An das
Bundeskanzleramt
IV/6 (Medien, Informationsgesellschaft, Parteienrecht, Parteien- und Parteienakademieförderungen)
Ballhausplatz 2,
1010 Wien

Geschäftszahl: BKA-671.828/0003-IV/6/2019

E-Mail: medienrecht@bka.gv.at, begutachtungsverfahren@parlament.gv.at

Wien, am 20. Mai 2019

ISPA STELLUNGNAHME IM RAHMEN DER ÖFFENTLICHEN KONSULTATION DES BUNDESKANZLERAMTES ÜBER EIN BUNDESGESETZ, MIT DEM EIN BUNDESGESETZ ÜBER SORGFALT UND VERANTWORTUNG IM NETZ ERLASSEN UND DAS KOMMAUSTRIA-GESETZ GEÄNDERT WIRD

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich, in Zusammenhang mit der öffentlichen Konsultation des Bundeskanzleramtes betreffend das Bundesgesetz, mit dem ein Bundesgesetz über Sorgfalt und Verantwortung im Netz (SVN-G) erlassen und das KommAustria-Gesetz geändert wird, wie folgt Stellung zu nehmen:

Zusammengefasst betont die ISPA, dass die Anforderungen an die Diensteanbieter im Entwurf nicht nur unverhältnismäßig, sondern auch widersprüchlich und unklar sind, wodurch ein Verstoß gegen das verfassungsrechtliche Determinierungsgebot vorliegt. Insbesondere widersprechen die im Entwurf enthaltenen Übermittlungspflichten zum Teil den Ausführungen in den Erläuternden Bemerkungen und müssen jedenfalls näher präzisiert werden. Zudem hebt die ISPA hervor, dass eine Differenzierung von auf Österreich ausgerichteten Foren und Kommentarfunktionen bei international tätigen Diensteanbietern nicht möglich ist und daher erhebliche Auswirkungen auf die Nutzung dieser Dienste zu erwarten sind. Darüber hinaus macht die ISPA darauf aufmerksam, dass die vorgesehenen Speicherpflichten Gefahren für den Datenschutz und die Privatsphäre bergen. Ferner droht die angedachte Maßnahme die freie Meinungsäußerung zu beeinträchtigen. Aus Sicht der ISPA ist zudem auch die Wirksamkeit sowie die Erforderlichkeit einer gesetzlichen Registrierungspflicht zu hinterfragen.

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 Anforderungen an die Diensteanbieter im Entwurf sind widersprüchlich und unverhältnismäßig**

Im Zusammenhang mit dem Kampf gegen „Hass im Netz“ möchte der Gesetzgeber eine Ausweispflicht einführen, welche dazu führen soll, dass sich Nutzerinnen und Nutzer eines Online-Forums unter Angabe ihres vollständigen Namens und ihrer Adresse registrieren. Diese Angaben sind vom Diensteanbieter zu verifizieren. Die Nutzerinnen und Nutzer sollen demnach weiterhin unter Angabe eines Pseudonyms auf Online-Plattformen Nachrichten verfassen können, jedoch soll es möglich sein, dass im Fall des Verdachts eines strafrechtlich relevanten Postings Rechtsdurchsetzungsbehörden ein Auskunftsersuchen an den Diensteanbieter richten können, welcher die registrierten Daten zu dieser Nutzerin bzw. diesem Nutzer beauskunften muss.

Es ist darauf hinzuweisen, dass es sich dabei um eine Registrierungs- und Authentifizierungspflicht für sämtliche Nutzerinnen und Nutzer von Online-Plattformen handelt und nicht um ein „Vermummungsverbot“, wie medial dargestellt. Die Maßnahme richtet sich konkret an Dienstanabieter, welche als Bestandteil des Dienstes selbst ein Diskussionsforum einrichten und betreiben, das auf Nutzerinnen und Nutzer in Österreich ausgerichtet ist, oder die ergänzend zu ihrem Informationsangebot auch die Funktion eines Forums entweder selbst bereitstellen oder ihren Nutzerinnen und Nutzern die Möglichkeit einräumen, gleichsam zur Kommentierung der online angebotenen Informationen ein Forum einzurichten. In diesem Zusammenhang ist es nach Ansicht der ISPA verwunderlich, dass die entsprechende Verpflichtung nur Plattformen einer bestimmten Größenordnung treffen soll, da der von der Regierung kritisierte „Hass im Netz“ nicht nur auf große Plattformen beschränkt ist, sondern gerade auch auf einigen kleineren Plattformen zu finden ist, welche die Gesetzesanforderungen nicht erfüllen.

Aus Sicht der ISPA ist der Entwurf mit zahlreichen Mängeln und Widersprüchen behaftet, welche schließlich nur zu Rechtsunsicherheit und Intransparenz sowohl für die betroffenen Dienstanbieter als auch für die Nutzerinnen und Nutzer führen werden. In den Erläuterungen wird einerseits festgehalten, dass der Diensteanbieter nur bei begründetem Verdacht, dass die Registrierungsangaben unrichtig sind oder wurden (etwa, weil das Registrierungsprofil nicht mehr eindeutig zuordenbar ist), die Nutzerin bzw. den Nutzer zum Nachweis der Richtigkeit der Angaben aufzufordern hat. Eine bloße Vermutung soll nicht ausreichend sein. Andererseits ist jedoch der Diensteanbieter aufgefordert, durch routinemäßig periodisch vorgenommene Überprüfungsvorgänge nicht nur längere Inaktivität festzustellen, sondern auch die Richtigkeit der Daten zu hinterfragen. Diese widersprüchlichen Anforderungen an den Diensteanbieter, einerseits nur im Anlassfall die Angaben der Nutzerin bzw. des Nutzers zu authentifizieren, aber dennoch periodisch und routinemäßig die Richtigkeit der Daten zu hinterfragen, sind in der Praxis nicht miteinander zu vereinbaren und führen nur zu Rechtsunsicherheit beim Rechtsanwender.

Ferner ist laut Erläuterungen die gesetzlich angeordnete Speicherung der Nutzerdaten nicht dahingehend zu interpretieren, dass sie einen Rechtfertigungsgrund für eine dauerhafte Speicherung bzw. Verarbeitung sämtlicher Daten darstellt, die dem Dienstanbieter im Wege der Registrierung bekannt werden. Dennoch enthält der Entwurf keine Angaben darüber, wie lang die Daten, welche gegebenenfalls bei einer Auskunftsanfrage zu übermitteln wären, nämlich Name und Anschrift, aufzuheben sind. Abgesehen von der Inaktivität eines Profils oder bei

Geltendmachung des Rechts auf Löschung gemäß Art. 17 DSGVO sind keine Schranken im Entwurf vorgesehen, die der uneingeschränkten Speicherung dieser Daten entgegenstehen würden. Sollte daher eine Nutzerin bzw. ein Nutzer zwanzig Jahre lang in einem Forum aktiv sein, bedeutet das, dass seine bzw. ihre Namen und Anschrift auch zwanzig Jahre lang vom Diensteanbieter zu speichern sind.

Zudem sind die aufgestellten Kriterien im Gesetzesentwurf, ab wann ein Registrierungsprofil als inaktiv gilt, um gegebenenfalls die Löschung dieses veranlassen zu können, aus Sicht der ISPA ausufernd und unverhältnismäßig. Der Diensteanbieter hat ein Registrierungsprofil erst nach einer längeren Periode der Inaktivität, wobei hier der Zeitraum von einem Jahr in den Erläuterungen festgelegt wird, zu löschen. Dabei ist es nicht erforderlich, dass der Poster regelmäßig Postings veranlasst, um als aktiv zu gelten, sondern es wäre ausreichend, wenn die registrierte Nutzerin bzw. der Nutzer einfach das Online-Informationsangebot nutzt, indem sie oder er beispielsweise nur hin und wieder einen Zeitungsartikel liest. Daher würde dieser misslungene Versuch des Gesetzgebers eine Speicherminimierung der Nutzerdaten auf Grund von Inaktivität eines Registrierungsprofils herbeizuführen, in der Praxis keine Wirkung haben, da die Anforderungen für die Feststellung der Inaktivität eines Profils zu hoch angesetzt sind.

Hinsichtlich der konkreten Maßnahme zur Identifizierung der Nutzerin bzw. des Nutzers wird in den Erläuterungen ausgeführt, dass die gesetzlichen Anforderungen u.a. jedenfalls dann erfüllt sind, wenn die für die Rechtsverfolgung notwendigen Daten mittels 2-Faktor Authentifizierung mit Mobiltelefonnummer bestätigt werden. Es stellt sich dabei jedoch die Frage, wie mit ausländischen Nutzerinnen und Nutzern, etwa Auslandsösterreicherinnen und -österreichern oder anderen deutschsprachigen Nutzerinnen und Nutzern bspw. aus Deutschland oder der Schweiz, welche sich an Diskussionen in österreichischen Medien beteiligen wollen, umgegangen werden soll, da diese in der Regel über keine österreichische Rufnummer verfügen. Es ist zu erwarten, dass eine Einschränkung der Plattformen auf Nutzerinnen und Nutzer, welche über eine österreichische Rufnummer verfügen, wiederum zu Einschnitten in der Meinungsvielfalt auf diesen Plattformen führt.

Daher lehnt die ISPA die im Entwurf angedachten Maßnahmen und die Anforderungen an die Diensteanbieter strikt ab. Diese sind unverhältnismäßig und widersprechen zudem klar den Prinzipen der Speicherminimierung und Datenminimierung in Art. 5 DSGVO. Die Anforderungen an die Diensteanbieter sind zudem in der Praxis nicht miteinander zu vereinbaren und führen zu Rechtsunsicherheit. Angesichts der noch näher auszuführenden erheblichen Grundrechtseingriffe welche dieses Gesetz bewirkt ist darauf hinzuweisen, dass ein derart unpräzises und widersprüchliches Gesetz jedenfalls gegen das Determinierungsgebot gemäß Art 18 Abs. 1 B-VG verstößt, welches erfordert, dass der jeweilige Eingriffstatbestand besonders präzise umschrieben wird.[1]

[1] VfGH VfSlg. 10.737/1985, 11.455/1987

2. Die Ausführungen hinsichtlich der Übermittlungsverpflichtungen sind unklar

Laut § 4 SVN-G hat der Diensteanbieter Vorname, Nachname sowie die Adresse des Posters einer dritten Person bzw. kriminalpolizeilichen Behörden, Staatsanwaltschaften und Gerichten auf deren begründetes schriftliches Verlangen bekannt zu geben. Bezüglich des in den Erläuterungen angegebenen Grund, wonach diese Bestimmung als „Mehrwert" gegenüber der derzeitigen Rechtslage in § 90 Abs. 7 TKG zu sehen ist, muss zunächst darauf hingewiesen werden, dass Anbieter von Diensten der Informationsgesellschaft in der Regel nicht unter das Telekommunikationsgesetz fallen, welches ausschließlich für Betreiber von Kommunikationsnetzen bzw. -diensten gilt. Die entsprechenden Pflichten der Diensteanbieter finden sich vielmehr in § 18 E-Commerce Gesetz, wonach dieser bereits bislang nach Anordnung des zuständigen Gerichts zur Herausgabe von Nutzerdaten verpflichtet ist (Abs. 2), bzw. auch gegenüber Dritten Name und Adresse eines Nutzers offenlegen muss „*sofern dieser ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers und eines bestimmten rechtswidrigen Sachverhalts* [hat] *sowie überdies glaubhaft machen [kann], dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet*". (§ 18 Abs. 4 ECG). Es erscheint daher unklar, in welchem Verhältnis § 4 des Entwurfs und § 18 E-Commerce Gesetz zu sehen sind, da auf dies vom Gesetzgeber an keiner Stelle eingegangen wird.

Sofern angesichts des grundsätzlich gleichen Regelungsinhaltes die Grundsätze der bisherigen Rechtsprechung zu § 18 Abs. 4 ECG übernommen werden ist ferner darauf hinzuweisen, dass es bislang ausreicht, dass eine Privatperson glaubhaft macht, dass eine Verurteilung des potentiellen Verletzers „*nicht gänzlich auszuschließen*" ist.[2] Der vom Gesetzgeber angenommene Umstand, eine solche Herausgabe von Daten würde nur „*ausnahmsweise*" erfolgen ist daher verfehlt. Angesichts der Tatsache, dass eine Beauskunftung des Diensteanbieters gemäß dem vorliegenden Gesetzesentwurf nicht nur mögliche detailreiche Einblicke in das Privatleben der Nutzerin bzw. des Nutzers gewährt, sondern darüber hinaus auch deren private Wohnadresse umfasst, drohen gerade Personen, die sich an sensiblen Debatten beteiligen, gravierende negative Auswirkungen bis hin zu Gefährdung der eigenen Sicherheit. Daher sollten im Gesetz darüber hinaus auch Anforderungen zur Identifizierung der Privatperson welche eine Auskunft nach § 4 Abs. 2 begehrt, aufgenommen werden sowie auch eine Strafbestimmung für missbräuchliche Inanspruchnahme dieses Rechts, um etwa unzulässige private Nachforschungen zu unterbinden.

Andererseits wird in den Erläuterungen darauf verwiesen, dass der Betreiber eines Telefondienstes – sofern dieser offenbar im Wege der 2-Faktor-Authentifizierung herangezogen wurde – die von diesen verarbeiteten Stammdaten des Posters zu beauskunften hat. Wiederum erscheint das Gesetz in diesem Punkt äußerst unklar, da der Gesetzestext selbst eine Beauskunftung von Namen und Adresse durch den Diensteanbieter selbst vorsieht. Ferner ist darauf hinzuweisen, dass es Betreibern von Kommunikationsdiensten im Sinne des TKGs auch weiterhin untersagt ist, Stammdaten an Privatpersonen zu beauskunften, da sich deren Auskunftspflichten hinsichtlich Stammdaten ausschließlich nach § 90 TKG richten. Für eine

[2] Vgl u.a. OGH 30.01.2017, 6Ob188/16i

Weitergabe von Stammdaten an Private durch die Telekombetreiber wäre daher eine klare gesetzliche Grundlage in das TKG aufzunehmen.

Zudem sind die Telekommunikationsbetreiber gemäß der Identifizierungsverordnung (IVO) verpflichtet den Titel, Name und Geburtsdatum des Nutzers zu erfassen und durch ein entsprechendes Verfahren, das den Anforderungen der IVO entspricht, zu verifizieren. Das SVN-G zielt jedoch auf den Namen und die Adresse des Users ab. Nach aktueller Rechtslage sind Telekombetreiber nicht verpflichtet die Adresse des Kunden auf ihre Korrektheit zu überprüfen, daher würde eine derartige Anforderung, wie im SVN-G vorgesehen, nicht mit der IVO im Einklang stehen. Sollte es sich bei der Registrierungspflicht, gleich wie im Fall der Identifizierungspflicht gemäß der IVO, um einen hoheitlichen Akt handeln, würde die Authentifizierung im Sinne des SVN-G ferner eine Amtshandlung darstellen. Dementsprechend könnte eine fehlerhafte Authentifizierung strafrechtliche Folgen für den Bertreiber nach sich ziehen. Eine diesbezügliche Klarstellung, welche eine derartige Inanspruchnahme des Betreibers ausschließt, ist im Entwurf daher unbedingt erforderlich.

Bei begründeten Hinweisen, dass durch den Inhalt eines Postings der objektive Tatbestand der üblen Nachrede oder der Beleidigung erfüllt worden sein könnte oder dass der Inhalt sonst den konkreten Verdacht einer Straftat begründen könnte, hat der Diensteanbieter zudem von dem betreffenden Posting eine Aufzeichnung herzustellen, die eine vollständige und originalgetreue Wiedergabe ermöglicht. Aus dieser Verpflichtung geht jedoch nicht klar hervor, ob ein begründeter Hinweis erst bei einem begründeten schriftlichen Verlangen iSd Abs. 1 leg. cit. besteht und sollte jedenfalls näher erläutert werden. Fraglich erscheint darüber hinaus insbesondere, wie die Bestimmung, bei Diensteanbietern dürfe keine Verknüpfung zwischen der Identität eines Posters und dem Inhalt eines Postings vorgenommen werden, zu interpretieren ist. Dies widerspricht offensichtlich der Anforderung an den Betreiber, selbst Name und Adresse zu einem bestimmen Poster aufzubewahren, um diese auf Verlangen an Berechtigte herauszugeben. Sofern diese Daten beim Betreiber vorliegen, ist zumindest eine indirekte Verknüpfung mit den Postings, welche ebenfalls auf der vom Diensteanbieter betriebenen Plattform gespeichert werden, unmöglich auszuschließen. Zudem fehlen dem Gesetz jegliche Anhaltspunkte hinsichtlich einer maximal zulässigen Aufbewahrungsfrist solcher Aufzeichnungen obwohl der Gesetzgeber verpflichtet wäre, gemäß Art 6 Abs. 3 DSGVO in Gesetze welche die Verarbeitung bzw. Aufbewahrung personenbezogener Daten betreffen Angaben zur maximal zulässigen Speicherfrist aufzunehmen. In diesem Zusammenhang ist es ebenso unklar, ob eine Löschung des Registrierungsprofils gemäß § 3 Abs. 6 SVN-G bzw. ein Löschbegehren gemäß Art 17 DSGVO auch zu einer Löschung solcher Aufzeichnungen führt.

Abschließend ist darauf hinzuweisen, dass mit dem vorliegenden Gesetz eine Mitwirkungspflicht privater Unternehmen – sowohl der unter das Gesetz fallenden Diensteanbieter als auch der Telekombetreiber – an einer staatlichen Aufgabe, der Strafverfolgung, vorgesehen wird. In solchen Fällen ist gemäß ständiger Rechtsprechung des Verfassungsgerichtshofs hinsichtlich der Kostentragung jedenfalls der Verhältnismäßigkeitsgrundsatz zu beachten.[3] Die ISPA fordert daher, dass zumindest 80 % der anfallenden Kosten für den technischen Aufwand sowie der

[3] Verfassungsgerichtshof 27.02.2003, G 37/02 ua, V 42/02

Personalkosten durch den Bund übernommen werden. Dies beinhaltet sowohl die Kosten für die Umsetzung und laufende Überprüfung der Registrierungspflicht sowie auch den Aufwand im Rahmen der Beauskunftung von Nutzerdaten, sowohl des Diensteanbieters als auch des Telekombetreibers.

3. Die Unmöglichkeit der Differenzierung von „auf Österreich ausgerichteten" Foren führt zu erheblichen Einschnitten in die Nutzung dieser Dienste

Gemäß § 3 Abs. 1 SVN-G sind vom Anwendungsbereich des Gesetzes sowohl Diensteanbieter erfasst, welche ein Forum einrichten und betreiben, das „auf Österreich ausgerichtet ist" sowie auch jene welche die „Einrichtung eines solchen Forums durch ihre Nutzerinnen und Nutzer ermöglichen". Der Gesetzestext selbst bietet jedoch keine Anhaltspunkte oder eine Definition, wann ein Forum „auf Nutzer in Österreich" ausgerichtet" ist. Unzulänglich sind in dieser Hinsicht auch die Ausführungen in den Erläuterungen wonach ein Forum erfasst wird das „durch den Inhalt, die Zielgruppe, [oder] die Sprache als auf Nutzer in Österreich ausgerichtet" ist sowie „einen Marktplatz für den Meinungsaustausch in Österreich einräumt."

Solche allgemeinen Ausführungen führen gerade bei international agierenden Diensteanbietern, welche im Rahmen ihres Online-Informationsangebotes sowohl auf die österreichische Zielgruppe ausgerichtete Inhalte als auch international ausgerichtete Inhalte mit entsprechender Kommentar oder Forenfunktion anbieten, bzw. einen solchen „Marktplatz für den Meinungsaustausch" sowohl für Österreich als auch andere Länder anbieten, zu erheblicher Rechtsunsicherheit.

Gerade da auch die Einrichtung von Foren durch Nutzerinnen und Nutzer vom Gesetzesentwurf erfasst wird, hätte dies im Endeffekt eine gänzliche Inhaltsüberwachung solcher Foren durch den Diensteanbieter zur Folge, damit der Diensteanbieter feststellen kann ob ein solches durch einen Nutzer bzw. eine Nutzerin eröffnetes Forum „auf Nutzer in Österreich ausgerichtet ist". Speziell ist hierbei darauf hinzuweisen, dass der Gesetzgeber in § 3 Abs. 2 SVN-G als Anwendungsschwelle 100.000 im Inland registrierte Nutzer des jeweiligen Dienstes festsetzt und nicht von tatsächlichen Nutzern (bzw. „Postern") in dem jeweiligen Forum ausgeht. Das bedeutet, dass bereits ein einziges durch eine Nutzerin bzw. einen Nutzer oder den Diensteanbieter eingerichtetes „auf Österreich ausgerichtetes" Forum bzw. eine Kommentarfunktion, den Anwendungsbereich auslöst, sofern der Dienst an sich mehr als 100.000 registrierte Nutzerinnen und Nutzer in Österreich hat.

Selbst unter der Annahme, dass dem Diensteanbieter eine solche Überwachung der durch Nutzer erstellten Foren und Kommentarfunktionen möglich wäre und trotz des Verbots der Inhaltsüberwachung in Art 15 E-Commerce RL[4] dies auch rechtlich zulässig wäre, müsste demnach ein Anbieter, welcher bereits ein einziges solches auf Österreich gerichtetes Forum einrichtet bzw. dies seinen Nutzern ermöglicht, nicht nur österreichische Nutzerinnen und Nutzer sondern sämtliche weltweiten Nutzerinnen und Nutzer des Dienstes – und nicht nur des Forums -

[4] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr") OJ 178/1

identifizieren, da sich diese an den jeweiligen „auf Österreich ausgerichteten“ Diskussionen beteiligen könnten. Ein solcher Effekt ist offensichtlich klar überschießend.

Andernfalls, sofern der Gesetzgeber davon ausgeht, dass der Diensteanbieter eine Registrierung auf entsprechende „auf Österreich ausgerichtete“ Foren oder Kommentarfunktionen reduzieren kann und daher sämtliche registrierte Nutzerinnen und Nutzer des Dienstes von der Kommentierung ausschließen könne, ist darauf hinzuweisen, dass eine solche Trennung gerade auf Plattformen, auf welchen gleichermaßen auf Österreich gerichtete sowie auch international ausgerichtete Inhalte geteilt werden und eine Kommentar- oder Bewertungsfunktion eingerichtet ist, in der Praxis in der Regel nicht möglich ist, speziell sofern es sich dabei um von Nutzerinnen und Nutzern eingerichtete Kommentarfunktionen zu Beiträgen handelt. Wiederum ist darauf hinzuweisen, dass dies eine de-facto Inhaltsüberwachung der von Nutzerinnen und Nutzern eingerichteten Foren zur Folge hätte.

Als einzig durchführbare Maßnahme um eine solche Differenzierung zu ermöglichen, müssten Diensteanbieter letztlich Nutzerinnen und Nutzer in Österreich gänzlich von der Kommentierung von Beiträgen ausschließen, sofern sich diese nicht registriert bzw. authentifiziert haben, da vom Diensteanbieter angenommen werden müsste, dass sich ein in Österreich befindlicher Nutzer – sofern dies bestimmbar ist – auch an auf Österreich ausgerichtete Diskussionen beteiligen würde.

Damit würden etwa auch Touristinnen und Touristen sobald deren Endgeräte dem Diensteanbieter den Standort „Österreich“ übermitteln, nicht mehr auf diesen Plattformen tätig sein können. Der hierdurch zu erwartende gravierende Image-Schaden für Österreich ist evident und würde erhebliche Auswirkungen auf die heimische Tourismus- und Kongresswirtschaft nach sich ziehen, welche 7 % zum Bruttoinlandsprodukt beitragen,[5] da ein entsprechend restriktives Land klar an Attraktivität einbüßen wird.

Die ISPA weist zudem darauf hin, dass auch Online-Communities von dem Gesetz erfasst sein würden, da die Erfüllung der Kriterien z.B. durch Wikipedia Österreich durchaus realistisch ist[6]. Eine Registrierungspflicht für z.B. Wikipedia Österreich würde dem Grundgedanken der freien Wissensvermittlung geradezu entgegenstehen und im *worst case* zu einer Schädigung dieses historisch einzigartigen Projektes, welches einen Grundpfeiler für die Dokumentation und die Weitergabe von Wissen sowie der Wahrung der österreichischen Kultur und Identität darstellt, durch den österreichischen Gesetzgeber führen.

[5] Bundesministerium für Nachhaltigkeit und Tourismus „Tourismus und Freizeitwirtschaft 2017“ (Oktober 2018) S. 25
[6] Wikimedia, Wikimedia Jahresbericht 2017/2018, https://mitglieder.wikimedia.at/images/d/d9/WMAT-Jahresbericht_2017-18.pdf S 7.

4. Die gesetzlichen Speicherpflichten stellen einen unverhältnismäßigen Eingriff in das Recht auf Privatsphäre dar

Obwohl es sich bei den zu registrierenden Namen oder Adressen zunächst um keine Daten handelt, mittels derer sensible Rückschlüsse auf das Privatleben der Nutzerinnen und Nutzer möglich sind, ist zu berücksichtigen, dass jeweils darauf abzustellen ist, welche Rückschlüsse auf das Privatleben aus der Gesamtheit der Daten gewonnen werden können.[7] Gerade im Fall von Online-Medien werden oftmals politische und gesellschaftliche Diskussionen zu polarisierenden und zum Teil sensiblen Themen geführt. Nutzerinnen und Nutzer geben dabei sensible Daten preis, etwa zu ihrer politischen oder religiösen Überzeugung sowie zu ihrer sexuellen Orientierung. All diese Informationen, welche bislang anonym waren, wären zukünftig auf einzelne identifizierbare Personen rückführbar. Dem vom Gesetzgeber vorgebrachten Argument, wonach von einer Aufhebung der Anonymität „*keine Rede*“ sein kann, ist damit klar zu widersprechen, da es für die Frage, ob es sich um personenbezogene Daten handelt relevant ist, ob sich die Daten auf eine „*identifizierbare*“ Person beziehen. Da gerade die Identifizierbarkeit der Nutzerinnen und Nutzer der Kern des vorgesehenen Gesetzesvorhabens ist, ist die Aufhebung der Anonymität der Daten sohin evident.

Ein solcher Eingriff in das Recht auf Privatsphäre gemäß Art 8 EMRK, selbst wenn dieser dem Schutz der Rechte Dritter, und somit derer, die von Hasspostings betroffenen sind, dient, ist nur dann zulässig, wenn dieser verhältnismäßig ist. Hierzu müssen die involvierten Interessen gegeneinander abgewogen werden. Das bedeutet im vorliegenden Fall jedoch nicht, den Schutz der Rechte der Betroffenen lediglich dem Eingriff in das Recht auf Privatsphäre der Verfasserinnen und Verfasser von Hasspostings gegenüberzustellen, sondern vielmehr dem Eingriff in das Recht aller Nutzerinnen und Nutzer der Plattform. Angesichts der Breitenwirksamkeit und Schwere des Eingriffs sowie auch der mangelnden Wirksamkeit, welche unten noch näher ausgeführt wird, ist zu bezweifeln, dass der Grundsatz der Verhältnismäßigkeit gewahrt ist.

Die Verpflichtung zur Erhebung zusätzlicher personenbezogener Daten sowie der Umstand, dass hierdurch Daten, die bislang anonym gespeichert wurden, nunmehr einen Personenbezug aufweisen, widerspricht zudem klar den Prinzipen der Speicherminimierung und Datenminimierung in Art. 5 DSGVO, durch welche unter anderem die Risiken für die Rechte und Freiheiten der Nutzerinnen und Nutzer geringgehalten werden sollen. Speziell durch die Verknüpfung der sensiblen Informationen mit identifizierbaren Nutzerinnen und Nutzern wird für diese ein enormes Risiko geschaffen, dass aufgrund einer Datenpanne oder eines Hacking-Angriffs äußerst sensible und detailreiche Informationen nach außen bzw. in unbefugte Hände geraten können. Es ist fraglich, ob das hierdurch geschaffene Risiko mit dem potentiellen Nutzen dieser Maßnahme im Verhältnis steht.

[7] EuGH 16.5.2014, C-293/12, Digital Rights Ireland Rz 27, EuGH 21.12.2016, C 203/15 Tele2 Sverige Rz 99

5. Die angedachte Registrierungspflicht droht die freie Meinungsäußerung zu beeinträchtigen

Das Internet ist heute eines der zentralen Mittel zur Ausübung der Meinungsfreiheit. Jede noch so kleine Veränderung kann daher weitreichende Folgen mit sich ziehen und sollte vorab genauestens evaluiert werden, um nachteilige Auswirkungen, die in keinem Verhältnis zum erzielten Nutzen stehen, hintanzuhalten. Aus Sicht der ISPA stellt die angedachte Registrierungspflicht einen bedeutenden Eingriff in das Recht der Meinungsfreiheit dar.

Neben der Bedeutung für den Datenschutz und den Schutz der Privatsphäre ist die anonyme Nutzung der betroffenen Dienste auch eine wichtige Voraussetzung für die Gewährleistung der Meinungsfreiheit und -vielfalt, da gerade jene Nutzerinnen und Nutzer, welche für eine offene Kommunikation ihrer Gedanken erhebliche Konsequenzen fürchten müssten, eher unter dem Schutz der Anonymität hierzu bereit sind. Selbst im Zusammenhang mit dem „analogen" Vermummungsverbot wurde diese Notwendigkeit der Anonymität in bestimmten Situationen anerkannt, indem in den entsprechenden Gesetzesmaterialien festgehalten wurde, dass eine Ausnahme vom Vermummungsverbot „*insbesondere dann angezeigt sein* [wird], *wenn in besonders gelagerten Fällen ein berechtigtes Interesse etwa ausländischer Demonstrationsteilnehmer besteht, die Repressalien gegen Angehörige in ihrem Heimatstaat befürchten müssen*."[8] Die gleichen Bedenken bestehen hinsichtlich der Teilnahme solcher Personen an Diskussionen auf Online-Plattformen, sofern diese etwa durch einen Hacking-Angriff identifiziert werden. Dies kann äußerst negative Folgen für diese nach sich ziehen, die weit über jene von Hasspostings hinaus gehen.

Generell ist anzunehmen, dass aufgrund dieser Gefahr, dass im Zuge von Datenpannen oder Datendiebstählen die Klarnamen der Nutzerinnen und Nutzer samt deren Nachrichten in unbefugte Hände geraten, speziell jene Nutzerinnen und Nutzer, die ein starkes Interesse an der Geheimhaltung von sensiblen Informationen über ihr Privatleben haben, eher davor zurückschrecken werden, weiterhin an den Diskussionen teilzunehmen, wodurch die Vielfalt der Meinungen speziell zu polarisierenden Themen erheblich eingeschränkt wird. Ein solcher „chilling effect", d.h. dass Nutzerinnen und Nutzer ihre Meinungsfreiheit selbst beschränken aufgrund drohender negativer Konsequenzen, sollte jedenfalls vermieden werden, da dies in keinem Verhältnis zum potentiellen Nutzen steht. Die Bedeutung der Anonymität der Nutzerinnen und Nutzer für das Recht auf freie Meinungsäußerung im Internet wurde auch durch den UN-Sonderberichterstatter für Meinungsfreiheit betont, welcher sich klar gegen gesetzliche Maßnahmen, welche die Identifizierung der Nutzerinnen und Nutzer vorschreiben, ausgesprochen hat.[9]

Auch der deutsche Bundesverfassungsgerichtshof hat durch einen Nichtannahmebeschluss ein Urteil des deutschen Bundesgerichtshofs bestätigt, in dem dieser festgehalten hat, dass eine Beschränkung der Meinungsäußerungsfreiheit auf solche Äußerungen, die einem bestimmten

[8] 680/A XXI.GP Antrag der Abgeordneten Dr. Andreas Khol, Ing. Peter Westenthaler, Kolleginnen und Kollegen betreffend ein Bundesgesetz, mit dem das Versammlungsgesetz 1953 geändert wird

[9] United Nations, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2015) A/HRC/29/32 s. 20

Individuum zugeordnet werden können, mit Art. 5 Abs. 1 Satz 1 des Deutschen Grundgesetzes unvereinbar ist. Als Begründung hierzu wird angeführt, dass aufgrund einer solchen Verpflichtung die bereits angedeutete Gefahr der Selbstzensur aus Angst vor Repressalien besteht, welcher durch das Grundrecht auf Meinungsfreiheit entgegengewirkt werden soll.[10]

Obwohl der Klarname der Nutzerin bzw. des Nutzers nach außen nicht offengelegt werden soll, erzeugt bereits die Speicherung der Daten ein Gefühl ständiger Überwachung, welches sich negativ auf die freie Meinungsäußerung auswirkt.[11] Auch unter diesem Gesichtspunkt lehnt die ISPA die angedachte Registrierungspflicht ab.

6. Die Wirksamkeit einer gesetzlichen Registrierungspflicht ist zu hinterfragen

Zwar ist das Ziel der Bekämpfung von Hasspostings und anderen strafbaren Nachrichten grundsätzlich zu begrüßen, jedoch stellt die Aufhebung der Anonymität bzw. eine verpflichtende Registrierung und Verifizierung keine geeignete Maßnahme zur Erreichung dieses Ziels dar. Vielmehr haben Studien bereits gezeigt, dass Nutzerinnen und Nutzer selbst unter ihrem Klarnamen sogar noch verstärkt zu Hasspostings neigen.[12] Beispielsweise sind Jahr 2018 beim Verein für Zivilcourage und Anti-Rassismus-Arbeit- ZARA ca. 1740 Vorfälle von Hass im Netz gemeldet worden. Davon haben in über 68% der Fälle die Täterinnen und Tätern zumindest dem Anschein nach unter einem Klarnamen gepostet. Lediglich 17% der Täterinnen und Tätern haben eindeutige Phantasienamen verwendet. Bei den restlichen 15% der Täterinnen und Tätern handelte es sich u. a. um Blogger, Webseitenbetreiber und Politiker, die auch nicht mit Phantasienamen auftreten. Aus diesem Grund ist auch nicht zu erwarten, dass die angedachte Lösung, bei der der Klarname nur beim Diensteanbieter vorliegt, zu einer Änderung des Posting-Verhaltens führen wird. Dies zeigt sich auch anhand des Nutzerverhaltens auf Social-Media Webseiten, auf welchen bereits seit Anbeginn eine Klarnamenpflicht besteht und Hasspostings auch unter dem Klarnamen verfasst werden.

Darüber hinaus wird diese Annahme auch durch die Erfahrung aus anderen Ländern bestätigt. In Südkorea wurde bereits 2007 eine Identifikationspflicht eingeführt, welche dem angedachten österreichischen Modell sehr stark ähnelt. Auch in diesem Modell konnten Nutzerinnen und Nutzer zwar weiterhin unter einem Pseudonym Nachrichten verfassen, jedoch vom Betreiber umgehend identifiziert werden. Die Maßnahme zeigte jedoch keine Wirkung, da die Anzahl an Hasspostings beinahe konstant blieb. Darüber hinaus verschafften sich Hacker Zugriff auf einzelne Server, auf welchen die Daten der Nutzerinnen und Nutzer gespeichert waren, und erhielten somit sensible Informationen zum Privatleben von 70 Prozent der Bevölkerung. Aufgrund dessen hob der südkoreanische Verfassungsgerichtshof die Maßnahme im Jahr 2012 als ungerechtfertigten Eingriff in die Meinungsfreiheit auf.

Im Endeffekt bedeutet dies, dass die angedachte Maßnahme zwar die Verbreitung von Hasspostings nicht verhindern wird, jedoch Nutzerinnen und Nutzer, die sich bislang innerhalb des

[10] BGH 23.6.2009 - VI ZR 196/08, Rz. 38 = MMR 2009, 608, 612
[11] EuGH 16.5.2014, C-293/12, Digital Rights Ireland Rz 37, EuGH 21.12.2016, C 203/15 Tele2 Sverige Rz 100
[12] Rost, Stahel, Frey "*Digital Social Norm Enforcement: Online Firestorms in Social Media*", Universität Zürich (2016)

rechtlichen Rahmens an Diskussionen beteiligt haben, von der Benutzung dieser Plattform Abstand nehmen werden. Daher ist die Wirksamkeit und letztendlich die Erforderlichkeit dieser Maßnahme aus Sicht der ISPA zu hinterfragen und der Gesetzesvorschlag soll auch unter diesen Gesichtspunkt neu überdacht werden.

Zudem wäre es anstelle eines Lösungsvorschlags, welcher zahlreiche zusätzliche Risken schafft, ohne dass ein konkreter Nutzen zu erwarten ist, zielführender, Medienkompetenz zu forcieren sowie das bestehende Notice-and-take-down System weiter zu verbessern. Durch effektive Meldemöglichkeiten, welche zu raschen Reaktionen bzw. Löschungen führen, wird gerade den Verfasserinnen und Verfassern von Hass-Postings ein grundlegender Aspekt ihrer Motivation genommen, indem verhindert wird, dass sich ihre Nachricht verbreitet bzw. möglichst vielen anderen Nutzerinnen und Nutzern zugänglich gemacht wird. Auf diese Weise werden auch die Auswirkungen auf die jeweiligen Opfer vermindert. Eine wichtige Rolle kann dabei sogenannten „trusted flaggern“ also besonders vertrauenswürdigen Nutzerinnen und Nutzern, deren Meldungen in einem beschleunigten Verfahren behandelt werden, sowie speziell geschulten Inhalts-Moderatoren in Diskussionsforen, zukommen. Von einer gesetzlichen Verpflichtung samt Löschfrist wie dies etwa das deutsche NetzDG beinhaltet, sollte jedoch in jedem Fall abgesehen werden, da einem solchen Gesetz die Gefahr des „Overblockings“ bzw. von überschießenden Löschungen immanent ist.

In diesem Sinne fordert die ISPA, dass überhastete Lösungen mit keiner nennenswerten Wirkung hintangehalten werden und stattdessen bereits existierende Lösungsmodelle angepasst und optimiert werden, um das durchaus legitime Ziel der Bekämpfung von Hasspostings und anderen strafbaren Nachrichten im Internet zu erreichen.

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