



T-MOBILE AUSTRIA GMBH
A-1030 Wien, Rennweg 97-99

An das
Bundesministerium für Justiz
Museumstraße 7
1070 Wien

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

Wien, 14.10.2020

Stellungnahme der TMA 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-Bekämpfungsgesetz, HiNBG)

Sehr geehrte Damen und Herren,

mit diesem Schreiben nimmt die T-Mobile Austria GmbH (TMA) zum Bundesgesetz, mit dem zivilrechtliche und zivilprozessuale Maßnahmen zur Bekämpfung von Hass im Netz getroffen werden (Hass-im-Netz-Bekämpfungsgesetz – HiNBG), wie folgt Stellung:

Die Schaffung eines neuen Unterlassungsanspruchs gegenüber Access-Providern, die diesen mithilfe von Netzsperrern umzusetzen müssten, ist unbegründet

Die neue Bestimmung des § 20 ABGB zielt darauf ab, den bisher schon in der Rechtsprechung und Literatur anerkannten Anspruch auf Beseitigung und Unterlassung aufgrund von Persönlichkeitsverletzungen zu normieren. Technisch umgesetzt wurde ein solcher Anspruch bisher durch die Löschung oder Sperre des rechtsverletzenden Inhalts, was zur Folge hatte, dass dessen Weiterverbreitung unterbunden werden konnte.

Ein solcher Unterlassungsanspruch soll nun gem § 20 Abs 3 ABGB auch gegenüber sogenannten „Vermittlern“ geltend gemacht werden können. Dies wäre eine erheblich belastende Neuerung für Access-Provider und ein gravierender Einschnitt in die bestehende Rechtslage:

Nach der geltenden Rechtslage ist der Begriff „Vermittler“ nicht im ABGB enthalten und wurde für die Zwecke der vorliegenden Novellierung, wie den Erläuternden Bemerkungen zu entnehmen ist, aus dem § 81 Abs 1a UrhG übernommen. Die Orientierung an dieser Bestimmung wird in den Erläuternden Bemerkungen insbesondere durch den Verweis auf die zu § 81 UrhG ergangene Rechtsprechung und Literatur verdeutlicht, die nach Ansicht des Gesetzgebers zur Auslegung des neuen Begriffs „Vermittler“ herangezogen werden soll. Da § 81 Abs 1a Satz 2 UrhG auf die Bestimmungen der §§ 13 bis 17 ECG verweist und damit sowohl den Access-Provider als auch Host-Provider umfasst, ist davon auszugehen, dass der Begriff des „Vermittlers“ den Access-Provider jedenfalls mitumfasst. Bestätigt wird dies zusätzlich dadurch, dass § 81 Abs 1a UrhG in Umsetzung unionsrechtlicher Vorgaben zum Urheberrecht (RL 2001/29/EG [Urheberrechtsrichtlinie]) erlassen wurde und der EuGH bei der Auslegung des urheberrechtlichen Begriffs „Vermittler“ bereits bestätigt hat, dass dieser zwingend auch Access-Provider mitumfasst (EuGH 19.02.2009, C-557/07). Daraus folgt, dass der Unterlassungsanspruch durch die Novellierung gegenüber Host Providern, jedoch nun auch gegenüber Access Providern, eingeklagt und damit geltend gemacht werden könnte. Im Gegensatz zu Host-Providern, die dem Unterlassungsanspruch in der Regel bereits durch das Löschen des rechtsverletzenden Inhalts nachkommen können, müssen Access-Provider laut einer EuGH Leitentscheidung dafür sorgen, dass der Zugang zu einer gesamten strukturell rechtswidrigen Webseite unterbunden wird. Die weitaus komplexere Umsetzung des Unterlassungsanspruchs belastet den Access-Provider daher wesentlich stärker als den Host-Provider.

In Anbetracht dieser Argumente muss daher festgestellt werden, dass der Gesetzgeber durch diese Novelle ganz eindeutig einen neuen gesetzlichen Unterlassungsanspruch gegenüber dem Access-Provider geschaffen hat, den dieser alleine mittels Zugangssperre umsetzen kann.

Das in den Erläuternden Bemerkungen genannte Argument des Gesetzgebers, wonach der normierte Unterlassungsanspruch gegenüber dem „Vermittler“, konkret also gegenüber dem Access- und Host-Provider bereits aus dem zivilrechtlichen Ingerenzprinzip abzuleiten wäre, kann aus Sicht der TMA nicht bestätigt werden. Damit der Vermittler allerdings als mittelbarer Störer nach dem zivilrechtlichen Ingerenzprinzip in Anspruch genommen werden kann, ist es dennoch notwendig, dass der Vermittler zuvor eine Gefahrensituation geschaffen hat, die auf

seine pflichtwidrige Handlung oder Unterlassung zurückgeht und der Vermittler so insgesamt eine Voraussetzung für einen Dritten geschaffen, die Störung zu begehen (vgl OGH RS RS0011737). Eine solche Gefahrensituation wird nach Ansicht der TMA noch nicht durch das Angebot der Zugangsleistung an Kunden geschaffen. Das Ingerenzprinzip kommt daher nicht zur Anwendung und kann auch nicht als Begründung des Unterlassungsanspruchs gegenüber Access Providern herangezogen werden.

Die zusätzliche in den Erläuternden Bemerkungen angeführte Begründung, wonach der Unterlassungsanspruch gegen den „Vermittler“ zulässig sei, weil gegen den „mittelbaren Störer“ ein zivilrechtlicher Unterlassungsanspruch geltend gemacht werden kann, ist nach Ansicht der TMA ebenfalls kein zutreffendes Argument. Wie in den Erläuternden Bemerkungen angemerkt, ist es für den zivilrechtlichen Unterlassungsanspruch notwendig, dass der „mittelbare Störer“ die tatsächliche und rechtliche Möglichkeit haben muss, die auf ihn zurückgehende, seiner Interessenwahrung dienende, aber unmittelbar von Dritten vorgenommene Störhandlung zu steuern und gegebenenfalls auch zu verhindern. Was jedoch in den Erläuternden Bemerkungen unerwähnt bleibt ist, dass nach der Rechtsprechung des OGH, der „mittelbare Störer“ die rechtliche Möglichkeit oder gar Pflicht haben muss, den Eingriff durch Verbote oder Anweisungen abzustellen (siehe OGH 7Ob80/17s). Die bloß faktische, im Falle von Access-Provider bloß technische, Möglichkeit der Einflussnahme auf den Dritten ist laut OGH nicht ausreichend, um auf Unterlassung geklagt werden zu können. Dieser Begründung zufolge kann ein Access-Provider daher nicht als „mittelbarer Störer“ gelten und ein zivilrechtlicher Unterlassungsanspruch nach aktueller Rechtslage daher nicht gegen den Access-Provider durchgesetzt werden. An dieser Stelle sei auch angemerkt, dass der Unterlassungsanspruch gegen den Host-Provider, der gem § 1330 Abs 2 ABGB möglich ist, ebenfalls nicht auf das Prinzip der Haftung des mittelbaren Störers zurückzuführen ist, sondern darauf, dass der Host-Provider laut OGH (siehe OGH 6Ob178/04a) als unmittelbarer Verbreiter der Inhalte angesehen wird. Hierbei sei angemerkt, dass der Access-Provider gar nicht als unmittelbarer Verbreiter eingestuft wird.

In Anbetracht dieser Argumente lässt sich daher schlussfolgern, dass der Gesetzgeber durch § 20 Abs 3 ABGB einen neuen Unterlassungsanspruch gegenüber Access Providern schaffen will, dem diese mit Hilfe von Netzsperrern nachkommen müssten. Dies stünde im Widerspruch zur Absicht des Gesetzgeber, der in den Erläuternden Bemerkungen zum medienrechtlichen Durchgriffsrecht auf Host-Provider in § 36b MedienG ausdrücklich festlegt, dass Zugangssperren nicht zur Bekämpfung von Hass eingesetzt werden sollen, weil dadurch der freie Zugang zum Internet eingeschränkt würde.

Die TMA fordert den Gesetzgeber daher auf keinen neuen Unterlassungsanspruch gegenüber dem Access-Provider zu schaffen und den Begriff „Vermittler“ durch „Hostingdiensteanbieter“ zu ersetzen. Damit würden Host-Provider, insbesondere Plattformen, weiterhin vom gesetzlichen Anwendungsbereich erfasst und Access-Provider und Netzsperrern ausgenommen sein.

Netzsperrern sind für die Bekämpfung von Hass im Netz nicht geeignet

a) Netzsperrern im Kontext ihrer technischen Unzulänglichkeit im Kampf gegen Hass im Netz

Zu Beginn sollte verdeutlicht werden, dass eine Netzsperrere aus technischer Sicht grundsätzlich entweder in Form einer DNS-Sperre oder einer IP-Sperre umgesetzt werden kann. Vor dem Hintergrund des verfolgten gesetzgeberischen Ziels, das auf die Bekämpfung von Hass im Netz abzielt, muss deutlich darauf hingewiesen werden, dass beide technischen Umsetzungsoptionen schwerwiegende Problematiken aufwerfen und dadurch das verfolgte Ziel verfehlen:

- Bei der DNS-Sperre werden die an den DNS-Server des Access-Providers gerichtete Anfragen, die sich auf eine bestimmte Domain beziehen vom Access-Provider auf eine andere Website umgeleitet oder gar nicht beantwortet. Hierbei kann allerdings nur der Zugriff auf eine gesamte Domain verhindert werden, nicht jedoch der Zugriff auf einzelne Sub-Domains (wie etwa einzelne Foren auf einer Diskussionsplattform). Gleichzeitig können DNS-Sperrern von sowohl von IT-Nutzern (beispielsweise durch die Nutzung eines anderen DNS-Servers) als auch von Betreibern (beispielsweise durch die Änderung der jeweiligen Top-Level-Domain .net anstelle von .org) sehr einfach und mit marginalen IT-Kenntnissen umgangen werden.
- Bei der IP-Sperre hingegen wird vom Access-Provider der direkte Zugriff der Nutzer auf die IP-Adresse des Servers, auf dem die rechtsverletzende Website gehostet wird, blockiert. Dabei können aber oft mehrere voneinander unabhängige Webseiten unter derselben IP-Adresse erreichbar sein, was zu dem ungewollten Ergebnis führt, dass eine IP-Sperre einer einzelnen Webseite ganz häufig mehrere hundert rechtlich vollkommen unbedenkliche Webseiten erfasst und damit blockiert. Der Europäische Gerichtshof für Menschenrechte hat daher in seiner Judikatur (siehe EGMR Vladimir Kharitonov v. Russia (application no. 10795/14)) bereits bestätigt, dass die Sperre einer rechtskonformen Webseite mit der gleichen IP-Adresse wie eine als rechtswidrig eingestufte Webseite rechtsgrundlos erfolgt und damit unzulässig ist. Zusätzlich sollte

betont werden, dass Nutzer eine IP-Sperre sehr einfach durch das Benützen von VPN-Verbindungen umgehen können.

b) Netzsperrern im Kontext ihrer unverhältnismäßigen und ungeeigneten Wirkung

Wie im letzten Absatz verdeutlicht, kann ein Access-Provider mit der Netzsperrre (sowohl mittels DNS- als auch IP-Sperre) nur die gesamte Webseite sperren und nicht einzelne, ausgewählte Inhalte wie Postings, Videos etc. Neben dem technischen Grund, können Access-Provider jedoch auch aus rechtlichen Gründen keine einzelnen Inhalte sperren, da eine Sperre einzelner Inhalte eine nicht zulässige globale Deep Packet Inspection voraussetzen würde (vgl hierfür das EuGH Urteil vom 24.11.2011 Az. C-70/10 „Scarlet Extended SA/SABAM“, wonach Internetanbieter nicht gezwungen werden können den Datenverkehr ihrer Netze inhaltlich zu filtern, um das illegale Herunterladen etwa von Musikdateien zu verhindern). Dies wird auch von BEREC und EDSA¹ bestätigt, wonach es äußerst unwahrscheinlich ist, dass DPI auf rechtmäßige Art und Weise zum Einsatz kommen kann. Das Sperren einzelner Inhalte durch Access-Provider ist darüber hinaus auch durch den Umstand erschwert, dass rund 75% des Datenverkehrs verschlüsselt ist und Access-Provider zusätzlich bereits gemäß der grundsätzlichen Vorgaben des Art 5 Abs 1 E-Privacy-RL keinen Einblick in den Datenverkehr ihrer Kunden haben dürfen. Aus diesen Gründen sind Netzsperrern ein ungeeignetes Mittel, um Hass im Netz entgegenzuwirken, da sich diese Problematik weitgehend in Nutzerbeiträgen, Postings und einzelnen Beiträgen anstatt in der Gesamtheit einer Webseite manifestiert.

Dabei ist gemäß gefestigter Rechtsprechung des Europäischen Gerichtshofs jede Sperre einer Website ein erheblicher Eingriff in das Recht auf freie Meinungsäußerung, sowohl der Internetnutzer als auch der Webseitenbetreiber. Dieser Eingriff ist ausschließlich dann gerechtfertigt ist, wenn er auf einer klaren rechtlichen Grundlage beruht und gleichzeitig die Verhältnismäßigkeit zur Erreichung eines der in Art 10 Abs 2 EMRK genannten Eingriffsziele gewahrt bleibt. Der Schutz des guten Rufes oder der Rechte anderer stellt ein solches Eingriffsrecht dar, weshalb davon ausgegangen werden kann, dass grundsätzlich auch der Schutz vor ehrenverletzenden Postings davon umfasst wäre. Weitgehend unverhältnismäßig und damit unzulässig im Sinne dieser Rechtsprechung wäre hingegen die Sperre einer gesamten Website (wie beispielsweise eines gesamten Diskussionsforums oder einer Social Media Webseite).

¹ EDPB Response to BEREC request for guidance on the revision of its guidelines on net neutrality rules, URL: https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-berec-request-guidance-revision-its-guidelines_de

Die TMA fordert den Gesetzgeber daher auf, zu erkennen, dass Netzsperrern eine ungeeignete und unverhältnismäßige Maßnahme zur Bekämpfung von Hass im Netz sind und daher keinesfalls gesetzlich vorgesehen sein sollten.

c) Netzsperrern im Kontext ihrer unmöglichen Umsetzung in Folge einer bloßen Abmahnung

Sollten Netzsperrern – entgegen der oben dargelegten Ansicht der TMA – trotzdem als eine Maßnahme zur Bekämpfung von Hass im Netz gesetzlich festgelegt werden, so muss deutlich betont werden, dass nach ständiger Rechtsprechung (vgl. ua. EGMR OOO Flavius and Others v Russia, EuGH C-314/12, OGH 4Ob121/17y) die Sperre einer Webseite nur dann zulässig ist, wenn es sich bei der besagten Webseite um eine strukturell rechtsverletzende Webseite handelt. Die Beurteilung der Rechtsfrage, wann ein solches Kriterium der strukturellen Rechtsverletzung erfüllt ist, stellt sich in der Realität als eine häufig unüberwindbare Hürde für Access-Provider heraus. Denn im Gegensatz zu Host-Provider, die nur die offenkundige Rechtswidrigkeit eines einzigen bestimmten Inhalts überprüfen müssen, sind Access-Provider vor die schwerwiegende Aufgabe gestellt, die gesamte Webseite auf das Vorliegen einer strukturellen Rechtsverletzung zu prüfen. Dies kann nur in den seltensten Fällen mit Gewissheit gesagt werden und bindet in der Beurteilung erhebliche zeitliche und personelle Ressourcen innerhalb der Rechtsabteilung des Unternehmens. Besonders belastend ist eine solche Überprüfung für Access-Provider, die nur über eine kleine oder gar keine eigene Rechtsabteilung verfügen. Durch die Notwendigkeit der detailreichen inhaltlichen Prüfung, ist es aus Sicht der TMA daher unmöglich und unzumutbar dem Unterlassungsanspruch und der Webseitensperre bereits aufgrund einer Abmahnung, dh. einer formlosen Mitteilung durch eine Privatperson, nachzukommen.

Die Ansicht, dass eine Webseitensperre nicht lediglich aufgrund einer bloßen Abmahnung durchgeführt werden kann, wird auch durch Art 3 Abs 3 UAbs 3 lit a Telekom-Single-Market Verordnung² sowie durch Ausführungen der Telekom-Control-Kommission³ bestärkt. Diesen Ausführungen zufolge dürfen Inhalte, Anwendungen und Dienste im Internet nur dann von Anbietern von Internetzugangsdiensten blockiert oder eingeschränkt werden, wenn es dafür einen gesetzlichen oder gerichtlich festgestellten Unterlassungsanspruch gibt und die ergriffene Maßnahme nicht unverhältnismäßig in die Rechte des Betreibers und des Nutzers eingreift. Eine formlose Abmahnung durch eine Privatperson ist daher nicht ausreichend, um eine Sperre nach der TSM-VO als zulässig zu erklären. Die Zulässigkeit eines in der

² 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

³ Bescheid der Telekom-Control-Kommission vom 19.08.2019, GZ: S 6/19-14.

Abmahnung vorgebrachten Unterlassungsanspruchs muss vielmehr vom Unternehmen geprüft werden. Dies stellt Unternehmen aber erneut vor erhebliche Risiken, da die Regulierungsbehörde in einem nachgelagerten Aufsichtsverfahren die Zulässigkeit der Errichtung von Zugangssperren anders als das Unternehmen beurteilen kann, was letztlich gem § 109 Abs 4 Z 10 TKG eine Verwaltungsstrafe iHv bis zu EUR 58 000 auslösen kann. Aus diesem Grund kann der Access-Provider die Unterlassung immer nur aufgrund einer richterlichen oder behördlichen Unterlassungsanordnung treffen, die er jedes Mal aufs Neue abwarten muss. Dennoch schützt ein solches Vorgehen den Access-Provider nicht davor, die Gerichtsgebühren und etwaige Kosten der Rechtsvertretung der im Gerichtsverfahren unterliegenden Partei zu übernehmen. Dies bürdet Access-Providern eine enorme finanzielle Last auf, der sie auch durch rechtskonformes Verhalten nicht entgehen können.

Falls der Gesetzgeber trotz der oben genannten Argumente dennoch Netzsperrern als Mittel zur Bekämpfung von Hass im Netz etablieren möchte, so fordert die TMA, dass Access-Provider erst aufgrund einer gerichtlichen oder behördlichen Anordnung zu einer Netzsperrre verpflichtet werden können oder erst nachdem eine unabhängige Behörde das Vorliegen einer strukturellen Rechtswidrigkeit und Konformität mit den Vorgaben der Netzneutralität bestätigt hat. Die TMA regt an, die Telekom-Control-Kommission als eine solche unabhängige Behörde festzulegen, da diese 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. Die damit verbundenen Verfahrenskosten sollten durch das Bundesbudget beglichen werden, da Netzsperrern der Bekämpfung von Hass im Netz dienen und damit im öffentlichen Interesse stehen würden.

Die TMA hofft, dass der Gesetzgeber die in dieser Stellungnahme genannten Aspekte berücksichtigt.

Mit freundlichen Grüßen



T-Mobile Austria GmbH

VP Corporate Affairs