



Bundeskanzleramt
Ballhausplatz 2
1010 Wien

medienrecht@bka.gv.at

BUNDESARBEITSKAMMER
PRINZ EUGEN STRASSE 20-22
1040 WIEN
T 01 501 65
www.arbeiterkammer.at
DVR 1048384

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel 501 65 Fax 501 65	Datum
BKA-	BAK/KS-	Mag Daniela	DW 12722DW 12693	14.05.2019
671.828/000	GSt/DZ/Ho	Zimmer		
3-IV/6/2019				

Bundesgesetz über Sorgfalt und Verantwortung im Netz (SVN-G)

Die Bundesarbeitskammer (BAK) bedankt sich für die Übermittlung des im Betreff genannten Entwurfes und nimmt dazu wie folgt Stellung:

Zusammenfassende Bewertung

„Grenzüberschreitungen, Herabwürdigungen, Demütigungen und Übergriffe“ kommen in Internetforen vermehrt vor, so die Erläuterungen zum Entwurf. Die BAK begrüßt grundsätzlich die Auseinandersetzung mit der Frage, wie unsere Gesellschaft mit einem sich verschärfenden Meinungsklima im Internet gegenüber Einzelpersonen, die öffentlich exponiert sind, aber auch ganzen gesellschaftlichen Gruppen umgehen soll. Mit dem vorliegenden Entwurf dürfte das angestrebte Ziel – einer spürbaren Erleichterung eines straf- oder zivilrechtlichen Vorgehens gegen die Verletzung von Persönlichkeitsrechten – aber weitgehend verfehlt werden. Dafür greift das Vorhaben maßgeblich in die Grundrechte der ForennutzerInnen und -betreiber ein.

Der Entwurf richtet sich an Dienstanbieter, die soziale Netzwerke und Foren betreiben bzw an Medieninhaber, die in ihren Onlineausgaben die Möglichkeit bieten, Kommentare abzugeben und sich mit anderen Personen auszutauschen. Soweit diese Anbieter gewisse Umsatz- oder Nutzerzahlen erreichen bzw Förderungen erhalten, müssen sie sicherstellen, dass sich die DienstnutzerInnen vorab identifizieren, um den Dienst in Anspruch nehmen zu können.

Dienstanbieter können auch jetzt schon vorsehen, dass sich NutzerInnen mit ihrem Klarnamen registrieren. Entscheidend ist, dass in der Forenkommunikation die Nutzung von Pseudonymen uneingeschränkt möglich ist. Mit der Einführung einer „Ausweispflicht“ würde die anonyme Nutzung in den vom Entwurf erfassten Onlineforen ausnahmslos unterbunden. Forenbetreiber müssten künftig auch die Nutzerangaben prüfen und deren Freischaltung von ihrer eindeutigen Identifizierung (samt Adressangabe) abhängig machen. Dafür haben sie „Dokumente, Daten oder Informationen, die von einer glaubwürdigen, unabhängigen Quelle stammen“ heranzuziehen. Gespeicherte Nutzernamen und Adressen können durch Sicherheitsbehörden und Gerichte für die Strafverfolgung und für Privatankläger bei Verletzung bestimmter Persönlichkeitsrechte vom Forenbetreiber angefordert werden.

Grundrechtseingriff und erwartbarer Nutzen stehen aus BAK-Sicht in keinem angemessenen Verhältnis. Die BAK ersucht daher, das gesamte Vorhaben nochmals zu überdenken und von der „Ausweispflicht“ Abstand zu nehmen.

Grundrechtsschutz würde gelockert, das angestrebte Ziel aber weitgehend verfehlt:

- Respektlose Poster können leicht auf vom Entwurf nicht erfasste Foren ausweichen.
- Viele inkriminierte Beiträge erfolgen schon jetzt oft unter Angabe des Klarnamens. Eine Verschleierung der Identität ist offenkundig nicht das vorrangige Problem.
- Die Rechtsverfolgung dürfte wesentlich häufiger an der aufwändigen Prozessführung (fehlende Rechtskunde, finanzielle Hürden, offene Rechtsfragen) scheitern, als an der Identitätsklärung des Täters.
- Den Betroffenen ist mit einer raschen Entfernung verletzender Inhalte aus dem Internet meist mehr gedient, als mit der Feststellung der Rechtswidrigkeit und einem allfälligen Schadenersatzbetrag nach einem langwierigen Prozess.

Umso mehr fällt ins Gewicht, dass der Entwurf in die Grundrechte der ForennutzerInnen und ForenbetreiberInnen (Meinungsfreiheit, Privatsphäre, Datenschutz, Erwerbsfreiheit) wesentlich eingreift. Die Erläuterungen bieten keine überzeugenden Belege für die Angemessenheit der Maßnahme. An der Erforderlichkeit, Verhältnismäßigkeit und Übereinstimmung der Maßnahme mit den Grundrechten und der E-Commerce Richtlinie (RL) bestehen BAK-seits Zweifel.

Die EU-Konformität des Vorhabens ist zweifelhaft:

- Die **E-Commerce RL** verpflichtet zur Beachtung des Herkunftslandprinzips. Nicht im Inland niedergelassene Anbieter (wie Facebook) dürften grundsätzlich nicht zur Einhaltung einer „Ausweispflicht“ angehalten werden. Der erhoffte Nutzen würde maßgeblich geschmälert, dafür würden österreichische Medien belastet (Inländerdiskriminierung). Der Gesetzgeber kann sich zwar auf einzelne in der Richtlinie aufgezählte Ausnahmen zum Herkunftslandprinzip berufen. Inwieweit die EU-Kommission dies akzeptiert, ist unklar.
- Die E-Commerce RL untersagt zudem, Hostprovider dazu zu verpflichten, „die von ihnen gespeicherten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen“. Es ist durchaus denkbar, dass sich das Verbot allgemeiner Überwachung auch auf die anlasslose, vorbeugende, zweifelsfreie Identitätsfeststellung sämtlicher KundInnen erstreckt. So hat der Europäische Gerichtshof (EuGH) schon mehrfach festgehalten, dass die

Anordnung eines Überwachungssystems (bezogen auf gespeicherte Inhalte), das präventiv, auf alle KundInnen anwendbar, ausschließlich auf Betreiberkosten eingerichtet und zeitlich unbegrenzt ist, gegen die Haftungsbeschränkung nach der E-Commerce RL verstößt.

- Die **Datenschutz-Grundverordnung (DSGVO)** verlangt, dass Gesetze nur soweit in Datenschutzrechte eingreifen dürfen, als sie in einer demokratischen Gesellschaft notwendig, geeignet und verhältnismäßig sind. Eine generelle „Ausweispflicht“ weist Merkmale einer anlasslosen Vorratsdatenspeicherung auf, die mit der Judikatur des EuGH nicht im Einklang stehen dürften. Dieser hat ab 2014 mehrfach betont, dass eine anlasslose Speicherung von Daten bspw „über sämtliche Personen, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten vorzusehen“ unverhältnismäßig sei.
- Das Recht auf **freie Meinungsäußerung** schließt die Freiheit ein, Informationen ohne behördliche Eingriffe zu empfangen und weiterzugeben. Die Ausübung dieser Freiheiten ist zwar mit Pflichten verbunden; diese müssen aber in einer demokratischen Gesellschaft für die öffentliche Sicherheit, zur Verhütung von Straftaten oder zum Schutz des guten Rufes oder der Rechte anderer notwendig sein. Aus BAK-Sicht fehlt der Nachweis, dass die Ausweispflicht für eines der genannten Schutzgüter zwingend erforderlich ist.

Zweifel an der Verhältnismäßigkeit und Erforderlichkeit ergeben sich also daraus, dass

- ...ausländische Betreiber aufgrund EU-Rechts bestenfalls teilweise erfasst würden.
- ...nur „große“ Plattformen einbezogen werden (hohe Schwellwerte in Bezug auf registrierte NutzerInnen, Vorjahresumsatz bzw erhaltene Presseförderung). Beleidigungen in gut moderierten „großen“ Foren können seltener vorkommen, als auf schlecht moderierten Foren unterhalb der Schwellwerte. Die Zeitung „der Standard“ wies am 11.04.2019 darauf hin, dass Foren wie „unzensuriert.at“ immer wieder negativ auffallen, aber vom Entwurf nicht erfasst würden.
- ...der EuGH das Verbot einer Vorratsdatenspeicherung mehrfach bekräftigt und die Grenzen für die Zulässigkeit von anlasslosen Datenspeicherungen extrem eng gezogen hat.
- ...NutzerInnen unter Umständen abgeschreckt würden, ihre Meinung zu äußern. Notorische „Hassposter“ mit fehlendem Unrechtsbewusstsein verwenden schon jetzt zumeist ihren korrekten Klarnamen.
- ...Forenbetreiber staatliche Aufgaben aufgebürdet bekommen, für die sie nicht geeignet sind (Umgang mit gefälschten Dokumenten; ständig aktualisierte Adressverwaltung).
- ...es Alternativen gibt. Forenbetreiber könnten angehalten werden, zweifelsfrei inkriminierte Postings rascher zu löschen. Im Streitfall sollte eine unabhängige außergerichtliche Schlichtungsstelle unter staatlicher Aufsicht vermitteln. Das deutsche Netzwerkdurchsetzungsgesetz ist zwar ebenfalls umstritten (Vorwurf der „Privatisierung der Rechtsdurchsetzung“), zeigt aber mit rigiden Löschfristen zumindest alternative Regulierungswege für „Hass im Netz“ auf, die EU-seits

anerkannt

wurden.

- ...die Ausforschung von Personen schon jetzt oft gelingt (unter Inanspruchnahme von § 18 E-Commerce Gesetz (ECG)). Die erfolgreiche Ausforschung allein garantiert aber noch keinen Prozess Erfolg (siehe den nicht rechtskräftig abgeschlossenen Fall der ehemaligen Politikerin Sigrid Maurer). Das Einrichten eines Accounts reicht offenbar nicht für den Anscheinsbeweis, dass Postings dem/der Account-InhaberIn auch stets zurechenbar sind.

Zu den Details des Entwurfes

Eckpunkte

Künftig sollen Diensteanbieter, die Internetforen betreiben oder zur Verfügung stellen, verpflichtet werden, die Identität der BeitragsverfasserInnen („Poster“) zu überprüfen. Die Einführung einer derartigen „Ausweispflicht im Internet“ soll die Verfolgung von Rechtsansprüchen im Falle rechtswidriger Beiträge („Postings“) erleichtern und den respektvollen Umgang von Postern untereinander in Onlineforen fördern. Die im Entwurf enthaltene Pflicht, die Identität des Posters festzustellen und zu verifizieren, richtet sich an Anbieter von „Online-Infoangeboten“, die selbst ein Forum betreiben, das auf österreichische NutzerInnen ausgerichtet ist bzw die die Einrichtung eines Forums durch NutzerInnen ermöglichen, soweit sie eine maßgebliche Größe aufweisen (mehr als 100.000 registrierte NutzerInnen in Österreich, Vorjahresumsatz von über 500.000 Euro, EmpfängerInnen von Förderungen von mehr als 50.000 Euro nach dem Presseförderungsgesetz). Zur Unterstützung einer gegen einen Poster gerichtete Privatanklage wegen übler Nachrede, Beleidigung oder Ehrverletzung haben die genannten Anbieter die Pflicht, den Vornamen, Nachnamen und die Adresse eines Posters Dritten zu beauskunften, andernfalls drohen Sanktionen von bis zu einer halben Million Euro und im Wiederholungsfall bis zu einer Million Euro.

Motive

Die im Ministerratsvortrag als „digitales Vermummungsverbot“ bezeichnete Maßnahme wird damit begründet, dass „in der digitalen Welt die gleichen Prinzipien gelten müssen, wie in der real gelebten Welt“. Dieser Vergleich ist aus BAK-Sicht nur bedingt zutreffend:

Online-Offline-Vergleich: Die Identität der VerfasserInnen von Leserbriefen, deren Beiträge in klassischen Zeitungen veröffentlicht werden, wird nicht weiter geprüft. Darauf weist auch der Verband der österreichischen Internetprovider hin („Ich muss mich nicht ausweisen, bevor ich mich offline zu einem Thema äußere“; ISPA-Presseaussendung vom 10.04.2019).

Überwiegend korrekte Klarnamen: Kritiker des Entwurfes haben darauf hingewiesen, dass die Mehrzahl unakzeptabler Inhalte ohnedies unter Angabe des korrekten Klarnamens gepostet werden. Eine Ausweispflicht dürfte wenig präventive Wirkung entfalten: ForennutzerInnen entgleisen verbal auch bei Angabe ihres richtigen Namens. Dass Poster signifikant öfter im Schutz der Anonymität die Persönlichkeitsrechte Dritter verletzen, wird in den Erläuterungen zum Entwurf nicht behauptet. Vielmehr dürfte das Phänomen „Hass im Netz“ oft auf ein mangelndes Unrechtsbewusstsein der Poster zurückzuführen sein. Die Schulung von Medienkompetenz könnte eine zielführendere Maßnahme sein.

Vorratsdatenspeicherung: Eine Vorab-Ausweispflicht für alle NutzerInnen von Internetforen wäre ein überaus tiefer Eingriff in die Privatsphäre, da sie ausnahmslos alle NutzerInnen von Internetforen trifft und damit die vom EuGH und Österreichischen Verfassungsgerichtshof (VfGH) verworfene Vorratsdatenspeicherung für Verbindungsdaten wie IP-Adressen im Telekommunikationsgesetz in Erinnerung ruft. Die Gesamtheit der NutzerInnen würde unterschiedslos unter Generalverdacht gestellt und müsste sich der Ausweispflicht unterwerfen. Vergleichbare Situationen in der realen Welt werden in den Erläuterungen nicht skizziert.

Meinungsfreiheit: ForennutzerInnen könnten davon abgehalten werden, sich offen zu kontroversiellen Themen zu äußern. Poster, die die Grenzen des Rechts und Anstands überschreiten, scheuen hingegen nicht so sehr davor zurück, rechtswidrige Inhalte unter ihrem korrekten Namen zu verbreiten. Egal ob reale oder virtuelle Welt: Die Folgen eines nicht mehr offenen, meinungsvielfältigen Diskurses wären demokratiepolitisch bedenklich.

Foren sind auch jetzt kein rechtsfreier Raum: Der Maxime „das Internet darf kein rechtsfreier Raum sein“ (siehe Erläuterungen zum Entwurf) ist natürlich uneingeschränkt beizupflichten. Betont werden muss dies in Bezug auf Onlineforen jedoch nicht. Zivil- und strafrechtliche Tatbestände wie üble Nachrede, Beleidigung oder Ehrverletzung sind on- wie offline gleichermaßen verfolg- und strafbar.

Nicht bearbeitete Handlungsfelder: Die Ankündigung „Sich in der Anonymität des Internets verstecken zu können, darf in strafrechtsrelevanten Fällen nicht mehr möglich sein“ weckt auch unberechtigte Hoffnungen. So wächst bspw die Internetkriminalität in Österreich kontinuierlich (von 2017 auf 2018 um 16,8 Prozent von rund 17.000 auf fast 20.000 Fälle laut Kriminalitätsstatistik des Bundesministeriums für Inneres). Die Anonymität von Internetbetrügern, Hackern etc stellt die größte Hürde für die Rechtsverfolgung dar. Angesichts des Zuwachs betrügerischer Onlinefallen drängt sich bisweilen der Eindruck auf, dass das Internet eher in diesem Kontext „ein rechtsfreier Raum“ sei. Es sind der BAK keine Gesetzesinitiativen bekannt, die den Missbrauch der Anonymität in diesen Fällen wirksam verringern sollen. Ein europaweites, öffentlich gewartetes und zugängliches Firmenbuch wäre bspw ein wichtiger Beitrag zur Rechtsverfolgung betrügerischer Onlinepraktiken.

„Relevante“ Anbieter im Sinn des § 3

Hasspostings oder bewusst falsche Informationen kommen auch in Foren vor, die nach dem Entwurf keine relevante Größe haben. Es ist nicht nachvollziehbar, eine Ausweispflicht einzuführen und kleinere Dienste davon auszunehmen. Neue Registrierungshürden bei großen Webseiten könnten den Zulauf von „Hass“-Postern bei kleineren Internetforen verstärken. In Foren, die außerhalb des Anwendungsbereichs des Entwurfs liegen, werden oft Kampagneninhalte angeboten, die von einschlägig interessierten NutzerInnen auf andere Plattformen weitergetragen werden. Die Ziele des Entwurfes würden so komplett verfehlt.

Alternative Handlungsmöglichkeiten

Defizite bei der Rechtsdurchsetzung könnten grundrechtsschonender verringert werden:

Das deutsche Netzwerkdurchsetzungsgesetz (Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken) enthält sanktionsbewehrte Compliance-Regeln für Anbieter sozialer Netzwerke zum Umgang mit Nutzer-Beschwerden bei Hasskriminalität und andere strafbaren Inhalten sowie eine vierteljährliche Berichtspflicht der Plattformanbieter.

Provider genießen aufgrund der E-Commerce RL eine Haftungsbefreiung, wenn sie den Zugang zu Informationen schnellstmöglich entfernen oder deaktivieren, sobald sie Kenntnis von deren rechtswidrigem Charakter erlangen. Das deutsche Gesetz präzisiert den Zeitraum, innerhalb dessen die Anbieter tätig werden müssen. Betreiber sozialer Netzwerke wie Facebook, Twitter oder YouTube müssen „offensichtlich rechtswidrige Inhalte innerhalb von 24 Stunden“ nach Eingang einer Beschwerde löschen oder sperren. Bei komplexen Fällen gilt in der Regel eine Sieben-Tages-Frist, um über eine Löschung oder Sperrung zu entscheiden. Mögliche Rechtfertigungsgründe müssen berücksichtigt werden. Die Prüfung kann auch einer vom Justizressort beaufsichtigten Einrichtung zur freiwilligen Selbstkontrolle überantwortet werden.

Zwar bestehen BAK-seits Bedenken, straf-, zivil- und grundrechtliche Abwägungen in die Hand von Unternehmen zu legen. Plattformbetreibern derartige außergerichtliche Prüfungen zu übertragen, wird auch als „Privatisierung der Rechtsdurchsetzung“ kritisiert. Weigern sich Betreiber, Inhalte zu löschen, riskieren sie, für diese Inhalte haftbar gemacht zu werden. Um Kosten und Rechtsstreitigkeiten zu vermeiden, dürften Betreiber deshalb dazu tendieren, eher zu viel als zu wenig zu löschen („Overblocking“).

Die Einführung eines außergerichtlichen Schlichtungsverfahrens für Forenkonflikte könnte aber die gerichtsförmige Abklärung unter Umständen sinnvoll ergänzen. Die Schlichtungseinrichtung muss ausreichende Kompetenz und Unabhängigkeit aufweisen, behördlich beaufsichtigt werden und Entscheidungen transparent veröffentlichen. Es muss möglich sein, die Entscheidung auf Löschung oder Beibehaltung des Forenbeitrages gerichtlich anzufechten.

Beweisprobleme: Die Rechtsdurchsetzung dürfte in der Praxis auch seltener an „Vermummungs“-Absichten des Posters als an Beweisproblemen scheitern (siehe die nicht rechtskräftige Entscheidung „Sigrid Maurer“, <https://www.respekt.net/projekte-unterstuetzen/details/projekt/1775/>). So dürfte der Nachweis, dass der/die Account-InhaberIn selbst (und nicht eine dritte Person) einen inkriminierten Beitrag hochgeladen hat, schwer zu erbringen sein. Allenfalls wäre es zweckmäßig, über Beweiserleichterungen nachzudenken.

Die E-Commerce-Richtlinie (RL)

Herkunftslandprinzip: Die Erläuterungen zu § 3 Abs 1 führen aus: *„Selbstverständlich sollen die Regelungen nicht auf sämtliche Foren weltweit Anwendung finden, sondern der gegenständliche Entwurf verlangt ausdrücklich einen klaren Konnex zu Österreich, weil nur Poster und Foren erfasst werden, die zB durch den Inhalt, die Zielgruppe, die Sprache als Nutzer in Österreich ausgerichtet qualifiziert werden können.“*

Unklar bleibt, ob und vor allem wie Facebook, Twitter usw ihre Registrierungspraxis aufgrund des vorliegenden Gesetzesentwurfes abändern werden. Gerade auf Facebook werden nicht wenige hasserfüllte, verhetzende Botschaften vielfach „geteilt“.

§ 18 ECG legt die Dienstanbieterpflichten (Überwachung im Einzelfall, Auskunftspflicht, Löschung) abschließend fest und richtet sich (aufgrund des Herkunftslandprinzips) grundsätzlich nur an Inlandsanbieter. Es stellt sich die Frage nach der Erforderlichkeit einer Maßnahme, die wichtige ausländische Akteure nicht (immer) umfasst und nur inländische Anbieter gesichert in die Pflicht nimmt. Die Ausnahme des Art 3 Abs 4 E-Commerce RL vom Herkunftslandprinzip erstreckt sich nur auf Maßnahmen, die der Verhütung, Ermittlung und Verfolgung von Straftaten dienen. Selbst wenn eine Ausweitung des Anwendungsbereichs des „Vermummungsverbots“ auf ausländische Anbieter RL-konform wäre, so würde sie nur für die Strafrechtsverfolgung gelten, nicht aber für die Verletzung zivilrechtlicher Persönlichkeitsrechte.

Verbot allgemeiner Überwachungspflichten: Hostprovider sind dem ECG zufolge nicht verpflichtet, die von ihnen gespeicherten, übermittelten oder zugänglich gemachten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen. Die BAK hält die Auslegung für vertretbar, dass mit „gespeicherten Informationen“ auch die Registrierungsprofile von ForennutzerInnen gemeint sind. Diesfalls dürften die Anbieter nicht zu „allgemeinen Überwachungsmaßnahmen“ (alle Kunden unterschiedslos betreffend, präventiv, zeitlich unbegrenzt usw) angehalten werden. Die im Entwurf vorgesehene Ausweispflicht könnte – in Hinblick auf die bislang strenge EuGH-Judikatur – als unzulässige Anordnung einer generellen Überwachungspflicht qualifiziert werden.

Ausreichende, bewährte Auskunfts- und Löschpflichten im ECG: Zusätzliche Regeln zur Herausgabe von Stammdaten von Kunden (wie in § 3 Abs 4 des Entwurfes vorgesehen) bedarf es nicht. Die Dienstanbieter haben nach dem ECG jetzt schon einem Gericht „alle Informationen zu übermitteln, an Hand derer die Nutzer ihres Dienstes zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen ermittelt werden können“. Hostprovider haben auch gegenwärtig „den Namen und die Adresse eines Nutzers ihres Dienstes auf Verlangen dritten Personen zu übermitteln, sofern diese ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers und eines bestimmten rechtswidrigen Sachverhalts haben sowie überdies glaubhaft machen, dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet“.

Die technische Umsetzung der Identitätsprüfung

Wie die „Ausweispflicht“ in der Praxis umgesetzt wird, bleibt dem Anbieter überlassen. Die Erläuterungen verweisen auf mögliche Lösungen in Form eines zweistufigen Verifizierungsprozesses. So könnten Namen und Adresse mittels 2-Faktor-Authentifizierung mit Mobiltelefonnummer bestätigt werden. Der Diensteanbieter könne auch sicherstellen, dass „er – gegebenenfalls in Kooperation mit dem Betreiber des Telefondienstes – bei begründeten Anfragen die für die Rechtsverfolgung notwendigen Daten in Erfahrung bringen kann“.

Anzumerken ist, dass Stammdaten von Telefonnutzern nach dem TelekommunikationsG (§§ 96 ff TKG) nicht für andere als die im TKG festgelegten Zwecke verwendet werden dürfen. Ohne explizite Zustimmung der Telefonkunden dürften damit auch nicht Handy-Identifikations-Dienste wie Mobileconnect (<https://de.mobileconnect.io/>) auf den Smartphones NutzerInnen freigeschaltet werden.

Wir ersuchen um Berücksichtigung unserer Anliegen und Anregungen.

