An das
Bundesministerium für Justiz
Museumstraße 7
1070 Wien

E-Mail: abt.i7@bmj.gv.at; katharina.nagl@bmj.gv.at

Wien, am 29. Jänner 2021

ISPA STELLUNGNAHME ZUM VORSCHLAG FÜR EINE VERORDNUNG DER EUROPÄISCHEN PARLAMENTS UND DES RATES ÜBER EINEN BINNENMARKT FÜR DIGITALE DIENSTE („DIGITAL SERVICES ACT“)

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich, in Zusammenhang mit der öffentlichen Konsultation des Bundesministeriums für Justiz betreffend den Vorschlag für eine Verordnung der Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste („Digital Services Act“) wie folgt Stellung zu nehmen:

Zwar ist es zu begrüßen, dass sowohl die Haftungsfreistellung für Access- und Host-Provider sowie auch das Verbot allgemeiner Überwachungspflichten aus der E-Commerce-RL übernommen wird, dennoch möchte die ISPA anregen klarzustellen, dass auch die Pflicht zur Löschung spezifischer Informationen nicht zur Überwachung sämtlicher Inhalte führen darf. Darüber hinaus fordert die ISPA, dass die Ausgestaltung der Trusted Flagger Funktion weiterhin den Unternehmen überlassen bleiben sollte. Des Weiteren sollte das Verhältnis der Transparenzmaßnahmen in Art 12 und 13 zu jenen in Art 4 VO 2120/2015 geklärt werden und die Expertise der RTR-GmbH bei der Umsetzung der Verordnung mit einbezogen werden. Die Beurteilung der „tatsächlichen Kenntnis“ eines rechtswidrigen Inhalts sollte im Einklang mit der höchstgerichtlichen Rechtsprechung in Österreich weiterhin flexibel erfolgen und Online-Plattformen darüber hinaus nicht zur Offenlegung von Nutzerdaten auf Eigeninitiative bei Verdacht einer Straftat verpflichtet werden. Abschließend möchte die ISPA betonen, dass Zugangssperren auch als letztmögliche Durchsetzungsmaßnahme ungeeignet erscheinen. Sollte dennoch daran festgehalten werden sollte es sich ausschließlich um DNS-Sperren handeln.

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 Pflicht zur Löschung spezifischer Inhalte darf nicht das Verbot allgemeiner Überwachungspflichten untergraben

Die ISPA begrüßt, dass der Vorschlag des Digital Services Act nicht nur die bewährten Haftungsprivilegien der E-Commerce-Richtlinie, sondern auch das bislang darin geregelte Verbot allgemeiner Überwachungspflichten in Art 7 übernimmt.

Wie die Kommission jedoch u.a. auf S. 4 der Erläuterungen verdeutlicht, soll dennoch an der zuletzt ergangenen Judikatur des Gerichtshofs der Europäischen Union (EuGH) festgehalten werden, wobei explizit auf die Entscheidung C-18/18[1] verwiesen wird. In dieser – von zahlreichen Seiten heftig kritisierten – Entscheidung, kam der EuGH zu dem Ergebnis, dass trotz des Verbots allgemeiner Überwachungspflichten Online-Plattformen aufgetragen werden kann, sämtliche Inhalte nach spezifischen (wort- bzw. sinngleichen) Informationen zu durchsuchen. Darüber hinaus führt die EU-Kommission weiter aus, dass der Verordnungsvorschlag die Grundlage für den Einsatz von Technologien schaffen soll, welche das erneute Hochladen bereits gelöschter Inhalte verhindert. Solche „stay-down" Pflichten erfordern ebenso wie die Suche nach wort- und sinngleichen Informationen, dass der Host-Provider digitale Fingerabdrücke der als rechtswidrig eingestuften Inhalte erstellt und automatisierte Tools implementiert, mit denen Uploads anhand dieser Fingerabdrücke bewertet werden können. Letztendlich würde eine solche Pflicht es also erfordern, dass Online-Plattformen im Allgemeinen alle Uploads überwachen und sie auf mögliche Übereinstimmungen mit ihrer internen Datenbank hin überwachen müssen.

Auch wenn sowohl im Fall von stay-down Pflichten als auch bei der Suche nach wort- und sinngleichen Inhalten also nach spezifischen Informationen gesucht wird, ist es erforderlich, dass der Host-Provider kontinuierlich, und ohne zeitliche Befristung, sämtliche Inhalte auf seinem Dienst überwacht. Dabei handelt es sich somit nicht um eine spezifische Überwachungspflicht, die vom EuGH etwa im Bereich des Urheberrechts bislang dadurch definiert wurde, dass sie nur einen bestimmten Benutzer sowie Verstöße des gleichen Typs betrifft, und nur für einen begrenzten Zeitraum bestehen darf.[2]

Anders als in den einführenden Bemerkungen angedacht, sollte der Verordnungsvorschlag daher dazu genutzt werden, eine Klarstellung unter Einbeziehung sämtlicher involvierter (Grund-)Rechte zu treffen. Aus dieser sollte hervorgehen, dass auch die Pflicht zur Löschung spezifischer (wort- bzw. sinngleicher) Inhalte nicht zu einer Pflicht zur allgemeinen Überwachung sämtlicher Inhalte führen darf, da andernfalls das Verbot allgemeiner Überwachungspflichten erheblich ausgehöhlt werden würde.

2) Die Ausgestaltung der trusted flagger Funktion sollte weiterhin den Unternehmen überlassen bleiben

In ihrem Bemühen rechtswidrige Inhalte möglichst rasch zu entfernen, arbeiten Online-Plattformen bereits bislang mit einer Vielzahl an Organisationen zusammen, deren Meldungen priorisiert

[1] EuGH 03.10.2019, C-18/18 (Glawischnig-Piesczek/Facebook)
[2] EuGH 07.07.2016, C-494/15 (Tommy Hilfiger) Rz 34

behandelt werden. Zu diesen „trusted flaggers“ gehören unter anderem zivilgesellschaftliche Organisationen oder Hotlines wie beispielsweise in Österreich die Meldestelle für sexuelle Missbrauchsdarstellungen Minderjähriger sowie nationalsozialistische Inhalte (Stopline.at).

Wie aus der Bezeichnung wörtlich hervorgeht ist das Charakteristikum eines trusted flaggers das Vertrauen, welches Online-Plattformen diesen Organisationen entgegenbringen. Welchen konkreten Organisationen eine Online-Plattform das notwendige Vertrauen ausspricht, hängt unter anderem von der Art der angebotenen Dienstleistung, der Unternehmenskultur und seinen Erwartungen ab.

Obwohl die ISPA das Konzept eines trusted flaggers daher an sich begrüßt, und als sinnvolle Maßnahme erachtet, um rasch gegen illegale Inhalte vorzugehen, ist der gewählte Weg in Artikel 19 des Vorschlags zu hinterfragen. Möglicherweise ist dieser sogar kontraproduktiv für die reibungslose Funktionsweise von trusted-flagger-Kanälen. Denn gerade aufgrund der unterschiedlichen Arten von Online-Plattform bzw. der illegalen Inhalte, die auf diesen aufscheinen können, ist es nach Ansicht der ISPA nicht zweckmäßig, allgemeine Kriterien aufzustellen, die, sofern sie der nationalen Koordinierungsstelle für digitale Dienste bescheinigt werden können, umgehend zur Ernennung als trusted flagger für sämtliche Online-Plattformen führen.

Eine solche Ernennung als trusted flagger durch eine externe Behörde und für sämtliche Plattformen widerspricht geradezu dem Grundgedanken, dass die trusted flagger Funktion von der Beziehung zwischen einer bestimmten Plattform und einer bestimmten Organisation geprägt ist. Denn das Verhältnis zwischen einem trusted flagger und einer Online-Plattform muss in erster Linie durch die Plattform selbst bestimmt werden können, welche dem trusted flagger auch das entsprechende Vertrauen entgegenbringen und von dessen Fähigkeiten im Umgang mit illegalen Inhalten überzeugt sein muss.

Vielmehr ist zu erwarten, dass es durch die vorgesehene Regelung zu einer überschießenden Anzahl an Anträgen bei den nationalen Koordinierungsstellen kommen wird. Schon in der Vergangenheit hat sich gezeigt, dass bei vielen Organisationen zwar das Interesse an der Funktion als trusted flagger besteht, nicht jedoch das Interesse an den notwendigen Einschulungen im Umgang mit dieser Funktion. In Anbetracht des vorgesehenen Konzeptes in Artikel 19 scheint es aber als müssten die Meldungen von trusted flaggern in jedem Fall priorisiert behandelt werden, unabhängig von deren Qualität.

Darüber hinaus ist auch zu befürchten, dass aufgrund der erheblichen Anzahl zusätzlicher trusted flagger es zu einer Überlastung der entsprechenden Meldemechanismen kommen würde, die nur für eine gewisse Anzahl an Meldungen ausgelegt sind. Damit würde der ursprüngliche Zweck dieser Kanäle, eine möglichst rasche Behandlung der Meldungen zu ermöglichen, erheblich gefährdet werden.

Anstatt eines starren Prozederes sollte der Vorschlag daher Online-Plattformen auch weiterhin die notwendige Flexibilität gewähren, wem und in welchem Umfang sie trusted flagger Funktionen zusprechen. Als Mindestmaß jedoch sollte eine konkrete Prüfpflicht der zuständigen nationalen Koordinierungsstelle vorgesehen werden, in der diese sich von den Fähigkeiten der antragstellenden Organisationen überzeugen und diese auch begründen muss. Eine reine

Bescheinigungserfordernis der noch dazu sehr allgemein formulierten Kriterien erscheint in jedem Fall unzureichend.

3) Das Verhältnis der Transparenzmaßnahmen in Art 12 und 13 zu jenen in Art 4 VO 2120/2015 ist zu klären

Gemäß Artikel 12 des Verordnungsvorschlags sollen sämtliche Diensteanbieter Informationen zu Inhaltsmoderationsmaßnahmen veröffentlichen die sie in Bezug auf Informationen ergreifen, die von Nutzern bereitgestellt werden. Angesichts der breiten Definition von Inhaltsmoderationsmaßnahmen in Artikel 2 lit. p sowie der Tatsache, dass diese Pflicht sämtliche Diensteanbieter – und daher auch Anbieter von Internetzugangsdiensten – betrifft, ist es fraglich welche Informationen von dieser Transparenzpflicht konkret erfasst werden.

Die ISPA möchte darauf hinweisen, dass Anbieter von Internetzugangsdiensten bereits gemäß Artikel 4 VO 2120/2015[3] umfangreichen Transparenzpflichten in Bezug auf die von ihnen ergriffenen Verkehrsmanagementmaßnahmen unterliegen, worunter unter anderem auch Maßnahmen verstanden werden, mit denen der Zugang zu bestimmten Informationen (Webseiten) verhindert wird (Zugangssperren).

Da Zugangsdiensteanbieter keine anderen Maßnahmen in Bezug auf von Nutzern bereitgestellte Inhalte ergreifen – und dies aufgrund der Vorgaben in Artikel 5 Abs. 1 E-Privacy-RL[4] auch nicht dürfen – und um zu verhindern, dass in dieser Hinsicht überschneidende Informationspflichten vorgesehen werden, sollte daher die Verordnung 2120/2015 ebenfalls in die Liste der Spezialnormen in Artikel 1 Abs. 5 des Verordnungsvorschlags aufgenommen werden, und klargestellt werden, dass Zugansgdiensteanbieter den in Artikel 12 und 13 genannten Transparenzpflichten bereits durch Erfüllung der darin geregelten Informationspflichten in hinreichendem Ausmaß nachkommen.

4) Die Expertise der RTR-GmbH sollte bei der Umsetzung der Verordnung mit einbezogen werden

Wie aus Artikel 38 des Verordnungsvorschlags hervorgeht soll jeder Mitgliedstaat die zuständigen Behörden zur Umsetzung der Verordnung benennen. Aus Sicht der ISPA wäre es naheliegend, dabei der Rundfunk und Telekom Regulierungs-GmbH (RTR) eine tragende Rolle zuzusprechen, die bereits über das notwendige Fachwissen im Bereich der digitalen Dienste verfügt, und gleichermaßen mit den Anliegen der Diensteanbieter sowie auch der Nutzerinnen und Nutzer vertraut ist.

---

[3] Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union (Text von Bedeutung für den EWR)

[4] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)

Aus Sicht der ISPA bietet sich die Behörde speziell auch daher an, da sie bereits heute gemäß § 115 Abs. 1b TKG für die Einhaltung der Vorgaben der Netzneutralität zuständig ist, und dabei bereits die notwendigen Abwägungen zu treffen hat, etwa wann ein Eingriff in von Nutzern bereitgestellte Inhalte in Form von Verkehrsmanagementmaßnahmen zulässig ist und welche Rechte dabei abzuwägen sind. Darüber hinaus erfordert auch die VO 2120/2015 wie zuvor unter Punkt 3 ausgeführt bereits die Bereitstellung umfangreicher Informationen über den Einsatz von Verkehrsmanagementmaßnahmen, welche von der RTR geprüft werden. Auf die dabei angereicherte Expertise kann gleichermaßen bei der Prüfung der Transparenzpflichten des Digital Services Acts zurück gegriffen werden.

Um daher auf nationaler Ebene einen einheitlichen Ansatz im Umgang mit illegalen Inhalten durch Anbieter digitaler Dienste sicherzustellen sowie um Doppelgleisigkeiten und Überschneidungen in der Regulierung zu vermeiden, ersucht die ISPA darum die RTR-GmbH an den relevanten Stellen als zuständige Behörde vorzusehen.

5) Die Beurteilung der „tatsächlichen Kenntnis“ der Rechtswidrigkeit eines Inhalts sollte weiterhin flexibel erfolgen

In Artikel 14 konkretisiert der Vorschlag das Meldesystem welches Host-Provider zur Meldung illegaler Inhalte bereitstellen müssen. Es ist begrüßenswert, dass damit erstmals auch klare formelle und inhaltliche Kriterien genannt werden, die eine entsprechende Meldung zu erfüllen hat, wie insbesondere eine Spezifizierung des Speicherorts sowie der Gründe für die Rechtswidrigkeit des Inhalts.

Grundsätzlich möchte die ISPA dennoch darauf hinweisen, dass jegliche Verpflichtung eines Host-Providers, Inhalte aufgrund einer Nutzermeldung zu löschen, die betroffenen Unternehmen in eine Richterrolle drängt, in der die Rechtswidrigkeit eines Inhalts selbstständig beurteilt werden muss, in vielen Fällen ohne eigene Rechtsabteilung sowie generell ohne Expertise in der damit einhergehenden Rechteabwägung. Die angeführten Kriterien erleichtern die Beurteilung zwar bis zu einem gewissen Grad, lassen das grundsätzliche Problem jedoch unberührt, dass die notwendige Expertise zur Beurteilung der Inhalte nur bei den zuständigen Gerichten oder unabhängigen Behörden zu finden ist. Rechtssicherheit auf Seiten des betroffenen Unternehmens ist letztlich daher auch nur dann gegeben, wenn die Rechtswidrigkeit des Inhalts zuvor durch ein Gericht oder eine unabhängige Behörde festgestellt wurde.

Darüber hinaus geht der Verordnungsvorschlag jedoch auch zu weit, indem in Abs. 3 festgehalten wird, dass jede Meldung die rein objektiv die angeführten Kriterien erfüllt – unabhängig davon, ob etwa die Angaben zur Rechtswidrigkeit zutreffend sind – auch bereits „tatsächliche Kenntnis“ der Rechtswidrigkeit iSd Artikel 5 auslöst. Damit wird das Unternehmen dazu verpflichtet, den Inhalt umgehend zu löschen – sofern dieser tatsächlich rechtswidrig ist – oder andernfalls dafür zu haften.

In Österreich gilt bislang, dass es sich bei der „tatsächlichen Kenntnis“ um eine subjektive Tatbestandsvoraussetzung handelt, bei deren Beurteilung auf die Fähigkeiten und das Wissen eines juristischen Laien abzustellen ist. Demnach ist ein Diensteanbieter dann von der Haftung für Inhalte

von Dritten befreit, wenn er sich keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird. Hierfür ist wie bereits ausgeführt auf die Fähigkeiten eines juristischen Laien abzustellen.[5]

Der Verordnungsvorschlag würde dies jedoch nun offensichtlich ändern, indem jede Meldung welche die objektiven Voraussetzungen in Artikel 14 Abs. 1 erfüllt, automatisch „tatsächliche Kenntnis" bewirkt, unabhängig davon, ob anhand der genannten Informationen für einen juristischen Laien die Rechtswidrigkeit offenkundig wäre. Eine solche Regelung geht nach Ansicht der ISPA klar an der Realität vorbei.

Denn trotz der entsprechenden Angaben in der Meldung, wird es gerade bei zahlreichen kontextbezogenen Inhalten auf den ersten Blick dennoch nicht ersichtlich sein, ob der Inhalt rechtswidrig ist oder nicht. Die genannten Kriterien erleichtern also zwar wesentlich die Behandlung der Meldung durch den jeweiligen Host-Provider, dennoch würde auch durch eine solche Meldung nicht in jedem Fall die Rechtswidrigkeit eines Inhalts für das Unternehmen offenkundig werden.

Die ISPA ersucht daher, im Rahmen der Verhandlungen innerhalb des Rats darauf hinzuwirken, dass diese Passage gestrichen wird, um ein Fortbestehen der in Österreich bereits etablierten Rechtsprechung des OGHs sicherzustellen, welche das notwendige Maß an Flexibilität im Einzelfall gewährleistet.

Darüber hinaus sollte nach Ansicht der ISPA auch ergänzt werden, dass sofern ein Host-Provider auf Grund der Art oder der Häufigkeit der eingelangten Meldungen eines Nutzers davon ausgehen kann, dass die Meldungen auf missbräuchliche Art veranlasst wurden, die Meldungen dieses Nutzers nicht behandeln muss und diese in keinem Fall „tatsächliche Kenntnis" auslösen können.

6) Online-Plattformen sollen nicht dazu veranlasst werden auf Eigeninitiative Daten ihrer Nutzer herausgeben zu müssen

In Artikel 21 des Vorschlags wird vorgesehen, dass Online-Plattformen in Hinkunft einer Meldepflicht an Strafverfolgungsbehörden unterliegen sollen, sofern ihnen Informationen zur Kenntnis gelangen, die den *Verdacht* nahelegen, dass eine schwere Straftat mit Gefahr für Leib und Leben einer Person begangen wurde, begangen wird oder begangen werden *könnte*. Diese Meldepflicht soll nicht nur den Verdacht einer Straftat, sondern „sämtliche vorhandenen relevanten Informationen" umfassen.

Diese Formulierung legt nahe, dass die Meldepflicht auch eine Auskunftspflicht, über die bei der Online-Plattform vorhandenen Nutzerdaten beinhaltet. Eine solche proaktive Auskunftspflicht gegenüber Strafverfolgungsbehörden ist nach Ansicht der ISPA klar abzulehnen. Online-Plattformen sind bereits heute stark daran bemüht ihren Pflichten zur Unterstützung der Strafverfolgung nachzukommen und das gemeinsame Ziel, ein sicheres Internet für alle Nutzerinnen und Nutzer zu gewährleisten.

Die vorgesehene Pflicht ist jedoch in mehrerer Hinsicht zu kritisieren. Zunächst ist darauf

[5] Vgl u.a. OGH 15 Os 14/15w

hinzuweisen, dass Online-Plattformen Informationen ihrer Nutzerinnen und Nutzer nur in den in Art 6 Abs. 1 DSGVO definierten Fällen verarbeiten – und daher auch an Dritte übermitteln – dürfen. Im Fall der herkömmlichen Auskunft über Nutzerdaten, erfolgt die Übermittlung von Nutzerdaten auf Grundlage einer gerichtlichen oder behördlichen Anordnung die wiederum auf einer klar definierten gesetzlichen Regelung beruht und damit gemäß Art 6 Abs. 1 lit c DSGVO zulässig ist. Auf diese Weise ist auch auf Seiten des Unternehmens Rechtssicherheit gewährleistet. In Bezug auf die im Verordnungsvorschlag vorgesehene Auskunftspflicht ist jedoch fraglich, ob diese ausreichend bestimmt iSd Art 6 Abs. 3 DSGVO ist, um ebenfalls als zulässige Rechtsgrundlage zur Datenverarbeitung herangezogen werden zu können.

Die nun vorgesehene Pflicht würde Plattformen darüber hinaus zum wiederholten Male in die Verantwortung nehmen selbstständig zu prüfen, ob eine schwere Straftat begangen wurde oder möglicherweise begangen werden wird, und welche Informationen zur Verfolgung der Straftat an die Strafverfolgungsbehörde übermittelt werden dürfen bzw. müssen. Dabei hat die Plattform wie auch in Erwägungsgrund 48 betont wird, sämtliche anderen anwendbaren Rechtsvorschriften zu beachten. Es ist offensichtlich, dass eine solche Rechteabwägung für jeden Einzelfall gerade für Online-Plattformen ohne eigene Rechtsabteilung, aber selbst für große Unternehmen, nicht möglich ist, ohne dabei ein erhebliches Strafrisiko einzugehen.

Gerade der Umstand, dass der Wortlaut der Bestimmung eine Meldepflicht sogar für mögliche – aber noch nicht begangenen – Straftaten beinhaltet würde in der Praxis außerdem zu erheblichen Problemen führen. Denn selbst Strafverfolgungsbehörden dürfen – sofern es kein eigenständiges Vorbereitungsdelikt in der nationalen Rechtsordnung gibt – eine Auskunft über Informationen grundsätzlich nur dann verlangen, wenn ein konkreter Anfangsverdacht über eine begangene Straftat vorliegt. Diese Regelung würde damit umgangen werden. Überhaupt bleiben zahlreiche Fragen ungeklärt, etwa, welche Folgen es für die Online-Plattform hätte, wenn Nutzerdaten an eine Strafverfolgungsbehörde übermittelt werden – da angenommen wird, dass eine Straftat begangen werden könnte - am Ende jedoch tatsächlich keine Straftat begangen wird.

Die ISPA fordert daher, dass die Meldepflicht in Artikel 21 gänzlich gestrichen wird, zumindest aber der Wortlaut des Artikel 15 Abs. 2 2. Halbsatz der E-Commcerce-RL übernommen wird, der bislang bereits klarstellte, dass Nutzerdaten nur auf Verlangen der zuständigen Behörde übermitteln müssen, und nicht auf Eigeninitiative.

7) Zugangssperren sollten, wenn, dann ausschließlich in Form von DNS-Sperren umgesetzt werden müssen

In Artikel 41 Abs. 3 lit. b wird vorgesehen, dass sofern alle anderen, der nationalen Koordinierungsstelle zur Verfügung stehenden, Mittel zur Einstellung eines Verstoßes nach dieser Verordnung ausgeschöpft wurden und die Behörde der Ansicht ist, dass die Zuwiderhandlung fortbesteht und schwerwiegenden Schaden verursacht und der Verstoß zudem eine schwere Straftat bewirkt die das Leben oder die Sicherheit von Personen gefährdet, die Behörde die national zuständige Justizbehörde ersuchen kann, vorrübergehend die Sperre des Zugangs zu dem betroffenen Dienst anzuordnen. Auch wenn es in dieser Bestimmung nicht ausdrücklich festgehalten

wird, kommen als Empfänger einer solchen Anordnung im Wesentlichen die nationalen Anbieter von Internetzugangsdiensten in Betracht.

Die ISPA begrüßt grundsätzlich das Konzept, dass Zugangssperren nur als letzte mögliche Maßnahme zur Einstellung eines schwerwiegenden Verstoßes vorgesehen werden, und auch dafür die Einbeziehung einer richterlichen Behörde notwendig ist. Dennoch möchte die ISPA darauf aufmerksam machen, dass Zugangssperren auch in diesem Fall eine ungeeignete Durchsetzungsmaßnahme darstellen. Denn generell bestehen nur zwei Möglichkeiten eine solche Sperre umzusetzen.

Im Rahmen einer DNS-Sperre leitet der Access-Provider Anfragen an seinen DNS-Server, die sich auf eine bestimmte Domain beziehen, bewusst auf eine andere Webseite um, oder beantwortet sie gar nicht. Auf diese Weise kann jedoch nur der Zugriff auf eine gesamte Domain verhindert werden. Gerade angesichts der Tatsache, dass viele Diensteanbieter mehrere Dienste auf der gleichen Domain zur Verfügung stehen würde eine solche Sperre daher wohl häufig überschießend sein.

Darüber hinaus sind DNS-Sperren durch Nutzerinnen und Nutzer mit rudimentären IT-Kenntnissen sehr einfach zu umgehen. Während der Betreiber der jeweiligen Webseite die Sperre schlicht durch Änderung der jeweiligen Top-Level-Domain (beispielsweise .net anstelle von .org) umgehen kann, besteht für den anfragenden Nutzer die Möglichkeit, einen anderen DNS-Server zu nutzen.

Daneben bestehet die Möglichkeit, den Zugang zu einem Dienst durch eine IP-Sperre zu blockieren. Dabei verhindert der Access-Provider direkt den Zugriff seiner Nutzerinnen und Nutzer auf die IP-Adresse des Servers, auf welchem die inkriminierende Webseite gehostet wird. Ebenso würde davon jedoch nicht nur ein bestimmter Dienst, sondern häufig die gesamte Webseite des Diensteanbieters betroffen sein. Darüber hinaus teilen sich in der Praxis häufig mehrere voneinander unabhängige Webseiten die gleiche IP-Adresse wodurch noch weitaus höhere Kollateralschäden zu erwarten sind. Die angedachte Sperre einer einzelnen Webseite kann dabei schnell mehrere hundert – rechtlich gänzlich unbedenkliche – Webseiten miterfassen.

Abschließend ist darauf hinzuweisen, dass selbst IP-Sperren darüber hinaus ebenfalls durch Nutzerinnen und Nutzer umgangen werden können, indem diese beispielsweise VPN-Verbindungen nutzen. Die Effektivität der Maßnahme ist daher ebenfalls nicht gegeben.

Die ISPA fordert daher, grundsätzlich von Zugangssperren selbst als letztmögliche Maßnahme abzusehen. Sollte dennoch daran festgehalten werden, sollte es jedoch auf DNS-Sperren eingeschränkt werden.

Die ISPA hofft auf die Berücksichtigung ihrer Bedenken und Anregungen.

Mit freundlichen Grüßen,

ISPA - Internet Service Providers Austria

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

Mag. Charlotte Steenbergen

Generalsekretärin

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