An den
Österreichischen Nationalrat,
Justizausschuss
Dr.-Karl-Renner-Ring 3
1017 Wien, Österreich

E-Mail: ausschussbegutachtung.justizausschuss@parlament.gv.at
begutachtung@parlament.gv.at

Wien, am 26. März 2018

BETREFF: ISPA-STELLUNGNAHME ZU DEM BUNDESGESETZ, MIT DEM DIE STRAFPROZEßORDNUNG 1975, DAS STAATSANWALTSCHAFTSGESETZ UND DAS TELEKOMMUNIKATIONSGESETZ 2003 GEÄNDERT WERDEN (STRAFPROZESSRECHTSÄNDERUNGSGESETZ 2018)

Sehr geehrte Damen und Herren,

zunächst möchte die ISPA festhalten, dass bereits zu den Ministerialentwürfen 325/ME XXV. GP und 326/ME XXV. GP, auf welchen die vorliegenden Regierungsvorlagen überwiegend beruhen, jeweils eine ausführliche Stellungnahme abgegeben wurde. Insofern die darin enthaltenen Kritikpunkte in der vorliegenden Stellungnahme nicht erneut ausgeführt werden, verbleiben diese dennoch aufrecht, sofern die jeweiligen Bestimmungen ident übernommen wurden.

Darüber hinaus erlaubt sich die ISPA im Zusammenhang mit der Konsultation des Justizausschusses wie folgt Stellung zu nehmen:

Hinsichtlich der vorgeschlagenen Anlassdatenspeicherung besteht nach Meinung der ISPA in einigen Bereichen noch Klärungs- bzw. Konkretisierungsbedarf und wird um eine Verlängerung der Umsetzungsfrist ersucht. Darüber hinaus möchten die Betreiber anmerken, dass sie sich jedenfalls ihrer Mitwirkungspflicht im Rahmen der Strafverfolgung bewusst sind, eine gesetzliche Verpflichtung zur ständigen Verfügbarkeit jedoch gerade für kleine Betreiber nicht umsetzbar ist. Außerdem erachtet die ISPA die Ausdehnung der Legaldefinition zur „Überwachung von Nachrichten“ als überschießend und lehnt weiterhin den Einsatz von Überwachungssoftware durch welchen die IT-Sicherheit gefährdet wird strikt ab.

ISPA – Internet Service Providers Austria
Währingerstrasse 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675

1) Hinsichtlich der Umsetzung der Anlassdatenspeicherung bestehen weiterhin Unklarheiten

Zunächst begrüßt die ISPA, dass die im Rahmen des letzten Begutachtungsverfahrens 325/ME XXV. GP vorgebrachte Kritik, wonach die korrespondierenden Ermittlungsbefugnisse der Staatsanwaltschaft fehlen, offenbar berücksichtigt wurden und nun entsprechende Regelungen in die Strafprozessordnung aufgenommen wurden. Jedoch bestehen weiterhin einige Unklarheiten welche im Folgenden aufgezeigt werden sollen:

- Fehlende Einschränkung auf Bekämpfung schwerer Kriminalität

Wie bereits in der ISPA Stellungnahme zum Ministerialentwurf 325/ME XXV. GP vorgebracht, ist eine Vorratsdatenspeicherung – und darum handelt sich bei einer „Aussetzung der Löschverpflichtung" – ausschließlich zur Bekämpfung schwerer Kriminalität zulässig[1].

Eine Definition von schwerer Kriminalität bzw. Straftat existiert weder in der Rechtsprechung des EuGHs – der dies den nationalen Gesetzen überlässt - noch in der österreichischen Rechtsordnung. Angesichts der Wortwahl des EuGHs muss es sich hierbei jedoch um solches Verhalten handeln, dessen Unwert sich gerade dadurch äußert, dass dieser gegenüber anderen Straftaten als „schwer" einzustufen ist. Somit muss es sich um jene Straftaten handeln, deren Strafrahmen am oberen Ende angesiedelt ist.

Naheliegend wäre daher zum einen ein Rückgriff auf die Unterscheidung zwischen Vergehen und Verbrechen im österreichischen Strafrecht, wonach ein Verbrechen gemäß § 17 Abs. 1 StGB eine vorsätzliche Handlung ist, die mit lebenslanger oder mit mehr als dreijähriger Freiheitsstrafe bedroht ist. Daneben besteht auch die Möglichkeit, die Bestimmungen zur Gerichtszuständigkeit im Strafprozess heranzuziehen und eine Straftat ab Zuständigkeit des Landesgerichts als Schöffengericht als schwer zu qualifizieren.

Grundsätzlich wäre auch der Verweis auf einen Strafrahmen ab drei Jahren Freiheitstrafe denkbar. Hierfür spräche, dass ausgenommen der „schweren Sachbeschädigung", sämtliche der als „schwer" qualifizierten Grunddelikte (etwa „Schwerer Diebstahl", „Schwerer Betrug", „schwere Nötigung", „schwere Körperverletzung"…) bei einem Strafrahmen von zumindest drei Jahren ansetzen.

Aufgrund des Verweises auf § 135 Abs. 2 Z 2 bis 4 StPO wäre nach der vorgesehenen Rechtslage eine entsprechende Anordnung zur Vorratsdatenspeicherung jedoch bereits zur Ermittlung, Feststellung und Verfolgung von Straftaten zulässig, deren Strafrahmen ein Jahr übersteigt, im Fall der Zustimmung des Betroffenen sogar bei Delikten mit einer Höchststrafe von sechs Monaten. Diese niedrig angesetzte Zulässigkeitsschranke kann in keinem Fall der Rechtsprechung des EuGHs entsprechen und muss daher in jedem Fall geändert werden.

[1] EuGH 16.5.2014, C-293/12, *Digital Rights Ireland* Rz 60, EuGH 21.12.2016, C 203/15 *Tele2 Sverige* Rz 102

- Unklarheiten bezüglich des Umfangs der zu speichernden Daten

Wie bereits in der ISPA Stellungnahme zum Ministerialentwurf 325/ME XXV. GP vorgebracht, ist es zweifelhaft ob der Umfang der zu speichernden Daten tatsächlich den Kriterien des EuGHs nach einer Beschränkung auf das Notwendigste entspricht[2]. Die ISPA begrüßt jedoch den Ansatz, dass ausschließlich Daten, welche vom Betreiber bereits aus Betriebszwecken gespeichert werden, länger aufbewahrt werden sollen, es jedoch zu keiner zusätzlichen Speicherverpflichtung kommt.

Im Zusammenhang mit den tatsächlich von einer entsprechenden Anordnung betroffenen Nutzerinnen und Nutzern sind speziell die notwendigen Identifizierungsmerkmale iSd § 138 Abs. 1 Z 1 StPO von Bedeutung. Aufgrund des Gesetzeswortlauts ist jedoch unklar, ob sich eine entsprechende Anordnung etwa auch auf eine oder mehrere Funkzellen, etwa im Rahmen einer Großveranstaltung, beziehen dürfte. Von der ISPA wird eine solche Auslegung strikt abgelehnt, da hierdurch unverhältnismäßig viele unbeteiligte Nutzerinnen und Nutzer betroffen wären und entspräche dies nicht dem Grundsatz wonach ein Konnex zwischen der betroffenen Person und der Straftat bestehen muss. Als zulässige Identifizierungskriterien kommen nach Ansicht der ISPA daher nur die von einer eindeutig identifizierbaren Person verwendeten Anschluss- oder Teilnehmerkennung, wie die verwendete Ruf-, IMSI- oder IMEI-Nummer des jeweiligen Kunden des Betreibers in Frage.

Darüber hinaus versteht die ISPA die aufzubewahrenden Daten jedenfalls im Sinne der Datenkategorien der EP020 Richtlinie[3], da auch nur für diese Daten eine verschlüsselte Übermittlung nach § 94 Abs. 4 TKG möglich ist.

- Zweckgebundenheit der aufzubewahrenden Daten

Einen Problempunkt stellt nach Ansicht der ISPA auch die Zweckgebundenheit der aufgrund des Anfangsverdachts aufbewahrten Daten dar. Es ist nach dem vorliegenden Entwurf unklar, ob etwa ein Gericht in einem anderen Strafverfahren als jenem welches sich auf den Anfangsverdacht gründet, auf die Daten zugreifen dürfte, speziell da gemäß dem Entwurf die gespeicherten Daten nicht als „Ergebnis“ iSd § 134 Z 5 gelten und daher vom Beweisverbot in § 140 nicht erfasst sind.

Im Sinne der Rechtsprechung des EuGHs wäre nach Ansicht der ISPA nur ein Zugriff in einem Strafverfahren welches sich auf den ursprünglichen Anfangsverdacht gründet zulässig, da die Daten auch nur aus diesem Grund länger als betriebsnotwendig gespeichert werden. Jedoch ist es für den Betreiber grundsätzlich nicht möglich überhaupt zu überprüfen, ob die Anfrage eines Gerichts oder einer Staatsanwaltschaft sich auf den gleichen Anfangsverdacht stützt, aufgrund dessen auch die erste Anordnung erfolgte da eine Betreiberausfertigung keine entsprechenden Angaben enthält.

Die ISPA ersucht daher um eine diesbezügliche Klarstellung durch den Gesetzgeber.

[2] EuGH 16.5.2014, C-293/12, *Digital Rights Ireland* Rz 51, EuGH 21.12.2016, C 203/15 *Tele2 Sverige* Rz 103
[3] Technische Richtlinie zur CSV-Datei für die Beantwortung von Auskunftsbegehren gemäß § 94 Abs. 4 TKG 2003 – EP020

- Maximal zulässige Speicherfrist

Da die Bestimmung nicht als Speicheranordnung für einen bestimmten Zeitraum konzipiert ist sondern nur eine bestehende Löschpflicht für einen bestimmten Zeitraum außer Kraft setzen soll, ist der tatsächlich maximal zulässige Zeitraum für eine Speicherung der Daten aus den Gesetzesmaterialien nicht klar ersichtlich. Aufgrund der Ausführungen des Gesetzgebers in den Erläuternden Bemerkungen[4] wonach „*die Speicherfrist individuell in der Anordnung zu bestimmen und mit höchstens zwölf Monaten begrenzt ist*" sowie „*bei der Anlassdatenspeicherung keine „Ergebnisse" iSd § 134 Z 5 StPO entstehen, weil nur bereits vorhandene Daten (für die angeordnete Frist, maximal jedoch für zwölf Monate) nicht gelöscht, nicht hingegen erst Daten neu gespeichert werden"* ergibt sich jedoch nach Ansicht der ISPA eine maximal zulässige Speicherfrist von zwölf Monaten sowie eine anschließende Verpflichtung die Daten umgehend zu löschen um keine Verwaltungsübertretung, welche ebenfalls im Gesetzesentwurf vorgesehen wird, zu begehen. Daten welche zum Zeitpunkt der Anordnung bereits zu Betriebszwecken gespeichert werden, müssen daher nach Ansicht der ISPA auch bei einer Anordnung die sich auf einen Zeitraum von zwölf Monaten bezieht, früher – nämlich jeweils zu dem Zeitpunkt an dem sie in Summe 12 Monate gespeichert sind – gelöscht werden. Damit wäre auch eher den Anforderungen des EuGHs entsprochen, wonach die Speicherdauer auf das absolut Notwendigste zu beschränken ist.

Sofern dies nicht der Interpretation des Gesetzgebers entspricht, ersucht die ISPA um entsprechende Richtig- bzw. Klarstellung im Gesetzesentwurf, um für die notwendige Rechtssicherheit auf Seiten der Betreiber zu sorgen.

- Verlängerung der Umsetzungsfrist auf ein Jahr ab Beschlussfassung

Der Gesetzgeber sieht vor, dass die Bestimmungen zur anlassbezogenen Datenspeicherung bereits mit 1. Juni 2018 in Kraft treten sollen. Dies würde eine Umsetzungsfrist nach Beschlussfassung im Parlament von weniger als zwei Monaten bedeuten. Eine solch kurz bemessene Umsetzungsfrist ist nicht nur äußerst ungewöhnlich, sondern für die notwendigen Umstellungen auf Seiten der Betreiber auch bei weitem nicht ausreichend.

Der Gesetzgeber geht offenbar missverständlich davon aus, dass zur Umsetzung der Bestimmung lediglich ein Absehen von der Löschung der Daten notwendig sei und dies mit einer einfachen Konfigurationsänderung möglich wäre. Dies ist jedoch nicht der Fall.

Vielmehr entsteht ein weitaus größerer Aufwand, da die Daten an einem neuen Ort gespeichert werden müssen und technische bzw. organisatorische Maßnahmen ergriffen werden müssen, um zu gewährleisten, dass die auf Vorrat gespeicherten Daten wirksam vor Missbrauchsmöglichkeiten sowie vor jedem unberechtigten Zugang geschützt sind. Dies ergibt sich sowohl aus Art 24 als auch Art 32 DSGVO und wäre eine Missachtung dieser Vorgaben mit drakonischen Verwaltungsstrafen sanktioniert. Darüber hinaus sind die Speichersysteme der Betreiber bislang nur darauf ausgelegt, sämtliche Daten für einen bestimmten Zeitraum zu speichern und nicht einzelne Daten zu filtern und diese länger aufzubewahren. Eine entsprechende Umsetzung würde

[4] Vgl EB S. 7

daher auch eine Änderung bzw. Erweiterung der Speichervorgänge miteinbeziehen. Auf diese Weise entsteht beim Betreiber jedoch der gleiche bzw. sogar ein höherer Aufwand, als jener der mit einer neuen Speicherung der Daten entstehen würde und ist daher auch eine entsprechende Umsetzungsfrist vorzusehen. So wurde den Betreibern etwa im Rahmen der Umsetzung der mittlerweile aufgehobenen Vorratsdatenspeicherung eine Frist von neun Monaten für die erforderlichen technischen Anpassungen gewährt, wobei dabei jedoch kein Aussondern einzelner Datensätze notwendig war.

Die ISPA fordert daher den Gesetzgeber dazu auf, eine entsprechende Umsetzungsfrist von zumindest einem Jahr ab Beschlussfassung im Nationalrat zu gewähren um eine reibungslose Umsetzung der Verpflichtungen zu gewährleisten.

- Fehlender Kostenersatz

Da die Betreiber auch in diesem Fall ausschließlich entsprechend ihrer Mitwirkungspflicht an einer staatlichen Aufgabe tätig werden würden und in keiner Weise selbst davon profitieren, ist nach Ansicht der ISPA ein vollständiger Kostenersatz vorzusehen, zumindest jedoch 80 % des personellen und finanziellen Aufwands gemäß geltender Rechtslage nach dem TKG sowie der Rechtsprechung des Verfassungsgerichtshofs[5].

Da der Aufwand auf Seiten des Betreibers bereits durch das Absehen von der Löschung bzw. durch den Eingriff in die Speichersysteme und den damit einhergehenden Dokumentierungspflichten entsteht, ist nach Ansicht der ISPA der laufende Kostenersatz bereits für die Umsetzung der entsprechenden Anordnung zur Anlassdatenspeicherung vorzusehen und nicht erst – wie dies bereits geltende Rechtslage ist – im Rahmen der anschließenden Beauskunftung. Denn auch das Aussondieren und Speichern der Daten geschieht ausschließlich in Mitwirkung an einer staatlichen Aufgabe und nicht im Eigeninteresse des Betreibers.

Aufgrund dessen wäre auch sowohl die Aufnahme einer Bestimmung zum Ersatz der laufenden Personal- und Sachaufwendungen in der Überwachungskostenverordnung (ÜKVO) sowie auch zum Ersatz der Investitionskosten in der Investitionskostenverordnung (IKVO) zwingend notwendig.

- Eingeschränkter Rechtsschutz

In § 147 Abs. 1 Z 5 soll die Anlassdatenspeicherung als einzige der in § 135 angeführten Ermittlungsmaßnahmen nicht der Kontrolle durch den Rechtsschutzbeauftragten unterworfen werden, ohne dass hierfür in den Erläuternden Bemerkungen eine Begründung angegeben wird. Anders als es in den Gesetzesmaterialen dargestellt wird, handelt es sich bei der Anlassdatenspeicherung jedoch sehr wohl um einen erheblichen Eingriff in die Grundrechte des Betroffenen, der weit über die betriebsnotwendige Speicherung von Daten hinausgeht.

Die Rolle des Rechtsschutzbeauftragten liegt zum einen in der Wahrnehmung spezieller Kontrollaufgaben sowie darin die Rechte des Betroffenen der über die Ermittlungsmaßnahme nicht informiert ist für diesen wahrzunehmen. Gerade im Fall der anlassbezogenen Datenspeicherung

[5] Verfassungsgerichtshof, 27.02.2003, G 37/02 ua, V 42/02

wären die Betroffenen in der Regel nicht über die von ihnen gespeicherten Daten informiert. Es ist nach Ansicht der ISPA absolut unverständlich weshalb hier der Rechtsschutz bewusst reduziert werden soll und eine solche Ermittlungsmaßnahme ohne Kontrolle durch den Rechtsschutzbeauftragten erfolgen soll.

- Verschlüsselte Übermittlung der Daten

Die ISPA begrüßt grundsätzlich den Ansatz im vorliegenden Entwurf, die verschlüsselte Übermittlung der Daten gemäß § 94 Abs. 4 TKG aufgrund deren besonderer Bedeutung und Vertraulichkeit forcieren zu wollen. Da nunmehr jedoch eine Verwaltungsstrafe für eine nicht-verschlüsselte Übermittlung vorgesehen werden soll, muss jedenfalls gewährleistet sein, dass auch kleine Betreiber sich ohne größeren Verwaltungsaufwand an die Durchlaufstelle anschließen können. Die ISPA fordert daher, dass gerade diese Unternehmen bei der Umsetzung entsprechend unterstützt werden und sichergestellt wird, dass sich diese an die Durchlaufstelle anschließen können noch bevor die Verwaltungsstrafbestimmung in Kraft tritt. Andernfalls würde sich eine solche Strafbestimmung ausnahmslos zu Lasten der kleinen und mittelgroßen Betreiber auswirken. Darüber hinaus müssen dem Bundesrechenzentrum als abwickelnder Stelle ebenfalls die notwendigen Ressourcen zur Verfügung gestellt werden.

2) Die Betreiber sind sich ihrer Mitwirkungspflicht im Rahmen der Strafverfolgung bewusst

In den Erläuternden Bemerkungen[6] zur Novellierung der Mitwirkungspflicht der Betreiber in § 138 Abs. 2 u. 3 StPO wird darauf hingewiesen, dass der Betreiber von einer Prüfung einer gerichtlichen oder staatsanwaltschaftlichen Anordnung Abstand nehmen solle, da ihm eine solche Überprüfung nicht zusteht.

Die ISPA möchte in diesem Zusammenhang zunächst betonen, dass die Betreiber sich ihrer Mitwirkungspflicht bei der Strafverfolgung vollends bewusst sind und auch bereit sind diese im Rahmen der gesetzlichen Verpflichtungen zu erfüllen. Die Betreiber werden jedoch weiterhin daran festhalten Anfragen zumindest auf ihre formellen Voraussetzungen zu prüfen, da diese in der Vergangenheit zum Teil nicht erfüllt waren (z.B. fehlende Unterschrift) oder der Inhalt von Betreiberausfertigungen oftmals mit dem Inhalt einer gerichtlichen Bewilligung nicht im Einklang stand. Grundsätzlich muss der Betreiber bei Zweifeln und Unklarheiten im Zusammenhang mit der Auskunftsanfrage daher jedenfalls die Möglichkeit zu Rückfragen haben.

Auch hinsichtlich der Formulierung, dass Betreiber „unverzüglich“ – also ohne schuldhaftes Verzögern - tätig werden müssen besteht Unklarheit. Nach Ansicht der ISPA kann diese Formulierung keine ständige Verfügbarkeit – insbesondere auch an Wochenenden – implizieren, da eine solche Verpflichtung nur von den größten Betreibern am Markt erfüllbar wäre und der Rest somit vom Markt gedrängt werden würde.

[6] Vgl EB S. 20 zu Z 24 und 25 (§ 138 Abs. 2 und 3 StPO)

In großen Unternehmen wurde bereits zur besseren Erreichbarkeit jeweils eine Ansprechperson (Single Point of Contact – SPOC) eingerichtet, welche auch an Wochenenden entsprechende Anfragen bei Gefahr im Verzug behandelt. Speziell für kleine und mittelgroße Betreiber ist dies jedoch bereits aufgrund des mangelnden Personals nicht umsetzbar. Jedoch sind auch diese bemüht einer Ermittlungsanordnung ohne Verzögern nachzukommen.

Ferner begrüßt die ISPA, dass der Gesetzgeber ausdrücklich anführt, dass die neue Ermittlungsmaßnahme der Überwachung verschlüsselter Nachrichten nach § 135a StPO jedenfalls keine Mitwirkung der Betreiber vorsieht und spricht sich klar gegen jegliche anderwärtige Novellierung oder Auslegung in der Zukunft aus.

3) Die geänderte Definition der „Überwachung von Nachrichten“ ist überschießend

Gemäß dem Entwurf soll die Definition der „Überwachung von Nachrichten“ in § 134 Z 3 StPO geändert und eine eigenständige und neutrale Definition, losgelöst von dem Nachrichtenbegriff im Telekommunikationsgesetz (§ 90 Abs. 3 Z 7 TKG) geschaffen werden. Hiervon sollen nun nicht nur menschliche Gedankeninhalte, sondern auch Kommunikation „*im technischen Sinn*“ und damit grundsätzlich jegliche über ein Kommunikationsnetz oder einen Dienst der Informationsgesellschaft gesendete Information erfasst werden, die von einer natürlichen Person gesendet, übermittelt oder empfangen wird, darunter etwa auch Online-Bestellvorgänge, Webseite-Aufrufe etc.

Der Argumentation, dass dabei nur zu einem kleinen Teil höchstvertrauliche Kommunikationsdaten erfasst werden würden kann nach Ansicht der ISPA nicht gefolgt werden, da dies wohl im Einzelfall zu evaluieren sein wird und gerade die Kombination vieler unterschiedlicher Daten oft sehr sensible Rückschlüsse zulässt. Zwar erscheint es plausibel, dass der Gesetzgeber viel Wert auf eine technologieneutrale und möglichst offene Formulierung legt um keine Rechtslücken zu schaffen welche die Effektivität von Ermittlungsmaßnahmen untergraben würden. Jedoch ist es gerade aufgrund der Eingriffsintensität solcher Maßnahmen notwendig, diese konkret zu umschreiben. Der Verweis auf die gesamte Kommunikation und Information *„im technischen Sinn“* geht dabei jedenfalls zu weit. Die rechtliche Begleitung der zunehmenden Digitalisierung stellt zweifelsfrei eine große legistische Herausforderung dar, speziell da die technologische Entwicklung ständig und rasch voranschreitet. Es ist jedoch unumgänglich klare und präzise Regelungen zu finden, um Streueffekte und Einschnitte in das Leben von Nutzerinnen und Nutzern sowie in das wirtschaftliche Fortkommen von Unternehmen gering zu halten. Diese Notwendigkeit kann nicht durch einfache, generelle Bestimmungen ausgesessen werden.

Die derzeit in den Erläuterungen vorgesehene Interpretation kommt einer Internet-Inhaltsüberwachung gleich, welche von Seiten der ISPA als klar unverhältnismäßig abgelehnt wird. Speziell der Umstand, dass auch unverschlüsselte Übertragungsvorgänge in eine Cloud erfasst werden sollen, geht weit über die bisherige Definition hinaus. Viele Geräte führen ständig back-ups in eine Cloud durch, dies hätte zur Folge, dass durch die Überwachung der Übertragungsvorgänge auch quasi alle Daten auf dem Gerät erfasst wären. Das wiederum entspricht einer „Online-

Durchsuchung“, also dem Zugriff auf privat abgespeicherte Daten, wie sie bereits wiederholt als verfassungswidrig eingestuft wurde.

Auch der Umstand, dass bereits das Abspeichern von E-Mail Entwürfen über ein Webmail-Programm erfasst wird ist höchst bedenklich. Der Natur der Sache entsprechend handelt es sich bei Entwürfen gerade noch um keine Kommunikation, sondern um privat gespeicherte Daten welche bewusst mit niemandem geteilt werden, dies gilt im Übrigen auch für die back-up Vorgänge in einer Cloud. Ebenso erscheint es gleichheitswidrig weswegen der Zugriff auf Daten welche lokal auf einem Computersystem gespeichert sind, dazu zählen auch Entwürfe in E-Mail Desktop-Anwendungen, ein unverhältnismäßiger Eingriff in die Grundrechte wäre, während die gleichen Daten, lediglich da sie über ein Kommunikationsnetz iSv § 3 Z 11 TKG übermittelt und auf einem Server gespeichert werden, durch die Überwachungsmaßnahme erfasst sein sollen.

Die ISPA begrüßt jedoch, dass entgegen dem Ministerialentwurf 325/ME XXV. GP nunmehr reine M2M-Kommunikation ausdrücklich ausgenommen wurde und jedenfalls die Beteiligung einer natürlichen Person vorgesehen wird, da andernfalls dies jedenfalls über den Zweck der Bestimmung, die Überwachung menschlichen Verhaltens im weitesten Sinne, hinaus gehen würde.

Die ISPA spricht sich daher grundsätzlich für eine Beibehaltung der derzeitigen Definition von „Nachrichten“ bzw. der „Überwachung von Nachrichten“ aus, speziell auch angesichts der Rechtssicherheit welche durch eine einheitliche Definition des Begriffs „Nachrichten“ im Telekommunikationsgesetz und der StPO gegeben wäre.

4) Der Einsatz von Überwachungssoftware durch welche die IT-Sicherheit gefährdet wird ist weiterhin abzulehnen

Die ISPA begrüßt zunächst, dass die Zulässigkeitsvoraussetzungen für den Einsatz von Software zur Überwachung verschlüsselter Kommunikation erhöht und der Rechtsschutz in einigen Teilen verbessert wurde. Speziell die erweiterten Befugnisse des Rechtsschutzbeauftragten sind für die Wahrung der Rechte des Betroffenen essentiell.

Leider wird der Anwendungsbereich der Ermittlungsmaßnahme jedoch in § 135a Abs. 1 Z 3 lit b weiterhin sehr breit gehalten indem vorgesehen wird, dass eine entsprechende Software auch auf die Endgeräte von Personen mit denen der Verdächtige potentiell in Kontakt treten könnte, installiert werden darf. Hiermit verbunden besteht ein evidentes Risiko, dass zahlreiche Unbeteiligte von einer solchen Ermittlungsmaßnahme betroffen sein könnten, ohne dass ausreichend Schutz für deren Daten gewährleistet wird. Damit würde die Maßnahme weiterhin weit über die Überwachung konkret Verdächtiger hinausgehen.

Weiters muss die ISPA ihre grundsätzlichen Bedenken hinsichtlich der konkreten technischen Ausgestaltung der Ermittlungsmaßnahme, die bereits sowohl in unserer Stellungnahme zum Ministerialentwurf 325/ME XXV. GP als auch in einem offenen Brief an die Abgeordneten des Nationalrats dargelegt wurden, weiterhin aufrechterhalten.

Der vorliegende Gesetzesentwurf ist mittlerweile der dritte Versuch innerhalb von zwei Jahren, eine entsprechende Ermittlungsmaßnahme in Österreich umzusetzen. Bislang wurde diese jedoch auch aufgrund zahlreicher technischer Bedenken von der breiten Öffentlichkeit abgelehnt. So ist es trotz mehrfacher Nachfrage in den vergangenen Jahren weiterhin unklar wie gewährleistet werden soll, dass eine entsprechende Software ausschließlich zur Überwachung der ausgehenden Kommunikation geeignet ist, nicht jedoch eine Durchsuchung der gespeicherten Daten erlaubt. Sowohl nach Ansicht der ISPA als auch zahlreicher Technik-Experten, ist dies rein technisch überhaupt nicht umsetzbar, obwohl dies von den Herstellern entsprechender Software oftmals so dargestellt wird. 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, die nicht vorab ausgeschlossen werden können.

Leider wird in der nun vorliegenden Regierungsvorlage erneut nicht auf diese weiterhin offenen Fragen eingegangen. Vielmehr wurde sowohl die Gesetzesbestimmung als auch die Erläuternden Bemerkungen zu § 135a beinahe unverändert aus dem Ministerialentwurf 325/ME XXV. GP übernommen, abgesehen von den erwähnten Änderungen im Rechtsschutz und den Zulässigkeitsvoraussetzungen. Aus Sicht der ISPA ist dies unverständlich, da in den vergangenen Jahren bereits ausreichend Zeit gewesen wäre, eine technisch unbedenkliche Lösung auszuarbeiten, die tatsächlich die rechtlichen Anforderungen erfüllt.

Da die entsprechende Software erst in den nächsten Jahren vom BMI angeschafft werden soll ist eine Überprüfung, ob diese tatsächlich über die notwendigen technischen Beschränkungen verfügt erst zu einem späteren Zeitpunkt möglich. Die ISPA lehnt das Vorgehen, wonach ein Gesetz beschlossen werden soll, dessen rechtmäßige technische Umsetzung in der Praxis erst im Anschluss während der Legisvakanz bis 2020 geprüft werden kann, dem Grunde nach ab, fordert jedoch jedenfalls eine ex-ante Überprüfung der Software durch unabhängige technische Experten, bevor diese für den Praxiseinsatz genehmigt wird. Dieser Ansatz wird auch durch den UN-Sonderbeauftragten für das Recht auf Privatsphäre unterstützt, der ebenfalls eine solche unabhängige Überprüfung neuer Überwachungsmaßnahmen zum Schutz der Grundrechte fordert[7].

Weiterhin sieht es die ISPA zudem äußerst kritisch, dass die Ferninstallation der Überwachungssoftware mithilfe einer „Backdoor“ bzw. eines „Exploits“ (also der Ausnutzung von Schwachstellen die bei der Entwicklung eines Programms nicht berücksichtigt wurden) vorgenommen werden soll.

Nutzerinnen und Nutzer vertrauen derzeit darauf, dass ihre Daten in den von ihnen genutzten Diensten sicher vor fremden Zugriffen sind. Dieses Vertrauen basiert auf der intensiven Arbeit, welche die IT-Branche über Jahre in die Etablierung von Sicherheitsstandards, wie einer effektiven Verschlüsselung der Daten, investiert hat. Um die praktische Umsetzung der Ermittlungsmaßnahme zu garantieren, muss eine Sicherheitslücke jedoch offen und damit geheim

[7] UN Human Rights Council A/HRC/37/62, Report of the Special Rapporteur on the right to privacy, Appendix 7, Working Draft Legal Instrument on Government-led Surveillance and Privacy, Art 7

gehalten werden, anstatt sie dem jeweiligen Unternehmen zu melden, da ansonsten das Aufspielen des Programms nicht mehr möglich wäre. Die Auswirkungen solch bewusst nicht geschlossener Backdoors haben sich in den vergangenen Jahren wiederholt bei zum Teil gravierenden Angriffen mittels Ransomware („WannaCry“ bzw. „Petrwrap“) gezeigt, die enormen Schaden für die Wirtschaft verursacht haben. Darüber hinaus fördert die staatliche Nutzung von Sicherheitsschwachstellen einen illegalen Markt für Sicherheitslücken und damit die Internetkriminalität. 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.

Für Rückfragen oder weitere Auskünfte stehen wir jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen,

ISPA - Internet Service Providers Austria

Dr. Maximilian Schubert

Generalsekretär

Die ISPA – Internet Service Providers Austria – ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von über 200 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.