WIEN / 22. Mai 2019

STELLUNGNAHME

Zum Ministerialentwurf für ein Bundesgesetz über Sorgfalt und Verantwortung im Netz (SVN-G) (134/ME XXVI. GP)

Für epicenter.works
Mag.ª Angelika Adensamer, MSc
Andreas Czák, BSc
Mag.ª Marlene Kreil
Iwona Laub
Thomas Lohninger
Levin Wotke, BA

EPICENTER .WORKS
for digital rights

Inhaltsverzeichnis

VORWORT

Die Bundesregierung hat das Gesetz über Sorgfalt und Verantwortung im Netz[1] entwickelt, um dem Hass im Netz den Kampf anzusagen. Mit der Bekämpfung von Hassnachrichten im Internet hat der Gesetzesentwurf allerdings nur wenig gemein. Kurz nach dem Bekanntwerden der Hassnachrichten im medienöffentlichen Fall Sigi Maurer wurde ein Gipfel zu Hass im Netz abgehalten, bei dem führende ExpertInnen erst gar nicht eingeladen wurden. Angekündigt wurde ein Gesetzesentwurf zur Bekämpfung von Hassnachrichten, herausgekommen ist aber ein Gesetz, das darauf abzielt, regierungskritische Medien und deren DiskussionsteilnehmerInnen als auch ForenbetreiberInnen mit hohen UserInnenzahlen an die kurze Leine zu nehmen und so den Diskurs in der Öffentlichkeit klein zu halten.

Die Umsetzung dieses Gesetzesentwurfs würde bedeuten, dass den PlattformbetreiberInnen für strafrechtliche und privatrechtliche Rechtsdurchsetzung ein enormes Risiko umgehängt wird. Abgesehen von den drakonischen Strafen, die hier verhängt werden können und die für kein Medium leistbar sind, wird hier der Versuch unternommen, Risiken und Pflichten einzelnen Medien aufzubürden, von denen diverse Hass-Verbreitungsportale völlig unbetroffen bleiben. Angriffe, wie sie die oben bereits genannte Sigi Maurer erlebt hat, bleiben weiterhin legal. Der Tatsache, dass die meisten Hassnachrichten ohnehin bereits mit Klarnamen abgesetzt werden, wurde beim Erstellen des Gesetzesentwurfes auch nicht besonders viel Augenmerk geschenkt.

Neben den wirtschaftlichen Aspekten, die vor allem neue Medienbetreiber davon abschrecken werden, überhaupt neue Medien zu schaffen, ist es höchst problematisch, privaten Unternehmen eine Speicherverpflichtung umzuhängen, die nicht klar geregelt ist. Der Gesetzgeber scheint nicht beachtet zu haben, dass der Gesetzesvorschlag Missbrauchspotential fördert und zu einer Datensammlung führt, die - wie bereits in Südkorea[2] - irgendwann nach außen geraten könnte. Datensicherheit ist nicht 100%ig zu garantieren und so könnte es beispielsweise zu Identitätsdiebstählen, Ausforschung von Gewaltopfern, Stalking und anderen Folgeverbrechen kommen.

Wer Zugriff auf personenbezogene Daten bekommen darf, sollen die PlattformbetreiberInnen entscheiden. Die Frage, ob ein privates Unternehmen eindeutig beurteilen kann, ob es auf straf- oder privatrechtlicher Ebene tatsächlich ein berechtigte Interesse gibt, stellt sich nicht, da selbst diese Prüfung nicht vorgesehen ist. Die Folgen können schwer sein: Angefangen von Menschen, die bei kritischen PosterInnen ungebetene Hausbesuche machen, bis zu einer möglichen späteren Ausweitung der Auskunftspflichten auf andere rechtliche Bereiche. Diese sogenannten „mission creeps“ waren bereits in der Vergangenheit bei diversen Gesetzen üblich und sind auch hier zu befürchten.

Diese Art der Speicherung von Daten kann man getrost auch Vorratsdatenspeicherung nennen. Es werden Daten prophylaktisch gesammelt, um sie im Falle des Falles zu haben. Diese Art der Speicherung von Daten ist aber laut EuGH unzulässig und nicht mit demokratischen Grundwerten vereinbar. Zudem ist es laut E-Commerce-Richtlinie unzulässig, Überwachungspflichten dieser Art

1 https://www.parlament.gv.at/PAKT/VHG/XXVI/ME/ME_00134/index.shtml
2 http://www.chinadaily.com.cn/world/2011-08/11/content_13095102.htm

abzuverlangen. Insgesamt stellt der Gesetzesentwurf eine Verletzung des Rechts auf Achtung der Privatsphäre dar und stellt unsere Gesellschaft vor eine grundlegende Frage: Wollen wir, dass Menschen nicht mehr das Gefühl haben, sich frei äußern zu können und brauchen wir dieses Gesetz tatsächlich in unserer demokratischen Gesellschaft? Unsere Antwort darauf ist ganz klar: Nein. Die Verhältnismäßigkeit des Gesetzes ist nicht gegeben, der Gesetzgeber hat bereits zahlreiche andere Mittel, die Herausgabe von Daten von InternetnutzerInnen einzufordern. Der Gesetzesentwurf stellt also nicht das gelindeste Mittel zur Verfolgung strafrechtlich relevanter Nachrichten oder Foreneinträge dar.

Daneben sollte auch das Redaktionsgeheimnis gewahrt werden. Eine Redaktion lebt nicht zuletzt davon, dass sie mit ihren LeserInnen interagiert und auch von dieser Gruppe Informationen bekommt oder zumindest Hinweise darauf, welche Inhalte die LeserInnen besonders interessieren. Das Redaktionsgeheimnis wird durch die Europäischen Menschenrechtskonvention garantiert und ist eine Grundbedingung der hoch geschätzten Pressefreiheit. Da dies aber weder Erwähnung noch Relevanz im Gesetzesvorschlag findet, ist ein problematisches Verhältnis zum Redaktionsgeheimnis anzunehmen - ob erwünscht oder durch schlechte Legistik.

Als Grundrechts-NGO möchten wir darauf hinweisen, dass dieses Gesetz in seiner jetzigen Form nicht nur teilweise oder stellenweise, sondern gänzlich abzulehnen ist. Der Versuch oder scheinbare Versuch, Hass im Netz zu minimieren, bedeutet nämlich hier in Wirklichkeit die Drangsalierung von Medien- und Forenbetreibenden und eine Schmälerung des öffentlichen Diskurses.

EINLEITUNG

Das SVN-G normiert die auch als „digitaler Ausweiszwang“ bezeichnete Pflicht, UserInnen in (bestimmten) Online-Foren mit Vor- und Nachnamen sowie Adresse zu registrieren, um die straf- und privatrechtliche Rechtsverfolgung in derartigen Foren zu erleichtern. Im Folgenden sollen zunächst einfachgesetzliche und darüber hinaus verfassungs- sowie unionsrechtliche Probleme des vorliegenden Ministerialentwurfes, der sich derzeit in Begutachtung befindet, dargestellt werden.

ERMITTLUNGS- UND SPEICHERVERPFLICHTUNG

Nach § 3 Abs 4 SVN-G soll künftig für NutzerInnen die Verpflichtung bestehen, Vorname, Nachname und Adresse bei Diensten der Informationsgesellschaften im Anwendungsbereich des § 3 Abs 1 und Abs 2 SVN-G (zur einfacheren Lesbarkeit in Folge Foren) zu registrieren. Die Foren müssen diese Daten bereithalten, um sie gem § 4 Abs 1 und Abs 2 Dritten auf begründetes Verlangen und gem § 4 Abs 3 kriminalpolizeilichen Behörden, Staatsanwaltschaften und Gerichte bekannt zu geben.

Während Stammdaten nach § 92 Abs 3 Z 3 TKG Daten sind, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen der/m BenutzerIn und der/m AnbieterIn oder zur Erstellung und Herausgabe von TeilnehmerInnenverzeichnissen erforderlich sind, sind die Daten, die der Speicherverpflichtung nach dem SVN-G unterliegen, nicht erforderlich. Die meisten Foren funktionieren heute ohne Bedarf an Klarnamen und Adressen. Obwohl Name und Adresse also Teil der Stammdaten im Sinne des Telekommunikationsgesetzes sind, sind sie im SVN-G aber keine Stammdaten im engeren Sinn.

Verkehrs- und Inhaltsdaten

Um alle Pflichten, die das SVN-G den Diensten der Informationsgesellschaft auferlegt, zu erfüllen, müssen diese jedoch noch mehr als nur Namen und Adresse bei der Registrierung speichern, insbesondere ist die Pflichterfüllung ohne die Speicherung von Verkehrsdaten nicht möglich:

- Mit dem SVN-G soll laut § 1 die Verfolgung von Rechtsansprüchen erleichtert werden. Dazu sollen Klarnamen und Adresse bei der/dem ForenbetreiberIn gespeichert werden und bei problematischen Postings, die unter einem NutzerInnennamen gepostet werden, herausgegeben werden. Damit diese Daten aber zur Rechtsverfolgung taugen, muss sowohl eine Verknüpfung zwischen Klarname und NutzerInnenname, als auch zwischen NutzerInnenname und Posting gegeben sein. Gibt es beide, lässt sich natürlich auch eine Verbindung zwischen Klarname und Posting herstellen. Es ist also nicht möglich, den Zweck des Gesetzes zu erfüllen, ohne auch Verkehrs- und Inhaltsdaten insbesondere die Verknüpfung zwischen Postings und Klarname, sei es auch über die Ecke des NutzerInnennamens, zu verarbeiten.
- Nach § 3 Abs 6 Z 3 SVN-G sind die ForenbetreiberInnen zu periodischen Überprüfung der Inaktivität der NutzerInnen verpflichtet. Die Aktivität oder Inaktivität kann nur mittels Verkehrsdaten festgestellt werden.
- Auch die Überprüfung eines „begründeten Verlangens" der Herausgabe von Daten seitens einer/s Dritten nach § 4 Abs 2 SVN-G kann substantiell nicht sinnvoll ausgeführt werden, ohne auch zu überprüfen ob das beanstandete Posting tatsächlich von der/dem behaupteten PosterIn stammt.
- Gem § 4 Abs 4 SVN-G hat die/der ForenbetreiberIn bei begründeten Hinweisen auf üble Nachrede oder Beleidigung eine Aufzeichnung eines Postings herzustellen, die „eine vollständige und originalgetreue Wiedergabe ermöglicht". Diese könnte den Zweck der Rechtsdurchsetzung nicht erfüllen, wenn nicht auch ein Nachweis darüber gespeichert wird, welche/r NutzerIn das Posting tatsächlich verfasst hat.
- Gem § 3 Abs 1 Z 1 SVN-G gilt das Gesetz für Dienste, die „auf Nutzer in Österreich ausgerichtet" sind. Zur Feststellung dieser Ausrichtung soll gem der Erläuterungen (S. 3) auch der Inhalt dienen.

Insb führt das dazu, dass die Argumente der Judikatur zur Vorratsdatenspeicherung (insb Digital Rights Ireland und Tele 2) auch auf das SVN-G zutreffen.

Grundrechtswidrige Vorratsdatenspeicherung

Der EuGH hat schon mehrmals festgestellt, dass eine Vorratsdatenspeicherung, also die Speicherverpflichtung personenbezogener Daten ohne jeglichen Anlass, das Grundrecht auf Achtung der Privatsphäre nach Art 7 GRC und das Grundrecht auf Datenschutz nach Art 8 GRC verletzt.

Mit dieser Rechtsprechung kann die Speicherverpflichtung des SVN-G nicht in Einklang gebracht werden. So sagte der EuGH etwa im Rahmen seiner Entscheidung zur Vorratsdatenspeicherung: „Zur Erforderlichkeit der durch die Richtlinie 2006/24 vorgeschriebenen Vorratsspeicherung der Daten ist festzustellen, dass zwar die Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, von größter Bedeutung für die Gewährleistung der öffentlichen Sicherheit ist und dass ihre Wirksamkeit in hohem Maß von der Nutzung moderner

Ermittlungstechniken abhängen kann. Eine solche dem Gemeinwohl dienende Zielsetzung kann jedoch, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer Speicherungsmaßnahme – wie sie die Richtlinie 2006/24 vorsieht – für die Kriminalitätsbekämpfung nicht rechtfertigen", vielmehr müsse sich jeder Eingriff und jede Ausnahme vom Schutz personenbezogener Daten auf das „absolut Notwendige beschränken."[3] In seiner zweiten Entscheidung zur Vorratsdatenspeicherung entschied der EuGH noch einmal, dass "allein die Bekämpfung der schweren Kriminalität eine solche Maßnahme zu rechtfertigen" weiß (gemeint war die anlasslose Vorratsdatenspeicherung).[4] Die Speicherverpflichtung im SVN-G dient aber nicht nur der Verfolgung schwerer Straftaten, sondern einerseits der privaten Rechtsverfolgung bei den Privatanklagedelikten der üblen Nachrede (§ 111 Abs 2 StGB), Beleidigung und sogar dem zivilrechtlichen Anspruch nach § 1330 ABGB und andererseits der Verfolgung aller Straftaten durch Behörden (§ 4 Abs 3 SVN-G).

Die Einschränkung der Datenspeicherung auf das absolut Notwendige sowie die notwendigen klaren und präzisen Regeln[5], sind eindeutig in einer Gesamtschau bei den Speicherpflichten des SVN-G nicht gegeben, womit es das Grundrecht auf Achtung der Privatsphäre nach Art 7 GRC und das Grundrecht auf Datenschutz nach Art 8 GRC verletzt.

VERBOTENE ÜBERWACHUNGSPFLICHTEN (E-COMMERCE RL)

Insoweit, als das SVN-G auch Überwachungspflichten normiert (s.o. unter Verkehrs- und Inhaltsdaten), verletzt es die EU E-Commerce RL (2001/31/EG). Nach Art 15 der Richtlinie dürfen die Mitgliedsstaaten Diensten der Informationsgesellschaft keine allgemeine Verpflichtung auferlegen, „die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen". Dies ist bislang durch § 18 Abs 1 ECG umgesetzt: „Die in den §§ 13 bis 17 genannten Diensteanbieter sind 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."

In den Erläuterungen zur damaligen Regierungsvorlage zum E-Commerce-Gesetz wird das Verbot der Einführung allgemeiner Überwachungspflichten sogar noch expliziter ausgeführt: „Die Richtlinie hindert die Mitgliedstaaten in Art 15 Abs 1 daran, eine allgemeine Überwachungspflicht der Access oder Host Provider für die von ihnen übermittelten oder gespeicherten Informationen vorzusehen. Auch können die Mitgliedstaaten diese Provider nicht dazu verpflichten, von sich aus Umstände über eine allenfalls rechtswidrige Tätigkeit zu ermitteln. Die in den Art 12 bis 14 der Richtlinie (§§ 13, 15 und 16 ECG) genannten Anbieter sind nicht verpflichtet, die von ihnen gespeicherten oder übermittelten Informationen und Inhalte vorweg einer Kontrolle auf deren Rechtskonformität zu unterziehen."[6]

Dieser Ausschluss einer allgemeinen Überwachungspflicht soll nun aber zumindest an zwei Stellen im neuen Gesetz umgangen werden. Im § 3 SVN-G, der sich mit „Registrierung und Authentifizierung" beschäftigt, werden die DiensteanbieterInnen gem Abs 4 verpflichtet, die Registrierungsprofile zu

3 EuGH, Digital Rights Ireland Rz 51f.
4 EuGH Tele 2, Rz 102.
5 EuGH Digital Rights Ireland, Rz 52, 54.
6 https://www.parlament.gv.at/PAKT/VHG/XXI/I/I_00817/fname_604961.pdf, 37f.

erstellen und Vor- sowie Nachname und Adresse der PosterInnen zu registrieren, dafür sollen diese Dokumente, Daten oder Informationen von glaubwürdigen und unabhängigen Quellen vorlegen. Schon diese Speicherung aller NutzerInnen, die ein Forum verwenden wollen, stellt eine allgemeine Überwachung dar, zu der die Mitgliedstaaten gem Art 15 E-Commerce RL explizit nicht verpflichten dürfen. Ein noch klarerer Verstoß und offensichtliche Einführung einer allgemeinen Überwachungspflicht sind aber § 3 Abs 5 und Abs 6 SVN-G.

Folgende Bestimmungen des SVN-G sehen allgemeine Überwachungspflichten vor:

- Um festzustellen, ob der eigene Dienst in den Anwendungsbereich iSd § 3 Abs 1 Z 1 des Gesetzes fällt, wird die/der DiensteanbieterIn gezwungen sein, auch die Inhalte ob ihrer Ausrichtung auf NutzerInnen in Österreich regelmäßig zu überprüfen, also zu überwachen.
- § 3 Abs 6 SVN-G normiert außerdem, dass DiensteanbieterInnen das Registrierungsprofil von UserInnen unter anderem „jedenfalls" zu löschen haben „bei im Rahmen von routinemäßig periodisch vorgenommenen Überprüfungsvorgängen festgestellter Inaktivität von mehr als einem Jahr". Die Verpflichtung zu „routinemäßig periodisch vorgenommenen Überprüfungsvorgängen" stellt jedenfalls eine allgemeine Überwachungspflicht dar.
- Gem § 3 Abs 5 SVN-G hat die/der DienstanbieterIn bei begründetem Verdacht auf unrichtige oder unrichtig gewordene Daten die betreffenden NutzerInnen zur Berichtigung aufzufordern oder die NutzerInnenprofile zu löschen. Laut den Erläuterungen (S. 5) ist auch dies in den routinemäßig, periodisch vorgenommenen Überprüfungen, in denen auch die Inaktivität der NutzerInnen festgestellt werden soll (s.o.), festzustellen.

Diese Überwachungsverpflichtungen verletzen Artikel 15 der E-Commerce-Richtlinie.

AUSKUNFTSPFLICHTEN

Nach § 4 Abs 3 und Abs 3 SVN-G müssen die Daten nicht nur gespeichert und an Strafverfolgungsbehörden herausgegeben werden (Abs 3), sondern auch an Dritte, also Privatpersonen herausgegeben werden, wenn diese dritte Person ihr eigene Identität nachweist und „glaubhaft macht dass die Feststellung der Identität des Posters eine unabdingbare Voraussetzung bildet, um wegen des Inhalts eines Postings gegen diesen Poster mittels Privatanklage wegen übler Nachrede (§ 111 Abs 2 StGB) oder wegen Beleidigung (§ 115 StGB) strafgerichtlich oder wegen Verletzungen an der Ehre (§ 1330 ABGB) zivilgerichtlich vorzugehen." (Abs 2) Hierbei ist also nach dem Gesetzeswortlaut bei Privatpersonen nicht einmal die Begründung des Verdachts notwendig, glaubhaft muss lediglich gemacht werden, dass man nicht schon auf anderem Weg Vor-, Nachname und Wohnadresse erfahren der/s PosterIn/s hat.

Da diese Auskunftsverpflichtung schon bei sehr geringen Voraussetzungen besteht, ist das Missbrauchspotential dieser Regelung hoch. Es steht zu befürchten, dass diese Möglichkeit insbesondere auch zum Zweck der Begehung von Straftaten, wie Stalking oder zur Ausforschung von Gewaltopfern, die sich vor TäterInnen schützen wollen, verwendet werden kann.

Nach § 18 Abs 4 iVm § 16 ECG sind Host-Provider auch heute schon verpflichtet, Namen und Adressen von NutzerInnen an Dritte herauszugeben, sofern diese „ein überwiegendes rechtliches Interesse an der Feststellung der Identität des Nutzers und eines bestimmten rechtswidrigen Sachverhalts haben". Eine Entscheidung aus der Praxis zur Herausgabe von UserInnen-Daten im

Rahmen von Foren ist die Rechtssache 6Ob188/16i. Darin führte der OGH aus, dass ein überwiegendes rechtliches Interesse an der Feststellung der Identität nur dann besteht, wenn die Rechtsverfolgung aufgrund einer groben Prüfung der von der/m KlägerIn geltend gemachten Verletzungen eine gewisse Aussicht auf Erfolg hat. Den Grad der Wahrscheinlichkeit einer Verurteilung nach § 1330 ABGB, die eine Herausgabe der Daten der/s VerletzerIn/s rechtfertigt, hat der erkennende Senat damit umschrieben, dass eine Verurteilung „nicht gänzlich auszuschließen“[7] sein dürfe bzw. dass eine solche „möglich“ erscheine.[8] Eine ähnliche Voraussetzung, die auf die Aussichten der Rechtsverfolgung im konkreten Einzelfall abstellt, fehlt im SVN-G komplett. Auch das Verhältnis der Verpflichtung in § 4 Abs 2 SVN-G zu der parallelen Herausgabeverpflichtung nach § 18 Abs 4 ECG wird nicht geklärt.

Die Herausgabeverpflichtungen von Stammdaten, die die TelekommunikationsbetreiberInnen betreffen, sind taxativ in § 90 Abs 6 und Abs 7 TKG aufgezählt. Auskunftspflichten zur Verfolgung von Privatanklagedelikten und zivilrechtlichen Ansprüchen finden sich dort nicht. Unklar ist, wieso diese unsachliche Differenzierung gerechtfertigt sein soll. Aus Art 2 StGG sowie Art 7 Abs 1 B-VG wurde der allgemeine Gleichheitssatz herausgebildet. Dieser bindet laut VfGH (und überdies absolut hM) auch (ua) den Bundesgesetzgeber.

Eine Differenzierung ist laut VfGH nur dann rechtskonform, wenn sie sachlich gerechtfertigt ist und sich auf objektive Unterscheidungsmerkmale knüpft.[9] Wird einE DiensteanbieterIn nach dem neuen SVN-G nun von einem „Dritten“ (ie einer Privatperson, die ohne Hoheitsgewalt auftritt) unter bestimmten Umständen kontaktiert, um einen Verdacht etwa einer üblen Nachrede verfolgen zu können, so ist diesEr verpflichtet, Vorname, Name und Adresse herauszugeben. BereitstellerInnen iSd TKG sind in keinster Weise dazu verpflichtet (in Hinblick auf den möglichen Missbrauch dieser Verpflichtung ist dies auch rechtspolitisch vollkommen nachvollziehbar). Dass nun aber im Gegensatz zu BereitstellerInnen iSd TKG den DiensteanbieterInnen iSd SVN-G derartig umfassende Pflichten auferlegt werden (in Verbindung mit ebenso weitläufigen Möglichkeiten der Bestrafung) ist eine unsachliche Differenzierung und somit Verstoß gegen den allgemeinen Gleichheitssatz.

7 6 Ob 133/13x [2.], 6 Ob 188/14m [4.1.]
8 6 Ob 188/14m [3.3.]) erscheine.
9 vgl Mayer/Kucsko-Stadlmayer/Stöger, Bundesverfassungsrecht11, Rz 1357.

GRUNDRECHTLICHE PROBLEME

Verletzung des Rechts auf Achtung der Privatsphäre (Art 8 EMRK)

Art. 8 EMRK:

(1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.

(2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.

Das in Art 8 EMRK normierte Grundrecht auf Achtung des Privat- und Familienlebens wird durch mehrerlei Punkte des SVN-G berührt. Geschützt ist jedenfalls das Privatleben von natürlichen Personen, in das das SVN-G eingreift. Der Begriff des Privatlebens wird vom EGMR weit ausgelegt, wodurch Schutzlücken vermieden werden sollen. Eine abschließende Definition des Begriffs ist nicht möglich. Grundsätzlich umfasst das Privatleben im Sinne des Art 8 EMRK aber alle Dimensionen, die der individuellen Persönlichkeitssphäre zurechenbar sind, wodurch die Identität, Entwicklung und Verwirklichung der einzelnen Person gewährleistet werden soll.[10] Es wird also im Rahmen des Privatlebens die gesamte individuelle Persönlichkeitssphäre vom Schutzbereich umfasst, somit schützt Art 8 EMRK die GrundrechtsträgerInnen, also die dem österreichischen Recht Unterworfenen, vor polizeistaatlicher Überwachung oder Datensammlung und -speicherung.[11] Personenbezogene Daten, „also alle Daten über eine bestimmte oder bestimmbare Person“[12], sind vom Privatleben mitumfasst und daher von Art 8 EMRK geschützt. Es handelt sich dabei um solche Daten, die eine Identifikation der betroffenen Person ermöglichen.[13]

Speicherverpflichtung

Durch die weitreichende Pflicht zu Speicherung der Daten von NutzerInnen wird stark in Art 8 EMRK eingegriffen. Die derart normierte Speicherung von Vor-, Nachname und Wohnadresse ist für sich bereits problematisch. Diese Daten müssen gem § 3 Abs 4 SVN-G vor jeder Registrierung einer/s PosterIn/s in einem Forum von DiensteanbieterInnen aufgenommen werden, überprüft werden sollen diese Informationen auf Grundlage von „Dokumenten, Daten oder Informationen, die von einer

10 Vgl. Grabenwarter/Pabel (2012): Europäische Menschenrechtskonvention, § 18 Rn. 14 ff.
11 Mayer/Kucsko-Stadlmayer/Stöger, Bundesverfassungsrecht11; 744ff.
12 Vgl. Paefgen (2016): Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet, 157.
13 Vgl. ebd., 67.

glaubwürdigen und unabhängigen Quelle stammen". Der Schutzbereich des Art 8 EMRK ist jedenfalls berührt, da hier personenbezogene Daten gespeichert werden müssen.

Rechtfertigung

Gemäß Art 8 Abs 2 EMRK ist ein Eingriff gerechtfertigt – und somit keine rechtswidrige Verletzung – wenn der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist. Die legitimen Ziele, die einen Eingriff rechtfertigen, werden von Art 8 Abs 2 EMRK taxativ aufgezählt. Eingriffe können demnach gerechtfertigt sein, wenn: der Eingriff gesetzlich vorgesehen ist, er außerdem in einer demokratischen Gesellschaft notwendig ist für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer.

Der EGMR hat mehrmals festgestellt, dass die Voraussetzung in Art 8 Abs 2 EMRK, wonach ein Eingriff „gesetzlich vorgesehen" (eng. „in accordance with the law") sein muss, mehr als die bloße Existenz eines Gesetzes erfordert. Vielmehr muss das Gesetz, das den Eingriff legitimiert, eine gewisse Qualität aufweisen. Außerdem benötigt es dem EGMR zufolge aber auch eine Vereinbarkeit mit der Rechtsstaatlichkeit, Zugänglichkeit und Vorhersehbarkeit[14] des Gesetzes. Das Merkmal der Vorhersehbarkeit ist im SVN-G mitunter als äußerst kritisch zu sehen, weil (wie unter „Legalitätsprinzip" ausgeführt) schon gar nicht klar ist, welche DiensteanbieterInnen überhaupt unter die Pflichten des SVN-G fallen und daher im Fall einer Verletzung mit Strafen zu rechnen haben und diese sich somit in großer Rechtsunsicherheit befinden.

Daneben ist auch die Notwendigkeit für ein solches Gesetz in einer demokratischen Gesellschaft kritisch zu sehen. Laut EGMR gilt grundsätzlich, dass ein Eingriff notwendig ist, wenn ein dringendes soziales Bedürfnis („pressing social need"[15]) besteht, das legitime Ziel zu erreichen, und die dafür vorgesehenen Mittel verhältnismäßig sind. Notwendigkeit bedeutet, dass der Eingriff nicht bloß nützlich oder zweckmäßig sein darf.[16] Einen wichtiger Schritt der Notwendigkeitsprüfung bildet die Beurteilung der Verhältnismäßigkeit, d.h. die ergriffene Maßnahme muss im Hinblick auf das legitime Ziel verhältnismäßig sein.[17] Im Rahmen einer Interessenabwägung muss das Interesse der Öffentlichkeit („pressing social need") an der Verfolgung des legitimen Ziels mit dem Interesse der betroffenen Person abgewogen werden.[18]

Auf das SVN-G angewandt sieht diese Prüfung wie folgt aus: Zunächst ist das verfolgte Ziel zu analysieren. Dies ist gem § 1 SVN-G die „Förderung des respektvollen Umgangs der Poster in online-Foren miteinander und [die] Erleichterung der Verfolgung von Rechtsansprüchen im Falle tatsächlich rechtswidriger Postings". Dieses Ziel ist wohl am ehesten subsumierbar unter „die öffentliche Ruhe und Ordnung", „die Verhinderung von strafbaren Handlungen" bzw. dem „Schutz der Rechte und Freiheiten anderer." Fraglich ist aber, ob die Maßnahmen des SVN-G überhaupt geeignet sind, um ein derartiges Ziel zu erreichen. Wie das Beispiel einer Klarnamenpflicht in Südkorea zeigte, änderten Klarnamen praktisch nichts an dem Umgang von UserInnen in Online-Foren.[19] Dies ist als Beispiel durchaus vergleichbar, weil die minimalen Voraussetzungen zur Herausgabe der Daten von

14 Vgl. Meyer-Ladewig et al. (2017): EMRK. Europäische Menschenrechtskonvention, 357.
15 EGMR, 04.12.2008, 30562/04 und 30566/04 (S. und Marper gegen Vereinigtes Königreich) Rn. 101.
16 Vgl. Meyer-Ladewig et al. (2017): EMRK. Europäische Menschenrechtskonvention, 359.
17 EGMR, 04.12.2008, 30562/04 und 30566/04 (S. und Marper gegen Vereinigtes Königreich) Rn. 102.
18 Vgl. Paefgen (2016): Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet, 157.
19 https://techcrunch.com/2012/07/29/surprisingly-good-evidence-that-real-name-policies-fail-to-improve-comments/?guccounter=1.

PosterInnen an Behörden und vor allem auch an Dritte im SVN-G es in der Praxis kaum mehr einen Unterschied zur Klarnamenpflicht geben wird. Zudem zeigt sich auch in der österreichischen Praxis, dass viele Menschen selbst durch die Anzeige ihres Klarnamens (z.B. auf Facebook) nicht davon abgehalten werden, Beschimpfungen, Anfeindungen und insbesondere auch strafrechtlich relevante Äußerungen zu tätigen.

Auch inwiefern die Strafverfolgung davon profitiert, kann in Zweifel gezogen werden, so bestanden schließlich schon bisher im Rahmen des § 18 ECG beispielsweise Pflichten, Daten von PosterInnen herauszugeben, die nicht allzu hoch angelegt waren. Dass aber nun alle PosterInnen ausnahmslos im Vorhinein registriert werden sollen, ist im Hinblick auf die Verhältnismäßigkeit des Gesetzes jedenfalls hochproblematisch. Einerseits ist die Speicherung durch private DiensteanbieterInnen eine massive Belastung dieser, außerdem wird damit ein hohes Risiko eingegangen, weil in großem Stil personenbezogene Daten bei diesen AnbieterInnen gesammelt werden.

Auskunftspflicht gegenüber Dritten

Ein Eingriff in das Privatleben liegt insb auch bei der Auskunftspflicht gegenüber Dritten in § 4 Abs 2 SVN-G vor, da die Wohnadresse eines Menschen nicht klar als allgemein verfügbar definiert werden kann.[20] Auch die Weiterleitung an Dritte oder Behörden greift in Art 8 EMRK ein. Ohne konkrete inhaltliche Verdachtsmomente sind die DiensteanbieterInnen verpflichtet, sofort Daten der PosterInnen herauszugeben und das Posting zu speichern, widrigenfalls sie eine Strafe gem § 7 Abs 1 Z 5 erhalten könnten. Hier wird das Interesse auf Achtung des Privatlebens der UserInnen jedenfalls verletzt, da nun der Preis für die Nutzung eines Online-Forums jener ist, dass Personen noch leichter als nach dem MeldeG oder ECG Name und Adresse einer fremden Person herausfinden können.

Die Maßnahme ist unverhältnismäßig, da es nicht das gelindeste Mittel darstellt, auf unbegründete Behauptungen hin, personenbezogene Daten inklusive der Wohnadresse an Dritte herauszugeben. Somit stellt auch die Auskunftspflicht für sich einen eigenständigen Grundrechtseingriff dar, da dadurch die ständige Gefahr droht, dass Dritte personenbezogene Daten eines Registrierungsprofils herausverlangen können, was permanente Eingriffe in das Privatleben durch Dritte ermöglichen kann.

Verletzung des Grundrechts auf Datenschutz (Art 1 § 1 DSG)

Die Speicher-, Überwachungs- und Auskunftspflichten im SVN-G stellen außerdem einen Eingriff in das Grundrecht auf Datenschutz nach Art 1 § 1 DSG dar. Auch ein Eingriff in dieses Grundrecht muss gem § 1 Abs 2 DSG den Gesetzesvorbehalt des Art 8 Abs 2 EMRK erfüllen. Da dies nicht erfüllt wird (siehe oben) verletzt der Entwurf auch § 1 DSG.

Fehlende Verhältnismäßigkeitsprüfung

Eine Rechtfertigung der Verhältnismäßigkeitsprüfung im Bezug auf das Recht auf Achtung der Privatsphäre und das Grundrecht auf Datenschutz fehlt in den Erläuterungen komplett. Damit wird verkannt, dass der Gesetzgeber in der Pflicht ist, Eingriffe in Grundrechte der BürgerInnen zu rechtfertigen.

20 Auch bei einer Auskunft nach dem Meldegesetz muss ein bestimmtes zusätzliches Merkmal, das eine Person eindeutig identifiziert, abgesehen von Vor- und Nachname genannt werden, um eine Wohnadresse zu erhalten.

Recht auf Meinungsfreiheit und Redaktionsgeheimnis (Art 10 EMRK)

Art. 10 EMRK:

(1) Jedermann hat Anspruch auf freie Meinungsäußerung. Dieses Recht schließt die Freiheit der Meinung und die Freiheit zum Empfang und zur Mitteilung von Nachrichten oder Ideen ohne Eingriffe öffentlicher Behörden und ohne Rücksicht auf Landesgrenzen ein. Dieser Artikel schließt nicht aus, dass die Staaten Rundfunk-, Lichtspiel- oder Fernsehunternehmen einem Genehmigungsverfahren unterwerfen.

Das Recht auf Meinungsfreiheit bildet einen der Grundpfeiler einer demokratischen Gesellschaft, da es gewährleistet, dass sich Menschen frei von staatlicher Einflussnahme eine Meinung bilden und diese auch frei äußern können. Dadurch sollen demokratische Werte wie Toleranz, Pluralismus und Weltoffenheit gewahrt bleiben.

Eine weitreichende Überwachung von Verhalten und Kommunikation ist allerdings dazu geeignet ein Klima zu schaffen, in dem Menschen sich in ihrer Meinungsäußerungsfreiheit sowie beim Konsum von – selbst legalen – Informationen zur Meinungsbildung selbst beschränken. Diese Gefahr besteht insbesondere dann, wenn der von der Überwachungsmaßnahme betroffene Personenkreis nur vage definiert ist und nur schwache Kontroll- und Rechtsschutzmechanismen vorhanden sind. Diese Selbstbeschränkung wird auch als „chilling effect" – eine potentiell abschreckende Wirkung für BürgerInnen – bezeichnet.[21] Durch die Registrierung ausnahmslos aller NutzerInnen der Dienstleistungen im Anwendungsbereich wird es verunmöglicht, in größeren Foren anonym zu posten. Dies könnte einen solchen „chilling effect" herbeiführen, der die Meinungsfreiheit einschränkt und Art10 EMRK verletzt.

Da das SVN-G keine Ausnahmen der Herausgabeverpflichtung für Redaktionen vorsieht, verletzt es das durch Art 10 EMRK garantierte Redaktionsgeheimnis. Das in § 31 Abs 1 MedienG geregelte Redaktionsgeheimnis ist eine Konsequenz bzw. bestimmte Ausformung des Rechts auf freie Meinungsäußerung iSd Art 10 EMRK. Das Redaktionsgeheimnis bezieht seine Rechtfertigung daher auch unmittelbar aus dem Grundrecht. Auf dieses kann man sich selbst dann stützen, „wenn die verlangte Auskunft Aufschluss über schwere und schwerste Verbrechen geben könnte."[22] Der Schutz der Vertraulichkeit journalistischer Quellen ist außerdem „eine der Grundbedingungen der Pressefreiheit"[23] und dadurch auch ein wesentlicher Bestandteil der konventionsrechtlichen Garantie des Art 10 EMRK.

Das Redaktionsgeheimnis (§ 31 Abs 1 MedienG) wurde auch im Kontext von Online-Foren bereits ins Treffen geführt. Mit dieser Frage setzte sich der OGH in der Rechtssache 6Ob188/14m auseinander. Darin bezog sich der OGH auf eine Entscheidung des OLG Wien (19 Bs 504/12z), in der dieses

21 Vgl. Auslegung EGMR 22.11.2007, RS0126501.
22 OGH, 16.12.2010, 13Os130/10g (13Os136/10i).
23 Gahleitner/Windhager, Redaktionsgeheimnis 2.0 – Sind Userdaten von § 31 MedienG geschützt?, Medien und Recht 3/2013, S. 108.

entschieden hatte, dass ein Online-Medium, das gleichzeitig als Provider und als Anbieter von Inhalten auftrat, sich auch bezüglich der Foren-Beiträge von Usern auf das Redaktionsgeheimnis berufen konnte und somit die Weitergabe von Daten an die Staatsanwaltschaft verweigern konnte. Der OGH schränkte dies aber folgendermaßen ein: „Eine Berufung auf das Redaktionsgeheimnis ist dann unzulässig, wenn ein Posting in keinerlei Zusammenhang mit einer journalistischen Tätigkeit steht. Es muss also zumindest irgendeine Tätigkeit, Kontrolle oder Kenntnisnahme eines Medienmitarbeiters intendiert sein, damit der Schutz des § 31 MedienG in Anspruch genommen werden kann."

In der Rechtssache 6Ob133/13x sprach der OGH außerdem aus, es erscheine richtig, „dass es Postings, die völlig ohne journalistische Kontrolle und Bearbeitung und allein aus dem eigenen Antrieb des Nutzers veröffentlicht werden, am notwendigen Zusammenhang mit der journalistischen Tätigkeit der in § 31 Abs 1 MedienG genannten Personen mangelt. Es muss also zumindest irgendeine Tätigkeit/Kontrolle/Kenntnisnahme eines Medienmitarbeiters intendiert sein, damit der Schutz des § 31 MedienG in Anspruch genommen werden kann. Allein die durch das Zurverfügungstellen des Online-Forums erklärte Absicht, alles zu veröffentlichen, was die Nutzer posten, reicht hingegen nicht aus, um den notwendigen Mindestzusammenhang zur Tätigkeit der Presse herzustellen."

In den Entscheidungsgründen zum obigen ersten Judikat schreibt das OLG Wien auch: „Die Betreiberin einer Onlinetageszeitung ist jedenfalls ein Medienunternehmen, sodass sie berechtigt ist, Antworten auf Fragen, welche die Person eines Einsenders von Beiträgen betreffen, zu verweigern. Dieses Verweigerungsrecht bezieht sich auch auf die Daten der Person eines Leserbriefschreibers und ist durch das Umgehungsverbot des § 31 Abs 2 MedienG zusätzlich abgesichert." Und weiter: „Die Anwendbarkeit des § 18 ECG ist nämlich davon abhängig, ob der Provider zugleich Medieninhaber ist oder nicht, das heißt, dass sich nur der Provider, der zugleich Medieninhaber ist, auf das Redaktionsgeheimnis in Bezug auf die Person des Posters berufen kann und daher nicht nach § 18 ECG zur Herausgabe verpflichtet ist." Alexander Koukal argumentiert zwar in einem Beitrag zu dem Erkenntnis des OLG Wien (wie auch der OGH I später entscheiden sollte), man müsse unterscheiden, ob Postings als Beiträge iSd § 1 MedienG gesehen werden können. Die PosterInnen teilen ihre Inhalte ja nicht primär nur den JournalistInnen mit, sondern auch anderen NutzerInnen bzw. einer bestimmten Öffentlichkeit. In der Regel könnten NutzerInnen auch ihre Postings selbstständig veröffentlichen und es gebe nur eine Nachkontrolle. Laut Koukal müsse man (auch im Einklang mit nunmehriger OGH-Judikatur) unterscheiden: lediglich wenn es um den Schutz von Personen gehe, die JournalistInnen geheime Informationen und vertrauliche Hinweise geben, könnten PosterInnen in Online-Foren durch das Redaktionsgeheimnis geschützt werden.[24]

Trotz all dieser Differenzierungen und Detailfragen ist aber eines klar festzustellen: Das gänzliche Ignorieren der Rechtsprechung in der Schaffung des neuen SVN-G zeugt von einem problematischen Verhältnis zum Redaktionsgeheimnis. Dies ist - wenn auch nicht in allen Fällen - auch im Rahmen von Online-Foren eine essentielle Rechtfertigung, um freien und unabhängigen Journalismus garantieren zu können. Dass sie im Gesetz nicht erwähnt wird kann auf mangelnde Legistik, aber auch darüber zurückführen sein, dass versucht werden soll, das Redaktionsgeheimnis in diesem Hinblick zu beschneiden, was als höchst bedenklich erscheint.

24 ZIR 2013/3, 187, https://h-i-p.at/Content/uploads/2018/04/ZIR3_Koukal.pdf und MR 2013/3, 107, http://weberling.de/images/Beitraege/windhager-mr-2013-3-107.pdf

BRUCH MIT DEM HERKUNFTSLANDPRINZIP

Nach der E-Commerce-RL gilt im Bereich des digitalen Binnenmarkts das Herkunftslandprinzip, was bedeutet, dass AnbieterInnen digitaler Dienste grundsätzlich den Bestimmungen des Landes unterworfen sind, in denen sie ihren Sitz haben. Nach § 3 Abs 1 SVN-G fallen aber alle DiensteanbieterInnen in seinen Anwendungsbereich, die ein Forum betreiben, das „auf Österreich ausgerichtet ist" (Z 1) oder die Einrichtung eines auf Österreich ausgerichteten Forum auch nur ermöglichen (Z 2), egal wo sie ihren Sitz haben. Damit wird dem Herkunftslandprinzip widersprochen. Problematisch ist dies insbesondere wegen des Verweises auf § 1330 ABGB in § 4 Abs 3 SVN-G.In Art 2 lit h i) 1. Teilstrich der E-Commerce-RL wird der sogenannte „koordinierte Bereich" definiert. Dieser umfasst: „Ausübung der Tätigkeit eines Dienstes der Informationsgesellschaft, beispielsweise Anforderungen betreffend das Verhalten des Diensteanbieters, Anforderungen betreffend Qualität oder Inhalt des Dienstes, einschließlich der auf Werbung und Verträge anwendbaren Anforderungen, sowie Anforderungen betreffend die Verantwortlichkeit des Diensteanbieters." Gem Art 3 Abs 2 E-Commerce-Richtlinie dürfen Mitgliedstaaten den freien Verkehr von Diensten der Informationsgesellschaft aus einem anderen Mitgliedstaat nicht aus Gründen einschränken, die in den koordinierten Bereich fallen. Dafür gibt es allerdings wiederum Ausnahmen gem. Art 3 Abs 4 E-Commerce-RL: Abweichungen vom Herkunftslandprinzip sind unter anderem möglich im Bereich des Strafrechts (in § 22 Abs 2 Z 1 ECG umgesetzt). Auch in den Erläuterungen zum ECG steht zum Herkunftslandprinzip im koordinierten Bereich: „Auch können die Behörden der Mitgliedstaaten nach ihrem Recht im Einzelfall gegen fremde Anbieter vorgehen, wenn diese gegen bestimmte Schutzgüter verstoßen (z.B.: bei strafbaren Handlungen im Internet)."[25] Damit könnte also die Anwendung auf AnbieterInnen außerhalb von Österreich in anderen Mitgliedstaaten gerechtfertigt werden in Bezug auf §§ 111 und 115 StGB. Der § 1330 ABGB normiert aber einen zivilrechtlichen Anspruch. **Damit ist diese vorgeschlagene Regelung in § 4 Abs 2 SVN-G ein eindeutiger Verstoß gegen die E-Commerce-Richtlinie und somit unionsrechtswidrig.**

DATENSCHUTZ IN DRITTSTAATEN

Nach dem SVN-G müssen personenbezogene Daten gespeichert werden, egal, in welchem Land die/der DiensteanbieterIn ihren/seinen Sitz hat, solange ihr/sein Dienst „auf Nutzer in Österreich ausgerichtet ist" (§ 3 Abs 1 Z 1 SVN-G) oder dies ermöglicht wird (§ 3 Abs 1 Z 2 SVN-G). Potentiell kann dies also auch in Ländern sein, in denen weder die hohen Datenschutzstandards der EU gelten, noch mit diesen vergleichbare. **Mit dieser Regelung wird also in Kauf genommen, dass der Schutz dieser personenbezogenen Daten und der Privatsphäre nicht gewährleistet werden kann.**[26]

LEGALITÄTSPRINZIP

Große Probleme weist das Gesetz vor allem in Bezug auf die Determinierungsschärfe auf, die besonders bei eingriffsintensiven Normen von höchster Relevanz ist. Das sogenannte Bestimmtheitsgebot (bzw. auch Determinierungsgebot/-pflicht) ist als Ausfluss des rechtstaatlichen Prinzips auch eines der tragenden Prinzipien des österreichischen Rechtsstaates. Rechte und Pflichten

25 Erläuterungen ECG S. 3 letzter Absatz.
26 Vgl. dazu auch EuGH Digital Rights Ireland, Rz 68.

der Rechtsunterworfenen (aber auch die Befugnisse derjenigen, die das Recht zu vollziehen haben) müssen präzise festgelegt werden, denn, so etwa Mayer/Kucsko-Stadlmayer/Stöger: „Durch die Bestimmtheit -genauer: Vorausbestimmtheit - der Rechte und Pflichten durch Gesetz unterscheidet sich der Rechtsstaat von seinem Gegentyp, dem Polizeistaat; der Rechtsstaat ist ‚berechenbar'."[27] Besonders bei „eingriffsnahen" Gesetzen, solchen Gesetzen also, die in die Grundrechte von Personen eingreifen, muss besonders klar vordefiniert sein, wie weit Behörden gehen dürfen. Als ein solches Gesetz kann das SVN-G jedenfalls gesehen werden. Gleichzeitig lässt es mit unklaren Definitionen genau die in derartigen Fällen geforderte Klarheit vermissen.

Besonders problematisch sind die unklaren Definitionen in den §§ 3 und 4 SVN-G, die Registrierung und Authentifizierung respektive Übermittlungspflichten regeln. In § 3 Abs 1 werden die nach dem SVN-G Verpflichteten aufgezählt. Darunter fallen gem Z 1 DiensteanbieterInnen, die ein Forum einrichten und betreiben, „das auf Nutzer in Österreich ausgerichtet ist". Was diese „Ausrichtung" aber bedeuten soll, bleibt im Entwurf, sowie in den Erläuterungen unklar. So steht in den Erläuterungen zu § 3 SVN-G etwa:„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 auf Nutzer in Österreich ausgerichtet qualifiziert werden können. Das etwa von einem Zeitungsunternehmen in Frankreich bereitgestellte Forum zur Kommentierung des Webangebots der französischen Zeitung fällt daher selbstverständlich auch dann nicht unter den Anwendungsbereich, wenn sich 'österreichische' Nutzer in diesem Forum beteiligen oder auf Österreich bezogene Inhalte vorzufinden sind."

Für die Beurteilung dieser Frage wird im Anschluss auch bloß lapidar das Kriterium „etwa Werbeeinnahmen" genannt. Und obwohl die französische Zeitung „selbstverständlich nicht" in den Anwendungsbereich falle, beschließt der Absatz zu den Erläuterungen zu § 3 Abs 1 SVN-G mit der Feststellung: „Ein angebotenes Forum (dh. ‚sein' Diensteanbieter) fällt aber nicht aber schon deswegen aus dem Anwendungsbereich heraus, weil in dem Forum europäische oder internationale Themen zur Debatte gestellt werden, die mit Österreich nichts oder wenig zu tun haben." Wo hier die Grenze gezogen wird, bleibt daher unklar. Insbesondere im Hinblick auf die hohen Strafdrohungen bei Missachtung der Regelungen des § 7 SVN-G ist Klarheit darüber, welche Dienste genau in seinen Anwendungsbereich fallen aber unumgänglich.

VERRINGERUNG DES MISSBRAUCHSPOTENTIALS

Sollte trotz der massiven grundsätzlichen Grundrechtsbedenken dieses Vorhaben dennoch durchgesetzt werden, muss dies mit geeigneten Maßnahmen zur Verringerung des Missbrauchspotentials einhergehen.

Etablierung einer Durchlaufstelle

Mit dem vorgeschlagenen Entwurf wird ein großer und sehr diverser Kreis an privatwirtschaftlichen Plattformen und ForenbetreiberInnen zur Kooperation mit Gerichten, Staatsanwaltschaften, Polizei und Privatpersonen verpflichtet. Die Herausgabe von identifizierenden Informationen einer/s PosterIn/s stellt einen Eingriff in dessen Privatsphäre dar, welcher nur aufgrund einer gesetzlichen Grundlage im Falle eines gültigen Anspruches durchgeführt werden darf. Die Prüfung, ob eine Anfrage

27 Mayer/Kucsko-Stadlmayer/Stöger, Bundesverfasssungsrecht[11], 92.

ausreichend begründet ist, würde vor allem kleinere Plattformen vor große Herausforderungen stellen. Verschiedene Plattformen würden darüber hinaus sehr wahrscheinlich zu unterschiedlichen Entscheidungen in der Prüfung der Zulässigkeit von ähnlichen Anträgen kommen. Ein direkter Kontakt zu den Dritten, die die Herausgabe verlangen, könnte darüber hinaus Auswirkungen auf die Moderation von Postings haben und womöglich das Löschverhalten verändern.

Aufgrund ähnlicher Problemfelder hatte der österreichische Gesetzgeber in der Normierung der Vorratsdatenspeicherung deshalb das Instrument einer Durchlaufstelle[28] festgeschrieben (siehe §§ 102a, 102b und 103c TKG), welche als Sicherungsschutzschicht zwischen privaten DatenverarbeiterInnen und InteressensträgerInnen an deren Daten fungiert. Durch dieses Instrument in Form einer staatlichen Stelle wurden folgende Vorteile erzielt:

1) Die staatliche Durchlaufstelle prüft die Korrektheit aller Anfragen und sorgt damit für einen robusten und nachvollziehbaren Standard, welche Anfragen auskunftsberechtigt sind und welche aufgrund welcher Begründung nicht. Interessierte Stellen sind somit nicht einer unterschiedlichen Handhabung ihrer Anfragen durch verschiedene Plattformen ausgesetzt

2) Plattformen können sich auf die Prüfung der Durchlaufstelle verlassen und sind keinem direkten Kontakt durch PolizeibeamtInnen oder Privatpersonen mit einem Informationsinteresse ausgesetzt. Jede von der Durchlaufstelle weitergeleitete Anfrage erfüllt die Anforderungen des Gesetzgebers.

3) Durch das Modell der Durchlaufstelle gibt es eine verpflichtende Statistik, aufgrund welcher Rechtsgrundlage von welchen Stellen von welchen Betreibern wie oft welche Daten beauskunftet werden. Durch dieses Datenmaterial wird eine sachliche Überprüfung der vorgeschlagenen Maßnahme erst ermöglicht. Der Gesetzgeber ist zum Nachweis der Notwendigkeit, Nützlichkeit und Verhältnismäßigkeit jedes Grundrechtseingriffs angehalten und im Falle der Beauskunftung aufgrund von Privatanklagedelikten wäre ein Nachweis sonst nicht erreichbar.

Gefahren einer zentralisierten Datenspeicherung

Aufgrund der öffentlichen Debatte scheint es bei einigen größeren Forenbetreibern die Vorstellung einer Auslagerung oder Zentralisierung des Identifikations- und Auskunftssystems zu geben. Einer derartigen Idee kann aus Grundrechtsperspektive nur eine entschiedene Absage erteilt werden. Die entscheidende Messlatte dieses Gesetzes ist, wie verhältnismäßig die neuen Speicher- und Kontrollverpflichtungen über die Identität aller Menschen in Österreich, die von ihrem Grundrecht auf Meinungsfreiheit Gebrauch machen ist, gegenüber der konkreten Verbesserung der spezifischen Aufklärungsquote. Mit der Auslagerung der Identifikationsdaten an eine staatliche oder zentralisierte privatwirtschaftliche Stelle würde der Grundrechtseingriff aufgrund des enormen Missbrauchspotentials einer solchen Stelle noch deutlich verstärkt.

28 Tschohl, C.: Dissertation: Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung in Österreich, approbiert im Dezember 2011 (Universität Wien, rechtswissenschaftliche Fakultät), abrufbar im online-Archiv der Universität Wien, online: http://othes.univie.ac.at/17556/1/2011-10-16_0207311.pdf (2011).

ZUSAMMENFASSUNG

- Die **Speicherverpflichtung von personenbezogenen Daten, wie sie im SVN-G vorgesehen ist, stellt eine Vorrastdatenspeicherung dar und ist damit grundrechtswidrig.** Eine anlasslose Speicherung von einer Masse an personenbezogenen Daten ist in einer Demokratie niemals verhältnismäßig und kein adäquates Mittel zu Rechtsdurchsetzung.
- Die **Auskunftspflichten** im SVN-G gehen – insb im Hinblick auf die Verpflichtung zur Herausgabe von personenbezogenen Daten gegenüber Dritten – **zu weit**. So wird der Schutz von Opfern von Gewalt und Stalking erschwert, das Redaktionsgeheimnis verletzt und die freie Meinungsäußerung erschwert.
- Durch die expliziten und impliziten **Überwachungspflichten im SVN-G wird die E-Commerce-Richtlinie verletzt.**
- Insbesondere bei einer Verpflichtung zur **Datenspeicherung im EU-Ausland durch das SVN-G kann der Schutz personenbezogener Daten nicht gewährleistet werden.**
- Das SVN-G **verletzt das Recht auf Achtung der Privatsphäre gem Art 7 GRC und Art 8 EMRK, das Grundrecht auf Datenschutz gem Art 8 GRC und § 1 DSG, sowie das Grundrecht auf Freiheit der Meinungsäußerung nach Art 10 EMRK.**
- Auch die unklare Bestimmung **des Anwendungsbereiches** ist insbesondere im Hinblick auf die hohen Strafdrohungen verfassungsrechtlich bedenklich.
- Sollte es trotz der massiven grundrechtlichen Bedenken zu einer Speicher- und Herausgabeverpflichtung der Dienstleister der Informationsgesellschaft kommen, muss die Datenweitergabe mittels einer **Durchlaufstelle** vorgesehen werden.