An das
Bundesministerium für Justiz
Museumstraße 7
1070 Wien

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

Wien, am 13. Oktober 2020

ISPA STELLUNGNAHME IM RAHMEN DER ÖFFENTLICHEN KONSULTATION DES BUNDESMINISTERIUMS FÜR JUSTIZ HINSICHTLICH EINES BUNDESGESETZES, MIT DEM STRAF- UND MEDIENRECHTLICHE MAßNAHMEN ZUR BEKÄMPFUNG VON HASS IM NETZ GETROFFEN WERDEN

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich, in Zusammenhang mit der öffentlichen Konsultation des Bundesministeriums für Justiz hinsichtlich eines Bundesgesetzes, mit dem straf- und medienrechtliche Maßnahmen zur Bekämpfung von Hass im Netz getroffen werden, wie folgt Stellung zu nehmen:

Die ISPA möchte darauf hinweisen, dass die Sperre einer gesamten Webseite zur Bekämpfung von Hass im Netz eine gleichermaßen unverhältnismäßige wie ungeeignete Maßnahme gegen Hass im Netz darstellt und daher abzulehnen ist. Die ISPA begrüßt daher, dass der Gesetzgeber von der Aufnahme eines entsprechenden Anspruchs gegenüber dem Zugangsanbieter in § 36b abgesehen hat und fordert, dass dies auch so beibehalten wird. Darüber hinaus möchte die ISPA auf grundrechtliche Bedenken hinsichtlich der Ausweitung der Ermittlungsmaßnahmen für Privatankläger in § 71 StPO hinweisen.

1) Netzsperren sind kein geeignetes Mittel zur Bekämpfung von Hass im Netz

Die ISPA steht Netzsperren traditionell ablehnend gegenüber, da es sich dabei um eine gleichermaßen überschießende und ineffektive Maßnahme handelt. Die nachfolgenden Bedenken sind daher als Antwort auf die Einladung in den Erläuternden Bemerkungen zu § 36b MedienG gedacht, in der dazu aufgefordert wird zum Thema Netzsperren Stellung zu nehmen.

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

- Bedenken hinsichtlich der technischen Umsetzung von Netzsperren

Einleitend möchte die ISPA darauf hinweisen, dass bislang im Grunde zwei technische Möglichkeiten bestehen, mit welchen Access-Provider Netzsperren umsetzen können.

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, den Zugriff auf einzelne Sub-Domains zu unterbinden, etwa einzelne Foren auf größeren Diskussionsplattformen, ist jedoch grundsätzlich nicht möglich.

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.

Alternativ besteht die Möglichkeit sogenannte IP-Sperren zu setzen. Dabei blockiert der Access-Provider direkt den Zugriff seiner Nutzerinnen und Nutzer auf die IP-Adresse des Servers, auf welchem die inkriminierende Webseite gehostet wird. Da es jedoch häufig vorkommt, dass mehrere voneinander unabhängige Webseiten unter derselben IP-Adresse erreichbar sind, kann die Sperre einer IP-Adresse zu immensen Kollateralschäden führen. Die angedachte Sperre einer einzelnen Webseite kann dabei schnell mehrere hundert – rechtlich gänzlich unbedenkliche – Webseiten miterfassen.

Auf diese Problematik hat auch der Europäische Gerichtshof für Menschenrechte bereits hingewiesen und klargestellt, dass die Sperre einer Webseite mit der gleichen IP-Adresse wie eine als rechtswidrig eingestufte Webseite ohne jegliche Rechtsgrundlage erfolgt und damit unzulässig ist.[1] Um den Anforderungen der Rechtmäßigkeit und Verhältnismäßigkeit zu entsprechen die grundsätzlich an jegliche Grundrechtseingriffe gestellt werden, darf sich eine Sperraufforderung daher jeweils nur auf eine bestimmte Domain beziehen.

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.

- Netzsperren als überschießende Maßnahme gegen Hass im Netz

Aus der technischen Umsetzung von Netzsperren folgt, dass ein Access-Provider in jedem Fall – sowohl mittels DNS als auch IP-Sperre nur den Zugang zu einer gesamten Webseite sperren kann. Bestimmte Inhalte, wie etwa einzelne Videos oder Postings auf einer Webseite, können keinesfalls gesperrt werden, insbesondere auch deshalb, weil Access-Provider keinen Einblick in den Datenverkehr ihrer Kundinnen und Kunden haben, da dies weder rechtlich zulässig wäre – aufgrund der klaren Vorgaben in Art 5 Abs. 1 E-Privacy-RL sowie § 101 TKG – sowie, da rund 95 % des Datenverkehrs verschlüsselt sind.

[1] EGMR Vladimir Kharitonov v. Russia (application no. 10795/14)

Bereits aus diesem Grund stellt sich nach Ansicht der ISPA die offenkundige Frage, inwiefern Netzsperren überhaupt ein geeignetes und verhältnismäßiges Mittel zur Bekämpfung von Hass im Netz darstellen. Denn während sich Hass im Netz anhand bestimmter Inhalte, insbesondere in Textform aber auch in Form von Bildern oder Videos äußert, beziehen sich Netzsperren immer auf eine gesamte Webseite – bzw. deren Domain oder IP-Adresse – als solche.

Wie auch der Europäische Gerichtshof für Menschenrechte wiederholt festgehalten hat, stellt jede Sperre einer Webseite einen erheblichen Eingriff in das Recht auf freie Meinungsäußerung sowohl der Internetnutzerinnen und -nutzer als auch der Webseitenbetreiber dar,[2] der nur dann gerechtfertigt ist, wenn er auf einer klaren rechtlichen Grundlage beruht und gleichzeitig verhältnismäßig zur Erreichung eines der in Art 10 Abs. 2 EMRK genannten Eingriffsziele ist. In diesem Zusammenhang ist festzuhalten, dass zwar der Schutz des guten Rufes oder der Rechte anderer eines der Eingriffsziele in Art 10 Abs. 2 EMRK darstellt, und damit der Schutz der Betroffenen von ehrenverletzenden Postings dem Grunde nach erfasst wäre, die Sperre einer gesamten Webseite, wie etwa eines Blogs, eines Diskussionsforums oder einer Social-Media-Webseite aufgrund einzelner Inhalte zur Erreichung dieses Ziels jedoch klar unverhältnismäßig und überschießend wäre.

Die ISPA fordert den Gesetzgeber daher dazu auf, von der Aufnahme von Netzsperren Abstand zu nehmen, da diese eine gleichermaßen ungeeignete wie auch unverhältnismäßige Maßnahme zur Bekämpfung von Hass im Netz darstellen.

- <u>Eine Sperre lediglich aufgrund einer Abmahnung ist nicht möglich</u>

Sofern Netzsperren dennoch als Mittel zur Bekämpfung von Hass im Netz herangezogen werden – was von der ISPA aus den bereits dargelegten Gründen abgelehnt wird - hat die Rechtsprechung in der Vergangenheit wiederholt darauf hingewiesen, dass ausschließlich die Sperre von strukturell rechtsverletzenden Webseiten zulässig ist.[3] Eine entsprechende Abwägung anhand quantitativer und qualitativer Merkmale ist einem Privatunternehmen, gerade den rund 400 österreichischen kleinen und mittelgroßen Access-Providern die über keine eigene Rechtsabteilung verfügen, jedoch in aller Regel nicht möglich. Die Pflicht eines Access-Providers würde sich auch eklatant von jener des Host-Providers unterscheiden, der nur die offenkundige Rechtswidrigkeit eines einzigen, bestimmten Inhalts prüfen müsste, während ein Access-Provider prüfen müsste ob die gesamte Webseite rechtsverletzend ist.

Bereits aufgrund der Tatsache, dass der Access-Provider eine detailreiche inhaltliche Prüfung der Webseite durchführen müsste, erscheint es unmöglich die Unterlassungshandlung, und damit die Sperre der Webseite, bereits aufgrund einer Abmahnung, also einer formlosen Mitteilung durch eine Privatperson, durchzuführen.

Bestärkt wird dies ferner durch die Vorgaben in Art 3 Abs. 3 UAbs. 3 lit a Telekom-Single-Market

[2] vgl u.a. EGMR Vladimir Kharitonov v. Russia (application no. 10795/14) OOO Flavus and Others v. Russia (application nos 12468/15, 23489/15, and 19074/16), Bulgakov v. Russia (no. 20159/15), and Engels v. Russia (no. 61919/16
[3] vgl u.a EGMR OOO Flavus and Others v Russia, EuGH C-314/12, OGH 4Ob121/17y

Verordnung[4] - die unter anderem der Sicherstellung des freien Informationszugangs im Internet dient - sowie auch den Ausführungen der Telekom-Control-Kommission.[5] Demgemäß darf ein Anbieter eines Internetzugangsdienstes Inhalte nur blockieren sofern sowohl ein gesetzlicher Unterlassungsanspruch tatsächlich besteht oder von einem Gericht festgestellt wurde sowie die ergriffene Maßnahme nicht unverhältnismäßig in die Rechte des Betreibers und des Nutzers eingreift. Eine einfache Abmahnung durch eine Privatperson, die behauptet in ihren Persönlichkeitsrechten verletzt worden zu sein, ist für den Provider daher nicht ausreichend, um die Zulässigkeit einer Sperre im Sinne der TSM-VO zu beurteilen.

Vielmehr muss zunächst geklärt werden, ob der Unterlassungsanspruch, der in der Abmahnung vorgebracht wird, zu Recht besteht. Prüfen Unternehmen den Unterlassungsanspruch selbstständig, riskieren sie dabei jedoch, dass die Regulierungsbehörde im nachgelagerten Aufsichtsverfahren zu einem anderen Ergebnis als der Provider kommt, die Einrichtung der Zugangssperre als rechtswidrig erachtet und daher eine Verwaltungsstrafe iHv bis zu EUR 58 000 ausgesprochen wird.[6] Im Wiederholungsfall ist eine Mindeststrafe iHv von EUR 10 000 je Verstoß vorgesehen. Es folgt somit, dass ein Access-Provider die Unterlassungshandlung stets erst aufgrund einer richterlichen oder behördlichen Unterlassungsanordnung („Sperranordnung“) treffen kann.

Leider führt dieser Umstand jedoch zu weiteren Problemen, denn obwohl dem Access-Provider keine andere Möglichkeit bleibt, als eine gerichtliche oder behördliche Entscheidung abzuwarten, muss dieser dennoch als im Gerichtsverfahren unterliegende Partei am Ende die Gerichtsgebühren und etwaigen Kosten der Rechtsvertretung der anderen Partei übernehmen. Die dabei entstehenden Kosten stellen gerade für kleine und mittelgroße Unternehmen einen erheblichen finanziellen Aufwand dar dem sie auch durch rechtskonformes Verhalten nicht entgehen können.

Im Bereich des Urheberrechts wurde aufgrund von § 81 Abs. 1a UrhG bereits eine solcher Konflikt für die betroffenen Unternehmen geschaffen, in welchem es diesen nicht möglich ist, Rechtssicherheit zu erlangen, ohne hierfür am Ende die Kosten tragen zu müssen. Die ISPA bzw. die ISP-Branche engagiert sich daher sowohl im Sinne der Rechtssicherheit sowie auch der Wahrung der Nutzerrechte bereits seit Jahren für die Erarbeitung eines Lösungsmodells, um diese untragbare Situation aufzulösen. Keinesfalls sollte § 81 Abs. 1a UrhG daher als best-practice Modell zur Umsetzung von Netzsperren herangezogen werden.

- <u>Lösungsmodell</u>

Sollte der Gesetzgeber trotz all der vorgebrachten Bedenken an Netzsperren festhalten, müsste ein Verfahren vorgesehen werden, in welchem ein Access-Provider erst aufgrund einer behördlichen oder gerichtlichen Anordnung zur Sperre einer Webseite aufgefordert werden kann, oder durch eine solche unabhängige Behörde in anderer Art und Weise zuvor die strukturelle Rechtswidrigkeit und Konformität mit den Vorgaben der Netzneutralität in der TSM-VO festgestellt wurde. Als

[4] 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
[5] Telekom-Control-Kommission, 19.08.2019, S 6/19-14 17.
[6] § 109 Abs. 4 Z 10 TKG

naheliegendste Stelle für diese Aufgabe würde die Telekom-Control-Kommission in Frage kommen, die bereits im Entwurf der gesetzlichen Umsetzung der „Verordnung über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden“ im Rahmen des Verbraucherbehördenkooperationsgesetzes (VBKG) als zuständige Stelle vorgesehen wurde.[7]

Um zu gewährleisten, dass ein einheitliches Verfahren gegenüber den betroffenen Zugangsanbietern zur Anwendung kommt, sollten die gesetzlichen Bestimmungen zu Ausgestaltung dieses Verfahrens in dem für die betroffenen Unternehmen anwendbaren Spezialgesetz, dem Telekommunikationsgesetz (TKG), aufgenommen werden. Dabei sollte in jedem Fall auch ein Verweis auf sämtliche andere Spezialnormen aufgenommen werden, gemäß derer Zugangsanbieter zur Sperre von Webseiten verpflichtet werden können, da nur auf diese Weise auch die Anforderungen in Art 3 Abs. 3 TSM-VO nach einer klaren gesetzlichen Grundlage für Netzsperren nach Ansicht der ISPA ausreichend erfüllt wäre. Eine ähnliche klare Auflistung existiert heute bereits in § 99 TKG in Bezug auf die Beauskunftung von Nutzerdaten gegenüber Rechtsdurchsetzungsbehörden, wodurch wesentlich zur Rechtssicherheit beigetragen wird.

Darüber hinaus möchte die ISPA betonen, dass es sich bei der Bekämpfung von Hass im Netz um ein Anliegen des Strafrechtswesen handelt, das nach verfassungsrechtlicher Wertung grundsätzlich Sache des Staates, in diesem Fall des Bundes ist.[8] Bei der Auferlegung gesetzlicher Pflichten zur Einrichtung von Zugangssperren um die weitere Verbreitung strafrechtswidriger Inhalte durch Dritte zu unterbinden handelt es sich somit um die Inpflichtnahme eines privaten Unternehmens zur Erfüllung einer staatlichen Aufgabe, die im Fall anderer Delikte durch die Strafverfolgungsbehörden in der Regel in Form der Einziehung (§ 26 StGB) bzw. Beschlagnahme (§ 115 StPO) erfüllt werden würde. Wie auch der VfGH bereits ausführlich festgestellt hat, ist eine solche Inpflichtnahme Privater jedoch nur dann verhältnismäßig, wenn dem privaten Unternehmen auch die dabei anfallenden Kosten ersetzt werden.[9] Den betroffenen Zugangsanbietern wäre daher ein vollständiger Ersatz der Kosten sowohl für die Einrichtung als auch Aufrechterhaltung der Zugangssperren zu gewähren.

2) Bezüglich der Ausweitung der Ermittlungsmaßnahmen für Privatankläger bestehen erhebliche grundrechtliche Bedenken

Der Gesetzgeber plant in § 71 StPO dem Opfer einer Straftat nach §§ 111 und 115 StGB, die nur auf Verlangen des Opfers zu verfolgen ist (Privatanklagedelikt), zusätzliche Möglichkeiten zur Ausforschung der Täterin bzw. des Täters einzuräumen, sofern die Straftat im Wege einer Telekommunikation oder unter Verwendung eines Computersystems begangen wurde. Das Opfer soll daher die Möglichkeit bekommen beim zuständigen Gericht einen Antrag auf Anordnung von Ermittlungsmaßnahmen nach § 76a, § 110, § 115 oder § 135 StPO zur Ausforschung der bzw. des Beschuldigten zu stellen.

[7] § 7b des Entwurfs eines Bundesgesetzes, mit dem das Verbraucherbehörden-Kooperationsgesetz, das Telekommunikationsgesetz 2003 und das Wettbewerbsgesetz geändert werden
[8] Vgl Art 10 Abs. 1 Z 6 B-VG
[9] Verfassungsgerichtshof, 27.02.2003, G 37/02 ua, V 42/02

Hiervon umfasst wäre somit unter anderem die Auskunft über den Namen und die Adresse der Nutzerin bzw. des Nutzers, dem bzw. der eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war, der die potentiell rechtswidrige Äußerung zuzuordnen ist sowie sogar die Standortdaten des Endgeräts, das hierzu genutzt wurde. Es handelt sich dabei um sensible personenbezogene Daten, welche Access-Provider bislang ausschließlich an Strafverfolgungsbehörden beauskunften, die für die weitere Verarbeitung der Daten einem strikten datenschutzrechtlichen Regime unterliegen.[10] Gerade aufgrund der Sensibilität der Daten wurde darüber hinaus auch ein technisches System zur sicheren Datenübertragung geschaffen, welches die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt („Durchlaufstelle“).[11]

Diese datenschutzrechtlichen Vorgaben würden durch die Gesetzesänderung erheblich unterwandert werden. Denn aufgrund der gesetzlichen Neuerung würden die entsprechenden Daten zwar zunächst weiterhin an Strafverfolgungsbehörden beauskunftet werden. Diese müsste die Daten jedoch umgehend an das Opfer weitergeben, ohne, dass hierfür ein der Durchlaufstelle entsprechendes System genutzt wird. Das Opfer hat im Anschluss die freie Wahl, ob eine Privatanklage erhoben wird oder nicht und unterliegt, abgesehen von den allgemeinen Vorgaben des Datenschutzrechts, keinen weiteren speziellen Verpflichtungen im Umgang mit diesen sensiblen Daten.

Diese Aushebelung des Schutzes bzw. der Sicherheit der betroffenen Nutzerdaten widerspricht nach Ansicht der ISPA eklatant dem bisherigen Umgang mit diesen sensiblen Daten.

Neben der grundsätzlichen Aushebelung der strikten datenschutzrechtlichen Vorgaben welchen Strafverfolgungsbehörden bei der Weiterverwendung der beauskunftete Daten unterliegen wird durch diese neue Bestimmung jedoch auch ganz generell die Anonymität im Internet gefährdet und dadurch die Meinungsvielfalt bedroht.

Denn gerade im Rahmen von Diskussionen zu kontroversiellen Themen können rasch Äußerungen getätigt werden, für die zumindest der Anfangsverdacht einer der beiden erfassten strafbaren Handlungen gegeben ist. Das zuständige Gericht hätte, sofern zumindest ein Anfangsverdacht gegeben ist, auf Antrag des Betroffenen eine Anordnung auf Beauskunftung des Namens und der Adresse des Verfassers der Nachricht an den Access-Provider gemäß §§ 76a Abs. 2, 135 Abs.2 StPO zu stellen, dem dieser umgehend nachzukommen hätte. Aus der analogen Anwendung der §§ 55 u. 104 StPO folgt, dass ein entsprechender Antrag vom Gericht nur in äußerst eingeschränkten Fällen abgewiesen werden kann, etwa wenn die Daten offenkundig zur Ausforschung des Täters ungeeignet wären, der Täter bereits ausgeforscht wurde oder die Auskunft offensichtlich unverhältnismäßig wäre. Eine inhaltliche Prüfung wird jedoch gerade nicht durchgeführt.

Daraus folgt, dass etwa auch nicht beurteilt wird, ob der Strafausschließungsgrund des § 111 Abs. 3 StGB erfüllt wird, da sich die Behauptung als wahr herausstellt. Daher müssten selbst Personen, die rechtmäßig eine andere Person online einer verächtlichen Eigenschaft bezeichnen –

[10] Vgl. Datenschutzgesetz 3. Hauptstück
[11] Vgl § 94 Abs. 2, § 102a – 102c TKG

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

etwa der Korruption, des Rassismus oder ähnlichem – damit rechnen, dass sensible Daten, insbesondere ihre Adresse, an gerade denjenigen offengelegt wird, der (zu Recht) der Eigenschaft bezeichnet wurde.

Darüber hinaus haben auch Personen, die sich im Rahmen von kontroversiellen Diskussionen zu Politik, Religion oder anderen gesellschaftlichen Themen zu Äußerungen im juristischen Graubereich gegenüber anderen Diskussionsteilnehmern hinreißen lassen, umgehend zu befürchten, dass diese Person sich deren Name und Adressdaten beschafft und im schlimmsten Fall für Zwecke der Selbstjustiz verwendet.

Die damit verbundene Angst über die eigene körperliche Unversehrtheit kann bewirken, dass Personen sich in Hinkunft vom öffentlichen Online-Diskurs zurückziehen wodurch gerade jene „chilling" Effekte gefördert werden, denen der Gesetzgeber durch den vorliegenden Gesetzesvorschlag begegnen möchte.

Angesichts der erheblichen Eingriffe in das Recht auf Datenschutz der Person deren Daten beauskunftet werden sowie das Recht auf freie Meinungsäußerung ist es somit auch fraglich, ob eine solche Bestimmung einer verhältnismäßigen Abwägung der involvierten Grundrechte entspricht.[12]

Die ISPA regt daher an, das angedachte Modell zu überarbeiten und weiterhin die sensiblen Daten bei den Strafverfolgungsbehörden zu belassen. Die naheliegendste Möglichkeit um dennoch das Ansinnen des Gesetzgebers umzusetzen, die Rechtsdurchsetzung bei übler Nachrede und Beleidigung im Internet zu erhöhen, wäre es, die relevanten Delikte – sofern sie im Wege der Telekommunikation begangen werden - in Hinkunft als Ermächtigungsdelikte zu definieren, bei welchen das Ermittlungsverfahren bei der Staatsanwaltschaft verbleibt. Einzig aufgrund der Tatsache, dass die notwendigen Ressourcen auf Seiten der Justiz leider fehlen sollten nach Ansicht der ISPA nicht die Grundrechte der Nutzerinnen und Nutzer massiv gefährdet werden.

Sollte dennoch an der vorgeschlagenen Variante festgehalten werden, regt die ISPA an, dass der Privatankläger zwar wie angedacht die entsprechenden Ermittlungsmaßnahmen beantragen kann, die Daten jedoch bei den Strafverfolgungsbehörden verbleiben, bis Anklage erhoben wird. Dadurch würde der Betroffene zwar nicht über die Identität des Verfassers Bescheid wissen, könnte aber dennoch Privatanklage erheben, da die Identität dem Gericht bekannt ist.

Auf diese Weise kann der Gefahr von Selbstjustiz zumindest in Teilen begegnet werden. Gleichzeitig würde dennoch die Rechtsdurchsetzung bei den beiden Delikten gefördert werden, da es im Sinne der Rechtsdurchsetzung nicht darauf ankommt, dass der bzw. die Betroffene die Identität kennt, sondern, dass Privatanklage gegen diese Person erhoben werden kann.

Um die Maßnahme im Sinne der Verhältnismäßigkeit auf das Notwendigste einzuschränken, fordert die ISPA zudem, dass im Gesetzestext die Ermittlungsmaßnahmen in § 135 StPO auf „Ermittlungsmaßnahmen gemäß § 135 Abs. 2 StPO" eingeschränkt werden und dadurch weitere, weitaus intensivere Maßnahmen wie Anlassdatenspeicherung (§ 135 Abs. 2b) sowie

[12] Vgl EuGH 29.01.2020 C-275/06

Inhaltsüberwachung (§ 135 Abs. 3), die zur Ermittlung des Täters nicht notwendig erscheinen, ausgenommen werden.

Die ISPA hofft auf die Berücksichtigung ihrer Bedenken und Anregungen.

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