An das
Bundesministerium für Justiz
Museumstraße 7,
A-1070 Wien

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

Wien, am 18. August 2017

BETREFF: ISPA-STELLUNGNAHME ZUM ENTWURF EINES BUNDESGESETZES MIT DEM DIE STRAFPROZESSORDNUNG 1975 GEÄNDERT WIRD (STRAFPROZESSRECHTSÄNDERUNGSGESETZ 2017)

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich im Zusammenhang mit der öffentlichen Konsultation des Bundesministeriums für Justiz zum Entwurf eines Bundesgesetzes mit dem die Strafprozessordnung geändert wird (Strafprozessrechtsänderungsgesetz 2017) wie folgt Stellung zu nehmen:

Die ISPA fordert, dass die Beauskunftung des PUK-Codes denselben Voraussetzungen wie auch die Nutzung der dadurch zugänglich gemachten Daten unterliegt. Ferner wird die nachträgliche gesetzliche Erlaubnis von IMSI-Catchern als bedenklich erachtet sowie sich gegen die Ausdehnung der Definition einer „Überwachung von Nachrichten“ ausgesprochen und weiterhin ein Kostenersatz für Betreiber die bei der Erfüllung staatlicher Aufgaben tätig werden gefordert. Darüber hinaus möchte die ISPA darauf aufmerksam machen, dass die Nutzung von Sicherheitslücken für Ermittlungsmaßnahmen die österreichischen Cybersicherheitsstandards schwächt und das Vertrauen in den österreichischen Wirtschaftsstandort untergräbt. Vielmehr regt die ISPA an, die vorgesehenen Investitionen für die Erforschung alternativer sowie die Verbesserung vorhandener Ermittlungsmaßnahmen einzusetzen. Gleichsam kann nach aktuellem technischen Stand eine verfassungswidrige „Online-Durchsuchung“ bei der Anwendung von Überwachungssoftware nicht ausgeschlossen werden und müssen nach Ansicht der ISPA die Zulässigkeitsvoraussetzungen jedenfalls der Eingriffsintensität entsprechen. Die Schaffung einer gesetzlichen Grundlage vor Prüfung der technischen Umsetzbarkeit wird abgelehnt und zudem angemerkt, dass die Anbieter von Telekommunikationsdiensten sich ihrer Mitwirkungspflicht im Rahmen der Strafverfolgung bewusst sind, sich jedoch weiterhin zur Überprüfung formaler Standards verpflichtet sehen.

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) Die Herausgabe des PUKs ist nicht mit der Auskunft über Stammdaten gleichzusetzen

Gemäß der Novellierung des § 76a Abs. 1 StPO sollen Anbieter von Kommunikationsdiensten in Hinkunft zur Herausgabe des PUK-Codes nach denselben Voraussetzungen wie zur Herausgabe von Stammdaten gemäß § 90 Abs. 7 TKG verpflichtet werden. Als Grund hierfür wird angeführt, es solle verhindert werden, dass Rechtsdurchsetzungsbehörden weiterhin gegenüber Betreibern die Verdachtslage gegen den Besitzer des PUK-Codes offenlegen müssen, wie dies derzeit im Rahmen der Sicherstellung des PUK-Codes nach § 110 StPO der Fall ist.

In diesem Zusammenhang ist darauf hinzuweisen, dass es sich bei Stammdaten um die notwendigen Informationen im Zusammenhang mit der Begründung, Abwicklung, Änderung oder Beendigung des Vertragsverhältnisses handelt (Vertragsdaten), diese sind taxativ in § 90 Abs. 7 TKG aufgezählt. Der PUK-Code hingegen stellt kein Stammdatum im herkömmlichen Sinn dar, sondern es handelt sich um einen Zugangscode durch welchen detaillierte Informationen, wie etwa alte SMS die auf der SIM-Karte gespeichert sind, eingesehen werden können. Speziell da im Zusammenhang mit personenbezogenen Daten stets der Kontext bzw. die mithilfe dieser Daten eruierbaren Informationen über eine Person beachtet werden müssen, ist der PUK-Code folglich in keiner Weise mit herkömmlichen Stammdaten, wie etwa Name, Adresse oder Teilnehmernummer der Nutzerin bzw. des Nutzers vergleichbar.

Dieser Ansicht folgte auch bereits das deutsche Bundesverfassungsgericht, welches eine Bestimmung im deutschen Telekommunikationsgesetz, worin eine generelle Auskunftspflicht hinsichtlich Zugangssicherungscodes (Passwörter, PIN, PUK) an Strafverfolgungs- und Sicherheitsbehörden im Rahmen der Strafverfolgung geregelt war, als verfassungswidrig aufgehoben hat.[1] In der Entscheidung wurde unter anderem darauf hingewiesen, dass im Zusammenhang mit der Beauskunftung von Zugangssicherungscodes stets auch der anschließende Zugriff auf dadurch ermittelbare Daten zu beachten ist. Ein Auskunftsersuchen bezüglich eines PUK-Codes ist demnach nur dann gerechtfertigt, wenn auch die Voraussetzungen für dessen Nutzung - etwa eine gerichtliche Bewilligung - gegeben sind. Die Auskunftserteilung über solche Zugangssicherungen müsse daher an diejenigen Voraussetzungen gebunden werden, die auch für einen Zugriff auf die dadurch zugänglich gemachten Daten zu erfüllen sind.

Es ist daher unverständlich weshalb eine inhaltsgleiche Bestimmung im österreichischen Recht verfassungskonform sein sollte. Die in den Erläuterungen angeführten Begründung, es müsse nach den Regeln der Stammdaten-Beauskunftung erfolgen lediglich da keine Verkehrsdaten verarbeitet werden, ist nicht schlüssig und daher abzulehnen.

Sofern daher eine eigenständige Bestimmung zur Beauskunftung des PUK-Codes aufgenommen werden soll, so muss diese jenen Voraussetzungen unterliegen, welchen auch die Nutzung der Daten unterliegt. Dabei wäre es ausreichend nicht auf den eingriffsintensivsten Nutzungszweck, sondern auf den in der Anfragesituation konkret angestrebten Nutzungszweck abzustellen, wobei es in diesem Fall zu keiner darüberhinausgehenden Nutzung kommen darf.

[1] BVerfG, 24.01.2012, 1 BvR 1299/05, Rz. 184 f

2) Die nachträgliche gesetzliche Erlaubnis von IMSI-Catchern ist bedenklich

Durch § 134 Z 2a StPO soll eine eigenständige Rechtsgrundlage für die Lokalisierung einer technischen Einrichtung durch Einsatz technischer Mittel zur Feststellung von geografischen Standorten und IMSI-Nummern geschaffen werden und damit den Einsatz von „IMSI-Catchern“ regeln. Bislang existierte eine entsprechende Rechtsgrundlage ausschließlich im Sicherheitspolizeigesetz[2], wonach die Lokalisierung von technischen Endeinrichtungen nur mithilfe von Betreibern und lediglich zur Abwehr einer gegenwärtigen Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen erlaubt war, nicht hingegen zur allgemeinen Strafverfolgung.

Daraus folgt, dass der Einsatz von IMSI-Catchern bislang ohne konkrete gesetzliche Grundlage erfolgte, ein Umstand der dem Gesetzgeber offenbar bewusst ist, wie aus den entsprechenden Erläuterungen hervorgeht. Darin wird ausgeführt, es handle sich hierbei um eine nachträgliche Anpassung der gesetzlichen Rahmenbedingung an eine bereits bestehende Praxis. Zwar wird in weiterer Folge richtigerweise auf die Rechtsprechung des OGH zur Überwachung von Funkzellen verwiesen[3], darin befasste sich dieser jedoch lediglich mit der Subsumtion der Standortkennung unter Verkehrsdaten nach § 92 Abs 3 Z 4 TKG und stellte fest, dass solche Daten von einer „Auskunft über Daten einer Nachrichtenübermittlung“ nach § 135 Abs. 2 StPO erfasst werden können. Dabei geht der OGH jedoch von einer Anordnung an einen Betreiber zur Beauskunftung solcher Daten aus und nicht von der Anwendung technischer Mittel wie dem IMSI-Catcher durch Ermittlungsbehörden ohne Mitwirkung des Betreibers. Der wesentliche Unterschied liegt darin, dass durch den Einsatz von IMSI-Catchern weitaus mehr Endgeräte erfasst werden, als durch die zielgerichtete Beauskunftungs-Anordnung an einen Betreiber.

Darüber hinaus möchte die ISPA anmerken, dass es sich bei IMSI-Catchern um keine Geräte handelt die ausschließlich zur Standorterfassung geeignet sind. Vielmehr ermöglichen solche Geräte, indem sie eine Funkzelle mimen, auch die Überwachung von Gesprächsinhalten über GSM-Mobilfunktechnologie. Der Einsatz von IMSI-Catchern ermöglicht somit weitaus gravierendere Eingriffe in das Recht auf Privatsphäre als eine Anordnung auf Beauskunftung von Standortdaten an Betreiber, da auch Kommunikationsinhaltsdaten erfasst werden können. Aufgrund der Eingriffsintensität dieser Ermittlungsmaßnahme sowie des bestehenden Missbrauchspotentials muss diese daher zumindest denselben Zulässigkeitsvoraussetzungen unterliegen, welche grundsätzlich an eine Kommunikationsinhaltsüberwachung geknüpft sind. Daher spricht sich die ISPA dafür aus, den Einsatz solcher technischeren Einrichtungen nicht wie vorgesehen analog zu § 135 Abs. 2 StPO (Auskunft über Daten einer Nachrichtenübermittlung) vorzusehen, sondern an Abs. 3 leg. cit. anzugleichen (Überwachung von Nachrichten). Hierdurch wäre auch weiterhin ein Einsatz zur Abwehr akuter Gefahren sowie im Fall von Entführungen möglich. Der Einsatz von IMSI-Catchern zur Bekämpfung einfacher Straftaten, wie im vorliegenden Entwurf vorgesehen, ist jedoch nicht gerechtfertigt.

Die ISPA sieht es zudem aus rechtsstaatlicher Sicht höchst bedenklich, dass Rechtsdurchsetzungsbehörden bislang in diesem Bereich offenbar ohne gesetzliche Grundlage

[2] § 53 Abs 3b SPG
[3] OGH, 5.3.2015, 12Os93/13i

agierten, speziell da es sich hierbei um eine grundrechtssensible Ermittlungsmaßnahme handelt und möchte sich entschieden gegen ein solches Vorgehen in der Zukunft aussprechen. Es muss darauf vertraut werden können, dass sich auch Rechtsdurchsetzungsbehörden an die geltende Rechtslage halten und sich nicht über bestehende Gesetze hinwegsetzen.

3) Die geänderte Definition der „Überwachung von Nachrichten" ist überschießend und birgt Risiken für das Internet der Dinge

Der Gesetzgeber sieht vor, die Definition der „Überwachung von Nachrichten" in § 134 Z 3 StPO zu ändern und eine eigenständige, technologieneutrale Definition, losgelöst von dem Nachrichtenbegriff im Telekommunikationsgesetz (§ 90 Abs. 3 Z 7 TKG) zu schaffen. Gemäß den Erläuterungen sollen davon nunmehr 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, darunter etwa auch Online-Bestellvorgänge, Webseite-Aufrufe etc.

Wiederum erscheint es äußerst zweifelhaft, dass der Gesetzgeber versucht das Argument zu konstruieren, dass all diese Daten bereits von der derzeitigen Formulierung erfasst seien. Sofern dies tatsächlich der Fall wäre, bestünde grundsätzlich keine Notwendigkeit für eine solch tiefgehende Novellierung des Begriffs. Zudem gab es bislang keine entsprechenden Anordnungen durch Behörden, obwohl diese sofern man den Ausführungen folgen kann, bereits rechtlich durchsetzbar gewesen wären.

Der Argumentation, dass dabei nur zu einem kleinen Teil höchstvertrauliche Kommunikationsdaten erfasst werden würden kann nach Ansicht der ISPA ebenfalls nicht gefolgt werden, da dies wohl einzelfallbezogen ist und gerade die Kombination vieler unterschiedlicher Daten oft sehr sensible Rückschlüsse zulässt, dies wurde auch bereits mehrfach in der Rechtsprechung des EuGHs bestätigt[4]. 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

[4] EuGH 16.5.2014, C-293/12, *Digital Rights Ireland*; EuGH 21.12.2016, C-203/15 *Tele2 Sverige*

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.

Darüber hinaus ist auch die Definition von „Computersystem“ in § 74 Abs 1 Z 8 StGB, auf welche sowohl in den Erläuterungen zu § 134 Z 3 als auch in § 134 Z 3a bzw. § 135a („Überwachung verschlüsselter Nachrichten“) Bezug genommen wird, ähnlich weitgehend. Diese umfasst sowohl einzelne als auch miteinander vernetzte oder auf andere Weise verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen. Hieraus folgt, dass prinzipiell auch die Kommunikation von Geräten im Internet der Dinge in Zukunft erfasst werden könnte. Der Gesetzgeber scheint dies nicht auszuschließen, indem er darauf verweist, dass eine Überwachung von Nachrichten nicht die Kommunikation einer endlichen Anzahl von Menschen voraussetzt, sondern auch bei einer unbestimmbaren Zahl von Menschen oder Computersystemen zulässig sei. Der Formulierung als Alternativvarianten folgend, wäre demnach auch die reine Kommunikation zwischen Computersystemen erfasst.

Darum möchte sich die ISPA dafür aussprechen, dass auch eine extensive Interpretation der „Überwachung von Nachrichten“ keine Ausdehnung auf reine Machine-to-Machine (M2M) Kommunikation zulassen würde, da dies jedenfalls über den Telos der Bestimmung, die Überwachung menschlichen Verhaltens im weitesten Sinne, hinaus gehen würde.

Gemäß aktueller Definition der RTR[5] handelt es sich bei M2M-Kommunikation um ein generisches Konzept, das den Informationsaustausch zwischen Maschinen (Automaten, Fahrzeuge, Messwerke...) über ein festes oder mobiles Netz und ohne Zutun bzw. mit limitierter Einflussnahme eines Menschen beschreibt. Eine begrenzte menschliche Beteiligung stehe somit der Einordnung als M2M-Kommunikation nicht entgegen.

Diese Einordnung entspricht im Wesentlichen der entsprechenden Definition der deutschen Bundesnetzagentur, welche im Rahmen einer Mitteilung zur „*Portierbarkeit von Rufnummern für Mobile Dienste im Falle von Machine-to-Machine (M2M)*“[6] ferner im Detail die Fälle ausführt, in welchen eine begrenzte menschliche Beteiligung einer Einordnung als M2M-Kommunikation nicht

[5] Präsentation der RTR im Rahmen des Regulierungsdialogs, 27.06.2016
[6] Mitteilung Nr. 770/2016, Amtsblatt Nr.11/2016 vom 15.06.2016

entgegensteht. Demnach steht weder Aktivierung/Bedienung/Steuerung/Überwachung einer M2M-Anwendung bzw. eines M2M-Gerätes über technische Einrichtungen wie z.B. Computer, Smartphones, Tablets etc. durch einen Menschen, noch die Aktivierung einer Anwendung, die eine Individualkommunikation im Sinne einer voreingestellten Punkt-zu-Punkt-Kommunikation ermöglicht (z.B. eCall in KFZ) einer Qualifikation als M2M-Kommunikation entgegen.

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. Darüber hinaus sollte nach Ansicht der ISPA jedoch in jedem Fall eine Klarstellung aufgenommen werden, dass reine M2M-Kommunikation nach den obigen Ausführungen nicht erfasst ist.

4) Der Aufwand der Betreiber zur Strafverfolgung muss ersetzt werden

Betreiber von Kommunikationsdiensten leisten bereits jetzt einen großen Beitrag zur Strafverfolgung. Im Rahmen ihrer gesetzlichen Verpflichtung unterstützen sie Strafverfolgungsbehörden sowohl durch die Beauskunftung von Kundendaten als auch durch die Mithilfe bei der Überwachung verdächtiger Personen. Keine anderen Unternehmen werden auf vergleichbare Weise zur Erfüllung ihrer Mitwirkungspflicht an einer staatlichen Aufgabe herangezogen.

Speziell die vorgesehene exzessive Ausweitung der Überwachung von Nachrichten iSd § 134 Z 3 würde bei den Betreibern einen enormen Aufwand verursachen, da entsprechende Schnittstellen zur Ausleitung der Daten aus dem Kommunikationsnetz geschaffen bzw. vorhandene Schnittstellen adaptiert werden müssten.

Mit der kostenlosen Zurverfügungstellung der technischen Einrichtungen zur Überwachung des Fernmeldeverkehrs durch Betreiber von Telekommunikationsdiensten befasste sich der Verfassungsgerichtshof (VfGH) bereits im Jahr 2003[7]. Darin wurde vom VfGH festgehalten, es sei in diesem Fall eine Verhältnismäßigkeitsprüfung notwendig, bei der *„eine Abwägung der Höhe der den Privaten erwachsenen Kosten einerseits und konkreter Kriterien, die eine besondere rechtliche und wirtschaftliche Beziehung begründen andererseits vorzunehmen* [ist]*."*

Ferner führt der VfGH aus, würde die Inpflichtnahme privater Betreiber von Telekommunikationsdiensten für die Überwachung des Fernmeldeverkehrs und die Bereitstellung entsprechender Einrichtungen zwar *„eine sachlich gerechtfertigte und daher verfassungsmäßige Mitwirkungspflicht Privater an einer staatlichen Aufgabe darstellen […] dennoch ist auch bei der Regelung der Kostentragung der Verhältnismäßigkeitsgrundsatz zu beachten."* Hierzu sei jedenfalls eine Belastungsgrenze festzusetzen.

Neben den Kosten für die technischen Schnittstellen fällt jedoch insbesondere auch ein hoher Personalaufwand an. Die zuständigen Juristinnen und Juristen bzw. Technikerinnen und Techniker

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

eines Unternehmens sind oft mehrere Stunden mit einzelnen Anfragen bzw. der Schaltung einer Überwachung beschäftigt, unter anderem durch die formelle Prüfung der Anordnung, den internen Austausch, die Protokollierung, den Kontakt mit der Behörde sowie die Durchführung der Maßnahme.

Die ISPA fordert daher – unter Aufrechterhaltung der grundsätzlichen Ablehnung der Ausweitung der Überwachung gemäß den obigen Erläuterungen – für jedweden zusätzlichen Aufwand, der Betreibern hierbei bei der Erfüllung einer staatlichen Aufgabe entsteht, einen vollständigen Kostenersatz vorzusehen, zumindest jedoch 80 % des personellen und finanziellen Aufwands. Eine Überwälzung der gesamten Kosten zur Einrichtung bzw. Adaptierung der Schnittstellen auf den Betreiber, welcher hier lediglich seine Mitwirkungspflicht an einer staatlichen Aufgabe erfüllt und in keinster Weise selbst profitiert, wäre jedenfalls klar unverhältnismäßig.

5) Die Nutzung von Sicherheitslücken untergräbt Cybersicherheitsstandards und das Vertrauen in den österreichischen Wirtschaftsstandort

Österreichische IKT-Unternehmen investieren jährliche hohe Summen um ihre Systeme und Netze vor nicht autorisierten Zugriffen zu schützen um damit Missbrauch von Daten ihrer Kundinnen und Kunden zu verhindern. Letztere danken dies bislang wiederum mit großem Vertrauen in österreichische Unternehmen.

Die nunmehr in § 135a StPO vorgesehene Ermittlungsbefugnis soll es jedoch erlauben, ohne Zustimmung des Inhabers ein Programm zur Überwachung verschlüsselter Nachrichten auf einem Computersystem zu installieren. Eine solche unbemerkte Installation einer Überwachungssoftware (etwa einer „Keylogger-Software“[8]) ist grundsätzlich auf drei Arten möglich: Zunächst besteht die Möglichkeit, dass ein Ermittler eine solche Software manuell auf das Computersystem aufspielt. Hierzu sieht die Gesetzesnovelle auch vor, dass zur Durchführung der Ermittlungsmaßnahme in durch das Hausrecht geschützte Räume eingedrungen und Behältnisse durchsucht werden dürfen. Trotzdem wird diese Möglichkeit in der Regel in der Praxis kaum Anwendung finden, da verdächtige Personen ihre Endgeräte, beispielsweise das Mobiltelefon, selten unbeaufsichtigt lassen.

Somit kommt in der Praxis grundsätzlich die Ferninstallation der Überwachungssoftware („remote“) mithilfe eines „Exploits“ (also der Ausnutzung von Schwachstellen die bei der Entwicklung eines Programms nicht berücksichtigt wurden) in Frage. Hierzu müssen die Ermittler einen Weg finden, das Sicherheitssystem des Geräts unbemerkt zu überwinden und anschließend die Überwachungssoftware auf das Gerät zu übermitteln und zu installieren. Einerseits besteht die Möglichkeit, eine solche Software unbemerkt an eine E-Mail anzuhängen, welche vom Nutzer anschließend auf sein Endgerät geladen wird und damit die Sicherung umgangen wird – sofern

[8] Eine Software, welche die Eingaben etwa in WhatsApp oder Telegram vor der Verschlüsselung ausliest und an die Sicherheitsbehörden übermittelt

nicht ein eventuelles Anti-Viren Programm die Datei als schädlich erkennen und die E-Mail daher abfangen würde.

Aufgrund der geringen Chance auf Erfolg auch bei dieser Maßnahme wäre in der Praxis jedoch die am häufigsten eingesetzte Möglichkeit, der Zugriff auf das Computersystem des Verdächtigen über sogenannte „backdoors“, also Sicherheitslücken im System die einen unbemerkten Zugriff erlauben. Grundsätzlich jedes Computersystem verfügt speziell in der Anfangszeit über solche Sicherheitslücken, jedoch arbeiten Unternehmen intensiv daran solche Sicherheitslücken zu suchen und über Updates zu schließen. Um die Effizienz der geplanten Ermittlungsmaßnahme sicherzustellen und eine praktische einfache Umsetzung für die Sicherheitsbehörden zu garantieren, muss eine solche „backdoor“ jedoch offen und damit geheim gehalten werden, da ansonsten das Aufspielen des Programms nicht mehr möglich wäre.

Dies führt jedoch zum einen dazu, dass Unternehmen nicht über bestehende Sicherheitslücken informiert werden und dadurch ihre Systeme bewusst angreifbar bleiben. Außerdem kann ein Unternehmen in Schwierigkeiten geraten, wenn es im Rahmen eines Sicherheitschecks die Sicherheitslücke selbst findet und schließt, oder sogar auf die Software oder ihre Installationsvektoren stößt und diese anschließend ordnungsgemäß an Anti-Virenhersteller sowie CERTs meldet wodurch womöglich die gesamte Ermittlung torpediert wäre. Handelt das Unternehmen jedoch entgegen seiner Sorgfalt und hält die Sicherheitslücken selbst bewusst offen, bestünde wiederum potentielle Haftung gegenüber Verbraucherinnen und Verbrauchern für den Schaden der daraus entsteht.

Darüber hinaus ist der Gesetzgeber bei der Ausforschung solcher Sicherheitslücken auf die Zusammenarbeit mit zweifelhaften Dienstleistern angewiesen, welche solche Sicherheitslücken ausforschen und für zum Teil horrende Summen am Markt anbieten.[9] Die gleichen Anbieter verkehren jedoch auch mit fremden Geheimdiensten und autokratischen Regimes, welche solche Sicherheitslücken zur Repression der eigenen Bevölkerung oder zur politischen Spionage missbrauchen können sowie auch mit Kriminellen die solche Sicherheitslücken beispielsweise für Cyber-Attacken ausnutzen. Darüber hinaus kann solche Software auch zur staatlich gelenkten Industriespionage missbraucht werden und österreichische Unternehmen dadurch in eine gefährliche Situation gebracht werden.

Eine sogenannte „NOBUS“ (Nobody but us) – Sicherheitslücke, also eine solche welche ausschließlich von Strafverfolgungsbehörden genutzt werden kann, ist auf Dauer in der Praxis unerreichbar, da niemals gesichert sein kann, dass diese nicht durch Dritte ebenfalls aufgedeckt wird, sei es durch Zufall oder auch durch Leak oder Zugriff auf staatliche Computersysteme. Der daraus potentiell resultierende Schaden wurde zuletzt durch die Cyberangriffe mittels Ransomware („WannaCry“ bzw. „Petrwrap“) deutlich, bei welchen eine dem amerikanischen Geheimdienst NSA zur Verfügung stehende Sicherheitslücke durch Kriminelle ausgenutzt wurde.

Die angeführten Risiken für die Cybersicherheit widersprechen deutlich den staatlichen Zielsetzungen etwa in Umsetzung der NIS-Richtlinie, das höchstmögliche Sicherheitsniveau von

[9] Das Unternehmen „Zerodium“ verkauft solche Exploits beispielsweise zur Preisen zwischen 5,000 und 1,5 Mio. Dollar pro exploit. Quelle: https://www.wired.com/2015/11/heres-a-spy-firms-price-list-for-secret-hacker-techniques/

Netz- und Informationssystemen zu garantieren.[10] Ein hohes Sicherheitsniveau ist mit der Forderung nach einer Abschwächung von Kryptografie bzw. dem Eingriff in Kommunikations- und Datenflüsse schlichtweg nicht vereinbar.

Aus diesen Gründen lehnt die ISPA die Aufnahme von § 135a StPO deutlich ab, da auch eine sicherheitspolizeiliche Ermittlungsmaßnahme nicht zu mehr Sicherheitsrisiken für die Internetnutzerinnen und -nutzer sowie die österreichischen Unternehmen führen darf.

6) Eine Investition in alternative Ermittlungsmethoden ist zweckdienlicher

Wie auch in den Erläuterungen bestätigt wird, verbraucht sowohl die Entwicklung als auch der Einsatz der geplanten Software immense Ressourcen. Auch das BMI gesteht in den Erläuterungen ein, selbst nach der vorgesehenen Regelung für jeden Fall eine individuelle Software zu benötigen, speziell da auch vorhandene Sicherheitslücken wieder geschlossen werden.[11] Zudem sind das Wissen und die Verfügbarkeit von Kryptografie bereits derart weit verbreitet, dass dieser Prozess nicht mehr umgekehrt werden kann. Entsprechende Überwachungssoftwares werden daher stets neuen Entwicklungen bzw. Kommunikationsdiensten hinterher sein.

Aufgrund dessen wäre es zur Steigerung der Erfolgsrate in Ermittlungen zweckdienlicher, zunächst die vorhandenen Ermittlungsmethoden effizienter auszugestalten. Speziell die Umsetzung der strafrechtlichen Amtshilfe (mutual legal assistance treaty - MLAT) birgt hohes Verbesserungspotential, um mit den bereits vorhandenen Ermittlungsmethoden bessere und vor allem schnellere Erfolge zu erzielen. Derzeit nehmen insbesondere die behördeninternen Prozesse oftmals eine enorme Zeitspanne in Anspruch weswegen beispielsweise Beauskunftungs-Anordnungen an Betreiber erst zu einem Zeitpunkt zugestellt werden, zu dem die angefragten Daten bereits gelöscht wurden. Solche Hindernisse im Rahmen der Ermittlungen wären einfach zu beseitigen, ohne dass neue Ermittlungsmaßnahmen von Nöten sind.

Zudem könnte der vorgesehene Arbeitsaufwand ebenso in die Entwicklung alternativer Ermittlungsmaßnahmen sowie in das Training von Ermittlern durch Sicherheitsexperten investiert werden. Eine Studie der Universität Harvard im Auftrag der EU-Kommission bietet sechs alternative Methoden, verschlüsselte Kommunikation ohne der diskutierten Überwachungssoftware zu erheben.[12] Dazu zählen unterschiedliche Methoden zur Erhebung oder Umgehung der Login-Daten oder dem Ausnutzen von Fehlern des Verdächtigen. Entsprechende Methoden haben bereits in der jüngsten Vergangenheit, beispielsweise bei der Bekämpfung von illegalen Kaufportalen im Darknet zu Erfolg geführt. Ferner erkennen die Studienautoren, dass es je nach Situation unterschiedlicher Ermittlungsmaßnahmen bedarf und die von Regierungen geforderte „*silver bullet*“ nicht existiert.

[10] Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL 2016/1148)
[11] Vgl Ausführungen SC Dr. Mathias Vogl
[12] Kerr, Schneier: Encryption Workarounds (2017)

Dem möchte sich die ISPA anschließen und darauf verweisen, dass es in jedem Fall sinnvoller erscheint, in individuell an die jeweilige Fallkonstellation angepasste Ermittlungsmethoden zu investieren, welche – wie in der Studie belegt – an unterschiedlichen Schwachstellen ansetzen können und zudem geringeres Risiko für unbeteiligte bzw. unschuldige Bürgerinnen und Bürger darstellen. Dies wäre auch angesichts des hohen Ressourcenaufwands in finanzieller Erwägung zweckdienlicher und darüber hinaus auch weitaus „technologieneutraler“, ein Ansatz der vom Gesetzgeber selbst wiederholt betont wird.

7) Eine „Online-Durchsuchung“ kann auch nach dem aktuellen Entwurf nicht ausgeschlossen werden

In den Erläuterungen wird mehrfach darauf hingewiesen, dass es sich bei der vorgesehenen Ermittlungsmaßnahme keinesfalls um eine „Online-Durchsuchung“ – also eine Durchsuchung aller gespeicherten Daten auf einem Computersystem - handle, die von Rechtsexperten wiederholt als unverhältnismäßig und verfassungswidrig eingestuft wurde. In diesem Zusammenhang wird ausgeführt, dass durch die Software ausschließlich die Kommunikation vor der Verschlüsselung erfasst werden soll und keine darüberhinausgehenden Daten durch die Maßnahme angegriffen werden.

Um jedoch Zugriff auf die Kommunikationsdaten vor der Verschlüsselung zu haben, muss die Software sich in den Übertragungsvorgang einschalten und den Datenverkehr nach Eingabe und vor der Verschlüsselung abfangen. Hierzu benötigt die Software umfangreiche Zugriffsrechte (Administratorenrechte) auf das Computersystem welche grundsätzlich auch zahlreiche weitere Funktionalitäten erlauben würden, die weit über das reine Ausleiten des Kommunikationsinhaltes hinausgehen. Solche Zugriffsrechte sind daneben auch notwendig, um vorhandene Anti-Virus Scanner zu identifizieren und nach Möglichkeit zu täuschen. Hierfür müssen zusätzlich Hilfsprogramme („rootkits“) auf das Endgerät aufgespielt werden, womit massive Eingriffe in das Betriebs- und Speichersystem einhergehen. Eine Programmierung der Software dahingehend, dass trotz dieser weitgehenden Zugriffsrechte nur Kommunikationsdaten ausgeleitet werden und nicht auf privat gespeicherte Daten auf den Endgeräten zugegriffen werden kann, ist technisch nicht umsetzbar. Bereits die Möglichkeit, dass über den geschaffenen Zugangskanal weitere Programme aufgespielt werden können, widerspricht der grundsätzlichen Annahme des Gesetzgebers, es könne eine Software entwickelt werden, die lediglich über die im Gesetz vorgesehenen Funktionen verfügt. Ferner ist aufgrund der umfangreichen Zugriffsrechte auch ein Eingriff in gespeicherte Dateien bzw. deren Veränderung möglich. Auch wenn hiervon kein Gebrauch gemacht wird, bereits der Umstand, dass dies während der Durchführung der Ermittlungsmaßnahme nicht ausgeschlossen werden kann schwächt die anschließende Beweisqualität der – auch im Rahmen anderer Ermittlungsmaßnahmen erhobenen - Daten massiv.

Die ISPA möchte daher an dieser Stelle den entsprechenden Ausführungen in den Erläuterungen deutlich widersprechen, welche die technische Umsetzbarkeit der rechtlichen Vorgaben ohne nähere Erklärung als gegeben ansehen. Davon zeugt auch die Tatsache, dass obwohl ähnliche Gesetze bereits in anderen Staaten verabschiedet wurden oder derzeit diskutiert werden, keine

solche Software, welche die angeführten Bedenken ausräumt, präsentiert werden konnte. Entsprechende Versprechen von Unternehmen die solche Softwares konzipieren haben sich bislang ausnahmslos als unwahr herausgestellt.

8) Die Zulässigkeitsvoraussetzungen müssen der Eingriffsintensität entsprechen

Aus den in den vorherigen Punkten detailliert beschriebenen Auswirkungen der vorgesehenen Ermittlungsmaßnahmen ergibt sich, dass es sich hierbei um einen intensiven Eingriff sowohl in das Grundrecht auf Datenschutz (Art. 8 EMRK, Art. 7 und 8 GRC) als auch in das Fernmeldegeheimnis (Art. 10a StGG) handelt. Der Rechtsprechung des Europäischen Gerichtshofs sowie des Verfassungsgerichts folgend, ist bei einer solchen Eingriffsintensität einer Ermittlungsmaßnahme, eine konkrete Auflistung der Zulässigkeitsvoraussetzungen notwendig, welche einen Eingriff nur in jenen Fällen erlaubt in welchen ein solcher zur Erreichung des Eingriffsziels, dem Schutz der nationalen Sicherheit, verhältnismäßig erscheint.

Es ist daher unverständlich, dass in den Erläuterungen betont wird, die Ermittlungsmaßnahme solle in Hinkunft an die gleichen Zulässigkeitsvoraussetzungen wie die bisherige Telekommunikationsüberwachung (TKÜ) nach § 135 Abs. 3 gebunden werden und der im Entwurf vorgesehene höhere Strafrahmen ausschließlich mit der vorrübergehenden Ressourcenintensität der Maßnahme und nicht mit den weitaus intensiveren Eingriffen begründet wird. Die Argumentation, die Überwachung verschlüsselter Nachrichten sei bereits nach der bisherigen Rechtslage zulässig weswegen es sich um die gleichen Zulässigkeitsvoraussetzungen wie in § 135 Abs. 3 StPO handeln müsse, ist nicht nachvollziehbar. Hierbei wird fälschlicherweise ausschließlich auf das Ergebnis der Ermittlungsmaßnahme und nicht auf die eingesetzten Mittel abgestellt.

Als eine der zusätzlichen Voraussetzungen wird zudem vorgesehen, dass die Software nach Beendigung der Ermittlungsmaßnahme funktionsunfähig ist oder ohne dauerhafte Schädigung des Computersystems und der in ihm gespeicherten Daten entfernt werden kann (Abs. 2 Z 1) sowie, dass es zu keiner Schädigung dritter Computersysteme kommt (Abs. 2 Z 2). Diese Formulierung lässt jedoch den Schluss zu, dass eine (dauerhafte) Schädigung des Computersystems oder der Daten zulässig wäre, sofern das Programm funktionsunfähig ist und damit nicht mehr entfernt werden müsste. Gerade aufgrund der Tatsache, dass ein vollständiges Entfernen remote nur sehr schwierig möglich ist, kommt gerade diese Alternative jedoch als wahrscheinlichste Praxisvariante in Frage. Entsprechende Folgeschäden, etwa wiederum durch eine mögliche nachträgliche Nutzung der Software als „Exploit“ durch Dritte, müssen nach Ansicht der ISPA ebenfalls von Vornhinein ausgeschlossen werden können, um eine solche Ermittlungsmaßnahme zuzulassen. Die Notwendigkeit, das Programm ohne weitere Schädigung des Computersystems anschließend zu entfernen wurde auch von den Mitgliedern der Expertengruppe erkannt.[13]

Die ISPA spricht sich daher – bei Beibehaltung der grundsätzlichen Ablehnung der Ermittlungsmaßnahme in der vorgesehenen Form – dafür aus, dass die

[13] Vgl. Ausführungen von Univ.-Prof. Dr Gerhard Dannecker

Zulässigkeitsvoraussetzungen hoch angesetzt werden und die Maßnahme tatsächlich nur zur Verfolgung schwerster Straftaten, insbesondere der Terrorismusbekämpfung zugelassen wird. Auch in Zukunft darf es keinesfalls zu einer Ausweitung dieser Maßnahme zur Anwendung in der allgemeinen Strafverfolgung kommen, da die Eingriffe in Abwägung mit jenen Straftaten für welche etwa eine Überwachung von Nachrichten nach bisherigen Rechtslage grundsätzlich zulässig wäre (Straftaten bei welchen der Strafrahmen 1 Jahr Freiheitstrafe übersteigt, z.B. Mehrfachehe oder wiederholte Verletzung der Unterhaltspflicht) jedenfalls unverhältnismäßig sind.

Darüber hinaus fordert die ISPA, dass in Abs. 2 Z 2 die erste Alternative (Funktionsunfähigkeit) gestrichen wird und die Ermittlungsmaßnahme ausschließlich zulässig ist wenn abgesichert werden kann, dass die Software nachträglich ohne dauerhafte Schädigung des Computersystems bzw. der darauf gespeicherten Daten entfernt werden kann. Sollte es dennoch zu einer Schädigung kommen so haftet der Bund hierfür im Rahmen der Amtshaftung.

Ferner führt speziell § 135 Abs. 1 lit. b zu einer unkontrollierbaren Ausweitung des Anwendungsbereichs indem es demnach bereits ausreichend ist, dass aufgrund bestimmter Tatsachen angenommen werden könnte, dass ein Verdächtiger möglicherweise mit einem Computersystem eine Verbindung herstellen würde. Diese äußerst unbestimmte Definition ließe die Infektion zahlreicher Endgeräte unbeteiligter Dritter zu, ohne dass ausreichend Schutz für deren Daten gewährleistet wird und geht damit weit über die Überwachung konkret Verdächtiger hinaus.

Davon betroffen wären speziell auch Journalistinnen und Journalisten welche investigativ im Milieu Terrorverdächtiger recherchieren. Da die Auslotung des Endgeräts eines Journalisten in der Regel einfacher wäre als jenes des Verdächtigen, ist damit zu befürchten, dass auf diesen bereits aufgrund der Möglichkeit, mit einem Verdächtigen in Kontakt zu treten eine Überwachungssoftware aufgespielt werden könnte. Speziell angesichts der Rolle freier Medien als „public watchdog“ über den Staat ist dies höchst kritisch zu werten, da auf den Endgeräten der Journalistinnen und Journalisten auch andere sensible Materialien gespeichert wären. Ein daraus resultierender „chilling effect“ auf die freie Arbeit der Presse sollte nach Ansicht der ISPA nach Möglichkeit verhindert werden.

Die ISPA spricht sich daher dafür aus, den Anwendungsfall in § 135 Abs. 1 lit. b gänzlich zu streichen, da angesichts der Eingriffsintensität lediglich der Zugriff auf das Endgerät des dringend Verdächtigen verhältnismäßig erscheint. Das Argument, hier wiederum lediglich eine Gleichstellung mit der bisherigen TKÜ herzustellen ist nicht zutreffend, da wie bereits ausgeführt, eine Gesamtbetrachtung der Auswirkungen, in diesem Fall speziell auch auf Dritte, vorzunehmen ist, um die Verhältnismäßigkeit des Eingriffs beurteilen zu können. Da die potentiellen negativen Folgen für Dritte um ein vielfaches gravierender sind als bei einer Ermittlungsmaßnahme nach § 135 Abs. 2. Z 3 lit. b ist von dieser Zulässigkeitsvoraussetzung abzusehen.

Bei Beibehaltung sollten jedoch jedenfalls spezielle Verdachtsmomente aufgenommen werden, welche einen Eingriff in Computersysteme Unbeteiligter hintanhalten. Hierzu zählt etwa eine wiederholt erfolgte Kontaktaufnahme in der jüngsten Vergangenheit oder ein enges familiäres Naheverhältnis. Zudem sollte am Ende der Bestimmung der Halbsatz *„[…] und eine solche*

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

Benützung oder Kontaktaufnahme unmittelbar bevorsteht“ angehängt werden. Hierdurch soll eine pro-forma Überwachung sämtlicher potentieller Kontaktpersonen unterbunden werden.

Zur Wahrung des besonderen Rechtschutzes ist im Entwurf vorgesehen, dass die Prüfung und Kontrolle der Ermittlungsmaßnahme gemäß § 147 Abs.1 Z 2a dem Rechtschutzbeauftragten (Rsb) des BMJ obliegt. Die ISPA steht der bisherigen Arbeit des Rsb etwa im Rahmen der Funkzellenüberwachung sehr positiv gegenüber und sieht durch hierdurch den Rechtschutz in dieser sensiblen Rechtsmaterie effizient gewährleistet. Zur Beurteilung des rechtmäßigen Einsatzes der geplanten Überwachungssoftware ist jedoch ein zum Teil hohes technisches Verständnis notwendig über welches der Rsb in der Regel nicht verfügt. Aufgrund dessen sieht der Gesetzesentwurf in § 147 Abs. 3a die Möglichkeit vor, dass der Rsb die Beiziehung eines Sachverständigen verlangen kann. Die ISPA ist jedoch der Ansicht, dass ein entsprechender technischer Sachverständiger nicht nur fakultativ sondern obligatorisch zur Beurteilung und Kontrolle der Ermittlungsmaßnahme beizuziehen ist, da eine effektive Kontrolle und Prüfung der Überwachungssoftware ohne diesen nicht möglich ist. Die ISPA regt daher an, sofern der Gesetzgeber nicht aufgrund der geäußerten Bedenken gänzlich von der Aufnahme der Gesetzesbestimmung absieht, die verpflichtende Beiziehung eines technischen Sachverständigen festzuschreiben.

9) Die Schaffung einer gesetzlichen Grundlage vor Prüfung der technischen Umsetzbarkeit wird abgelehnt

Die ISPA sieht es positiv, dass im Gesetzesentwurf auf die Vorbehalte aus den vergangenen Stellungnahmen eingegangen wird, und auch ein Expertenrat mit der Auffindung einer Lösung betraut wurde. Leider wurde jedoch nicht dem Vorschlag gefolgt, eine interdisziplinäre Arbeitsgruppe einzurichten, sondern setzte sich dieser Rat hauptsächlich aus Rechtsexpertinnen und Rechtsexperten zusammen, von einer effektiven Miteinbeziehung technischer Expertise wurde abgesehen.

Dies hatte zur Folge, dass der nunmehr vorliegende Gesetzesentwurf zwar die rechtlichen Rahmenbedingungen enthält, durch den Versuch es möglichst „technologieneutral“ zu formulieren werden jedoch die technischen Herausforderungen ausgeklammert und nun an das Bundeministerium für Inneres weitergeleitet, welches bis 2019 eine Lösung finden soll. Der Umstand einer Legisvakanz bis 2019 zeigt, dass auch dem Justizministerium bewusst ist, wie heikel dieses Thema ist und dass es aktuell noch keine technische Lösung gibt.

Aus diesem Grund wäre es jedoch naheliegender abzuwarten, ob es 2019 tatsächlich eine technische Lösung gibt welche die rechtlichen Voraussetzungen erfüllt um erst dann ein entsprechendes Gesetz zu beschließen. Hierzu sollte die Überwachungssoftware von unabhängigen technischen Experten evaluiert werden. Eine Anzeige an die Datenschutzbehörde wie sie im Entwurf vorgesehen ist, wäre jedenfalls bereits deshalb nicht ausreichend, da diese über keine technischen Experten verfügt. Im Rahmen dieser Evaluierung ist den Technikern der gesamte Quellcode der Software offenzulegen.

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

Der Beschluss eines Gesetzes auf „Vorrat“, noch vor einer technischen Lösung ist nach Ansicht der ISPA gefährlich und wird abgelehnt, da dies am Ende zu überhasteten, technisch unsauberen Lösungen führen kann.

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

In den Erläuterungen zur Novellierung der Mitwirkungspflicht der Betreiber im Rahmen der Strafverfolgung (§ 138 Abs. 2 StPO) durch welche klargestellt werden soll, dass die Mitwirkung *unverzüglich* zu erfolgen habe, verweist der Gesetzgeber auf „*nicht tolerierbare Verzögerungen bei der Aufklärung und Verfolgung von Strafverfahren, weil Anbieter und sonstige Diensteanbieter die Meinung vertreten haben, dass zu ihrer rechtlichen Absicherung vorab eine Prüfung der rechtlichen Voraussetzungen der Anordnung erforderlich sei.*“

Die ISPA möchte dieser Annahme dem Grunde nach widersprechen. Die Betreiber sind sich ihrer Mitwirkungspflicht bei der Strafverfolgung gänzlich bewusst und auch bereit diese im Rahmen der gesetzlichen Verpflichtungen zu erfüllen. Zwar ist es zutreffend, dass Rechtsabteilungen etwa an Wochenenden nicht umgehend zu erreichen sind, jedoch wurde aufgrund dessen in allen Unternehmen eine Ansprechperson (Single Point of Contact – SPOC) eingerichtet, welche auch an Wochenenden entsprechende Anfragen bei Gefahr im Verzug behandelt. Die ISPA möchte anmerken, dass die Verzögerungen in der Vergangenheit vielfach nicht der mangelnden Kooperationsbereitschaft der Betreiber, sondern Problemen bei der Übermittlung bzw. der Form der Anordnung (etwa an eine falsche Kontaktadresse trotz Angabe eines SPOC oder unvollständige Anordnungen) geschuldet waren. Die Betreiber werden weiterhin daran festhalten, Anfragen zumindest auf ihre formalen Voraussetzungen zu prüfen da in der Vergangenheit oftmals die formellen Voraussetzungen für eine gültige Anordnung nicht erfüllt waren (z.B. fehlende Unterschrift) und diese damit ungültig war.

Weiters lädt die ISPA die Vertreterinnen und Vertreter der Judikative und Exekutive zu einem offenen diesbezüglichen Gespräch ein, in dem konkrete Fälle besprochen und konstruktive Lösungsansätze erarbeitet werden können. Im Rahmen der strukturierten Aufarbeitung derselben in der Vergangenheit konnten oftmals konkrete Ansätze für Verbesserungen auf beiden Seiten gefunden werden.

Angesichts der zuletzt konstruktiven Gesprächsbasis zeigt die ISPA sich verwundert über die Art und Weise in der die Kritik an die Betreiber herangetragen wird. Die ISPA gibt zu bedenken, dass undifferenzierte Äußerungen bzw. Vorhaltungen die Zusammenarbeit belasten und somit im Lichte der guten Zusammenarbeit von Betreibern und Rechtsdurchsetzungsbehörden als kontraproduktiv anzusehen sind.

Die ISPA wiederholt daher ihre Gesprächsbereitschaft und ersucht die Vertreterinnen und Vertreter der Judikative und Exekutive ihren Teil zu einer produktiven Gesprächsatmosphäre beizutragen. Darüber hinaus verweist die ISPA auf die vom gegenseitigen Respekt getragene, hochgradig professionelle Zusammenarbeit mit der Abteilung IV/1/b des BMI, welche dort für die Übermittlung

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

von Anfragen über die Durchlaufstelle zuständig ist und diese zur allseitigen Zufriedenheit erledigt und damit nicht nur zu einer Steigerung der Qualität der Anfragen, sondern auch zu einer rascheren Beantwortung der Anfragen beigetragen hat.

Abschließend nimmt die ISPA zur Kenntnis, dass der Gesetzgeber dezidiert eine Einbeziehung der Betreiber im Rahmen der Überwachung verschlüsselter Nachrichten ausschließt und spricht sich klar gegen jegliche anderwärtige Novellierung oder Auslegung in der Zukunft aus.

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.