An das
Bundesministerium für Justiz
z.H. Mag. Christian Pilnacek
Museumstraße 7
1070 Wien

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

Wien, am 12. Mai 2016

**BETREFF: ISPA STELLUNGNAHME ZUM ENTWURF EINES BUNDESGESETZES, MIT DEM DIE STRAFPROZESSORDNUNG 1975 UND DAS STAATSANWALTSCHAFTSGESETZ GEÄNDERT WERDEN**

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich im Zusammenhang mit der öffentlichen Konsultation des Bundesministeriums für Justiz betreffend den Entwurf eines Bundesgesetzes, mit dem die Strafprozessordnung 1975 und das Staatsanwaltschaftsgesetz geändert werden, wie folgt Stellung zu nehmen:

Zusammengefasst merkt die ISPA an, dass die Optik einer Anlassgesetzgebung eine sachliche Diskussion erschwert und betont, dass die „Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden" (sog “Quellen-Telekommunikationsüberwachung“, kurz „Quellen-TKÜ“) de facto keinen praktischen Nutzen für die Strafverfolgung mit sich bringt. Aus Sicht der ISPA ist eine Trennung zwischen zulässiger „Online-Überwachung“ sowie einer unzulässigen „Online-Durchsuchung“ de facto nicht möglich. Aus Sicht der ISPA schafft die neue Ermittlungsmaßnahme enorme Sicherheitsrisiken. Die ISPA weist darauf hin, dass das Risiko einer schleichenden Ausweitung der Maßnahme immanent ist und betont, dass die Förderung des Vertrauens der Bürgerinnen und Bürger in hoheitliches Handeln essenziell für einen Rechtsstaat ist. Abschließend lehnt die ISPA die Quellen-TKÜ auch mit der Begründung ab, dass diese eine überschießende Ermittlungsmaßnahme darstellt und gegen den Verhältnismäßigkeitsgrundsatz verstößt.

**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 Optik einer Anlassgesetzgebung erschwert eine sachliche Diskussion

Da sich die Präsentation des Entwurfs in einem zeitlichen Naheverhältnis zu den Anschlägen von Brüssel 2016 befindet, erscheint der Vorwurf der Anlassgesetzgebung nachvollziehbar.

Der Entwurf basiert auf den Vorarbeiten einer Arbeitsgruppe aus dem Jahre 2008 und Teile des Entwurfs waren den Medien bereits seit letztem Herbst bekannt. Hieraus kann geschlossen werden, dass bereits seit Ende 2015 ein Entwurf verfügbar gewesen wäre. Es hätte somit hinreichend Zeit für eine Diskussion des Entwurfs bestanden, um den Anschein einer Anlassgesetzgebung zu vermeiden.

Die ISPA ersucht daher kommende Novellen im Rahmen von vorher einberufenen Arbeitsgruppen den relevanten Stakeholdern zu präsentieren, um so den Vorwurf hintanzuhalten, poltische Funktionsträger würden die Präsentation von Gesetzesentwürfen im Anschluss an Terroranschläge nutzen, um hieraus politisches Kapital zu schlagen oder die Ängste der Bevölkerung zu instrumentalisieren, um auf diese Weise Eingriffe in grundrechtsensible Bereiche zu ermöglichen. Die Notwendigkeit einer derart eingriffsintensiven Maßnahme soll sich aus sachlichen Argumenten ergeben und nicht allein auf aktuellen gesellschaftspolitischen Stimmungen gegründet sein, wie ein Anlassgesetzgebungsakt suggerieren würde.

## 2. Die Quellen-TKÜ scheint de facto keinen praktischen Nutzen für die Strafverfolgung mit sich zu bringen

Die ISPA weist im Zuge der Grundrechtsabwägung darauf hin, dass der Entwurf offensichtlich davon ausgeht, dass es sich bei den zu überwachenden Endgeräten um Standcomputer handelt, auf welchen die Überwachungssoftware unbemerkt installiert werden kann.

Nach Ansicht von Experten erfolgt der überwiegende Großteil der Kommunikation der angesprochenen Zielgruppen jedoch mittlerweile über mobile Endgeräte, welche von diesen nur in Ausnahmefällen unbeaufsichtigt gelassen werden. Endgeräte, bei welchen der Verdacht besteht, dass diese ggf. durch die Exekutive „verwanzt“ wurden, werden in der Regel von Verdächtigen unmittelbar entsorgt.

Die vorgeschlagene Bestimmung hat somit, abgesehen vielleicht von dem Einsatz von V-Leuten, denen es im Einzelfall gelingen könnte die Überwachungssoftware auf die betroffenen Endgeräte aufzuspielen, oder Verdächtige, die wirklich noch Standgeräte nutzen und diese hinreichend lange unbeobachtet lassen, keinen bzw. nur einen ausgesprochen begrenzten praktischen Nutzen, welchem ein enormes Missbrauchs- bzw. Sicherheitsrisiko, wie beispielsweise die Nutzung von den dadurch geschaffenen Sicherheitslücken durch Kriminelle oder unbefugte Nachrichtendienste gegenüber steht.

Gleichzeitig wirft die sehr eingeschränkte Installationsmöglichkeit für einen Bundestrojaner zudem die Frage auf, ob dies nicht letztlich als *ultima ratio* dazu führt, dass Betreiber gezwungen werden bei der Installation der Überwachungssoftware mitzuwirken. Die ISPA steht auch jeder Form einer indirekten Mitwirkung ablehnend gegenüber.

**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 Entwurf lässt wesentliche Fragen in Zusammenhang mit dem Anwendungsbereich der Bestimmung offen, wie beispielsweise, ob diese Überwachungsmaßnahme auch zukunftsträchtige Technologien wie das Internet der Dinge (z. B. Smart Meter) erfassen soll. Die weitgefasste Definition vom Begriff „Computersystem“ in § 74 Abs. 1 Z. 8 StGB würde eine derartig ausgedehnte Auslegung zulassen, daher fordert die ISPA eine ausdrückliche Präzisierung des Anwendungsbereichs der Bestimmung durch eine Klarstellung, dass die Überwachungsmaßnahme in § 136a StPO-Entwurf Technologien wie Internet der Dinge nicht umfassen soll.

Darüber hinaus hinterfragt die ISPA die Qualität der Daten, die durch den Einsatz des Bundestrojaners gewonnen werden, sofern das Programm auch Daten am Endgerät manipulieren kann. Aus Sicht der ISPA haben derartig ermittelte Beweise trotz Protokollierungsverpflichtung gemäß § 145 Abs. 4 StPO-Entwurf mehr als eine zweifelhafte Beweis-Qualität.

### 3. Eine Trennung zwischen zulässiger „Online-Überwachung“ sowie einer unzulässigen „Online-Durchsuchung“ ist de facto nicht möglich

Verdeckte Ermittlungsmaßnahmen wurden bereits im Rahmen der Arbeitsgruppe „OnlineDurchsuchung" im Jahr 2008 diskutiert. Anhand der Materialien[1] und des Schlussberichts[2] der Arbeitsgruppe vom März 2008 ist zu entnehmen, dass der Einsatz von Programmen, die unbemerkt auf einem Computer installiert werden und es ermöglichen, den Inhalt gespeicherter Daten zu durchsuchen („Online-Durchsuchung“), ohne dass es der Inhaber bemerkt, nach geltendem Recht nicht zulässig ist. Dieser Umstand soll auch durch die Novelle nicht geändert werden. Nach Ansicht der Autorinnen und Autoren des Entwurfs stellt die Quellen-Telekommunikationsüberwachung durch eine spezielle Überwachungssoftware gerade keine heimliche (Online-) Durchsuchung des elektronischen Geräts des Betroffenen dar, da die Ermittlung von sonstigen auf dem Computersystem gespeicherten Daten (z.B. Chat-History) nicht Gegenstand der vorgeschlagenen Maßnahme ist.

Im vorliegenden Gesetzesentwurf wird der Zugriff auf Adressbücher und Kontaktverzeichnisse (z.B.: Outlook, Skype, WhatsApp) ausdrücklich genannt und erlaubt. Obwohl die Autorinnen und Autoren des Entwurfs eine derartige Durchsuchung eines Computersystems nach Spuren zur Identifizierung einer Person oder sonstiger Dateien nicht als eine "Online-Durchsuchung" bewertet, ist aus technischer sowie aus praktischer Sicht eine Trennung von zulässiger "Online-Überwachung" und einer unzulässigen "Online-Durchsuchung" in der Realität nicht zu gewährleisten (da z. B. beim Aufrufen des Chatfensters oftmals auch die Chat-History dargestellt wird). Hinzu kommt, dass die Installation, der Betrieb und das Verstecken einer Überwachungssoftware umfangreiche Zugriffsrechte auf dem Zielsystem benötigen würde, welche dem Trojaner jede beliebige weitere Funktionalität erlauben würde, inklusive des Durchsuchens, Manipulierens und Erstellens von Dateien; dies wirft auch Fragen in Bezug auf die Qualität der so gewonnen Beweismittel auf.

[1] 192/ME XXV. GP Erläuterungen S 1.
[2] BMJ/BMI Interministerielle Arbeitsgruppe „Online-Durchsuchung“ Bericht, Endfassung vom 09.04.2008.

## 4. Eine Quellen-TKÜ schafft neue Sicherheitsrisiken

Die Einführung der neuen Ermittlungsmaßnahme würde dazu führen, dass bestehende Sicherheitslücken nicht geschlossen werden sowie unter Umständen neue geschaffen werden. So ist einerseits die Frage unklar woher die Exekutive die für die TKÜ zu verwendenden Programme bezieht, anderseits wie dafür gesorgt werden soll, dass gängige Sicherheits-Software diese nicht erkennt und den Benutzer oder die Benutzerin hierüber informiert.

Die neue Überwachungsmaßnahme nach § 136a StPO-Entwurf schafft aus Sicht der ISPA einen Interessenskonflikt für IT-Sicherheitsunternehmen, da die für die Überwachung verwendeten Programme Schwachstellen im Betriebssystem ausnützen, die eben von diesen Unternehmen eigentlich geschlossen werden sollten. Insofern bestünde ein Anreiz derartige Hintertüren „offen zu lassen“, was gleichzeitig die Gefahr mit sich bringt, dass diese auch von Kriminellen oder anderen dritten Institutionen (z.B. Nachrichtendiensten) genutzt werden und somit zu einer Schwächung der Cyber-Resilienz Österreichs bzw. Europas führt.

Die ISPA möchte nachdrücklich betonen, dass die Erfüllung der Kernaufgaben von IT-Sicherheitsdienstleistern, nämlich die Schließung von Sicherheitslücken in Software, durch diese Novelle nicht beeinträchtigt werden darf, da dies zu einer allgemeinen Verschlechterung des Cybersicherheitsniveaus in Österreich führen würde.

Es ist daher ausdrücklich auszuschließen, dass IT- Sicherheitsdienstleister durch die Exekutive dafür belangt werden, dass sie gewissenhaft ihrer Kernaufgabe nachkommen, die gerade darin besteht, allfällige bestehende „Backdoors“ zu schließen. Nach Ansicht der ISPA ist jedenfalls ein Zustand zu vermeiden in dem staatliche Organisationen Sicherheitsfirmen untersagen Sicherheitslücken zu schließen, mit der Begründung, dass diese die Ermittlungsarbeiten beeinträchtigen könnten.

## 5. Das Risiko einer schleichenden Ausweitung der Maßnahme ist immanent

Die ISPA anerkennt, dass der Entwurf in seiner derzeitigen Fassung hohe (bzw. im Rahmen der StPO „höchste“) formelle und materielle Anforderungen an den Einsatz der geplanten Maßnahmen stellt. Die ISPA verweist jedoch darauf, dass es auch im Rahmen der Vorratsdatenspeicherung im Gesetzgebungsverfahren zu einer weitestgehenden Aushebelung beinahe sämtlicher Schutzvorschriften bzw. zu einer massiven Ausdehnung des Anwendungsbereiches (Zugriff auf Vorratsdaten für sämtliche Strafdelikte) gekommen ist, was im Endeffekt auch zu einem Einschreiten der Höchstgerichte geführt hat.

Die ISPA ersucht daher den Gesetzgeber offen und transparent zu kommunizieren (also nicht Zulässigkeiten von einem Dschungel an Verweisen abhängig zu machen) und von einer schleichenden Ausweitung bzw. einer möglichen Verwässerung des Grundrechtsschutzes, beispielsweise durch den Ersatz der Anforderung einer richterlichen Bewilligung durch eine Verwässerung in Richtung einer Genehmigung des Rechtsschutzbeauftragten im BMI wie dies im

**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

Polizeilichen Staatsschutzgesetz vorgesehen ist, im Rahmen des Gesetzgebungsprozesses abzusehen.

## 6. Förderung des Vertrauens der Bürgerinnen und Bürger in hoheitliches Handeln ist essenziel für einen Rechtsstaat

Neben den oben angeführten Bedenken möchte die ISPA auf den öffentlichen Eindruck des stellenweise offensichtlich gänzlich fehlenden Problembewusstseins in Teilen der Exekutive für Aspekte des Grundrechtsschutzes im Internet hinweisen.[3]

Die ISPA ist zusammen mit den relevanten Stakeholdern nachdrücklich darum bemüht das Vertrauen der Nutzerinnen und Nutzer in die österreichische Strafrechtspflege zu fördern bzw. wo notwendig wiederherzustellen. Es scheint jedoch, dass ein Großteil der Nutzerinnen und Nutzer, eine generell ablehnende Haltung gegenüber Online-Ermittlungsmaßnahmen hat.

Maßnahmen wie die vorgeschlagenen könnten, indem diese ein Gefühl der Überwachung von staatlicher Seite vermitteln, zu wachsenden Vorbehalten der Bevölkerung gegenüber dem Staat führen. Ein derartiger Eindruck einer staatlichen Totalüberwachung würde sich zudem auch in einem Mangel an Vertrauen in digitale Technologien niederschlagen und dadurch zu einer Verzögerung des Take-Up´s der Internet-Nutzung führen.

Die ISPA spricht sich vor diesem Hintergrund für einen offenen Dialog aus, um den durch die Themen Netzsperren und Vorratsdatenspeicherung (Stichwort: intransparente Kommunikation der betroffenen Ministerien und Verwässerung des Entwurfs im legistischen Prozess) entstandenen Vertrauensverlust zu kompensieren und das Vertrauen in das staatliche Handeln auch bei der Strafrechtspflege im Internet wiederherzustellen.

## 7. Die Quellen-TKÜ stellt eine überschießende Ermittlungsmaßnahme dar und verstößt gegen den Verhältnismäßigkeitsgrundsatz

In den Erläuternden Bemerkungen zum vorliegenden Gesetzesentwurf wird die stetige Gefahr des Terrors hervorgehoben. Diese neuartige Ermittlungsmaßnahme soll nach Maßgabe der Erläuternden Bemerkungen vor allem dem Zwecke dienen, Menschen, welche in den Nahen Osten reisen wollen, zu überwachen, da sich diese möglicherweise in Terrorcamps zu potentiellen Terroristen ausbilden lassen könnten.[4] Es stellt sich somit die Frage, ob eine geplante Reise in bestimmte Gebiete bereits als konkreter Verdacht für die Ausbildung für terroristische Zwecke (§ 278e Abs.2 StGB) oder die Beteiligung an einer terroristischen Vereinigung (§ 278b Abs. 2 StGB) gewertet werden kann und somit unter Umständen die Grundlage für den Einsatz der Überwachungssoftware darstellen könnte.

[3] http://futurezone.at/netzpolitik/polizisten-greifen-unkontrolliert-auf-sozialversicherungsdaten-zu/192.503.348 (22.04.2016).
[4] 192/ME XXV. GP Erläuterungen S. 3.

Das Problem einer solchen "Stöberfahndung" ist aus Sicht der ISPA, dass der Anwendungsbereich für die Ermittlungsmaßnahme sehr ausgedehnt wird und der Einsatz überhaupt erst zur Schaffung von Verdachtslagen führen kann (dies würde jedoch dem Wortlaut des Gesetzestextes widersprechen). Die jüngere Vergangenheit in Österreich hat gezeigt, dass die bestehenden Antiterrorbestimmungen sehr oft angewendet wurden (z. B.: Tierschützerprozess in Wr. Neustadt; Uni Brennt Aktivistinnen; Anti-Akademikerball-DemonstrantInnen), um die Voraussetzungen für Ermittlungsmethoden zu schaffen, die sonst nicht angewendet werden dürften, weil die Strafdrohung der möglichen Grunddelikte ohne Terrorismuszusammenhang oft nicht die notwendigen Schwellen überschreitet. Der Verhältnismäßigkeitsgrundsatz wird dadurch zusehends in Frage gestellt.

Solche tiefgreifenden Grundrechtseingriffe sind nur zulässig, wenn diese dem Grundsatz der Verhältnismäßigkeit entsprechen. Der Verhältnismäßigkeitsgrundsatz verlangt, dass Ermittlungsmaßnahmen und deren gesetzliche Grundlangen durch öffentliche Interessen legitimiert sind. Aus technischer Sicht kommen berechtigte Zweifel auf, ob der Einsatz der geplanten Überwachungssoftware überhaupt geeignet ist, das legitime Ziel der Bekämpfung und Verfolgung von Terrorismus und (organisierter) schwerer Kriminalität zu verfolgen. Der aktuelle Stand der Technik lässt eine treffsichere, schadlose und zuverlässige Anwendung gar nicht zu. Daher fordert die ISPA die Streichung dieser eingriffsintensiven Ermittlungsmaßnahme vom Gesetzesentwurf.

Die ISPA ersucht um die Berücksichtigung ihrer Anregungen bei der Gestaltung des Gesetzesentwurfes.

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.

**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