sie sich nicht ohnehin bereits in den letzten Wochen und Monaten mit solchen eingedeckt haben. Ebenso stellen andere **Ausweichmöglichkeiten für Kriminelle** die Wirksamkeit in Frage, und die Wirksamkeit einer solchen Maßnahme zur Verbrechensaufklärung ist auch grundsätzlich nicht belegt.

Es ist auch auf die nicht unwesentliche **Belastung für die Mobilfunkanbieter** durch diese Maßnahme hinzuweisen. Diese trifft kleinere Anbieter ohne entsprechende Verkaufsinfrastruktur besonders hart und somit auch solche, die derzeit für viel Wettbewerb im Mobilfunkmarkt und folglich für günstige Preise sorgen. Die vorgeschlagene Maßnahme wirkt aus diesem Grund auch **wettbewerbsverzerrend**.

Somit bleiben in der Beurteilung dieser Maßnahme nur negative Folgen, währen die positiven, wie dargelegt, äußerst fraglich sind und wohl ausbleiben werden. Die Identifizierungspflicht beim Kauf von SIM-Karten ist daher abzulehnen.

Zu Quick Freeze (§ 99 Abs. 1a bis 1f TKG-E):

Die in § 99 Abs. 1a bis 1f TKG-E vorgeschlagene Regelung ist in mehrfacher Hinsicht dringend verbesserungsbedürftig. Zunächst ist die **Unvollständigkeit der Regelung** zu kritisieren, denn § 99 Abs. 1a TKG-E stellt auf eine staatsanwaltschaftliche Anordnung „gemäß den Bestimmungen der StPO" ab, die StPO enthält jedoch keine Befugnis zur Ausstellung einer solchen Anordnung, weder nach geltender Rechtslage noch nach dem vorliegenden Entwurf. Folglich ist auch § 109 Abs. 4 Z 9 TKG-E zu kritisieren, denn diese Bestimmung scheint davon auszugehen, dass ein Verbot der Löschung normiert ist, tatsächlich ist in § 99 Abs. 1a TKG-E aber nur eine Ausnahme von der Löschungsverpflichtung vorgesehen. Somit sanktioniert § 109 Abs. 4 Z 9 TKG-E ein Verhalten, das nicht gegen ein Gebot oder Verbot verstößt.

Bei Quick Freeze handelt es sich um eine (eingeschränkte) Form der Vorratsdatenspeicherung und somit um einen **schwerwiegenden Eingriff in die in Art. 7 und Art. 8 GRC verankerten Grundrechte**.[2] Ein solcher Eingriff ist **nur zur Bekämpfung schwerer Straftaten gerechtfertigt**[3] und auf das absolut Notwendigste zu beschränken.[4]

Aus dem Verweis auf § 135 Abs. 2 Z 2 bis 4 StPO ergibt sich, dass eine Anordnung zur Vorratsdatenspeicherung bereits zur Ermittlung, Feststellung und Verfolgung von Straftaten, die mit einer Freiheitsstrafe von mehr als einem Jahr bedroht sind, zulässig ist. Es existiert zwar keine Definition des Begriffs „schwere Straftaten", aber diese Schwelle erscheint jedenfalls zu niedrig, um ausschließlich Straftaten zu erfassen, die in Relation zu anderen Straftaten als „schwer" einzustufen sind. Die vorgeschlagene Regelung genügt daher nicht den Anforderungen der zitierten EuGH-Judikatur.

Ebenso genügt diese Regelung nicht den Anforderungen des EuGH hinsichtlich der **Beschränkung auf das absolut Notwendigste**. Die – derzeit bzw. im Entwurf nicht geregelte – Befugnis zur Ausstellung einer staatsanwaltschaftlichen Anordnung muss objektive Kriterien enthalten, aus denen sich ergibt, dass der **Umfang solcher Anordnungen und insbesondere der betroffenen Personenkreise stets wirksam begrenzt** wird.[5] Ebenso ist zu bezweifeln, dass die **Höchstspeicherdauer** von zwölf Monaten einer Beschränkung auf das Notwendigste entspricht, hielt doch der österreichische Gesetzgeber in der ursprünglichen – wegen Grundrechtswidrigkeit wieder aufgehobenen – Fassung der Vorratsdatenspeicherung eine Speicherdauer von sechs Monaten für ausreichend.

Schließlich ist vor allem das **Fehlen einer Pflicht zu kritisieren, von der Speicherung betroffene Personen im Nachhinein darüber zu informieren**, dass sie von dieser Maßnahme betroffen waren, entweder nach Ende des Verfahrens oder sobald sich herausstellt, dass die Speicherung nicht legitim oder nicht zweckdienlich war, insbesondere weil gerichtlich entschieden wurde, die Bewilligung zur Auskunft über die gespeicherten Daten nicht zu erteilen. Eine solche Pflicht erfüllt zwei Zwecke: Sie dient einerseits dem individuellen Datenschutz- und Rechtsschutzinteresse und andererseits führt sie im Vorhinein zu einer sorgsameren Prüfung bei der Ausstellung von Anordnungen und verhindert somit wirksam ein Ausufern der Maßnahme.

---

[2] EuGH 8.4.2014, C-293/12, *Digital Rights Ireland*, Rz. 37; EuGH 21.12.2016, C-203/15 *Tele2 Sverige*, Rz. 60.
[3] EuGH 8.4.2014, C-293/12, *Digital Rights Ireland*, Rz. 60; EuGH 21.12.2016, C-203/15 *Tele2 Sverige*, Rz. 102.
[4] EuGH 21.12.2016, C-203/15 *Tele2 Sverige*, Rz. 108.
[5] EuGH 21.12.2016, C-203/15 *Tele2 Sverige*, Rz. 108 ff.

OESTERREICHISCHE COMPUTER GESELLSCHAFT ®
AUSTRIAN COMPUTER SOCIETY

Für die Österreichische Computer Gesellschaft

Dipl.-Ing. Wilfried Seyruck
Präsident

Dr. Ronald Bieber
Generalsekretär

Dipl.-Ing. Dr. Walter Hötzendorfer
Co-Leiter OCG Forum Privacy