

An das
Bundesministerium für Justiz
Museumstraße 7
1070 Wien

E-Mail: team.s@bmj.gv.at, team.z@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 SOWIE HINSICHTLICH EINES BUNDESGESETZES, MIT DEM ZIVILRECHTLICHE UND ZIVILPROZESSUALE MAßNAHMEN ZUR BEKÄMPFUNG VON HASS IM NETZ GETROFFEN WERDEN (HASS-IM-NETZ-BEKÄMPFUNGS-GESETZ – HINBG)

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 sowie hinsichtlich eines
- Bundesgesetzes, mit dem zivilrechtliche und zivilprozessuale Maßnahmen zur Bekämpfung von Hass im Netz getroffen werden (Hass-im-Netz-Bekämpfungsgesetz – HiNBG)

wie folgt Stellung zu nehmen:

Zunächst möchte die ISPA darauf hinweisen, dass aufgrund der Wahl des Begriffs „Vermittler“ sowie klaren Verweise in den Erläuternden Bemerkungen zu § 20 Abs. 3 ABGB diese Bestimmung einen neuen Unterlassungsanspruch gegenüber Access-Providern einführt, der in Form von Netzsperrern umgesetzt werden müsste. Die Sperre einer gesamten Webseite stellt jedoch eine unverhältnismäßige und noch dazu ungeeignete Maßnahme gegen Hass im Netz dar, und ist daher abzulehnen. Darüber hinaus fordert die ISPA, dass der Gesetzgeber ein klares Bekenntnis gegen „Upload-Filter“ in die Erläuternden Bemerkungen zu § 20 Abs. 3 ABGB aufnimmt und weist auf die grundrechtlichen Bedenken hinsichtlich der Ausweitung der Ermittlungsmaßnahmen für Privatankläger in § 71 StPO hin.

1) Der neue Unterlassungsanspruch in § 20 Abs. 3 ABGB beinhaltet Netzsperrn

In § 20 ABGB soll der bislang bereits in Literatur und Rechtsprechung anerkannte, aus § 1330 Abs. 2 ABGB abgeleitete, Unterlassungsanspruch aufgrund von Persönlichkeitsrechtsverletzungen normiert werden, der in der Praxis durch die Löschung oder Sperre des inkriminierenden Inhalts technisch umgesetzt wird, wodurch die weitere Verbreitung des rechtsverletzenden Inhalts verhindert wird.

In Abs. 3 soll dieser Anspruch auch auf „Vermittler“ ausgeweitet werden, wobei der Gesetzgeber offenbar der Ansicht ist, dass sich ein entsprechender Anspruch bereits aus der aktuellen Rechtslage ergibt.

Hierzu möchte die ISPA festhalten, dass der Begriff des „Vermittlers“ dem ABGB bislang fremd ist und dieser offenbar aus § 81 Abs. 1a UrhG übernommen werden soll. In den EB wird auch explizit darauf verwiesen, dass die zu dieser Bestimmung ergangene Literatur und Rechtsprechung zur näheren Auslegung des Terminus herangezogen werden soll. Der „Vermittler“ Begriff in § 81 Abs. 1a UrhG entstammt wiederum der RL 2001/29/EG („Urheberrechtsrichtlinie“) und stellt damit einen urheberrechtsspezifischen Begriff dar, der gemäß der Rechtsauslegung durch den EuGH zwingend auch Access-Provider erfasst.¹ Folglich bezieht sich der in Abs. 3 normierte Unterlassungsanspruch gegenüber Vermittlern nicht nur auf Host-Provider, sondern auch auf Access-Provider.

Die Umsetzung des Unterlassungsanspruch durch den Access-Provider unterscheidet sich jedoch erheblich von jener durch den Host-Provider. Während Host-Provider einem Unterlassungsanspruch idR durch Löschung des jeweiligen Inhalts nachkommen, bezieht sich der Anspruch gegenüber Access-Providern – wie auch der EuGH in der Leitentscheidung *UPC Telekabel* festgehalten hat – darauf, dass dieser den Zugang zu einer gesamten – strukturell rechtswidrigen – Webseite unterbindet, um so die weitere Rechtsverletzung zumindest erheblich zu erschweren.² Dabei handelt es sich ganz offensichtlich um eine weitaus gravierendere Maßnahme.

Durch Aufnahme des Begriffs „Vermittler“ in § 20 Abs. 3 ABGB und dem klaren Hinweis in den Erläuternden Bemerkungen darauf, dass zu dessen Auslegung die zu § 81 Abs. 1a UrhG ergangene Judikatur herangezogen werden soll, wird sohin ein neuer gesetzlicher Unterlassungsanspruch auch gegenüber dem Access-Provider geschaffen, den dieser in Form einer Zugangssperre umzusetzen hat. Eine andere Auslegung des Begriffs ist angesichts der klaren Verweise in den Erläuternden Bemerkungen in der vorliegenden Fassung nicht möglich.

Ein solcher Unterlassungsanspruch würde eine erhebliche Änderung gegenüber dem Status Quo bedeuten, in dem Unterlassungsansprüche gegenüber Access-Providern in Form von Netzsperrn ausschließlich im Bereich des Immaterialgüterrechts und aufgrund der Umsetzung von EU-Recht bestehen.

Dem Hinweis in den EB, dass ein Anspruch gegenüber dem „Vermittler“ – und damit gegenüber dem Access-Provider - sich bereits bislang aus dem zivilrechtlichen Ingerenzprinzip ergäbe ist nach

¹ EuGH 19.02.2009, C-557/07

² EuGH 27.03.2014, C-314/12 Rz 63

Ansicht der ISPA nicht zu folgen. Denn dieses würde voraussetzen, dass der Vermittler eine Gefahrensituation geschaffen hat, also „durch pflichtwidrige Handlungen oder Unterlassungen die Voraussetzung dafür schuf, dass der Dritte die Störung begehen konnte“³ Nach Ansicht der ISPA wird eine solche pflichtwidrige Gefahrensituation nicht bereits durch das Angebot einer Zugangsleistung an den jeweiligen Kunden geschaffen und kommt das Ingerenzprinzip daher nicht zur Anwendung.

Darüber hinaus verweist der Gesetzgeber auch darauf, dass der Anspruch gegen einen „Vermittler“ im Sinne des UrhG auch bereits deshalb bestehe, da es einen zivilrechtlichen Unterlassungsanspruch auch gegen den „mittelbaren Störer“ gäbe. Die Haftung des mittelbaren Störers setzt jedoch wiederum die rechtliche Möglichkeit oder Pflicht voraus, den rechtswidrigen Eingriff durch Verbote oder Anweisungen abzustellen. Die bloß faktische (technische) Möglichkeit der Einflussnahme reicht nicht.⁴ Daraus folgt nach Ansicht der ISPA, dass der Access-Provider gerade kein "mittelbarer Störer" ist, gegenüber dem bereits ein Unterlassungsanspruch nach bisheriger Rechtslage besteht. Auch der bislang bereits bestehende Unterlassungsanspruch gegenüber Host-Providern gemäß § 1330 Abs. 2 ABGB entstammt nicht dem Grundsatz der Haftung des mittelbaren Störers, sondern wurde der Host-Provider dabei selbst als unmittelbarer Verbreiter der Inhalte betrachtet.⁵ Der Access-Provider wiederum wurde gerade nicht als unmittelbarer Verbreiter betrachtet.

Der Umstand, dass bislang kein Unterlassungsanspruch gegenüber dem Access-Provider besteht zeigt sich abschließend im Übrigen auch daran, dass bislang keine einzige Abmahnung oder Unterlassungsanordnung gegenüber dem Access-Provider ergangen ist, mit der dieser dazu aufgefordert wurde, die weitere Verbreitung ehrenverletzender Inhalte durch eine Zugangssperre zu verhindern.

Daraus folgt somit, dass anders als vom Gesetzgeber dargestellt, durch § 20 Abs. 3 ABGB ein **neuer Unterlassungsanspruch gegenüber Access-Providern eingeführt werden soll, der in Form von Netzsperrern umgesetzt werden müsste.**

Dies würde jedoch geradezu den Intentionen des Gesetzgebers widersprechen, der in den Erläuternden Bemerkungen zum medienrechtlichen Durchgriffsrecht auf Host-Provider in § 36b MedienG explizit darauf hinweist, dass keine Zugangssperren zur Bekämpfung von Hass im Netz aufgenommen wurden, da dies eine Beschränkung des freien Zugangs zum Internet bedeuten würde.

Sofern es sich hierbei um ein Versehen handelt, der Gesetzgeber also Access-Provider – wie auch im Entwurf zu § 36b MedienG – nicht miterfassen möchte, regt die ISPA daher an, die Terminologie entsprechend anzupassen, und anstelle von „Vermittler“ den Unterlassungsanspruch auf „Hostingdiensteanbieter“ im Sinne de s§ 16 ECG zu beziehen. Durch diese Präzisierung würden weiterhin jene Unternehmen, insbesondere Plattformen, erfasst werden, während Access-Provider und damit Netzsperrern aus dem Anwendungsbereich ausgenommen werden würden.

³ vgl u.a. OGH RS RS0011737

⁴ OGH 7Ob80/17s

⁵ Vgl u.a. OGH 6Ob178/04a

2) Netzsperrern sind kein geeignetes Mittel zur Bekämpfung von Hass im Netz

Die ISPA steht Netzsperrern traditionell ablehnend gegenüber, da es sich dabei um eine gleichermaßen überschießende und ineffektive Maßnahme handelt. Die nachfolgenden Bedenken richten sich daher sowohl gegen die Aufnahme von Netzsperrern in § 20 Abs 3 ABGB, sowie allgemein als Antwort auf die Einladung in den Erläuternden Bemerkungen zu § 36b MedienG zum Thema Netzsperrern zur Bekämpfung von Hass im Netz Stellung zu nehmen.

- Bedenken hinsichtlich der technischen Umsetzung von Netzsperrern

Einleitend möchte die ISPA darauf hinweisen, dass bislang im Grunde zwei technische Möglichkeiten bestehen, mit welchen Access-Provider Netzsperrern 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-Sperrern 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-Sperrern 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.⁶ 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-Sperrern 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.

⁶ EGMR Vladimir Kharitonov v. Russia (application no. 10795/14)

- Netzsperrern als überschießende Maßnahme gegen Hass im Netz

Aus der technischen Umsetzung von Netzsperrern 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.

Bereits aus diesem Grund stellt sich nach Ansicht der ISPA die offenkundige Frage, inwiefern Netzsperrern 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 Netzsperrern 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,⁷ 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 Netzsperrern Abstand zu nehmen, da diese eine gleichermaßen ungeeignete wie auch unverhältnismäßige Maßnahme zur Bekämpfung von Hass im Netz darstellen.

- Eine Sperre lediglich aufgrund einer Abmahnung ist nicht möglich

Sofern Netzsperrern 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.⁸ 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,

⁷ 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

⁸ vgl u.a. EGMR OOO Flavus and Others v Russia, EuGH C-314/12, OGH 4Ob121/17y

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 Verordnung⁹ - die unter anderem der Sicherstellung des freien Informationszugangs im Internet dient - sowie auch den Ausführungen der Telekom-Control-Kommission.¹⁰ 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.¹¹ 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, auf den der Gesetzgeber hier verweist, 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

⁹ 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

¹⁰ Telekom-Control-Kommission, 19.08.2019, S 6/19-14 17.

¹¹ § 109 Abs. 4 Z 10 TKG

§ 81 Abs. 1a UrhG daher als best-practice Modell zur Umsetzung von Netzsperrern herangezogen werden.

- Lösungsmodell

Sollte der Gesetzgeber trotz all der vorgebrachten Bedenken an Netzsperrern 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 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.¹²

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 Netzsperrern 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 Strafrechtswesens handelt, das nach verfassungsrechtlicher Wertung grundsätzlich Sache des Staates, in diesem Fall des Bundes ist.¹³ 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.¹⁴ Den betroffenen Zugangsanbietern wäre daher ein vollständiger Ersatz der Kosten sowohl für die Einrichtung als auch Aufrechterhaltung der Zugangssperren zu gewähren.

¹² § 7b des Entwurfs eines Bundesgesetzes, mit dem das Verbraucherbehörden-Kooperationsgesetz, das Telekommunikationsgesetz 2003 und das Wettbewerbsgesetz geändert werden

¹³ Vgl Art 10 Abs. 1 Z 6 B-VG

¹⁴ Verfassungsgerichtshof, 27.02.2003, G 37/02 ua, V 42/02

3) Upload-Filter sind als unverhältnismäßiger Eingriff in die Nutzerrechte abzulehnen

Während der Unterlassungsanspruch gegenüber Access-Providern wie oben dargestellt nach Ansicht der ISPA neu eingeführt werden würde, besteht ein Unterlassungsanspruch gegenüber dem Host-Provider als technischem Verbreiter der ehrenverletzenden Inhalte bereits schon nach geltender Rechtslage aufgrund von § 1330 Abs. 2 ABGB.

Wie der Gesetzgeber in den Erläuternden Bemerkungen jedoch betont, soll sich dieser Unterlassungsanspruch in Hinkunft nicht nur auf die Beseitigung eines bestimmten Postings beziehen, um dessen weitere Verbreitung zu verhindern, sondern auch darauf, dass in Hinkunft die ehrenverletzenden Inhalte nicht erneut verbreitet werden. Ein solcher Unterlassungsanspruch kann – auch wenn die konkrete Umsetzung dem betroffenen Unternehmen überlassen bleibt – ausschließlich mithilfe von Filtertechnologien umgesetzt werden. Diese würden sämtliche der von einem Host-Provider gespeicherten Informationen bzw. sämtliche Uploads der Nutzerinnen und Nutzer nach wortgleichen bzw. sinngleichen Inhalten¹⁵ untersuchen, und diese umgehend entfernen. Ein anderer Prozess ist bei Plattformen, auf welchen tägliche Ummengen an Inhalten geteilt und hochgeladen werden, nicht möglich.

Der ISPA ist bewusst, dass der Gesetzgeber hiermit der Rechtsprechung des EuGHs in der Rechtsache C-18/18 *Glawischnig-Piesczek* Rechnung tragen möchte, in der gerade die Möglichkeit einer solchen Verpflichtung, die Weiterverbreitung von wort- und sogar sinngleichen Postings, zu verhindern bejaht wurde.

Die ISPA möchte in diesem Zusammenhang jedoch darauf hinweisen, dass der EuGH einzig die Vorlagefrage des OGHs dahingehend beantwortet hat, dass eine Unterlassungsaufforderung, die sich auch auf wort- bzw. sinngleiche Inhalte bezieht, grundsätzlich im Einklang mit dem Verbot allgemeiner Überwachungspflichten für Host-Provider in Art 15 Abs. 1 E-Commerce-RL ist.¹⁶ Das bedeutet, dass der EuGH lediglich festgehalten hat, dass die Gerichte in den Mitgliedstaaten zwar eine entsprechende Unterlassungsaufforderung die sich auf wort- und sinngleiche Inhalte erstreckt verfassen *können*, ohne, dass hierdurch gegen die Vorgaben des E-Commerce-RL verstoßen wird. Keinesfalls ist das Urteil jedoch dahingehend auszulegen, dass eine Unterlassungsaufforderung jedenfalls auch wort- und sinngleiche Inhalte umfassen *muss*. Dies bereits deshalb, da es sich bei dem entsprechenden Unterlassungsanspruch um keine Rechtsnorm handelt, die der Umsetzung von Unionsrecht dient und damit deren konkrete Ausformung auch nicht in einem Vorabentscheidungsverfahren gemäß Art 267 AEUV durch den EuGH beurteilt werden kann.

Es obliegt daher weiterhin dem nationalen Gesetzgeber zu erwägen, ob eine entsprechende gesetzliche Pflicht bzw. deren technische Umsetzung, einen zulässigen Eingriff in die Grundrechte der betroffenen Nutzerinnen und Nutzer darstellt. Denn zum einen wird durch die Pflicht des Host-Providers, sämtliche Informationen der Nutzerinnen und Nutzer nach bestimmten Inhalten zu durchsuchen erheblich in deren Recht auf Privatsphäre eingegriffen, zum anderen, ist aufgrund der

¹⁵ EuGH 03.10.2019 C-18/18

¹⁶ Bereits diese Auslegung ist an sich zu hinterfragen. Denn bei der technischen Umsetzung besteht dem Grunde nach kein Unterschied zwischen der Pflicht sämtliche gespeicherte Informationen zu überwachen – die im Sinne des Art 15 Abs. 1 E-Commerce-RL unzulässig wäre – gegenüber einer Pflicht, sämtliche gespeicherte Informationen nach bestimmten wort- und sinngleiche Inhalte hin zu überwachen.

technischen Defizite von Filtertechnologien, auch den Kontext einer Äußerung mitzubedenken, zu erwarten, dass zahlreiche rechtskonforme Inhalte ebenfalls gelöscht werden. Dies zeigen etwa aktuelle Erfahrungen auf großen Plattformen, wo Beiträge von Opfern rassistischer Beleidigungen, die über ihre Erfahrungen berichteten, gelöscht wurden, weil sie die verwendeten – rechtswidrigen - Wörter wiederholt haben.¹⁷ Gleichermaßen ist zu erwarten, dass auch journalistische Inhalte, die über die entsprechenden Missstände berichten, betroffen wären.

Es liegt am österreichischen Gesetzgeber zu beurteilen ob diese zu befürchteten Auswirkungen verhältnismäßig zum Schutz der Betroffenen sind.

Darüber hinaus möchte die ISPA jedoch darauf aufmerksam machen, dass auch heimische klein- und mittelgroße Unternehmen, sowie auch sämtliche Medienunternehmen, die ein eigenes Diskussionsforum betreiben, diese Pflicht zum Einsatz automatisierter Filtertechnologien umzusetzen hätten. Während große internationale Plattformen den damit verbundenen Aufwand unter Umständen noch stemmen könnten, und zum Teil auch im Ansatz über die dafür notwendige Technologie verfügen, trifft dies mit Sicherheit nicht auf heimische KMUs zu.

Daraus folgt, dass die Bestimmung auch einen erheblich innovationshemmenden Effekt hätte, da KMUs im Verhältnis weitaus stärker belastet werden würden als große, etablierte Plattformen. Dies hätte eine weitere Konzentration des Marktes auf einige wenige Plattformen zu Folge, welche die finanziellen Ressourcen haben die rechtlichen Anforderungen zu erfüllen. Der damit verbundene Verlust der Vielfalt an Diensteanbietern sowie die klar innovationshemmende Wirkung einer solchen Maßnahme für heimische Unternehmen kann nach Ansicht der ISPA auch nicht im Interesse des Gesetzgebers sein. Zudem wären KMUs, für welche die selbstständige Entwicklung der entsprechenden technischen Filtersoftware zu aufwändig wäre, auf Produkte von Dritten angewiesen, um den gesetzlichen Anforderungen entsprechen zu können und wären daher dazu verpflichtet, sämtliche Informationen, die Nutzerinnen und Nutzer hochladen, an ein drittes Unternehmen auszuleiten.

Die ISPA ersucht aus diesem Grund, § 20 Abs. 3 ABGB sowie auch die EB zu dieser Bestimmung und zu § 549 ZPO dahingehend einzuschränken, dass von der Unterlassungsaufforderung jedenfalls nicht der Einsatz von technischen Filtersystemen erfasst ist.

4) 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

¹⁷ https://www.washingtonpost.com/business/economy/for-facebook-erasing-hate-speech-proves-a-daunting-challenge/2017/07/31/922d9bc6-6e3b-11e7-9c15-177740635e83_story.html (zuletzt abgerufen am 28.09.2020)

Beschuldigten zu stellen.

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.¹⁸ 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“).¹⁹

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

¹⁸ Vgl. Datenschutzgesetz 3. Hauptstück

¹⁹ Vgl § 94 Abs. 2, § 102a – 102c TKG

§ 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 – 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.²⁰

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

²⁰ Vgl. EuGH 29.01.2020 C-275/06

„Ermittlungsmaßnahmen gemäß § 135 Abs. 2 StPO“ eingeschränkt werden und dadurch weitere, weitaus intensivere Maßnahmen wie Anlassdatenspeicherung (§ 135 Abs. 2b) sowie 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.