# Kein neuer Regulierungsbedarf für Social Media

**Bern, 10.05.2017 - Der Bundesrat kommt in seiner am 10. Mai publizierten Standortbestimmung zur rechtlichen Basis für Social Media zum Schluss, dass zum gegenwärtigen Zeitpunkt kein Bedarf für neue Regulierungsmassnahmen besteht. Regulierungsvorhaben wie die Revision des Datenschutzgesetzes und die Arbeiten zum Ausbau des Jugendmedienschutzes werden den Schutz für die Nutzenden von sozialen Netzwerken in der Schweiz mittelfristig verbessern. Die Entwicklungen, auch auf internationaler Ebene, sind jedoch weiter zu beobachten.**

Im Oktober 2013 hatte der Bundesrat einen ersten Bericht "Rechtliche Basis für Social Media" in Erfüllung des Postulats Amherd 11.3912 zuhanden der Eidgenössischen Räte verabschiedet. Zum damaligen Zeitpunkt waren die rechtlichen Abklärungen bzw. Revisionsarbeiten insbesondere zum Datenschutz, zum Jugendmedienschutz und im Bereich des Fernmelderechts noch nicht weit genug fortgeschritten, um ihre Auswirkungen für eine Regulierung von Social Media beurteilen zu können. Der Bundesrat gab daher eine erneute Standortbestimmung in Auftrag. Der Bericht "Rechtliche Basis für Social Media: Erneute Standortbestimmung" zeigt neue Entwicklungen im Bereich Social Media der letzten Jahre auf und analysiert die Rechtslage in der Schweiz.

## "Fake News" und "Social Bots" als neue Phänomene

Die zunehmende Beeinflussung bzw. Manipulation des politischen Diskurses durch Falschinformationen ("Fake News") und der Umstand, dass sie zunehmend durch Programme (sog. "Social Bots") automatisch generiert werden, sind derzeit Thema einer intensiven Debatte. Social Media spielen bei der Verbreitung von "Fake News" eine zentrale Rolle. Der Bericht stellt fest, dass einzelne problematische Aspekte dabei bereits heute vom geltenden Recht abgedeckt sind. Plattformbetreiber und private Organisationen haben verschiedene Initiativen zur Selbstregulierung gegen absichtlich produzierte Falschinformationen lanciert.

Der Bundesrat ist der Ansicht, dass es vorerst nicht angezeigt ist, in diesem Bereich zusätzliche Normen zu schaffen. Die nationalen und internationalen Entwicklungen sind jedoch zu beobachten und es ist zu analysieren, ob der bestehende Rechtsrahmen zusammen mit den Instrumenten der Selbstregulierung genügt oder ob darüber hinaus weitere staatliche Regulierung notwendig sein wird.

## Immer mehr Werbung in sozialen Netzwerken

Mit der zunehmenden Popularität und Professionalisierung von "Social Media-Stars" werden soziale Netzwerke als Verbreitungskanäle für kommerzielle Werbebotschaften immer beliebter. Im Schweizer Recht fehlen heute spezifische Deklarationsvorschriften für Werbung auf Social Media. Zu beachten sind lediglich die Vorschriften des Lauterkeitsrechts.

Ob das für Radio- und Fernsehwerbung geltende Transparenzgebot auf Social Media auszudehnen ist, wird im Rahmen der Vorbereitungsarbeiten für ein Gesetz über elektronische Medien zu prüfen sein.

## Laufende Regulierungsvorhaben

Aktuell laufen verschiedene Regulierungsvorhaben, welche auch einen Bezug zu Social Media aufweisen und die Sicherheit der Nutzenden von sozialen Netzwerken mittelfristig verbessern werden.

**Datenschutz**
Das revidierte Datenschutzgesetz (DSG) regelt zahlreiche Aspekte, welche im Zusammenhang mit Social Media von Bedeutung sind, etwa die Pflicht zum Datenschutz durch Technik oder den Ausbau der Sorgfaltspflichten bei der Datenbearbeitung. Die Vernehmlassung zum DSG ging im April 2017 zu Ende, die Ergebnisse werden derzeit vom Eidgenössischen Justiz- und Polizeidepartement (EJPD)ausgewertet.

**Jugendschutz**
An einer Verbesserung des Jugendmedienschutzes auch auf Social Media arbeitet das Eidgenössische Departement des Inneren (EDI). Bis Ende 2017 soll ein Gesetzesentwurf zur einheitlichen Regelung von Alterskennzeichnungen und Abgabebeschränkungen für Games und Videos vorliegen. Mit dem nationalen Projekt "Jugend und Medien" werden Jugendliche für den Umgang mit Medien sensibilisiert.

**Telekommunikation**
Auch die Revision des Fernmeldegesetzes (FMG) sieht Vorgaben für eine Verbesserung des Kinder- und Jugendschutzes vor. Fernmeldedienstanbieterinnen sollen unter anderem verpflichtet werden, beim Kauf von Mobilfunk- und Internetabonnements eine Beratung über die Möglichkeiten zum Schutz von Kindern und Jugendlichen anzubieten.

**Sicherheit**
Das totalrevidierte Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) und das neue Nachrichtendienstgesetz (NDG), welche voraussichtlich 2018 in Kraft treten, werden dazu beitragen, Personen auf grösseren Social-Media-Plattformen zur Wahrung wichtiger Landesinteressen zu identifizieren und überwachen zu können.

## Internationale Rechtsdurchsetzung als Herausforderung

Der Bundesrat hält fest, dass es schwierig sein kann, Rechtsansprüche international geltend zu machen. Die laufenden Bestrebungen auf internationaler Ebene, etwa im Europarat, hier eine praxisgerechte Lösung zu finden, sind deshalb von der Schweiz mit Nachdruck voranzutreiben.

## Erneute Standortbestimmung

Der Bericht wurde drei Jahre nach der ersten Standortbestimmung vom Bundesrat zur rechtlichen Basis für Social Media erstellt. Die zwischenzeitlich begonnenen Revisionsarbeiten wurden berücksichtigt.

**Adresse für Rückfragen**

Bundesamt für Kommunikation BAKOM
Medienstelle
+41 58 460 55 50, media@bakom.admin.ch

**Herausgeber**

Der Bundesrat
https://www.admin.ch/gov/de/start.html

Bundesamt für Kommunikation
http://www.bakom.admin.ch

Generalsekretariat UVEK
https://www.uvek.admin.ch/uvek/de/home.html

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Der Bundesrat**

Bern, 10. Mai 2017

# Rechtliche Basis für Social Media: Erneute Standortbestimmung

## Nachfolgebericht des Bundesrates zum Postulatsbericht Amherd 11.3912 „Rechtliche Basis für Social Media“

# Zusammenfassung

Am 9. Oktober 2013 verabschiedete der Bundesrat in Erfüllung des Postulats Amherd 11.3912 vom 29. September 2011 den Bericht Rechtliche Basis für Social Media zuhanden der Eidgenössischen Räte (nachfolgend Social Media-Bericht 2013). Gleichzeitig beauftragte der Bundesrat das UVEK, ihm bis Ende 2016 eine erneute Standortbestimmung zur gesetzlichen Basis für Social Media vorzulegen.

Ein zusätzlicher Bericht ist insbesondere nötig, weil zur Zeit der Beurteilung der Thematik im Rahmen des Social Media-Berichtes 2013 diverse Gebiete Gegenstand vertiefter Abklärungen waren bzw. nationale Gesetze und internationale Bestimmungen einer umfassenden Revision unterzogen wurden.

Das Nutzungsverhalten auf sozialen Netzwerken (Facebook, Twitter, Youtube usw.) hat sich seit 2013 verändert und die Vielfalt möglicher Anwendungsformen und Angebote hat zugenommen. Ganz allgemein ist festzuhalten, dass Social Media bei der öffentlichen Meinungsbildung an Bedeutung gewinnen. Einerseits, weil sich vor allem jüngere Menschen vermehrt über diese Kanäle informieren und andererseits, weil auf Social Media veröffentlichte Inhalte zunehmend Eingang in die Berichterstattung der traditionellen Massenmedien finden. Die Abgrenzung zwischen herkömmlichen Massenmedien und Social Media-Plattformen verschwimmt zusehends.

International feststellbar ist eine zunehmende Beeinflussung bzw. Manipulation des politischen Diskurses durch Falschinformationen („Fake News“). Die Eigenheiten und die Funktionsweise von Social Media, wie höhere Anonymität der Autorenschaft und das gesteigerte Interesse an unglaublich erscheinenden, überraschenden Inhalten (Mechanismus der Aufmerksamkeitsökonomie), begünstigen dieses Phänomen. Eine neue Dimension erreichen „Fake News“ durch den Umstand, dass sie mittlerweile durch Programme automatisch generiert werden (sog. „Social Bots“). Im Ausland werden rechtliche Massnahmen gegen die negativen Auswirkungen von „Fake News“ ins Auge gefasst. In der Schweiz scheint es angezeigt, diese Entwicklungen vorerst zu beobachten.

Wichtige Akteure im Zusammenhang mit der Meldung von problematischen Inhalten auf sozialen Plattformen sind die sog. „Trusted Flaggers“. Melden diese z.B. ein Gewaltvideo, so wird ihr Antrag privilegiert behandelt und das Video sehr rasch wieder gelöscht. In der Schweiz übt das Bundesamt für Polizei fedpol diese Aufgabe bei Youtube aus und meldet hauptsächlich terroristische Propaganda und Gewaltdarstellungen. Es wäre sinnvoll, wenn fedpol diese Tätigkeit auch auf andere Social Media-Plattformen ausdehnen könnte.

Wie die vorliegende aktualisierte Standortbestimmung zeigt, sind die im Social Media-Bericht 2013 aufgeworfenen Fragen weitestgehend in den laufenden Regulierungsvorhaben berücksichtigt worden. Der Bundesrat kommt daher zum Schluss, dass derzeit keine zusätzlichen Regulierungsaktivitäten in Bezug auf Social Media ausgelöst werden müssen.

Das Recht auf Datenmitnahme ist Gegenstand einer umfassenden Analyse der Rechtslage in der Schweiz, der EU und in ausgewählten Vergleichsländern. Es ist vorgesehen, dass sie im Rahmen der Umsetzung der bundesrätlichen Strategie „Digitale Schweiz“ bis Ende 2017 vorgelegt wird. Die Federführung für diese Arbeiten liegt beim Eidgenössischen Justiz- und Polizeidepartement EJPD.

Spezifische Deklarationsvorschriften für Werbung in Social Media fehlen heute im geltenden Schweizer Recht. Zu beachten sind lediglich die allgemeinen Vorschriften des Lauterkeitsrechts. Mit der zunehmenden Popularität und Professionalisierung von Social Media-Stars erfreuen sich soziale Plattformen aber immer grösserer Beliebtheit als Verbreitungskanäle auch für kommerzielle Werbebotschaften. Die unverfälschte Meinungsbildung bei den Rezipienten legt es nahe, das für Radio- und Fernsehwerbung geltende Transparenzgebot auf Social Media auszudehnen. Diese und weitere Regulierungsfragen sind Gegenstand der aktuell laufenden Prüfung, ob das schweizerische Recht punktuell mit entsprechenden europäischen Vorschriften und Regulierungsvorhaben zu harmonisieren ist.

Problematisch bleibt die Rechtsdurchsetzung im grenzüberschreitenden Bereich im Zusammenhang mit Social Media. Wie verschiedene parlamentarische Vorstösse beweisen, findet das Thema auch

politisch Beachtung. Im März 2017 hat der Ständerat die Motion Levrat 16.4082 „Den Strafverfolgungsbehörden den Zugang zu Daten von sozialen Netzwerken erleichtern“ an die zuständige Kommission zur Vorprüfung überwiesen. Auch das Bundesgericht hat sich mit der Frage befasst. Die laufenden Bestrebungen auf internationaler Ebene, z.B. im Europarat, hier eine praxisgerechte Lösung zu finden, sind von der Schweiz mit Nachdruck voranzutreiben.

# Inhalt

# 1 Einleitung: Warum eine aktualisierte Standortbestimmung?

Ziel des vorliegenden Berichts ist eine aktualisierte Standortbestimmung zu den juristischen Grundlagen für soziale Netzwerke. Am 9. Oktober 2013 hatte der Bundesrat einen ersten Bericht in Erfüllung des Postulats Amherd 11.3912 Rechtliche Basis für Social Media vom 29. September 2011[1] zuhanden der Eidgenössischen Räte (nachfolgend: Social Media-Bericht 2013)[2] verabschiedet. Gleichzeitig beauftragte der Bundesrat das UVEK, ihm bis Ende 2016 eine aktualisierte Standortbestimmung zur gesetzlichen Basis für Social Media vorzulegen. Dabei sollten insbesondere die dannzumal laufenden rechtlichen Abklärungen bzw. Revisionsarbeiten im Jugendmedienschutz und im Datenschutz berücksichtigt werden. Aufgrund für die Standortbestimmung wichtiger neuer Entwicklungen, insbesondere im Bereich des Datenschutzgesetzes (welches Ende Dezember 2016 in die Vernehmlassung geschickt wurde), des Jugendmedienschutzes und anderer relevanter Rechtsgebiete hat das UVEK die erneute Standortbestimmung einige Monate später vorgelegt.

Der Bundesrat war in seinem Social Media-Bericht 2013 zum Schluss gekommen, dass aufgrund der bisherigen Erfahrungen im geltenden schweizerischen Recht keine grösseren Regelungslücken offenbar würden. Die allgemeinen gesetzlichen Regeln erlaubten bei umsichtiger Anwendung eine angemessene Antwort auf die meisten mit sozialen Netzwerken verbundenen Probleme für die Allgemeinheit und die Betroffenen. Die neuen Herausforderungen durch Social Media sind nicht mit einem Spezialgesetz zu bewältigen. Der Bundesrat hielt damals fest, dass punktuell rechtliche Verbesserungen denkbar wären. Aus diesem Grunde seien in verschiedener Hinsicht (z.B. im Datenschutz und im Jugendschutz) Abklärungen notwendig oder bereits im Gange.[3]

# 2 Neuerungen seit Einreichung des Postulats Amherd 11.3912

## 2.1 Allgemeines

Dieses Kapitel befasst sich mit den Entwicklungen, welche seit dem ersten Bericht im Jahre 2013 aufgrund des technischen Fortschritts und des gewandelten Nutzungsverhaltens in Bezug auf Social Media zu beobachten sind. Dazu gehören auch Phänomene, deren problematische Auswirkungen sich in den vergangenen Jahren akzentuiert haben (z.B. „Social Bots“).

Seit 2013 steigen die ohnehin hohen Nutzungszahlen im Internet stetig, und zwar je nach Nutzungsintensität um ca. 6% bzw. ca. 3%.[4] Gerade bei der Nutzung von Social Media ist eine deutliche Zunahme zu verzeichnen. Die mobile Internet-Nutzung in der Schweizer Bevölkerung lag bei 63% im Jahr 2015. Am meisten verbreitetes mobiles Zugangsgerät ist das Smartphone.[5]

Social Media können in den verschiedensten Formen auftreten. Zu erwähnen sind beispielsweise:

---

[1] 11.9312 „Rechtliche Basis für Social Media“. In ihrem Postulat vom 29.09.2011 wies Nationalrätin Viola Amherd darauf hin, dass Social Media eine neue Dimension in der Kommunikation und in der Mediennutzung bewirken, welche die Durchsetzung nationaler Gesetzte und Grundrechte auszuhebeln drohe. Dies betreffe insbesondere Regeln zum Datenschutz, gegen Rassismus oder allgemein den Schutz der Privatsphäre. Möglicherweise müsse diese Entwicklung mit einer Regelung der Social Media begegnet werden. Der Nationalrat beauftragte den Bundesrat durch die Überweisung des Postulats mit der Erarbeitung eines Berichts über die Rechtslage in Bezug auf Social Media; abrufbar unter: http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch id=20113912.

[2] https://www.bakom.admin.ch/bakom/de/home/das-bakom/medieninformationen/medienmitteilungen.msg-id-50504.html.

[3] Social Media-Bericht 2013, Ziff. 8, S. 79.

[4] Gemäss der Untersuchung des Bundesamtes für Statistik (BfS) „Internetnutzung in der Schweiz, Entwicklung in % der Bevölkerung ab 14 Jahren“ gaben in der Periode Oktober 2015 bis März 2016 84% an, das Internet mehrmals pro Woche zu nutzen. 88.9% gaben an, das Internet während den letzten 6 Monaten genützt zu haben. Im Jahr 2011 lagen die Zahlen bei 78.5 bzw. 85.2 %; abrufbar unter: https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/haushalte-bevoelkerung/internetnutzung.html.

[5] https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/haushalte-bevoelkerung/mobile-internetnutzung.html.

- Netzwerke (z.B. Facebook, Google+, Xing, LinkedIn, Myspace, Mixi, Taringa!, Orkut, Skyrock, Renren, Qzone, academia);
- Mikroblogs (Tumblr, Twitter, Sina Weibo);
- Wissenssammlungen (Wikipedia);
- Foren, Newsgroups und Mailinglisten;
- Social News (Huffington Post, Buzzfeed, Slashdot, Watson);
- Medienseiten (Youtube, Instagram, Flickr, SoundCloud, Last.fm, Musical.ly, Vine, DeviantArt);
- Soziale Frage-und-Antwortseiten (Yahoo Answers, Quora, Ask.fm);
- Portale für Kundenbewertungen (Amazon, Yelp);
- Überblicksseiten (Pinterest, Reddit, StumbleUpon, delicious);
- Messenger-Plattformen (Snapchat, WhatsApp, Kik);
- Plattformen zur Partnersuche (Tinder);
- ortsbasierte Netzwerke (Foursquare, Meetup).

## 2.2 Nutzung von Social Media

Im Jahr 2015 nutzten insgesamt 88% der Schweizer Bevölkerung das Internet. Gemäss einem Forschungsbericht der Universität Zürich aus dem Jahr 2015 geben 50% der Schweizer Nutzer an, private soziale Online-Netzwerke oder Online Communities zu verwenden, 30% auch für berufliche Zwecke. Gesamthaft machen 59% der Schweizer Internet-Nutzer beruflich oder privat von sozialen Netzwerken Gebrauch. Insgesamt 82% der Nutzenden (48% der Internet-User) gebrauchen soziale Online-Netzwerke mindestens einmal wöchentlich, 63% der Nutzer von sozialen Online-Netzwerken loggen sich täglich ein. Der Anteil der Schweizer Bevölkerung, der berufliche oder private soziale Netzwerke nutzt, ist seit 2011 um 10% gestiegen. Im Jahr 2015 ist gegenüber 2013 insbesondere eine deutliche Zunahme von Nutzern bei beruflichen Netzwerken zu verzeichnen (+12%). Social Media nutzen am häufigsten die 20-29 jährigen, gefolgt von den 14-19-Jährigen. Bei den 70-84-Jährigen nutzen 16% Online-Netzwerke.[6]

Weltweit am meisten Nutzende verzeichnet Facebook mit ca. 1.7 Mrd. (Stand Juli 2016). Weitere sehr häufig genutzte Social Media-Dienste im Jahr 2016 sind Instagram und Google+ mit jeweils 500 Mio. Usern, LinkedIn mit 433 Mio., gefolgt von Twitter mit 320 Mio., Snapchat und Pinterest mit je ca. 100 Mio. weltweiten Nutzern.[7]

Social Media haben sich in der Kommunikation von Unternehmen etabliert. Rund 90% aller befragten Schweizer Unternehmen, auch Behörden und Nonprofit-Organisationen sind auf Plattformen aktiv. An der Spitze finden sich Facebook sowie die Videoplattform YouTube. Es folgen Twitter, Xing und LinkedIn, Google+, Blogs und Instagram. Diese Kanäle entwickelten sich zu zentralen Werkzeugen der Kommunikation.[8]

Während die Nutzung im Radio- und Fernsehbereich im Zeitverlauf relativ stabil geblieben ist[9], verzeichnet die Nutzung des Internets und insbesondere von Social Media in den letzten 15 Jahren einen markanten Anstieg. Die Mediennutzung unterscheidet sich dabei stark nach dem Alter. Die jungen Menschen zwischen 15 und 34 Jahren nutzen das Internet täglich mit Abstand am längsten, nämlich

---

[6] Latzer Michael/Just Natascha/Metreveli Sulkhan/Saurwein Florian, Internet-Anwendungen und deren Nutzung in der Schweiz. Themenbericht aus dem World Internet Project-Switzerland 2013, Universität Zürich, Zürich, S. 21f http://www.mediachange.ch/media/pdf/publications/Anwendungen_Nutzung_2013.pdf.

[7] Übersicht aktueller Social Network Statistiken; abrufbar unter: http://socialmedia-institute.com/uebersicht-aktueller-social-media-nutzerzahlen/

[8] Bernet PR AG für Kommunikation ZHAW Studie Social Media Schweiz 2016; abrufbar unter: http://www.bernet.ch/Social Mediastudie.

[9] Bericht zur Überprüfung der Definition und der Leistung des Service public der SRG unter Berücksichtigung der privaten elektronischen Medien, Bericht des Bundesrates vom 17. Juni 2016 in Erfüllung des Postulates 14.3295 der Kommission für Verkehr und Fernmeldewesen des Ständerates (KVF-S), Kap. 9.1.2, S. 69; abrufbar unter: https://www.bakom.admin.ch/dam/bakom/de/dokumente/Elektronische%20Medien/Medienpolitik/service-public-bericht.pdf.download.pdf/Bericht%20Service%20public.pdf.

während ca. viereinhalb Stunden. Es zeigt sich auch, dass die junge Bevölkerungsgruppe weniger Radio- und Fernsehprogramme konsumiert, sondern die Zeit vermehrt im Internet verbringt.[10]

### 2.2.1 Social Media-Angebote journalistischer Unternehmen

Im Social Media-Bericht 2013 wurde auf das Zusammenspiel zwischen den sozialen Netzwerken und den herkömmlichen, nach journalistischen Kriterien gestalteten Medien hingewiesen.[11] Während die traditionellen Massenmedien den sozialen Netzwerken oft zu verstärkter Aufmerksamkeit verhelfen, dienen letztere den Massenmedien zunehmend als Lieferanten von Informationen und Neuigkeiten. Diese Entwicklung hat sich in den vergangenen Jahren akzentuiert.

#### 2.2.1.1 Entwicklungen beim übrigen publizistischen Angebot der SRG

Verstärkt hat sich auch der Trend, dass herkömmliche Medienhäuser (z.B. Rundfunkveranstalter) selber auf Social Media-Plattformen präsent sind. Dies gilt in besonderem Masse für die SRG. Deren Social Media-Auftritt gehört zum übrigen publizistischen Angebot (üpA), welches gemäss Art. 25 Abs. 3 Bst. b des Bundesgesetzes über Radio und Fernsehen (RTVG; SR 784.40) ebenfalls aus den Empfangsgebühren finanziert wird.[12]

Mit der Mitte 2016 in Kraft gesetzten Teilrevision des RTVG wurde die Zuständigkeit zur Aufsicht über das üpA der SRG vom BAKOM auf die Unabhängige Beschwerdeinstanz für Radio und Fernsehen (UBI) verlagert.[13] Interessierte können zunächst eine Beanstandung bei der zuständigen SRG-Ombudsstelle einreichen und 30 Tage nach deren Schlussbericht mit einer Beschwerde an die UBI überprüfen lassen, ob die SRG die rechtlichen Vorgaben eingehalten hat.

Die RTVG-Revision hat die rechtlichen Anforderungen verdeutlicht, welche die SRG ausserhalb ihrer herkömmlichen Radio- und Fernsehprogramme zu respektieren hat:

Durch die Redaktion gestaltete Inhalte im üpA der SRG müssen gemäss dem neuen Art. 5a RTVG den für herkömmliche Programme geltenden Mindestvorschriften in Art. 4 (z.B. Achtung der Menschenwürde und der Grundrechte, aber auch der Sachgerechtigkeit) und Art. 5 (Jugendschutz) des RTVG genügen. Das Vielfaltsgebot (Art. 4 Abs. 4 RTVG) gilt allerdings nicht für das gesamte üpA der SRG, sondern lediglich für Wahl- und Abstimmungsdossiers.

Von den Nutzenden gestaltete Inhalte (*user generated content*) im üpA der SRG fallen nicht unter die Mindestanforderungen des RTVG. Solche Einträge in den Kommentarspalten von Blogs oder in Foren haben kaum eine stärkere Wirkung als Publikationen in Printmedien.[14] Zudem unterliegen sie den hausinternen Regeln der SRG (Eigenkontrolle der SRG durch so genannte Netiquette).

Aufgrund einer Beanstandung aus dem Publikum hat sich die Ombudsstelle SRG Deutschschweiz 2017 grundsätzlich mit der Kommentarfunktion auf SRF News befasst.[15] Sie hielt in ihrem Schlussbericht fest, das Publikum sei heute als Diskurspartner wichtiger geworden. Die am digitalen Stammtisch

---

[10] Bericht zur Überprüfung der Definition und der Leistung des Service public der SRG unter Berücksichtigung der privaten elektronischen Medien, Bericht des Bundesrates vom 17. Juni 2016 in Erfüllung des Postulates 14.3295 der Kommission für Verkehr und Fernmeldewesen des Ständerates (KVF-S), Kap. 9.1.1, S. 68ff.

[11] Social Media-Bericht 2013, Ziff. 2.3.5, S. 12.

[12] Social Media-Bericht 2013, Ziff. 6.3, S. 71.

[13] Botschaft zur Änderung des Bundesgesetzes über Radio und Fernsehen vom 29.5.2013; BBl 2013 5014 https://www.admin.ch/opc/de/federal-gazette/2013/4975.pdf.; vgl. auch Rieder Pierre, Beschwerdemöglichkeit gegen Online-Inhalte der SRG – Die Neugestaltung der Aufsicht über das übrige publizistische Angebot der SRG, medialex Jahrbuch für Medienrecht 2016, S. 32ff.

[14] Botschaft zur Änderung des Bundesgesetzes über Radio und Fernsehen vom 29.5.2013; BBl 2013 5017 https://www.admin.ch/opc/de/federal-gazette/2013/4975.pdf.

[15] Schlussbericht der Ombudsstelle SRG Deutschschweiz vom 26.1.2017; https://www.srgd.ch/de/aktuelles/news/2017/01/26/online-kommentarfunktion-bei-srf-news-beanstandet/.

geäusserten Meinungen seien unerlässlich und es wäre absurd, die Kommentarfunktion wegen boshafter und beinahe rassistischer Ausrutscher aufzuheben. Es sei richtig, dass SRF News die Kommentare durch Redaktionsmitglieder sichte und auf der Basis der Netiquette manuell freischalte. Allerdings könnte SRF den Diskurs noch stärker steuern, z.B. durch das Hervorheben einzelner Publikumsbeiträge oder durch korrigierende Eingriffe mit kurzen eigenen Beiträgen der Redaktion.

#### 2.2.1.2 Online-Angebote anderer Medienunternehmen

Das Social Media-Angebot anderer Medienhäuser unterliegt einem weniger strengen rechtlichen Regime als das gebührenfinanzierte üpA der SRG. Zu beachten sind dort lediglich – aber immerhin – die allgemeinen rechtlichen Vorgaben für öffentliche Äusserungen (z.B. die Verbote der Ehrverletzung, der Rassendiskriminierung und des Aufrufs zu Straftaten).

Journalistisch gestaltete Social Media ritzen die vom Straf- und Zivilrecht gezogenen Grenzen erfahrungsgemäss weniger durch redaktionelle Beiträge als durch zugespitzte Kommentare aus der Leserschaft (User generated content). Diese haben mitunter Konsequenzen für die Kommentierenden. Nicht auszuschliessen wären auch rechtliche Folgen für verantwortliche Redaktoren (z.B. bei anonymen Nutzerkommentaren), doch gab es soweit ersichtlich in den vergangenen Jahren keine entsprechenden Urteile.

Der sich verschärfende Umgangston ist für Medienhäuser ein Problem. So hat die Neue Zürcher Zeitung seit dem 8. Februar 2017 die Kommentarspalte bei den meisten Online-Artikeln deaktiviert. Die NZZ begründet ihren Entschluss damit, dass sich die Leser und Leserinnen vermehrt beschimpften, wo früher kontroverse Diskussionen stattgefunden hätten. In vielen Kommentaren würden nicht mehr Informationen ausgetauscht, sondern in einer Absolutheit doziert, die andere per se ausschliesse. Ziel sei der Weg zurück zu einer konstruktiven Diskussionskultur.[16]

### 2.2.2 Übernahme von Social Media-Inhalten durch herkömmliche Medien

In den letzten Jahren ist die Tendenz zu beobachten, dass Journalisten für ihre Berichterstattung immer öfter ohne Rückfrage auf Inhalte zurückgreifen, die ursprünglich auf Social Media-Plattformen veröffentlicht worden sind. Durch die Wiedergabe in den Massenmedien erhalten die weitertransportierten Inhalte ein ungleich grösseres Publikum und entfalten so eine ungleich stärkere Wirkung. Geht es nicht um Äusserungen von Prominenten, so geschieht dies häufig gegen den Willen der Betroffenen und führt nicht selten zu Verfahren.

So hatte sich die Ombudsstelle SRG Deutschschweiz 2016 mit der Beanstandung eines unzufriedenen SBB-Kunden zu befassen, dessen Tweet unverpixelt in der Fernsehsendung „10vor10“ eingeblendet worden war.[17] Der Ombudsmann schloss sich den rechtlichen Ausführungen der Redaktion an, wonach gemäss Bundesgericht[18] jedem Twitterer bewusst sei, dass er über die weitere Verbreitung einer abgesandten Nachricht keinerlei Kontrolle hat. Auch aus medienethischer Sicht sei die Namensnennung nach Richtlinie 7.2 des Presserats unbedenklich, da der Betroffene im Zusammenhang mit dem Gegenstand des Medienberichts öffentlich aufgetreten sei.

Die für Twitter massgebenden Grundsätze lassen sich allerdings nicht unbesehen auf andere Plattformen (z.B. private Blogs oder Facebook) übertragen. So hat der Presserat deutlich gemacht, dass der journalistischen Weiterverbreitung privater Informationen aus dem Internet medienethische Grenzen gesetzt sind. Massgebend ist aus Sicht des Presserats, ob sich eine Person im öffentlichen Raum ex-

---

[16] In eigener Sache, Warum wir unsere Kommentarspalte umbauen, NZZ vom 4.2.2017; abrufbar unter: https://www.nzz.ch/feuilleton/in-eigener-sache-warum-wir-unsere-kommentarspalte-umbauen-ld.143568.

[17] Stellungnahme der Ombudsstelle SRG Deutschschweiz vom 2.10.2016: https://www.srgd.ch/de/aktuelles/2016/10/02/10vor10-beitrag-uber-testkunden-im-ov-beanstandet/.

[18] Bundesgerichtsurteil 5A_975/2015 vom 4.7.2016 (X. c. AZ Zeitungen AG: Persönlichkeitsverletzung).

poniert hat. Journalisten sollten sorgfältig zwischen öffentlichem Informationsinteresse und Privatsphärenschutz abwägen. So seien für einen kleinen Adressatenkreis bestimmte Mitteilungen in einem sozialen Netzwerk wie Facebook durch die Massenmedien zurückhaltender zu behandeln als auf die breite Öffentlichkeit zielende Publikationen institutioneller Websites.[19]

## 2.3 Neue Netzwerke auf dem Markt

Seit dem Social Media-Bericht 2013 haben zahlreiche neue soziale Netzwerke den Markt erobert. Die neuen Social Media-Dienste stammen hauptsächlich aus den USA und haben anschliessend auch in der Schweiz ihre Anhänger gefunden. Zu den bekanntesten neuen Diensten gehören die Plattformen Wanelo, Peach oder Yik Yak. Sie verfeinern teilweise das von Facebook bereits bekannte System, dass Nutzer Produkte, Fotos oder Äusserungen als gut oder schlecht beurteilen können. Das Angebot wird mit Kauftipps oder Punktekontos verknüpft.

Aus dem Gebiet schweizerischer Angebote ist etwa die Kommunikationsplattform Threema[20] zu erwähnen. Sie bietet eine Ende-zu-Ende Verschlüsselung an und kann anonym genutzt werden. Der Dienst ist kostenpflichtig und bleibt bisher eher ein Nischenprodukt.

## 2.4 Neue Bedrohungen/Entwicklungen

### 2.4.1 Rufschädigung / Trolling

Eine steigende Nutzung verzeichnen sog. Live Stream-Kanäle, d.h. Videoübertragungsplattformen, welche Inhalte in Echtzeit übermitteln. Dies führt u.a. dazu, dass sich bisher beobachtete problematische Phänomene zuspitzen können. Ein Schaden ist in mehrere Richtungen denkbar. So erhöht sich zum Beispiel mit der steigenden Anzahl von Nutzenden das Potenzial von Hackern mit finanziellen Motiven oder mit der Absicht, beim Gegenüber eine rufschädigende Handlung vorzunehmen.

Zunehmende Probleme verursacht auch das so genannte Trolling. Als Trolle werden Personen bezeichnet, die das Kommunizieren anderer dauernd und auf destruktive Weise behindern. Trolle verfassen Beiträge, die sich ausschliesslich auf die Provokation anderer Gesprächsteilnehmer beschränken und keinen sachbezogenen, konstruktiven Beitrag zur Diskussion leisten.[21] Die Provokationen sind oft unterschwellig und enthalten keine oder keine offensichtlichen Beleidigungen. Auf diese Weise können Trolle oft nicht aus der Community ausgeschlossen werden. Vermehrt gibt es auf (ausländischen) Social Media-Plattformen gar Personen, welche Trolling im Auftrag Dritter professionell betreiben.[22]

### 2.4.2 Chancen und Risiken für den politischen Diskurs

Nach journalistischen Kriterien gestaltete Medien, insbesondere Presse und Rundfunk, haben mit Social Media eine ernst zu nehmende Konkurrenz im Bereich der politischen Informationen erhalten.

In den USA informierten sich 2016 62% der Erwachsenen auch via Social Media über Politik.[23] Sie verbrachten 38% der Zeit, in der sie sich über die Präsidentschaftswahlen informierten, auf Social Media.[24] Der Zeitanteil, in dem sie sich in herkömmlichen Medien informierten, ist entsprechend gesun-

---

[19] Internet und Privatsphäre - Stellungnahme des Presserates 43/2010 vom 1.9.2010.

[20] https://threema.ch/de.

[21] Vgl. etwa www.stupidedia.org/stupi/Troll_(Internet) und https://de.wikipedia.org/wiki/Troll_(Netzkultur).

[22] Bekannt sind solche Praktiken aus Israel, Nordkorea, Russland und den USA. Vgl. etwa EVP-Fraktion im europäischen Parlament, On Russian trolls and hybrid warfare; abrufbar unter www.eppgroup.eu/news/On-Russian-trolls-and-hybrid-warfare.

[23] Pew Research Center, Mai 2016, "News Use Across Social Media Platforms 2016", http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/.

[24] Allcott Hunt/Gentzkow Matthew, Social Media and Fake News in the 2016 Election, March 2017; https://web.stanford.edu/~gentzkow/research/fakenews.pdf.

ken. Auch in der Schweiz erfreut sich das Internet als Informationsquelle gerade bei der jungen Bevölkerungsschicht zunehmender Beliebtheit, während der Konsum herkömmlicher Massenmedien abnehmende Tendenz aufweist.[25]

Social Media verschaffen auch der schweizerischen Bevölkerung vielfältige Artikulations- und Vernetzungsgelegenheiten. Dank ungefilterten Stellungnahmen zu sozialen wie politischen Vorgängen gewinnen zivilgesellschaftliche Gruppen, aber auch Einzelpersonen an Bedeutung für die öffentlich sichtbare Kommunikation.

Gerade im Bereich politischer Kommunikation eröffnen Social Media-Plattformen wertvolle neue Möglichkeiten zur Äusserung und Mobilisierung sowie zur Erschliessung vielfältiger Informationen.[26] Dass die sozialen Medien auch in der Schweiz auf politischer Ebene starken Einfluss haben können, zeigte sich erstmals in dieser Deutlichkeit beim Abstimmungskampf zur Durchsetzungsinitiative. Es gab bisher keine Abstimmung, bei der im Vorfeld so breit auf den Social Media-Kanälen mobilisiert wurde. Für die Schweiz ist das eine Zäsur in der Wahrnehmung.[27]

Neben Chancen gibt es aber auch Risiken: Dies gilt etwa für die intransparente Beeinflussung der öffentlichen Meinungsbildung.[28] So wird versucht, für Kandidierende oder für bestimmte politische Anliegen (z.B. im Abstimmungskampf) unter dem Anschein der Unabhängigkeit Werbung zu betreiben (sog. „Astroturfing).[29]

### 2.4.3 „Fake News“: Manipulation durch bewusst unzutreffende Tatsachenbehauptungen

Im Anschluss an die US-Wahlen vom Herbst 2016 gab es im In- und Ausland eine intensive Debatte um so genannte „Fake News“ in Social Media. „Fake News“ ist ein facettenreiches, umstrittenes und nicht klar definiertes Schlagwort, welches nicht selten als Kampfbegriff in der politischen Kontroverse benützt wird. Im Kern geht es vorliegend um wider besseres Wissen geäusserte, unwahre Tatsachenbehauptungen (Falschinformationen),

- die zu Zwecken der politischen Manipulation, aus finanziellen Interessen oder anderen eigennützigen Motiven verbreitet werden, und

- die ihre Wirkungsmacht aus der neuen Dynamik der sozialen Netzwerke beziehen (Anonymität der Autoren, Aufmerksamkeit für Überraschendes, sog. „virale“, d.h. extrem rasche und intensive Weiterverbreitung)[30].

Die Funktionsweise von Social Media begünstigt „Fake News“ mehrfach:

---

[25] Vgl. Bericht zur Überprüfung der Definition und der Leistung des Service public der SRG unter Berücksichtigung der privaten elektronischen Medien, Bericht des Bundesrates vom 17. Juni 2016 in Erfüllung des Postulates 14.3295 der Kommission für Verkehr und Fernmeldewesen des Ständerates (KVF-S), Kap. 9.1.1, S. 68ff.; abrufbar unter: https://www.bakom.admin.ch/dam/bakom/de/dokumente/Elektronische%20Medien/Medienpolitik/service-public-bericht.pdf.download.pdf/Bericht%20Service%20public.pdf; vgl. auch Kap. 2.3.2.3 sowie 2.4.3.2.

[26] Bond Robert M./Fariss Christopher J./Jones Jason J/Kramer Adam D. I./Marlow Cameron/Settle Jamie E./Fowler James H., A 61-million-person experiment in social influence an political mobilization, in nature international weekly journal of science, 13. September 2012, http://www.nature.com/nature/journal/v489/n7415/full/nature11421.html.

[27] Siehe etwa http://www.tagesanzeiger.ch/digital/internet/eine-zaesur-fuer-die-schweiz/story/26109438. Der Einfluss der Mobilisierung durch Social Media auf das Abstimmungsergebnis wurde bisher jedoch nicht im Detail analysiert; https://www.nzz.ch/schweiz/stimmfaule-junge-wissenschaft-widerlegt-zahlen-der-vox-analyse-1.18283206.

[28] Social Media-Bericht 2013, Ziff. 4.6.2.1, S. 50.

[29] Vgl. http://upload-magazin.de/blog/12683-astroturfing/; https://sharylattkisson.com/top-10-astroturfers/; http://www.economist.com/news/china/21699481-internet-nobody-knows-youre-running-dog-dark-art-astroturfing; http://ra.ethz.ch/CDstore/www2011/companion/p249.pdf.

[30] Vgl. auch die Definitionen von Ulbricht Carsten, Fake News & Recht – Pro und Contra einer gesetzlichen Regulierung, http://www.rechtzweinull.de/archives/2121-fake-news-recht-pro-und-contra-einer-gesetzlichen-regulierung.html sowie von Spiegel Online; http://www.spiegel.de/netzwelt/web/donald-trump-die-wahrheit-ueber-fake-news-a-1129628.html.

Zunächst ist die Identität des Autors einer Nachricht in Social Media schwieriger überprüfbar als bei traditionellen Medien: Zur Anmeldung unter einem beliebigen Namen ist in der Regel nur eine funktionierende E-Mail-Adresse erforderlich. Dies erschwert die Einschätzung von Quellen und damit die Nachvollziehbarkeit einer Information.

Darüber hinaus ist das Interesse an unglaublich erscheinenden Inhalten bedeutend grösser als das Interesse an seriösen, ohnehin erwarteten Inhalten. Falsche politische Behauptungen werden in den sozialen Medien gerne gelesen und weiterverbreitet. Auf Social Media verbreiten sich schnell unerwartete Falschnachrichten wie die, dass eine Präsidentschaftskandidatin in einen Kinderpornoring verwickelt sei („Pizzagate“[31]). Die erfolgreichsten 20 „Fake News“ wurden im US-Wahlkampf mehr geteilt und kommentiert als die erfolgreichsten 20 Artikel der grössten US-Nachrichtenquellen.[32] Gewiefte Social Media-Nutzer haben gelernt, die Mechanismen der Aufmerksamkeitsökonomie durch „Fake News“ auszunutzen.[33] „Fake News“ sprechen die Gefühle der Social Media-Nutzer an und werden darum von ihnen weiterverbreitet.[34] Schüren sie Emotionen auf die richtige Art und Weise, können sie sich „viral“ verbreiten, also freiwillig von Millionen von Nutzern mit deren Kontakten geteilt werden.

Die traditionellen Medien greifen „Fake News“ oftmals auf, u.a. weil diese auf Social Media weit verbreitet worden sind und darum als wichtige Nachricht erscheinen. Selbst wenn die herkömmlichen Massenmedien die Falschheit der Behauptungen nachzuweisen versuchen, machen sie die „Fake News“ dadurch bekannter. Dies machen sich einige aktuelle Werbe- und Wahlkampagnen zunutze: Sie produzieren Aufruhr und Empörung, wodurch sie weit grössere Bekanntheit erlangen als im Rahmen herkömmlicher Werbekampagnen. Letztlich erreichen sie so auch weit mehr potentielle Käufer oder Wähler, als sie mit herkömmlichen Kampagnen erreichen könnten.[35]

Tendenziell wird es für politische Akteure einfacher, Unwahrheiten zu behaupten. In einem Umfeld, in dem sich die Bevölkerung stets mehr mithilfe von Social Media über Politik informiert, wird es auch einfacher, den herkömmlichen Medien Lügen zu unterstellen. Durch Social Media wird die Manipulation der öffentlichen Meinung schneller, billiger, gezielter und anonymer möglich als in der Vergangenheit.[36]

### 2.4.4 „Social Bots“: automatisierte Programme treten auf Social Media wie Menschen auf

Dem Ziel der Beeinflussung der öffentlichen Meinung dienen nicht nur Handlungen menschlicher Akteure (z.B. das Verfassen von Falschmeldungen auf Social Media). Es gibt auch Benutzerkonten auf Social Media, deren Austausch mit anderen Benutzern durch Programme automatisiert ist („Bots“), welche das Verhalten von Menschen nachahmen („Social Bots“).[37]

„Social Bots“ können heute eine menschliche Identität gut vortäuschen. Komplexere „Social Bots“ können Kommunikationsinhalte analysieren und Dialoge führen. Sie kommen wohl am häufigsten auf der

---

[31] https://de.wikipedia.org/wiki/Pizzagate.

[32] Silverman Craig, Buzzfeed „This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook", https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.tsMGrKKPmZ#.wkLAZDD3pa

[33] Boyd Danah, Hacking the Attention Economy, Data & Society, 2017, https://points.datasociety.net/hacking-the-attention-economy-9fa1daca7a37#.1rnjpkkbv.

[34] Guierini Marco/Staiano Jacopo, Deep Feelings: A Massive Cross-Lingual Study on the Relation between Emotions and Virality, 16 Mar 2015, https://arxiv.org/pdf/1503.04723.pdf; Berger Jonah/Milkman Katherine L., What Makes Online Content Viral?; http://journals.ama.org/doi/abs/10.1509/jmr.10.0353?code=amma-site; Rees-Jones Liz/Milkman Katherine L./Berger Jonah, Scientific American, The Secret to Online Success: What Makes Content Go Viral, April 14. 2015; https://www.scientificamerican.com/article/the-secret-to-online-success-what-makes-content-go-viral/.

[35] https://www.nytimes.com/2016/03/16/upshot/measuring-donald-trumps-mammoth-advantage-in-free-media.html.

[36] Hwang Tim/Rosen Lea, Harder, Better, Faster, Stronger, CompProp Working Paper No. 1, http://politicalbots.org/wp-content/uploads/2017/02/Comprop-Working-Paper-Hwang-and-Rosen.pdf.

[37] Vgl. etwa Bienkowski Stefan, Worried about fake news? Then it's time we talked about social bots, 23.1.2017 http://www.dw.com/en/worried-about-fake-news-then-its-time-we-talked-about-social-bots/a-37193648.

Plattform Twitter vor, können aber grundsätzlich in allen sozialen Netzwerken mit nutzerfreundlichen Application Programming Interfaces (API) eingesetzt werden (z.B. auch Facebook oder Google+). Diese Programme können auf Stichworte oder Ereignisse reagieren, das Internet nach interessanten Inhalten absuchen und diese Inhalte selbst veröffentlichen, sich mit anderen Nutzern verbinden oder Kundenanfragen beantworten. Ihre Fähigkeiten ähneln den – in der Öffentlichkeit bereits bekannten – digitalen Assistenten wie Siri (Apple), Google Now (Google), Cortana (Microsoft) oder Alexa (Amazon).

Solche „Social Bots" lassen sich auch zu Gruppen zusammenschliessen. So können sie die Umwelt beeinflussen, indem sie zum Beispiel den Gesamtwert wertloser Unternehmen an der Börse durch ihre Äusserungen kurzfristig um Milliarden Dollar steigen lassen. Ein Beispiel dafür ist das Unternehmen „Cynk"[38].

„Social Bots" können einen Einfluss auf die Meinungsbildung gewinnen. Auf Twitter wurden im US-Wahlkampf 2016 annähernd 20% der Tweets durch „Social Bots" verbreitet.[39] Nach anderen Untersuchungen wurden in verschiedenen Wahlkampfphasen zwischen 18 und 27% der Nachrichten durch hoch automatisierte „Social Bots" mit über 450 Tweets täglich erzeugt.[40] Twitter selbst hat schon 2014 gegenüber der US-Börsenaufsicht angegeben, 23 Millionen seiner damals 271 Millionen Nutzerkonten seien automatisiert.[41]

Im politischen Umfeld können „Social Bots" Bürgerinnen und Bürger glauben machen, dass eine politische Ansicht von vielen Nutzern geteilt wird oder ein Kandidat viele Gefolgsleute hat.[42] Sie können Meldungen von Menschen in einer unerwünschten Diskussion unauffindbar machen und so diese politischen Äusserungen unterdrücken, indem sie Massen von anderen Meldungen zu demselben Thema fabrizieren.[43] Im U.S.-Wahlkampf 2016 unterstützten zum Wahlzeitpunkt 82% der automatischen Tweets – auch zu Wahlkampfthemen der demokratischen Kandidatin – den republikanischen Kandidaten.[44] „Social Bots" wurden nachweislich schon eingesetzt in Argentinien, Australien, Aserbaidschan, Bahrain, China, Grossbritannien, Iran, Italien, Mexiko, Marokko, Russland, Südkorea, Saudi Arabien, Türkei, USA und Venezuela.[45] Sie beeinflussen die öffentliche Meinung auf Social Media.[46]

---

[38] https://www.sec.gov/news/pressrelease/2015-157.html; Ferrara Emilio/Varol Onur/Davis Clyton/Menczer Filippo/Flammini Alessandro, Communication of the ACM, The Rise of Social Bots, http://cacm.acm.org/magazines/2016/7/204021-the-rise-of-social-bots/fulltext.

[39] Bessi Alessandro/Ferrara Emilio, Social bots distort the 2016 U.S. Presidential election online discussion, in: First Monday 2016, Vol. 21, Number 11. http://journals.uic.edu/ojs/index.php/fm/article/view/7090/5653.

[40] Bence Kollanyi/Howard Philip N./Woolley Samuel C., Bots and Automation over Twitter during the U.S. Election, 17. November 2016; http://politicalbots.org/wp-content/uploads/2016/11/Data-Memo-US-Election.pdf.

[41] U.S. SEC Form 10-Q Twitter, S. 3, https://www.sec.gov/Archives/edgar/data/1418091/000156459014003474/twtr-10q_20140630.htm#Item1A_RISK_FACTORS.

[42] https://www.theguardian.com/environment/2011/aug/05/fake-twitter-tar-sands-pipeline.

[43] http://www.bbc.com/news/technology-16108876, King/Pan/Roberts, How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument, http://gking.harvard.edu/files/gking/files/50c.pdf.

[44] Bence Kollanyi/Howard Philip N/Woolley Samuel C., Bots and Automation over Twitter during the U.S. Election, 17. November 2016; http://politicalbots.org/wp-content/uploads/2016/11/Data-Memo-US-Election.pdf.

[45] Forelle Michelle/Howard Phil/Monroy-Hernàndez Andrés/Savage Saiph, Political Bots and the Manipulation of Public Opinion in Venezuela, 25 Jul 2015; https://arxiv.org/abs/1507.07109; Howard Philip N./Kollanyi Bence, Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum, 20 Jun 2016; https://arxiv.org/abs/1606.06356 ; Cook David M/Waugh Benjamin/Maldini Abdipanah/Omid Hashemi, et al.. "Twitter Deception and Influence: Issues of Identity, Slacktivism, and Puppetry" Journal of Information Warfare Vol. 13 Iss. 1 (2014), https://works.bepress.com/david_cook/15/; Hegelich Simon/Janetzko Dietmar, Are Social Bots on Twitter Political Actors? Empirical Evidence from a Ukrainian Social Botnet, 2016; http://www.aaai.org/ocs/index.php/ICWSM/ICWSM16/paper/view/13015/12793; Woolley Samuel C., Automating power: Social bot interference in global politics; http://firstmonday.org/ojs/index.php/fm/article/view/6161/5300.

[46] Kramer Adam D. I/Guillory Jamie E./Hancock Jeffrey T., Experimental evidence of massive-scale emotional contagion through social networks, Jun 2 2014; https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4066473/.

Wissenschaftler haben verschiedene Methoden entwickelt, um „Social Bots“ mit automatischen Werkzeugen zu erkennen und von echten Menschen zu unterscheiden (Facebook Immune System[47], Copycatch[48], SynchroTrap[49], SybilRank[50], Souche[51], Renren Sybil Detector[52], BotOrNot[53]). Sie haben diverse Kriterien angewendet, um solche automatisierten Konten zu erkennen – etwa ihren Veröffentlichungsrhythmus für Meldungen[54], den Aufbau ihres Kontaktnetzes oder die Wortwahl (Stimmungserkennung)[55]. Dennoch sind „Social Bots“ nicht ohne weiteres erkennbar. Es ist auf diesem Gebiet ein Wettlauf zu erwarten, bei dem neue „Social Bots“ durch neue Forschungsansätze aufgedeckt werden, welche wieder zur Entwicklung noch besserer „Social Bots“ genutzt werden.

Die Betreiber der „Social Bots“ lassen sich meist weder identifizieren noch rückverfolgen.[56]

#### 2.4.4.1 Gegenwärtiger Rechtsrahmen in der Schweiz

Sofern Fake News oder „Social Bots“ diffamierende oder verleumderische Aussagen äussern, bzw. generieren, greifen die Tatbestände des Strafrechts. Hierbei sind insbesondere die Art. 173 und 174 StGB einschlägig, welche auch auf Internet-Plattformen wie soziale Netzwerke anwendbar sind (vgl. Kap. 5.3.1). Die grösste Schwierigkeit besteht hierbei darin, die hinter den „Social Bots“ stehende Täterschaft ins Recht zu fassen, da die Betreiber von „Social Bots“ wie erwähnt meist nicht identifizierbar sind.

Gemäss dem Bundesgesetz gegen den unlauteren Wettbewerb (UWG, SR 241) handelt unlauter, wer andere durch unrichtige, irreführende oder unnötig verletzende Äusserungen herabsetzt (Art. 3 Abs. 1 lit. a UWG). Diese Bestimmung ist insbesondere bei der Verbreitung von Unwahrheiten durch „Social Bots“ im Zusammenhang mit Werbebotschaften von Relevanz. Die Beeinflussung des politischen Klimas ist hingegen von den Bestimmungen des UWG nicht erfasst, bzw. nur dann, wenn herabsetzende Vorwürfe gegen einzelne Marktakteure geäussert werden.

Social Media-Inhalte fallen in aller Regel nicht unter das Radio- und Fernsehgesetz (RTVG). Eine Ausnahme gilt allerdings für das übrige publizistische Angebot (üpA) der SRG (vgl. vorne Ziff. 2.2.1.1).

In Radio- und Fernsehsendungen verstossen Fake News üblicherweise gegen das Gebot sachgerechter Darstellung von Tatsachen und Ereignissen (Art. 4 Abs. 2 RTVG). Es soll sicherstellen, dass sich das Publikum eine eigene Meinung über den Inhalt der Sendung bilden kann. Diese Anforderung wäre nicht nur verletzt, wenn ein Veranstalter in schweizerischen Radio- oder Fernsehsendungen

---

[47] Stein Tao/Chen Erdong/Mangla Karan, Facebook Immune System, https://css.csail.mit.edu/6.858/2012/readings/facebook-immune.pdf.

[48] Beutel Alex/Xu Wanhong/Guruswami Venkatesan/Palow Christopher/Faloutsos Christos, Copy-Catch: stopping group attacks by spotting lockstep behavior in social networks, http://alexbeutel.com/papers/www2013_copycatch.pdf.

[49] Cao Qiang/Yang Xiaowei/Yu Jieqi/Palow Christopher, Uncovering large groups of active malicious accounts in online social networks, https://users.cs.duke.edu/~xwy/publications/SynchroTrap-ccs14.pdf.

[50] Cao Qiang/Sirivianos Michael/Yang Xiaowei/Pregueiro Tiago, Aiding the Detection of Fake Accounts in Large Scale Social Online Services, https://www.usenix.org/system/files/conference/nsdi12/nsdi12-final42_2.pdf.

[51] Xie Yinglian/Yu Fang/Ke Qifa/Abadi Martín/Gillum Eliot/Vitaldevaria Krish, Innocent by association: Early recognition of legitimate users 2012, https://experts.umich.edu/en/publications/innocent-by-association-early-recognition-of-legitimate-users.

[52] Yang Zhi/Wilson Christo/Wang Xiao/Gao Tingting/Zhao Ben Y./Dai Yafei, Uncovering Social Network Sybils in the Wild, 2014, https://www.cs.ucsb.edu/~ravenben/publications/pdf/sybils-tkdd14.pdf.

[53] Davis Clyton A./Varol Onur/Ferrara Emilio/Flammini Alessandro/Menczer Filippo, BotOrNot: A system to evaluate social bots, May 2014, https://arxiv.org/pdf/1602.00975.pdf.

[54] Bence Kollanyi/Howard Philip N./Woolley Samuel C., Bots and Automation over Twitter during the U.S. Election, 17. November 2016, http://politicalbots.org/wp-content/uploads/2016/11/Data-Memo-US-Election.pdf.

[55] Ratkiewicz Jacob/Conover Michael D./Meiss Mark/Gonçalves Bruno/Flammini Alessandro/Menczer Filippo, Detecting and Tracking Political Abuse in Social Media 2011, http://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/view/2850.

[56] Kind Sonja/Bovenschulte Marc/Ehrenberg Sillies Simone/Jetzke Tobias/Weide Sebastian, Social Bots - Thesenpapier zum öffentlichen Fachgespräch „Social Bots – Diskussion und Validierung von Zwischenergebnissen“ am 26. Januar 2017 im Deutschen Bundestag: http://www.bundestag.de/blob/488564/4a87d2d5b867b0464ef457831fb8e642/thesenpapier-data.pdf, S. 5.

bzw. dem üpA der SRG wider besseres Wissen unwahre Tatsachenbehauptungen verbreiten würde. Nicht sachgerecht wäre auch die unsorgfältige Weitergabe falscher Fakten, welche der Programmveranstalter ohne ausreichende Recherche aus einem sozialen Netzwerk übernommen hat.

Im Bereich journalistischer Massenmedien ist auch die Selbstkontrolle relevant. Die Erklärung der Pflichten und Rechte der Journalistinnen und Journalisten[57] enthält in Ziffer 3 u.a. die Verpflichtung, nur Informationen, Dokumente, Bilder und Töne zu veröffentlichen, deren Quellen den Medienschaffenden bekannt sind. Sie dürfen weder wichtige Elemente von Informationen unterschlagen, noch von anderen geäusserte Meinungen entstellen. Unbestätigte Meldungen müssen als solche bezeichnet werden. Die Einhaltung dieser berufsethischen Grundregeln wird durch den Schweizer Presserat überprüft. Er nimmt Stellung zu Fragen, welche die journalistische Berufsethik betreffen. Der Presserat verlangt von Journalistinnen und Journalisten eine besondere Aufmerksamkeit, wenn sie Informationen aus sozialen Netzwerken transportieren oder bestimmte Trends beschreiben.[58]

In der schweizerischen Rechtsliteratur werden die durch „Social Bots" verursachten Probleme als ernsthaft eingeschätzt. Es sei deshalb durch stetige Beobachtung des Phänomens zu untersuchen, ob die bestehenden Massnahmen zusammen mit den Instrumenten der Selbstregulierung genügen oder ob zusätzlich ein staatliches Eingreifen notwendig ist.[59]

Darüber hinaus wird gefordert, der Staat müsse aufgrund seiner grundrechtlichen Schutzpflichten im Bereich der politischen Rechte durch geeignete Informationstätigkeit für die Sensibilisierung der Stimmberechtigten sorgen.[60]

#### 2.4.4.2 Selbstregulierung

Erste Plattformen haben in der Zwischenzeit angekündigt, Massnahmen gegen absichtlich produzierte Falschinformationen zu ergreifen. Nach der heftigen Kritik im Zusammenhang mit den Präsidentschaftswahlen in den Vereinigten Staaten haben Facebook und Google angekündigt, gegen die Verbreitung von Fehlinformationen vorzugehen. So wird es den Facebook-Nutzern künftig einfacher gemacht, falsche Nachrichten zu melden. Die Möglichkeit, einen Beitrag als Falschnachricht zu kennzeichnen, wird durch die besser sichtbare Anzeige erleichtert. Bislang war es lediglich möglich, zweifelhafte Links als „nervig oder uninteressant", „unpassend" oder „Spam" zu kennzeichnen. Gehen genügend Hinweise auf eine unzutreffende Tatsachenbehauptung ein, leitet Facebook diese Meldungen an ein Netzwerk weiter, das die Fakten anschliessend überprüft. Von Facebook-Nutzern gekennzeichnete Links werden von externen Organisationen[61] nach dem „International Fact Checking Code of Principles" geprüft[62] und unter Angabe von Gründen als streitbar markiert, wenn es sich um Falschmeldungen handelt. Markierte Links können zwar weiterhin geteilt werden, doch erscheint eine Warnung, wonach möglicherweise eine Falschmeldung vorliege. Darüber hinaus kann der Link nicht mehr beworben werden. Google hat 2016 angekündigt, „Fake News"-Internetseiten aus Googles Werbeprogramm auszuschliessen.[63] Derartige Massnahmen sind als erste Schritte zum Schutz vor absichtlichen Falschinformationen zu begrüssen.

---

[57] Erklärung der Pflichten und Rechte der Journalistinnen und Journalisten; abrufbar unter: http://www.presserat.ch/Documents/Erklaerung2008.pdf.

[58] Egli Patricia/Rechsteiner David, Social Bots und Meinungsbildung in der Demokratie, Aktuelle Juristische Praxis AJP 2017 S. 256f.

[59] Egli Patricia/Rechsteiner David, Social Bots und Meinungsbildung in der Demokratie, AJP 2017 S. 257f.

[60] Vgl. BGE 140 I 338, E. 5.1.

[61] Zu den externen Partnern gehören in den USA etwa Snopes, FactCheck.org und ABC News und in Deutschland das unabhängige und gemeinnützige Recherchebüro Correctiv; vgl. https://www.basicthinking.de/blog/2017/01/18/facebook-fake-news-correctiv/.

[62] http://www.sueddeutsche.de/digital/soziales-netzwerk-facebook-stellt-pilotprojekt-gegen-fake-news-vor-1.3297510.

[63] https://www.nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html?_r=0.

Das internationale Netzwerk First Draft News hat sich zum Ziel gesetzt, Verbreitungen von Falschinformationen zu verhindern. Diverse Informationsanbieter wie die grossen Nachrichtenagenturen und ferner Facebook und Youtube haben sich der Vereinigung bereits angeschlossen. Kürzlich sind vierzig weitere Organisationen aus der Kommunikationsbranche dem internationalen Netzwerk beigetreten.[64]

Bisher bestehen zwar noch keine „Codes of Conduct", welche für die Branche gelten und ein zielführendes Vorgehen festlegen. Dennoch dürften die einzelnen Social Media-Plattformen ein Interesse daran haben, die Verbreitung von „Social Bots" einzuschränken, denn die Nutzer sehen wohl wenig Sinn in der Kommunikation auf einer Plattform, auf der sich grösstenteils nur „Social Bots" als Gesprächspartner finden. Twitter bestätigte kürzlich, rund 150`000 Konten gesperrt zu haben.[65] In den Regeln und Richtlinien für die Benutzung ihrer Plattform untersagen die einzelnen Social Media-Anbieter zum Teil explizit den Zugriff mittels „Social Bots" auf ihr Netzwerk. Facebook beispielsweise fordert die Nutzer auf, durch automatisierte Mechanismen keine Inhalte oder Informationen von Nutzern zu erfassen oder mittels solcher auf Facebook zuzugreifen.[66]

#### 2.4.4.3 Ausländische Regulierungsansätze

Ob und welche Instrumente zur Bekämpfung von „Fake News" nötig sind, ist eine Frage, welche die meisten politischen Entscheidungsträger und Regulierungsbehörden europaweit beschäftigt.[67]

Der Rat der EU hat 2015 beschlossen, „Russlands laufenden Desinformationskampagnen entgegenzuwirken".[68] Die EU betreibt darauf basierend eine Stelle beim Europäischen Auswärtigen Dienst, die zum Ziel hat, russische „Fake News" über die europäische Politik zu enttarnen und richtig zu stellen.[69]

In *Tschechien* nahm 2017 das "Zentrum gegen Terrorismus und hybride Gefahren" seine Arbeit auf. Es hat u.a. die Aufgabe über schwere Fälle von Desinformation im Zusammenhang mit innerer Sicherheit zu orientieren und das Publikum sowie die tschechischen Behörden mit Einschätzungen von Sachverständigen (Expertisen) zu versorgen. Es kann weder Online-Inhalte entfernen noch Strafverfahren anstossen.[70]

In *Deutschland* wurde als Regelungsansatz vorgeschlagen, die Betreiber marktrelevanter Plattformen seien für den Fall der Kenntnis offensichtlich rechtswidriger, weil bewusste Falschinformationen enthaltender Nachrichten, zur Löschung zu verpflichten (Löschpflicht).[71] Nach einem Vorschlag der

---

[64] Gemeinsam gegen Fake News, Zuwachs für globales Netzwerk, NZZ vom 07.01.2017; weitere Informationen unter: https://de.firstdraftnews.com.

[65] Egli Patricia/Rechsteiner David, Social Bots und Meinungsbildung in der Demokratie, Aktuelle Juristische Praxis AJP 2017, S. 249, 256.

[66] Erklärung der Recht und Pflichten, Ziff 3, Ziff. 2 https://de-de.facebook.com/legal/terms.

[67] Cappello Maja, Europäische Audiovisuelle Informationsstelle (Hrsg.), Editorial zu IRIS Newsletter 2017-3, http://merlin.obs.coe.int/cgi-bin/email.php.

[68] Tagung des Europäischen Rates (19. und 20. März 2015) – Schlussfolgerungen, http://data.consilium.europa.eu/doc/document/ST-11-2015-INIT/de/pdf.

[69] https://euvsdisinfo.eu/.

[70] Vgl. dazu Fucík Jan, Zentrum gegen Terrorismus und hybride Gefahren nimmt die Arbeit auf, in: Europäische Audiovisuelle Informationsstelle (Hrsg.), IRIS 2017-3, S. 9. Zur Kontroverse um diese neue Institution vgl. etwa http://www.stuttgarter-nachrichten.de/inhalt.cyberwar-in-tschechien-prag-kaempft-gegen-fake-news.482850d7-d002-45d0-b8d0-06c89857bf38.html.

[71] Vgl. etwa Ulbricht Carsten, Fake News & Recht – Pro und Contra einer gesetzlichen Regulierung, http://www.rechtzwei-null.de/archives/2121-fake-news-recht-pro-und-contra-einer-gesetzlichen-regulierung.html.

CDU/CSU-Fraktion im Bundestag sollen die Betreiber sozialer Netzwerke ihren Nutzern Richtigstellungen anzeigen, sobald sie ein Posting als offensichtlich falsche Tatsachenbehauptung identifiziert haben (Informationspflicht).[72]

Die Notwendigkeit rechtlicher Regelungen wird auch in anderen Ländern geprüft und öffentlich diskutiert. Zu erwähnen ist etwa England, wo das Parlament eine öffentliche Konsultation zum Thema „Fake News" durchgeführt hat.[73] Ein Vorstoss im italienischen Senat verlangt strenge strafrechtliche Sanktionen für die Online-Verbreitung von „Fake News". Zudem sollten die Betreiber von Blogs oder News-Foren einer Lizenzierungspflicht unterworfen werden. Von der vorgeschlagenen Regelung ausgeklammert wären herkömmliche Medien wie die Presse und das Fernsehen, welche nicht unter die Regelung fallen würden.[74]

Die Debatte über mögliche Schutzmassnahmen steht erst am Anfang. Diskutierte Gegenmittel sind unter anderem eine regionale Zusammenarbeit der von vergleichbarer Desinformation betroffenen Staaten und die Gründung einer unabhängigen internationalen Agentur, welche Fälle von Desinformation benennt. Vorgeschlagen werden auch Browsererweiterungen, welche die Nutzer über die Glaubwürdigkeit der jeweiligen Quelle informieren, die Warnung der Bevölkerung vor der Möglichkeit von Desinformation, die Information betroffener Staaten durch Social Media-Plattformen über Desinformationskampagnen sowie die Abschaltung von „Social Bots" und von zur Desinformation genutzten Social Media-Nutzerkonten durch die Social Media-Plattformen.[75]

Auch in der Schweiz werden Massnahmen gegen Desinformation und „Social Bots" diskutiert. So wurde in der Rechtsliteratur die Auffassung vertreten, die unterschiedlichen Akteure der demokratischen Meinungsbildung müssten verstärkt sensibilisiert werden. Darüber hinaus sei abzuklären, ob allenfalls rechtlicher Regulierungsbedarf besteht (vgl. oben Ziff. 2.4.4.1).[76]

#### 2.4.4.4 Menschenrechtlicher Rahmen

Allfällige Massnahmen gegen „Fake News" müssen mit den Menschenrechten (v.a. dem Recht der Meinungsfreiheit in Art. 10 EMRK) vereinbar sein. Europarats-Generalsekretär Torbjörn Jaagland hat in ersten Stellungnahmen deutlich gemacht, dass „Fake News" eine grosse Gefahr für die Demokratie darstellen, das Problem aber nicht durch Zensurmassnahmen gelöst werden sollte.[77] Überschreiten Falschmeldungen die Grenze zur Hassrede (z.B. durch Aufruf zur Gewalt, Rassendiskriminierung oder Leugnung des Holocausts), so seien sie fast überall in Europa klar illegal und müssten von der Plattform entfernt werden. Anders seien manipulative Inhalte zu beurteilen, welche gegen keine Rechtsnorm verstossen. In solchen Fälle seien Massnahmen der privaten Plattformbetreiber einer behördlichen Intervention wegen der Zensurgefahr vorzuziehen. Es sei nötig, dass die Betreiber der Social

---

[72] https://www.wired.de/collection/tech/das-system-muss-sich-aendern-wie-die-union-facebook-zum-kampf-gegen-fake-news., Zur anschliessenden Kontroverse um die Notwendigkeit neuer Vorschriften vgl. etwa http://www.spiegel.de/netzwelt/netzpolitik/facebook-brigitte-zypries-warnt-vor-zu-strengen-regeln-wegen-fake-news-a-1137100.html.

[73] Die Konsultation dauerte bis zum 3. März 2017. http://www.parliament.uk/business/committees/committees-a-z/commons-select/culture-media-and-sport-committee/inquiries/parliament-2015/inquiry2/.

[74] https://www.rt.com/news/377765-italy-fake-news-bill/.

[75] Hwang Tim/Rosen Lea, Harder, Better, Faster, Stronger: International Law and the Future of Online PsyOps, http://politicalbots.org/wp-content/uploads/2017/02/Comprop-Working-Paper-Hwang-and-Rosen.pdf; vgl. auch den Vorschlag für die Schaffung eines Selbstregulierungsorgans von Prinzing Marlis, Digital-Rat für die Mediengesellschaft: Facebook und Co in die Pflicht nehmen; http://derstandard.at/2000056124038/Digital-Rat-fuer-die-Mediengesellschaft-Facebook-und-Co-in-die?_blogGroup=1.

[76] Egli Patricia/Rechsteiner David, Social Bots und Meinungsbildung in der Demokratie, Aktuelle Juristische Praxis AJP 2017, S. 249, 254.

[77] Vgl. etwa Jaaglands Interview mit Connor Richard, Democracy 'strong enough to deal with fake news' vom 26.1.2017, http://www.dw.com/en/democracy-strong-enough-to-deal-with-fake-news/a-37277497?maca=en-tco-dw.

Media eine grössere Verantwortung übernehmen. Wie dies geschehen kann, müsse mit ihnen diskutiert werden. Die Notwendigkeit einer staatlichen Regulierung schloss der Generalsekretär zwar nicht aus, doch plädiere der Europarat mit Rücksicht auf die Meinungsfreiheit für grösste Zurückhaltung.[78]

Auf Initiative des UNO-Sonderberichterstatters für Meinungsfreiheit (David Kaye) publizierten die Sonderberichterstatter der UNO, der OSZE, der OAS und der Afrikanischen Kommission der Menschenrechte (ACHPR) am 3. März 2017 eine gemeinsame Erklärung zu „Fake News", Desinformation und Propaganda.[79] Die Erklärung äussert die Besorgnis über die zunehmende Desinformation durch staatliche und nicht-staatliche Akteure und erinnert auch an die Verantwortung von Intermediären (z.B. Plattformbetreibern). Sie sollten die Entwicklung technologischer Lösungen vorantreiben, mit Fact-Checking-Initiativen zusammenarbeiten und darauf achten, dass ihre Werbemodelle keine negativen Effekte für die Meinungsvielfalt haben. Die Erklärung begrüsst und unterstützt Massnahmen der Zivilgesellschaft gegen willentliche Falschinformationen. Herkömmliche Medien sollten Desinformation und Propaganda kritisch begleiten und gerade vor Wahlen ihre Rolle als öffentliche Wachhunde wahrnehmen.

### 2.4.5 Social Media-Stars

Ein relativ neues Phänomen stellen die populären, zumeist jugendlichen Moderatorinnen und Moderatoren dar, die ihre eigenen Kanäle auf Social Media-Plattformen betreiben. Sie werden als „Social Media-Stars", „Influencer" oder „Youtuber" bezeichnet und verbreiten Webvideos, die von ihren Themen (z.B. Mode- und Kosmetikberatung, Videospieletests) oder ihrer Machart und Sprache her vor allem ein junges Zielpublikum ansprechen. Die weltweit erfolgreichsten „Youtuber" haben mittlerweile viele Millionen Abonnenten[80], der erfolgreichste 53 Millionen[81]. Mit der steigenden Professionalisierung der Social Media-Stars hat sich schnell ein neuer Markt entwickelt. Die Protagonisten werden heute von sog. „Multi-Channel-Netzwerk-Unternehmen", Aggregatoren und Medienagenturen betreut und erwirtschaften hohe Einkommen, die sie vor allem über Werbeverträge generieren. Entsprechend häufig werden in ihren Webvideos mittels Produkteplatzierungen und -präsentationen werbliche Botschaften verbreitet. Neben Werbung für Produkte und Dienstleistungen gegen Entgelt oder dem Platzieren von „affiliate links", die zu den beworbenen Produkten führen, werden auch gekaufte oder kostenlos zugeschickte Produkte oder gesponserte Reisen in Webvideos thematisiert.

Dieser Zustand wird bspw. in Deutschland von den zuständigen Medienregulierungsbehörden, den Deutschen Landesmedienanstalten (DLM), kritisch gesehen. Das deutsche Recht verlangt auch im Internet ein Transparenzgebot für Werbung. Sie muss deutlich und klar in einem Webvideo erkennbar sein und gekennzeichnet werden. Auch auf sozialen Plattformen muss Werbung nach deutschem Recht als solche leicht erkennbar und vom übrigen Inhalt der Angebote angemessen durch optische und akustische Mittel räumlich abgetrennt sein.[82] Da bei den Social Media-Stars zumeist das Wissen über die Werberegelungen fehlt, haben die Landesmedienanstalten beschlossen, sie auf das Thema zu sensibilisieren. Am 20. Oktober 2015 haben die DLM einen leicht verständlichen Leitfaden[83] mit Fragen und Antworten zu den Werberegeln in Youtube-Videos veröffentlicht.[84] Bei dessen Erarbeitung

---

[78] Interview Jaagland, Democracy 'strong enough to deal with fake news' vom 26.1.2017, http://www.dw.com/en/democracy-strong-enough-to-deal-with-fake-news/a-37277497?maca=en-tco-dw.

[79] http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21287&LangID=E.

[80] http://www.internetworld.de/bildergalerie/zehn-erfolgreichsten-youtube-kanaele-weltweit-922188.html?seite=9; http://www.businessinsider.com/the-most-popular-youtuber-stars-in-the-world/#15-ksi-1; https://www.welt.de/icon/news/article160112205/Das-sind-Deutschlands-erfolgreichste-YouTuber-2016.html.

[81] https://www.youtube.com/user/PewDiePie.

[82] FAQs, Antworten auf Werbefragen in sozialen Medien; abrufbar unter: http://www.die-medienanstalten.de/fileadmin/Download/Publikationen/FAQ-Flyer_Werbung_Social_Media.pdf.

[83] http://www.die-medienanstalten.de/fileadmin/Download/Publikationen/FAQ-Flyer_Werbung_Social_Media.pdf.

[84] http://www.die-medienanstalten.de/presse/pressemitteilungen/direktorenkonferenz-derlandesmedienanstalten/detailansicht/article/dlm-pressemitteilung-112015-was-ist-zu-beachten-bei-werbung-in-youtube-videos-medienanstalten-ste.html. Der

wurden Produzenten- und Medienagenturvertreter beigezogen. Der Leitfaden hat sich in Deutschland als wirksames und erfolgreiches Instrument erwiesen. Er wurde deshalb bereits ein Jahr später mit Informationen zum Auftritt in Facebook, Twitter, Instagram und Snapchat ergänzt und aktualisiert.[85] Ein Grund für den Erfolg war auch der Umstand, dass die Social Media-Stars selber daran interessiert sind, ihre Glaubwürdigkeit beim Zielpublikum nicht zu verlieren und sich andererseits gegenseitig auf mangelnde Kennzeichnungen in ihren Webvideos aufmerksam gemacht haben.

In der Schweiz spielt das Transparenzgebot im Internet ebenfalls eine Rolle. Es lässt sich u.a. aus der Generalklausel in Art. 2 UWG ableiten und verlangt, dass Werbung als solche ersichtlich ist. Damit soll gewährleistet werden, dass für das Publikum erkennbar ist, ob es sich bei einem Beitrag um eine Werbemassnahme oder eine unabhängige Berichterstattung handelt. Das Transparenzgebot betrifft nicht nur klassische Medienunternehmen und Journalisten, sondern auch Privatpersonen, die gegen Entgelt auf Blogs oder über Social Media-Profile Werbung in Form von positiver Berichterstattung über ein Unternehmen oder dessen Produkte oder Dienstleistungen verbreiten.[86]

## 2.5 Neue internationale Instrumente zur Regulierung von Social Media

### 2.5.1 Hängiger Ausbau der EU-Richtlinie über audiovisuelle Mediendienste

Spezifische internationale Regelungen für Social Media-Plattformen wurden in den vergangenen Jahren zwar nicht erlassen. Von besonderem Interesse ist aber die hängige Revision der Richtlinie 2010/13/EU über audiovisuelle Mediendienste.[87] Die Richtlinie setzt innerhalb der EU Mindeststandards für Fernseh- wie auch Video-on-Demand Inhalte. Im Rahmen der Revision wird u.a. die Erweiterung des Geltungsbereichs auf sog. „Videoplattformen“ vorgeschlagen.

Die bisherige Richtlinie ist nur bedingt relevant für Social Media-Formate. Sie wurde 2007 in Kraft gesetzt, mit dem Zweck einen europäischen Binnenmarkt für Fernsehprogramme und fernsehähnliche Mediendienste zu schaffen, welcher Transparenz, Vorhersehbarkeit und niedrige Marktzutrittsschranken garantiert. Gleichzeitig anerkannte die EU die kulturelle Relevanz der audiovisuellen Medien.[88] Die Richtlinie sichert vor diesem Hintergrund die Einhaltung grundsätzlicher Werte, indem sie Mindeststandards für die betroffenen Dienste aufstellt. Die Mediendienste sind beispielsweise verpflichtet, nicht zum Hass aufgrund von Rasse, Geschlecht, Religion oder Staatsangehörigkeit aufzustacheln oder Werbe- und Jugendschutzvorschriften einzuhalten. Der Geltungsbereich der Richtlinie erfasst Anbieter von linearen Fernsehprogrammen und von nichtlinearen, zeitversetzt abrufbaren „Video-on-Demand“-Diensten (VOD).

Hingegen fallen Plattformen, die keine redaktionelle Tätigkeit mittels Auswahl oder Bereitstellung von Videos wahrnehmen, bislang nicht unter den Anwendungsbereich der Richtlinie. Dasselbe gilt für Dienste, die nicht primär bezwecken, ein Videoangebot für die Allgemeinheit zur Verfügung stellen, d.h. bei denen Videos nur eine „Begleiterscheinung“ sind. Folglich stellen Social Media-Angebote wie YouTube, Facebook oder die Google Video grundsätzlich keine audiovisuellen Mediendienste im

---

Problematik hat sich z.B. auch das Commissariaat voor de Media angenommen, welches 2017 bei einer Untersuchung niederländischer Videos auf YouTube feststellte, dass bei mehr als 75% der gezeigten Produkte unklar war, ob die Platzierung gegen Bezahlung erfolgte: https://www.cvdm.nl/nieuws/betaling-is-vlogs-onduidelijk/.

[85] http://www.die-medienanstalten.de/presse/pressemitteilungen/direktorenkonferenz-der-landesmedienanstalten/detailansicht/article/dlm-pressemitteilung-172016-werbung-in-social-media-medienanstalten-publizieren-neue-faqs-zur.html.

[86] Keller Claudia, Werberecht in: Staffelbach Oliver/Keller Claudia (Hrsg.), Social Media und Recht für Unternehmen, Zürich 2015, S. 132 Rz. 4.11.

[87] Richtlinie 2010/13/EU des Europäischen Parlaments und des Rates vom 10. März 2010 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste, ABl. L 95 vom 15.4.2010, S. 1.

[88] IRIS Plus 2016-1, Abrufdienste und der sachliche Anwendungsbereich der AVMD-Richtlinie, Europäische Audiovisuelle Informationsstelle, Ziff. 2.2.1, S. 25.

Sinne der EU-Richtlinie dar.[89] Allerdings können jene Anbieter als VOD-Anbieter im Sinne der Richtlinie qualifiziert werden, welche auf Social Media Plattformen einen Katalog mit Video-Inhalten für die Öffentlichkeit bereitstellen, etwa in Form eines sog. „branded channels" auf YouTube. Die Praxis der EU-Mitgliedstaaten dazu ist nicht einheitlich.[90]

Um für mehr Kohärenz in der EU-Medienregulierung zu sorgen und der Entwicklung zum steigenden Konsum von nutzergenerierten Videos Rechnung zu tragen, will die Europäische Kommission mit der laufenden Revision der audiovisuellen Richtlinie künftig bestimmte Social Media-Anbieter ins Recht fassen. Konkret will sie die Anwendbarkeit der Richtlinie auf sog. „Videoplattformanbieter" („video-sharing platforms") wie YouTube erweitern.[91] Im Vorschlag vom 25. Mai 2016 zur Revision der audiovisuellen Richtlinie definiert die Europäische Kommission diese Plattformen als Dienste, die eine grosse Menge an Sendungen oder nutzergenerierten Videos speichern und die den Hauptzweck verfolgen, diese Videos der allgemeinen Öffentlichkeit zur Verfügung zu stellen. Die Plattformanbieter haben zwar keine redaktionelle Verantwortung, sie organisieren aber definitionsgemäss die Videos über Algorithmen oder andere automatische Mittel wie „hosting", „tagging" und „sequencing".

In Zukunft sollen die betroffenen Provider Massnahmen im Bereich des Jugendschutzes und des Verbots zur Aufstachelung von Gewalt oder Hass gegen bestimmte Gruppen oder Einzelpersonen vorsehen. Zu den Massnahmen gehören u.a. die Etablierung von Altersüberprüfungs-, Melde- und Bewertungsmechanismen oder das Anbieten von Systemen zur elterlichen Kontrolle von jugendgefährdenden Inhalten. Die Europäische Kommission will zudem die Mitgliedstaaten zur Einrichtung von entsprechenden Streitbeilegungsmechanismen zwischen Nutzern und Videoplattformen verpflichten. Weiter sollen der Austausch bewährter Praktiken und die Erstellung von Verhaltenskodizes gefördert werden. Im Übrigen stehen die geplanten Massnahmen im Einklang mit dem Plan der Europäischen Kommission, eine Allianz der Videoplattformen für einen besseren Schutz von Minderjährigen im Internet zu lancieren.[92]

### 2.5.2 Weitere internationale Instrumente mit Relevanz für Social Media

#### 2.5.2.1 Übereinkommen des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt (Istanbul-Konvention)

Das Übereinkommen des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt vom 11. Mai 2011 (sog. Istanbul-Konvention) ist am 1. August 2014 in Kraft getreten. Europaweit ist es das erste bindende Instrument, das Frauen und Mädchen umfassend vor Gewalt, inklusive häuslicher Gewalt, schützt. Die Unterzeichnerstaaten verpflichten sich u.a. dazu, psychische und physische Gewalt zu ahnden. Psychische Gewalt kann u.a. auch über Social Media-Plattformen ausgeübt werden. Zu denken ist hierbei etwa an Cybermobbing.

Die Schweiz hat das Übereinkommen am 13. September 2013 unterzeichnet. In seiner Sitzung vom 2. Dezember 2016 hat der Bundesrat die Botschaft zur Ratifikation dieser Konvention verabschiedet.[93]

---

[89] Die Plattformen können aber unter Umständen als sog. „Dienste der Informationsgesellschaft" in den Anwendungsbereich der EU Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr oder „e-Commerce-Richtlinie" fallen.

[90] Die Regulierungsbehörde des französischsprachigen Teil Belgiens CSA stützt diese Auslegung, s. IRIS Plus 2016-1, a.a.O. S. 43 Fn. 97; Hingegen hat im Vereinigten Königreich die Regulierungsbehörde Ofcom in mehreren Fällen professionelle Kanäle auf User-Generated-Content-Plattformen nicht als audiovisuelle Mediendienste qualifiziert, da diese nach Form und Inhalt keine fernsehähnlichen Angebote darstellen würden, s. IRIS Plus a.a.O. Ziff. 5.2.2.1, S. 52f.

[91] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2010/13/EU zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste im Hinblick auf sich verändernde Marktgegebenheiten; COM (2016) 287 final, abrufbar unter: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1464618463840&uri=COM:2016:287:FIN.

[92] Pressemitteilung der Europäischen Kommission; abrufbar unter: https://ec.europa.eu/digital-single-market/en/news/commission-broker-new-alliance-better-protect-minors-online.

[93] https://www.bj.admin.ch/bj/de/home/aktuell/news/2016/ref_2016-12-02.html.

#### 2.5.2.2 Empfehlung CM/Rec(2014)6 des Ministerkomitees des Europarates an die Mitgliedstaaten über den Leitfaden zu Menschenrechten für Internetnutzer

Gemäss der Empfehlung CM/Rec(2014)6 sind die Mitgliedstaaten des Europarats verpflichtet, jeder Person in ihrem Hoheitsgebiet die Menschenrechte und Grundfreiheiten zu sichern, welche in der Europäischen Menschenrechtskonvention (EMRK) verankert sind. Diese Verpflichtung gilt auch im Zusammenhang mit der Nutzung des Internets. Darin eingeschlossen ist auch die Aufsicht über Privatunternehmen. Universale und unteilbare Menschenrechte, sowie die damit verbunden Standards sollen gegenüber den allgemeinen Geschäftsbedingungen Vorrang geniessen.

Das Dokument enthält verschiedene Empfehlungen im Bereich der Medienkompetenz und im Bereich Kinder und Jugendliche.[94]

Ein weiterer Schwerpunkt liegt auf dem Datenschutz im Internet. Personenbezogene Daten sollten gemäss dieser Empfehlung nur verarbeitet werden, sofern eine gesetzliche Grundlage besteht oder der Verarbeitung zugestimmt wurde. Der Betroffene muss darüber in Kenntnis gesetzt werden, welche personenbezogenen Daten verarbeitet und/oder an Dritte weitergegeben werden, wann dies geschieht und zu welchem Zweck. Weiter wird empfohlen, dass jeder die Möglichkeit haben sollte, die personenbezogenen Daten hinsichtlich Richtigkeit, Löschung und Dauer der Aufbewahrung zu kontrollieren.

#### 2.5.2.3 Empfehlung der Parlamentarischen Versammlung des Europarats (PACE) zu Diskriminierung und Hass im Internet

In einer Empfehlung vom 25. Januar 2017 drängt die parlamentarische Versammlung des Europarats (PACE) die Mitgliedstaaten zu vermehrten Anstrengungen gegen rechtswidrige Online-Inhalte.[95] Dabei seien die Besonderheiten der Internetkommunikation zu berücksichtigen (sofortige und grenzüberschreitende Verbreitung der Inhalte, Möglichkeiten der Anonymität). Die Mitgliedstaaten sollten sicherstellen, dass Internetprovider und Plattformbetreiber die vom Europäischen Gerichtshof für Menschenrechte (EGMR) entwickelten Standards beachten. Nötig seien eindeutige und wirksame firmeninterne Prozesse zur Behandlung von Meldungen über Online-Hetze (z.B. antisemitischer, islamfeindlicher, frauenfeindlicher und homophober Hass).

Die Europaratsstaaten sollten Strafverfolgungsbehörden und gerichtliche Organe durch Schulungsangebote unterstützen und klare Leitlinien für die Registrierung aller gemeldeten Vorfälle entwickeln. Darüber hinaus sollten sie alle Aktivitäten fördern, welche das öffentliche Bewusstsein für die Auswirkungen von Hassrede – insbesondere auf Kinder – erhöhen.

### 2.5.3 Neue internationale Instrumente zur Stärkung des Datenschutzes

In den vergangenen Jahren haben sich die allgemeinen Bemühungen für einen Ausbau des Datenschutzes in einer Reihe von verbindlichen internationalen Vorschriften niedergeschlagen. Sie sind nicht nur, aber auch im Bereich der Social Media relevant. So hat die Europäische Union am 27. April 2016 ihre Datenschutzgesetzgebung revidiert. Dazu gehört insbesondere die Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutz-Grundverordnung; EU-DSGVO)[96]. Auf Ebene des Europarats soll die Revision des Übereinkommens SEV 108 zum

---

[94] Empfehlung CM/Rec(2014) des Ministerkomitees an die Mitgliedstaaten über den Leitfaden zu Menschenrechten für Internetnutzer, S. 1 und 5, weiter Empfehlungen des Europarats s. auch Recommandations and declarations of the Committee of Ministers of the Council of Europe in the field of media and informations society, S. 234 für CM/Rec(2014), https://rm.coe.int/CoERM-PublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680645b44.

[95] Empfehlung 2098 (2017) der parlamentarischen Versammlung des Europarats zur Beendigung von Diskriminierung und Hass im Internet, 25. Januar 2017: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=23457&lang=en.

[96] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S.1.

Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten im Jahre 2017 verabschiedet werden.[97]

#### 2.5.3.1 Verordnung 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung)

Die EU hat mit der Datenschutz-Grundverordnung[98] (EU-DSGVO) Bestimmungen erlassen, welche auch viele Schweizer Unternehmen betreffen können. Die Grundverordnung ist dann für Schweizer Unternehmen anwendbar, wenn diese sich auf den europäischen Markt ausrichten. Eine physische Präsenz des Datenverarbeiters in der Europäischen Union ist nicht verlangt. Die Verordnung erfasst auch nicht in der EU domizilierte Unternehmen, welche beim Angebot von Waren oder Dienstleistungen an natürliche Personen in der EU deren Personendaten bearbeiten oder welche deren Verhalten überwachen (soweit das Verhalten in der EU erfolgt). Die Ausrichtung der Geschäftstätigkeit eines Datenverarbeiters auf den europäischen Markt wird damit zu einem praktisch bedeutsamen Anknüpfungskriterium.[99]

Die Verordnung wird ab dem 25. Mai 2018 gelten. Mit den Massnahmen hin zu einem besseren Schutz der Privatsphäre in der elektronischen Kommunikation sollen die geltenden Regeln modernisiert und im Sinne der digitalen Strategie für einen Binnenmarkt umgesetzt werden.[100] Die EU-DSGVO soll den Bürgern eine bessere Kontrolle ihrer personenbezogenen Daten ermöglichen. Insbesondere die Vorschriften für einen einfacheren Zugang zu den eigenen Daten, zum Recht auf Datenübertragbarkeit, zum Recht auf Vergessenwerden stärken die bestehenden Rechte und geben den Nutzern mehr Kontrolle über ihre Daten.[101]

Die EU-DSGVO enthält insbesondere den Grundsatz der transparenten Verarbeitung von personenbezogenen Daten (Art. 26), die Informationspflicht und das Recht auf Auskunft, die Ausweitung des Rechtes auf Löschung („Recht auf Vergessenwerden"; Art. 17) sowie den Grundsatz des Datenschutzes durch geeignete technische und organisatorische Massnahmen (data protection by design und data protection by default).

Nach den Erwägungen zur EU-DSGVO[102] verlangen die Grundsätze einer fairen und transparenten Verarbeitung, dass die betroffenen Personen über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet werden. Der Verantwortliche sollte der betroffenen Person alle weiteren Informationen zur Verfügung stellen, die unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten. Werden die personenbezogenen Daten bei der betroffenen Person erhoben, so sollte dieser darüber hinaus mitgeteilt werden, ob sie verpflichtet ist, die personenbezogenen Daten bereitzustellen und welche Folgen eine Zurückhaltung der Daten nach sich ziehen würde. Die Tatsache, dass personenbezogene Daten verarbeitet werden, muss der betroffenen Person grundsätzlich zum Zeitpunkt der Erhebung mitgeteilt werden.

---

[97] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21.12.2016, S. 5.

[98] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016. S. 1.

[99] Vgl. etwa Passadelis Nicolas/Roth Simon, Weisser Rauch über Brüssel - Was Schweizer Unternehmen über die europäische Datenschutz-Grundverordnung wissen müssen, in: Jusletter 4. April 2016, Rz. 132ff.

[100] http://europa.eu/rapid/press-release_IP-15-4919_de.htm.

[101] http://europa.eu/rapid/press-release_IP-15-6321_de.htm.

[102] Erwägungsgründe 60 und 61.

#### 2.5.3.2 Verordnung über Privatsphäre und elektronische Kommunikation (ePrivacy-Verordnung)

Am 10. Januar 2017 hat die Europäische Kommission einen Vorschlag für eine Verordnung zur Achtung der Privatsphäre und den Schutz personenbezogener Daten in der elektronischen Kommunikation (Verordnung über Privatsphäre und elektronische Kommunikation) präsentiert.[103] Diese sogenannte ePrivacy-Verordnung soll ab Mitte 2018 die bisher geltende ePrivacy-Richtlinie und die ergänzende Cookie-Richtlinie aus dem Jahr 2009 ablösen. Sie zielt darauf ab, einen stärkeren Datenschutz in der elektronischen Kommunikation zu garantieren und gleichzeitig neue Geschäftsmöglichkeiten zu eröffnen. So erweitert der Vorschlag die Möglichkeiten von Unternehmen, elektronische Kommunikationsmetadaten wie Standortdaten zu verarbeiten.[104]

Die vorgeschlagene Verordnung über Privatsphäre und elektronische Kommunikation ist mit der Datenschutz-Grundverordnung verknüpft. Zum einen präzisiert (und erweitert) sie die allgemeinen Vorgaben der EU-DSGVO für den Umgang mit Personendaten durch elektronische Kommunikationsmittel. Zum anderen stösst sie in zusätzliche Regelungsgebiete vor. So erfasst der Vorschlag die Verarbeitung „elektronischer Kommunikationsdaten". Dazu gehören Inhalte und Metadaten elektronischer Kommunikation, die nicht unbedingt auf personenbezogene Daten beschränkt sind (z.B. machine-to-machine, Internet of Things, gespeicherte Daten auf Computer, Mobiltelefon, Smart Fridge). Die Vorschriften zum Schutz der Privatsphäre sollen sich künftig auch auf elektronische Kommunikationsdienste (wie VoIP Skype, Viber Out) und Messaging Services (Gmail, iMessage, Viber, WhatsApp, Facebook Messenger) erstrecken.

In Übereinstimmung mit den in der EU-DSGVO kodifizierten Datenschutzgrundsätzen „privacy by design" und „privacy by default" verlangen die vorgeschlagenen Vorschriften von den Internet-Browsern beispielsweise, dass sie Endnutzern die Option bieten, die Speicherung von Cookies Dritter auf ihren Endgeräten zu unterbinden.

Im Falle der Verabschiedung wird die Verordnung unmittelbar in der gesamten EU Gültigkeit haben. Sie soll für elektronische Kommunikationsdaten greifen, welche in Verbindung mit der Bereitstellung und Nutzung elektronischer Kommunikationsdienste in der EU verarbeitet werden. Dies gilt unabhängig davon, ob die Verarbeitung in der EU stattfindet. Der territoriale Anwendungsbereich ist somit nicht auf die EU begrenzt.

#### 2.5.3.3 Europarat: Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV 108)

Der Europarat hat einen Entwurf zur Modernisierung des Übereinkommens zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV 108) ausgearbeitet.[105] Das Protokoll zur Revision dieses Übereinkommens soll anfangs 2017 verabschiedet werden.[106] Die Schweiz wird bestrebt sein, den Entwurf in ihrer Gesetzgebung umzusetzen.[107]

---

[103] Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation); abrufbar unter: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

[104] Vgl. auch die Pressemitteilung der Europäischen Kommission vom 10.1.2017; http://europa.eu/rapid/press-release_IP-17-16_de.htm.

[105] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, SR 0.235.1, für die Schweiz in Kraft getreten am 1. Februar 1998.

[106] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21.12.2016, S. 5.

[107] Vgl. Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, S. 18, 30 und 46ff.

# 3 Hängige Regulierungsvorhaben in der Schweiz

## 3.1 Revision Datenschutzrecht

Der Bundesrat hat im Social Media-Bericht 2013 ausgeführt, die im Bericht aufgeworfenen datenschutzrechtlichen Fragen würden im Rahmen der laufenden Revisionsarbeiten zum Datenschutzgesetz (DSG) erörtert.

Das Eidgenössische Justiz- und Polizeidepartement (EJPD) hatte den Auftrag, dem Bundesrat bis Ende 2014 Vorschläge zum weiteren Vorgehen zu unterbreiten.[108] Der Bundesrat hat den Bericht anschliessend genehmigt und beauftragte das Bundesamt für Justiz (BJ), einen Gesetzesentwurf auszuarbeiten.[109]

An seiner Sitzung vom 21. Dezember 2016 hat der Bundesrat den Vorentwurf zu einer Totalrevision des Datenschutzes in die Vernehmlassung geschickt. Der Bundesrat will den Datenschutz stärken und an die wirtschaftlichen und technologischen Verhältnisse anpassen. Die Revision schafft die Voraussetzungen dafür, dass die Schweiz die Datenschutzkonvention des Europarates ratifizieren und die EU-Richtlinie über den Datenschutz im Bereich der Strafverfolgung übernehmen kann. Sie erlaubt auch eine Annäherung der schweizerischen Gesetzgebung an die Anforderungen der Datenschutz-Grundverordnung der Europäischen Union (EU-DSGVO). Mit der Revision soll zudem sichergestellt werden, dass die Gesetzgebung auf Bundesebene mit dem revidierten Europarats-Übereinkommen SEV 108 vereinbar ist und ratifiziert werden kann. Der Bundesrat will damit u.a. garantieren, dass die grenzüberschreitende Datenübermittlung weiterhin möglich bleibt.[110] Die Vernehmlassung zum Gesetzesprojekt, das die Revision des DSG, den Bundesbeschluss betreffend die Übernahme der EU-Richtlinie sowie die Modernisierung der Datenschutzkonvention des Europarates in einer Vorlage vereint, dauerte bis zum 4. April 2017.[111]

## 3.2 Jugendmedienschutz

Im Social Media-Bericht 2013 wurde ausgeführt, Fragen im Bereich des Jugendschutzes seien bis im Jahr 2015 im Rahmen des vom Bundesamt für Sozialversicherung betreuten Projekts „Jugend und Medien“ zu analysieren.[112] Dabei war abzuklären, ob auf Bundesebene ein Regulierungsbedarf besteht und gegebenenfalls neue rechtliche Grundlagen zum Schutz von Kindern und Jugendlichen nötig sind. Zudem waren Empfehlungen zur künftigen Ausgestaltung des Jugendmedienschutzes in der Schweiz zu erarbeiten.

In seinem Bericht „Jugend und Medien“ vom 13. Mai 2015[113] hat der Bundesrat aufgezeigt, welche Herausforderungen bestehen, inwieweit das bestehende Kinder- und Jugendmedienschutzsystem darauf reagieren kann und wie der regulierende und erzieherische Kinder- und Jugendmedienschutz in Zukunft ausgestaltet werden sollen (vgl. auch unten Ziff. 5.5.1).

Die Analyse hat ergeben, dass sich das Spektrum der Gefährdungen im Bereich elektronischer Medien in letzter Zeit aufgrund der dynamischen Medienentwicklung stark erweitert hat. Erforderlich erscheint ein ausgeprägter Schutz für Kinder und Jugendliche insbesondere in den Bereichen ungeeig-

---

[108] Social Media-Bericht 2013, Ziff. 9, S. 80.

[109] www.bj.admin.ch/bj/de/home/aktuell/news/2015/ref_2015-04-010.html.

[110] s. Medienmitteilung des Bundesrates vom 21. Dezember 2016, s. https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2016/2016-12-21.html.

[111] Medienmitteilung des Bundesrates vom 21. Dezember 2016, s. https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2016/2016-12-21.html.

[112] Social Media-Bericht 2013, Ziff. 9, S. 80.

[113] Jugend und Medien, Zukünftige Ausgestaltung des Kinder- und Jugendmedienschutzes der Schweiz 13. Mai 2015, Bericht des Bundesrates in Erfüllung der Motion Bischofberger 10.3466 „Effektivität und Effizienz im Bereich Jugendmedienschutz und Bekämpfung von Internetkriminalität“. Im Folgenden: Bericht Jugend und Medien 2015

neter Medieninhalte, beeinträchtigender Mitteilungen im Rahmen der Online-Kommunikation und intransparenter Bearbeitung persönlicher Daten. Vorzusehen sind sowohl regulierende als auch erzieherische Massnahmen, welche regelmässig zu überprüfen und bei Bedarf anzupassen sind. Der Bericht kommt zum Schluss, die bestehenden Massnahmen müssten weiterentwickelt und ergänzt werden, wobei der Bundesrat eine koordinierende Rolle übernehmen und die Zusammenarbeit mit der Wirtschaft und den Kantonen verstärken wolle.[114]

Der Bundesrat will aufgrund der Erfahrungen des Programms in Kollaboration mit denselben Akteuren den Jugendmedienschutz mit regulierenden Massnahmen stärken, da dieser rechtliche Lücken aufweist. Deshalb soll auf nationaler Ebene ein rechtlich verbindlicher Rahmen für die Regulierung der massgebenden Branchen geschaffen werden, wobei der Bund steuernde und überwachende Funktionen wahrnimmt.[115]

Vor diesem Hintergrund hat der Bundesrat das Eidgenössische Departement des Innern (EDI) damit beauftragt, bis Ende 2017 ein Gesetz auszuarbeiten, das Alterskennzeichnungen und Abgabebeschränkungen für Videos und Spiele schweizweit einheitlich regeln soll. Unter Einbezug der betroffenen Branchenverbände und der Kantone wird das EDI bis Ende 2017 eine Vernehmlassungsvorlage ausarbeiten.[116] In diesem Rahmen ist u.a. die Frage zu klären, ob der Schutz der Jugendlichen vor weiteren ungeeigneten Inhalten im Internet (z.B. auf YouTube) gesetzlich geregelt werden soll.[117] Wie oben (Ziff. 2.5.1) erwähnt, ist auf europäischer Ebene geplant, die Videoplattformdienste stärker zu regulieren. Der Bundesrat erachtet es als wichtig, dass die Schweiz im Jugendmedienschutz das Niveau erreicht, welches auch die EU vorsieht.

Neben dem regulierenden ist auch der erzieherische Kinder- und Jugendmedienschutz zu vertiefen. Der Bundesrat nimmt dabei eine koordinierende Rolle wahr. Zur diesem Zweck hat er zwei Stellen sowie finanzielle Mittel im Umfang von CHF 600`000 zur Durchführung von Vernetzungsanlässen, Konferenzen, Pilotprojekten und den Betrieb der Online-Plattform www.jugendundmedien.ch bewilligt. Er will den im Programm Jugend und Medien verfolgten Ansatz weiterführen und sich auch künftig auf die Sensibilisierung von Fachpersonen und die Unterstützung der wichtigen Akteure wie Verbände, nationale Organisation usw. konzentrieren.[118]

Das Bundesamt für Sozialversicherungen (BSV) betreibt mit dem erwähnten Angebot www.jugendundmedien.ch eine nationale Plattform zur Förderung von Medienkompetenzen.[119] Dazu gehört die Information und Sensibilisierung von Eltern, Lehr- Betreuungs- und Fachpersonen, die Unterstützung von Stakeholdern, die fachliche Entwicklung und die Zusammenarbeit und Vernetzung. Im Bereich des erzieherischen Kinder- und Jugendmedienschutzes möchte das BSV seine geplanten Arbeiten mit den betroffenen Bundesstellen und den Kantonen absprechen. Dabei bildet es eine „Kerngruppe Medienkompetenz“. Folgende Zielsetzungen werden dabei verfolgt:

- Strategische Begleitung der Arbeiten des BSV im erzieherischen Jugendmedienschutz;

- Abstimmung der Aktivitäten von Bundesstellen, Kantonen, Städten und Gemeinden;

---

[114] vgl. auch Interpellation Viola Amherd 13.4266 „Handlungsbedarf bei Sexting“, s. auch Anfrage Viola Amherd 15.1024 „Jugendschutzprogramme“.

[115] Medienmitteilung vom 19.10.2016, „Bundesrat will den Jugendmedienschutz bei Filmen und Computerspielen verstärken“; abrufbar unter: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-64171.html

[116] Medienmitteilung vom 19.10.2016; abrufbar unter: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-64171.html

[117] Medienmitteilung des Bundesrates vom 19.10.2016; abrufbar unter: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-64171.html

[118] Interpellation Schmid-Federer 15.3723, Kinder- und Jugendmedienschutz. Umsetzung der Empfehlung von Experten; Anfrage Amherd 15.1024 Jugendschutzprogramme.

[119] Bericht Jugend und Medien 2015, S. 138.

- Identifikation und Nutzung von Synergien.

Die Kerngruppe setzt sich aus Vertretern von Bund, Kantonen, Städten und Gemeinden zusammen.

## 3.3 Revision Fernmelderecht

Gesetzliche Regelungen zur Erbringung von Fernmeldediensten finden sich im Fernmeldegesetz (FMG, SR 784.10). Nach Art. 3 lit. b FMG bietet einen Fernmeldedienst an, wer zwischen mindestens zwei Parteien mittels Fernmeldetechnik Informationen transportiert. Betreiber von Social Media-Plattformen fallen in aller Regel nicht unter diese Bestimmung, da sie meistens lediglich eine der Parteien sind, zwischen denen Informationen übermittelt werden.[120] Sofern auf Social Media-Plattformen jedoch Fernmeldedienste angeboten werden (z.B. Mail- oder Messagingdienste), sind die fernmelderechtlichen Bestimmungen zu beachten.

Das FMG stammt aus einer Zeit, in der die Erbringung von Fernmeldediensten vom Besitz oder doch zumindest vom autorisierten Zugang zu einem spezifischen, diesem Zweck dienenden Netz, abhängig war. Durch die rasante technologische Entwicklung ist diese enge Bindung zwischen Netz und Diensten aufgehoben worden. Heute gelten völlig andere technische Bedingungen (Internet, Smartphones etc.) und Dienste können auf verschiedenste Weise und ohne aktives Zutun der Netzbetreiber erbracht werden. Diese Veränderung der technischen Umstände hat die Türen für neue Geschäftsmodelle geöffnet und die regulatorischen Rahmenbedingungen müssen den Entwicklungen angepasst werden, die in den letzten Jahren auf dem Fernmeldemarkt stattgefunden haben.

Der Bundesrat hat dem UVEK am 19. November 2014 den Auftrag erteilt, bis Ende 2015 eine Vernehmlassungsvorlage für die Revision des FMG zu erarbeiten.[121] Der Umfang der notwendigen Revisionsarbeiten ist bereits im Fernmeldebericht 2014 zur Entwicklung im schweizerischen Fernmeldemarkt und zu den damit verbundenen gesetzgeberischen Herausforderungen[122] diskutiert worden. Nachfolgend wird kurz auf jene Punkte der FMG-Revision eingegangen, die namentlich auch für Social Media-Plattformen relevant sein könnten.

Überprüft wurde unter anderem die geltende Pflicht, wonach sich ein Fernmeldedienstanbieter beim Bundesamt für Kommunikation (BAKOM) melden muss (Art. 4 FMG). Sie trifft auch Betreiber von Social Media-Plattformen, soweit sie Fernmeldedienste im Sinne des Gesetzes anbieten.

Gemäss einem weltweit zu beobachtenden Trend werden etwa mobile Nachrichten immer weniger per SMS über die Mobilfunkanbieterin, sondern über Internet-basierte Dienste (OTT IP messaging)[123] versendet. Es ist auch für kleine Unternehmen sehr einfach geworden, auf der Basis der Infrastruktur des Internets Fernmeldedienste für Kunden auf der ganzen Welt anzubieten. Sämtliche Unternehmen weltweit mit Internet-basiertem Fernmeldedienstangebot in der Schweiz sind gemäss der betreffenden Definition als Fernmeldedienstanbieterinnen zu betrachten und würden unter der bestehenden Regelung grundsätzlich der Meldepflicht unterliegen. Entsprechend bietet mittlerweile eine unübersehbare Zahl von global tätigen, irgendwo auf der Welt angesiedelten Akteuren ihre Dienste auch in der Schweiz an. Aktuell ist jedoch nur ein kleiner Teil dieser Unternehmen gemeldet. Die Meldepflicht führt sowohl bei den Meldepflichtigen als auch bei der die Meldepflicht überwachenden und die Meldungen

---

[120] Vgl. Social Media-Bericht 2013, Ziff. 2.4.2.2, S. 13.

[121] Medienmitteilung vom 14.11.2014; abrufbar unter: https://www.bakom.admin.ch/bakom/de/home/das-bakom/medieninformationen/medienmitteilungen.msg-id-55293.html.

[122] Abrufbar unter: https://www.bakom.admin.ch/bakom/de/home/das-bakom/organisation/rechtliche-grundlagen/bundesratsgeschaefte/fernmeldebericht-2014.html.

[123] Mobile Nachrichten, welche mittels Internetprotokoll (IP) erbracht werden. Jenes Protokoll wird sowohl von Mobilfunknetzbetreiber als auch von sog. OTT (Over The Top)- Anbieterinnen wie WhatsApp genutzt.

administrierenden Verwaltung zu Aufwänden, denen kein entsprechender Nutzen mehr gegenübersteht.[124] Die generelle Meldepflicht ist eine Regelung, die den technischen Entwicklungen und Möglichkeiten keine Rechnung trägt und nicht mehr praktikabel ist.

Auch in den Bereichen Konsumenten-, Kinder- und Jugendschutz bedürfen die sich aufgrund der Allgegenwärtigkeit des Internets stellenden Probleme neuer regulatorischer Lösungen, da die Branche sie nicht allein und unter ausgewogener Berücksichtigung sämtlicher in Frage stehender Interessen lösen kann.

Aus diesem Grund wurde im Rahmen der Vernehmlassungsvorlage zur Teilrevision des FMG vom 11. Dezember 2015 vorgeschlagen, dass der Bundesrat künftig ermächtigt werden soll, im Bereich des Jungendschutzes tätig zu werden. Er soll diesbezüglich die Anbieterinnen von Fernmeldediensten auf Verordnungsebene verpflichten können, beim Verkauf von Mobilfunkabonnements und festen Internetzugängen für die Eltern eine Beratung über die Möglichkeiten zum Schutz von Kindern und Jugendlichen anzubieten. Schutzmöglichkeiten können die Auswahl, Installation und Einstellung von Filtern darstellen. Aber auch auf weitere Handlungsmöglichkeiten sollten die Eltern hingewiesen werden.

Im Bereich der qualifizierten Pornografie sollen die Fernmeldedienstanbieterinnen verpflichtet werden, den Zugang zu nach Art. 197 Abs. 4 und 5 StGB verbotenen Inhalten gemäss den durch die KOBIK geführten Listen zu sperren.

Der Bundesrat hat am 23. September 2016 von den Ergebnissen der Vernehmlassung Kenntnis genommen und das UVEK beauftragt, bis September 2017 eine Botschaft zur Änderung des FMG auszuarbeiten. Zu den Eckwerten, die es dabei zu berücksichtigen gilt, gehören im Rahmen der Einführung weiterer Schutzvorschriften auch die erwähnten Regelungen bezüglich Jugendschutz und bezüglich Sperrung von Internetseiten mit qualifiziert pornografischen Inhalten.[125]

## 3.4 Bundesgesetz über elektronische Medien (GeM)

Der Bundesrat hat im Service-public-Bericht vom 17. Juni 2016[126] festgestellt, dass die technologischen und ökonomischen Entwicklungen (Digitalisierung, veränderte Mediennutzung) eine generelle Neuordnung der elektronischen Medienlandschaft erfordern. Das BAKOM befasst sich zurzeit mit den Vorbereitungsarbeiten eines neu zu schaffenden Gesetzes über elektronische Medien (GeM). Eine öffentliche Vernehmlassung zum Vorentwurf des Gesetzes ist für das Frühjahr 2018 geplant.

Im Rahmen dieses Vorhabens wird auch geprüft, inwieweit über Social Media-Plattformen verbreitete Inhalte gewissen Mindeststandards unterstellt werden sollen, u.a. hinsichtlich Jugendschutz und Kennzeichnung von Produkteplatzierungen. Dabei wird auch eine Harmonisierung mit den europäischen Regelwerken zu prüfen sein (s.o. Ziff. 2.5.1).

## 3.5 Totalrevision BÜPF

Das Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF; SR 780.1) wurde total revidiert. Das neue Gesetz vom 18. März 2016 (nBÜPF; BBl 2016 1991) wird voraussichtlich 2018 in Kraft treten. Es erfasst auch Anbieterinnen abgeleiteter Kommunikationsdienste. Gestützt auf Art. 22 Abs. 4 und 27 Abs. 3 nBÜPF kann der Bundesrat Anbieterinnen abgeleiteter Kommunikationsdienste, welche Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten, künftig strengeren Pflichten unterwerfen. Er kann an-

---

[124] https://www.bakom.admin.ch/bakom/de/home/das-bakom/organisation/rechtliche-grundlagen/bundesratsgeschaefte/fernmeldebericht-2014.html., Kap. 3.1.2.2

[125] Medienmitteilung vom 23.9.2016; abrufbar unter: www.bakom.admin.ch/bakom/de/home/das-bakom/medieninformationen/medienmitteilungen.msg-id-63882.html

[126] Bericht des Bundesrates vom 17. Juni 2016 zur Überprüfung der Definition und der Leistungen des Service public der SRG unter Berücksichtigung der privaten elektronischen Medien (nachfolgend Service-public-Bericht), Geschäftsnummer 16.043.

ordnen, dass sie Daten aufbewahren und liefern, wie dies bisher herkömmliche Fernmeldedienstanbieterinnen tun müssen. Auch Social Media kommen als Anbieterinnen abgeleiteter Kommunikationsdienste in Frage, was die Überwachung auch auf grossen Social Media-Plattformen erleichtern soll. Dies dient der besseren Durchsetzung des Strafrechts und, wie im folgenden Abschnitt dargestellt, weitergehenden Möglichkeiten für den Nachrichtendienst.

### 3.6 Nachrichtendienstgesetz

Auch dem Nachrichtendienst des Bundes erteilt der Dienst betreffend die Überwachung des Post- und Fernmeldeverkehrs die zum Vollzug des Bundesgesetzes vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (BWIS; SR 120) notwendigen Auskünfte nach Art. 14 Abs. 2$^{bis}$ BÜPF (bzw. Art. 15 Abs. 2 Bst. a nBÜPF). Dies erleichtert die Identifikation von Personen, welche die innere Sicherheit der Schweiz gefährden.

Das neue Bundesgesetz über den Nachrichtendienst (NDG) wurde vom Schweizer Stimmvolk am 25. September 2016 angenommen. Es wird voraussichtlich am 1. September 2017 in Kraft treten. Das NDG erlaubt dem Nachrichtendienst des Bundes gemäss Art. 25 Abs. 2, Auskünfte nach Artikel 14 des BÜPF (bzw. Art. 15 nBÜPF) einzuholen. Gemäss Art. 27 Abs. 1 i.V.m. Art. 26 Abs. 1 Bst. a kann der Nachrichtendienst auch Überwachungen anordnen. Dies verbessert die Identifikation und Überwachung von Personen zum Schutz wichtiger Landesinteressen, namentlich um Bedrohungen der inneren und äusseren Sicherheit zu erkennen und zu verhindern, auch auf Social Media-Plattformen.

## 4 Stand der Folgearbeiten zum Postulatsbericht 2013

### 4.1 Allgemeines

Der Social Media-Bericht 2013 verneinte die Notwendigkeit der Regulierung sozialer Netzwerke in einem Spezialgesetz. Der Bericht empfahl hingegen, allgemein formulierte Rechtsvorschriften zu überprüfen und nötigenfalls zu ergänzen.[127] Er erwähnte folgende Rechtsgebiete:

- Vertiefte Prüfung des Datenschutzrechts[128];
- Prüfung, ob die Zuordnung der Verantwortlichkeit von Plattformbetreibern und Providern zu regeln ist[129];
- Prüfung, ob Regeln des Fernmelderechts auf Social Media-Plattformen anzuwenden sein sollen[130];
- Beobachtung, ob die Mitnahme eigener Daten auf andere Plattformen geregelt werden soll[131].

Die vertiefte Prüfung des Datenschutzrechts ist Gegenstand der oben (Ziff. 3.1) geschilderten, umfassenden Revision des DSG. Die drei weiteren Prüfaufträge wurden ebenfalls erfüllt:

### 4.2 Zivilrecht: Verantwortlichkeit von Plattformbetreibern

Das Eidgenössische Justiz- und Polizeidepartement (EJPD) erhielt im Social Media-Bericht 2013 den Auftrag, die zivilrechtliche Verantwortlichkeit von Plattformbetreibern und Providern zu prüfen und bei allfälligem gesetzgeberischem Handlungsbedarf eine Vernehmlassungsvorlage zu erarbeiten. Zu diesem Zweck wurde unter Federführung des Bundesamtes für Justiz (BJ) mit Vertretern des Bundesamts für Kommunikation (BAKOM), des Eidgenössischen Instituts für Geistiges Eigentum (IGE) und

[127] Social Media-Bericht 2013, Ziff. 7.2.3 und 7.2.4, S. 74.

[128] Social Media-Bericht 2013, Ziff. 7.2.4.1, S. 74f.

[129] Social Media-Bericht 2013, Ziff. 7.2.4.2, S. 75.

[130] Social Media-Bericht 2013, Ziff. 7.2.4.3, S. 75.

[131] Social Media-Bericht 2013, Ziff. 7.2.4.4, S. 75.

des Staatssekretariats für Wirtschaft (SECO) eine interdepartementale Arbeitsgruppe eingesetzt. Gestützt auf deren Arbeiten veröffentlichte der Bundesrat am 11. Dezember 2015 den Bericht „Die zivilrechtliche Verantwortlichkeit von Providern".

Der Bundesrat kam in seinem Bericht zum Schluss, eine allgemeine, rechtsgebietsübergreifende gesetzliche Regulierung der zivilrechtlichen Verantwortlichkeit von Providern erscheine nicht angezeigt.[132] Der Bericht hat die geltende Rechtslage und Gerichtspraxis analysiert und gewürdigt. Dadurch will er einen Beitrag zur Rechtsentwicklung und zur weiteren Verbesserung der Rechtssicherheit leisten.

Er befasst sich auch mit Social Medial-Plattformen. So hält der Bericht fest, der Bundesrat begrüsse das Notice-and-Takedown-Verfahren, welches Social Media-Sites wie Facebook und Twitter in ihren allgemeinen Geschäftsbedingungen (AGB) vorsehen. Er sprach sich aber dagegen aus, dass solche Selbstregulierungsmassnahmen als Rechtspflichten kodifiziert werden.[133] Eine Pflicht, Rechtsverletzungen ohne konkreten Hinweis zu entdecken und zu entfernen, sollte nach Ansicht des Bundesrates höchstens inhaltsnahe Anbieter wie News-Portale sowie Hoster von Foren und Blogs treffen, bei denen davon ausgegangen werden kann, dass sie die bei ihnen aufgeschalteten Inhalte einigermassen überblicken und kontrollieren können. Die Frage der erforderlichen Sorgfalt ist gemäss dem Bericht von den Gerichten einzelfallweise zu klären.

Der Bericht spricht sich im Grundsatz dagegen aus, ein neues zivilrechtliches Instrument zur Herausgabe der Identität anonymer User zu schaffen. In der Regel solle ein Verhalten auch künftig strafrechtlich relevant sein, um die Aufhebung des Fernmeldegeheimnisses beziehungsweise der Anonymität im Internet zu rechtfertigen.

Der Bericht befasst sich auch mit Fragen der gerichtlichen Zuständigkeit, des anwendbaren Rechts und der Rechtsdurchsetzung im internationalen Verhältnis. Er spricht sich gegen unilaterale Schweizer Regelungen aus.[134] Geprüft wurde eine Verpflichtung ausländischer Provider, in der Schweiz ein Zustellungsdomizil zu bezeichnen, was die Rechtsdurchsetzung ihnen gegenüber erleichtern könnte. Auch hier spricht sich der Bericht gegen eine gesetzliche Regelung im schweizerischen Recht aus. Insgesamt scheine es zielführender, den Abschluss von Rechtshilfeabkommen voranzutreiben; dies gelte auch für Vereinbarungen, welche die direkte postalische Zustellung von Schriftstücken in Zivilsachen vorsehen.[135]

## 4.3 Recht auf Datenmitnahme (Datenportabilität)

Der Social Media-Bericht 2013 vertieft auch die Frage der Datenportabilität, d.h. der Mitnahme von Daten im Bereich der Social Media-Plattformen. Problematisch wäre es, wenn soziale Plattformen ihre Kundschaft dadurch an sich zu binden versuchen, dass sie die Mitnahme eigener Daten zu Konkurrenzunternehmen verhindern. Gemäss Bericht sollte der Bund diesen Markt beobachten und, sofern nötig, ein Recht zur Datenmitnahme einführen. Es könnte sich als sinnvoll erweisen, die Schnittstellen zwischen unterschiedlichen Social Media-Plattformen zu regulieren. Beispielsweise könnten die grössten Plattformen verpflichtet werden, ihrer Kundschaft ein Recht auf Datenaustausch mit den Nutzern anderer Plattformen einzuräumen. Zur Beurteilung eines allfälligen Regelungsbedarfs könnte es hilfreich sein, Erfahrungswerte aus dem Ausland zu berücksichtigen.[136]

---

[132] Die zivilrechtliche Verantwortlichkeit von Providern, Bericht des Bundesrates vom 11. Dezember 2015, S. 4. http://www.ejpd.admin.ch/dam/data/bj/aktuell/news/2015/2015-12-110/ber-br-d.pdf.

[133] Die zivilrechtliche Verantwortlichkeit von Providern, Bericht des Bundesrates vom 11. Dezember 2015, S. 100.

[134] Die zivilrechtliche Verantwortlichkeit von Providern, Bericht des Bundesrates vom 11. Dezember 2015, Ziff. 7.4.2, S. 102.

[135] Die zivilrechtliche Verantwortlichkeit von Providern, Bericht des Bundesrates vom 11. Dezember 2015, Ziff. 7.4.2, S. 102f.

[136] Social Media-Bericht 2013, Ziff. 7.2.4.4, S. 75.

Das Thema Datenportabilität wurde im Rahmen verschiedener hängiger Gesetzgebungsvorhaben verwaltungsintern geprüft. Dies gilt für die Revision des DSG, aber auch für die FMG-Revision. Die fraglichen Analysen haben ergeben, dass die Möglichkeit zur Datenmitnahme (z.B. beim Wechsel von einer Social Media-Plattform zu einer anderen) zumindest bei den grossen Anbietern bereits weitgehend gegeben ist. Im Rahmen der FMG-Revision wurde aus diesem Grund ein Bedarf für ein gesetzlich geregeltes Recht auf Datenmitnahme verneint.

Gemäss dem Erläuternden Bericht zum Vorentwurf für eine Totalrevision des DSG[137] wurde die Frage geprüft, ob ein Recht auf Datenportabilität der betroffenen Personen eingeführt werden soll, wie es in Artikel 20 der EU-Datenschutz-Grundverordnung vorgesehen ist. Der Bundesrat bezeichnet die Umsetzung eines solchen Rechts aus verschiedenen Gründen als schwierig: Es verlange eine gegenseitige Abstimmung unter den Verantwortlichen und zweifellos eine – zumindest implizite – Einigung über die verwendeten Datenträger und Informatikstandards. Zudem habe die Regulierungsfolgenabschätzung gezeigt, dass sich die Einführung eines Rechts auf Datenportabilität gerade für Unternehmen mit über fünfzig Angestellten als sehr kostenintensiv erweisen könnte. Der Bundesrat ziehe es vor, die Ergebnisse der Erfahrungen innerhalb der Europäischen Union abzuwarten, bevor die Einführung eines Rechts auf Datenportabilität in Betracht gezogen wird. Die Frage werde jedoch im Rahmen der Strategie „Digitale Schweiz“ weiter geprüft.[138]

Die bundesrätliche Strategie „Digitale Schweiz“ vom April 2016[139] setzt das Ziel, eine kohärente und zukunftsorientierte Datenpolitik für die Schweiz zu etablieren. Im Zusammenhang mit den Arbeiten zur Erreichung dieses Ziels wurde das EJPD beauftragt, die Rechtslage in der Schweiz, der EU und in ausgewählten Vergleichsländern im Hinblick auf eine Weiterverwendung von Personendaten, Sachdaten und anonymisierten Daten zu analysieren und allfälligen Regelungsbedarf zuhanden des Bundessrates bis Ende 2017 zu identifizieren.[140] Aspekte einer etwaigen Regelung der Datenportabilität, namentlich ihre Tragweite und Grenzen sowie die damit verbundenen Herausforderungen, sind im Rahmen dieser Analyse zu prüfen.

## 4.4 Fernmelderecht: Anwendung von FMG-Regeln auf Social Media-Plattformen

Wie unter Ziffer 3.3. ausgeführt, unterstehen Social Media-Plattformen dem Fernmeldegesetz, falls über sie Fernmeldedienste erbracht werden, was etwa bei Mail- oder Messagingdiensten der Fall ist. Werden über Social Media-Plattformen Fernmeldedienste „Over the top“ (d.h. über den Internetzugang) erbracht, so unterscheiden diese sich nicht von anderen OTT-Diensten, weshalb sie grundsätzlich ebenfalls unter das Fernmelderecht fallen. Dies ist allerdings die Ausnahme. Im Regelfall handelt es sich bei Social Media-Plattformen nicht um Fernmeldedienstanbieterinnen, da sie selbst nicht fernmeldetechnisch Informationen zwischen mehreren Beteiligten übermitteln. Sie beherbergen meist nur Daten, welche ein anderes Unternehmen (eine Fernmeldedienstanbieterin) zum abrufenden Internetanschluss übermittelt.

Der Bundesrat hat sich im Rahmen des Fernmeldeberichts 2014[141] der Frage gewidmet, inwieweit Social Media-Plattformen im Rahmen einer Revision des FMG spezifisch erfasst werden sollten. Er

---

[137] s. Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetztes und die Änderungen weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, Ziff. 1.6.4, S. 22, https://www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/vn-ber-d.pdf.

[138] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, Ziff. 1.6.4, S. 22, https://www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/vn-ber-d.pdf.

[139] BBl 2016 3985, Ziff. 4.2.1, https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/strategie-digitale-schweiz.html.

[140] Medienmitteilung vom 22. März 2017; abrufbar unter: https://www.bakom.admin.ch/bakom/de/home/das-bakom/medieninformationen/medienmitteilungen.msg-id-66068.html.

[141] https://www.bakom.admin.ch/bakom/de/home/das-bakom/organisation/rechtliche-grundlagen/bundesratsgeschaefte/fernmeldebericht-2014.html, Kap. 3.1.

hat dabei einerseits festgehalten, es scheine keine grundlegende Änderung in der Definition des Fernmeldedienstes angezeigt, um auch neuere Phänomene einschliessen zu können, denn die geltende Definition des Fernmeldedienstes habe sich grundsätzlich bewährt. Ausserdem hat er daran erinnert, dass Social Media sich nicht von vielen anderen über das Internet erbrachten Diensten unterscheiden[142]. Wie diese anderen Dienste dienen auch Social Media-Plattformen in der Regel nur der Speicherung, nicht aber dem Transport von Informationen für Dritte. Es sei daher angezeigt, auch bei Social Media die Unterstellung unter das FMG nach den bestehenden fernmelderechtlichen Kriterien vorzunehmen.[143]

Andererseits erachtete der Bundesrat eine Klarstellung als sinnvoll, dass das FMG auch OTT-Dienste erfasst, wenn sie für Dritte Informationen fernmeldetechnisch transportieren. Darüber hinaus wurde im Fernmeldebericht 2014 angeregt, die Abschaffung der generellen Meldepflicht für Fernmeldedienstanbieter zu prüfen, denn diese sei vor dem Hintergrund der bestehenden Definition und dem Aufkommen der OTT-Dienste im Internet nicht mehr praktikabel umzusetzen.

Die im Fernmeldebericht 2014 angesprochenen Themen wurden im Rahmen der Erarbeitung der Vernehmlassungsvorlage[144] für eine Teilrevision des FMG weiterverfolgt. So schlug der Bundesrat vor, dass an der bestehenden Definition des Fernmeldedienstes festzuhalten, die allgemeine Meldepflicht für Fernmeldedienstanbieterinnen hingegen abzuschaffen sei. An ihre Stelle soll eine Registrierung derjenigen Anbieterinnen treten, die vom BAKOM Adressierungselemente oder Frequenzen zugeteilt erhalten. Reine Social Media-Plattformen gehören nicht zu diesem Kreis, da sie zum Erbringen ihrer Leistungen keine vom BAKOM verwalteten Adressierungselemente oder Frequenzen benötigen.

## 4.5 Ausbau der Medienkompetenz der Bevölkerung

Der Social Media-Bericht 2013 hat geschildert, was im schulischen Umfeld (für Kinder und Jugendliche sowie für deren Betreuungspersonen) zur Verbesserung der Medienkompetenz getan wird und künftig zu tun ist.[145] Die einschlägigen Webseiten, Publikationen u.a. seien laufend auf ihre Aktualität hin zu überprüfen und gegebenenfalls zu überarbeiten. Ausserdem sei zu prüfen, inwiefern auch in anderen Zielgruppen der Ausbau der Medienkompetenz insbesondere auf den Umgang mit Social Media hin ein Thema ist. Darüber hinaus seien Social Media selbst für alle Zielgruppen vermehrt zur Vermittlung von Informationen und für die Sensibilisierung zu ausgewählten Fragen einzusetzen.[146]

Der Bundesrat ist nach wie vor bestrebt, die Verbesserung der Medienkompetenzen von Jugendlichen zu fördern.[147] Im Bereich des Jugendschutzes hat die Eidgenössische Kommission gegen Rassismus (EKR) im 2015 die Kampagne „Bunte Schweiz“[148] lanciert. Die Kampagne zielte darauf ab, die Öffentlichkeit für das Thema der Rassendiskriminierung und der Hassreden im Internet zu sensibilisieren. Auch der Europarat hat mit der Kampagne „No Hate Speech“ ein Sensibilisierungsprogramm gestartet, welches noch läuft.[149] Die Schweiz hat sich an der europäischen Kampagne mit verschiedenen Aktionen beteiligt. Unter der Leitung einer Steuergruppe (Bundesamt für Sozialversicherungen, Fach-

---

[142] https://www.bakom.admin.ch/bakom/de/home/das-bakom/organisation/rechtliche-grundlagen/bundesratsgeschaefte/fernmeldebericht-2014.html, Kap. 3.1.1.3.

[143] https://www.bakom.admin.ch/bakom/de/home/das-bakom/organisation/rechtliche-grundlagen/bundesratsgeschaefte/fernmeldebericht-2014.html, Kap. 3.1.2.1.

[144] https://www.bakom.admin.ch/dam/bakom/de/dokumente/2015/12/erlaeuterungsberichtzuraenderungdesfernmeldegesetzes.pdf.download.pdf/erlaeuterungsberichtzuraenderungdesfernmeldegesetzes.pdf, Kap. 2, Erläuterungen zu Art. 4 FMG.

[145] Social Media-Bericht 2013, Ziff. 7.3.4, S. 78.

[146] Social Media-Bericht 2013, Ziff. 7.3.4, S. 78.

[147] Interpellation Masshard 14.3969, Mit Medienkompetenz gegen Hasskampagnen.

[148] www.bunte-schweiz.ch.

[149] http://www.europewatchdog.info/instrumente/kampagnen/no-hate-speech/, https://www.nohatespeechmovement.org/.

stelle für Rassismusbekämpfung, Verein Co-habiter und SavoirLibre) wurde die Schweizerische Arbeitsgemeinschaft für Jugendverbände SAJV neben weiteren Aktivitäten mit der Erstellung der Seite http://www.nohatespeech.ch beauftragt.[150]

Die Kommission für Wissenschaft, Bildung und Kultur des Nationalrates hat sich am 27. Mai 2016 im Zusammenhang mit der Parlamentarischen Initiative Amherd[151] gegen die Schaffung eines Kompetenzzentrums für die Förderung der Medienkompetenz von Kindern und Jugendlichen ausgesprochen. Die Mehrheit der Kommission sieht mit Verweis auf die laufenden Arbeiten des Bundesrates keinen Handlungsbedarf. Die Kommission weist diesbezüglich auf die Arbeiten des Bundesrates hin. Die im Rahmen des Programms „Jugend und Medien" erfolgten Massnahmen im Bereich des erzieherischen Kinder- und Jugendmedienschutzes werden weitergeführt. Der Bundesrat hat zudem angekündigt, die Koordinations- und Regulierungsaufgaben des Bundes zu verstärken.[152]

# 5 Entwicklung der Rechtslage im Bereich sozialer Netzwerke

## 5.1 Allgemeines

In den vorherigen Kapiteln wurden die Entwicklungen seit dem Social Media-Bericht 2013 in ihren Hauptlinien aufgezeigt. Kapitel 5 analysiert die Situation für verschiedene im Bericht von 2013 abgehandelte Themen[153] in ihren Einzelheiten.

## 5.2 Beeinträchtigung von Individualinteressen durch Plattformbetreiber

### 5.2.1 Grundproblem: Mangelhafte Kontrolle der Nutzenden über ihre Daten

Der Bundesrat folgerte im Social Media-Bericht 2013, dass die rechtlichen Bestimmungen einen umfassenden Schutz der in sozialen Netzwerken üblichen Datenbearbeitungen ermöglichen. Er erwähnte jedoch auch Phänomene, die einem wirksamen Datenschutz im Wege stehen. Der Bundesrat sah Verbesserungspotenzial durch vermehrte datenschutzrechtliche Voreinstellungen (privacy by design und privacy by default), die Förderung datenschutzfreundlicher Technologien sowie Massnahmen zur Verbesserung der Datenkontrolle und –herrschaft (u.a. durch verständlichere Formulierung von Datenschutzerklärungen).[154]

Der geschilderten Problematik soll Art. 18 VE-DSG entgegen wirken. Diese Vorschrift führt die Pflicht zum Datenschutz durch Technik sowie durch datenschutzfreundliche Voreinstellungen ein (so auch Art. 8 Ziff. 3 E-SEV 108, Art. 20 Abs. 1 Richtlinie 2016/680 sowie Art. 25 EU-DSGVO). Der für die Bearbeitung Verantwortliche und der Auftragsbearbeiter sind gemäss Art. 18 VE-DSG verpflichtet, angemessene Massnahmen zu treffen. Diese sollen schon ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Persönlichkeits- oder Grundrechtsverletzungen verringern (Abs. 1, sog. Privacy by Design). Zudem haben der Verantwortliche und der Auftragsbearbeiter mittels Voreinstellungen dafür zu sorgen, dass grundsätzlich nur die für den jeweiligen Verwendungszweck erforderlichen Daten bearbeitet werden (Abs. 2, sog. Privacy by Default).

Darüber hinaus ist gemäss Art. 13 Abs. 1 VE-DSG jede Person über die sie betreffende Beschaffung von Daten zu informieren. Diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden. Nach bestehendem Datenschutzrecht beschränkt sich die Informationspflicht auf das Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen (Art. 14 DSG).

---

[150] http://www.sajv.ch/2014/12/10/bundespraesident-burkhalter-gemeinsam-mit-der-jugend-gegen-diskriminierung-im-internet/, www.nohatespeech.ch.

[151] Parlamentarische Initiative Amherd 15.466 „Schaffung eines Kompetenzzentrums für die Förderung der Medienkompetenz von Kindern und Jugendlichen https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20150466.

[152] https://www.parlament.ch/press-releases/Pages/mm-wbk-n-2016-05-27.aspx.

[153] Social Media-Bericht 2013, S. 16ff.

[154] Social Media-Bericht 2013, Ziff. 4.3.1.8, S. 25.

Der Gesetzesentwurf erstreckt diese Pflicht auf alle personenbezogenen Daten und erweitert den Katalog der zu liefernden Daten: Gemäss Art. 13 Abs. 2 VE-DSG hat der für die Bearbeitung Verantwortliche alle Informationen zu kommunizieren, die erforderlich sind, damit die betroffene Person ihre Rechte nach dem DSG geltend machen kann und damit eine transparente Datenbearbeitung gewährleistet ist. Dazu gehören insbesondere: Die Identität und Kontaktdaten des für die Bearbeitung Verantwortlichen (lit. a), die Daten oder die Kategorien der bearbeiteten Daten (lit. b) und der Zweck des Bearbeitens (lit. c). Werden Personendaten Dritten bekanntgegeben, so sind der betroffenen Person zudem die Datenempfänger oder die Kategorie der Datenempfänger (Art. 13 Abs. 3 VE-DSG) mitzuteilen.[155]

Informationspflichten sieht auch die Datenschutzgrundverordnung der EU vor (Art. 13ff. EU-DSGVO). Bei einer automatisierten Entscheidungsfindung verlangt die Verordnung u.a. aussagekräftige Angaben darüber, nach welcher Logik die Datenbearbeitung erfolgt und was deren angestrebte Auswirkungen sind (Art. 15 Abs. 1 lit. h EU-DSGVO). Art. 24 Abs. 1 EU-DSGVO verpflichtet die Verantwortlichen dazu, geeignete technische und organisatorische Massnahmen zum Datenschutz zu treffen. Deren Umfang hängt u.a. ab von der Art, dem Umfang, den Umständen und den Zwecken der Datenerarbeitung sowie der jeweiligen Eintrittswahrscheinlichkeit und der Schwere der Risiken für die Rechte der betroffenen Personen.

### 5.2.2 Recht auf Löschung

Beim Recht auf Löschung bzw. Vergessenwerden handelt es sich in Bezug auf soziale Netzwerke in der Regel um den Anspruch, dass von den Nutzenden veröffentlichte Inhalte wieder entfernt werden. Der Social Media-Bericht 2013 beschrieb die Schwierigkeit, Benutzerkonten unwiderruflich zu löschen und das Problem, dass die Daten auf dem Server des Plattformbetreibers weiterhin aufbewahrt werden. (s. oben Kap. 3.1).[156]

Wie vorne erwähnt (Ziffer 2.5.3.1), wird auf europäischer Ebene explizit ein Recht auf Vergessenwerden statuiert (Art. 17 EU-DSGVO: Recht auf Löschung [„Recht auf Vergessenwerden"]).

Im Rahmen der Revision des DSG hat der Bundesrat eingehend geprüft, ob auch in der Schweiz ein gesetzlich statuiertes Recht auf Vergessenwerden eingeführt werden soll und wie sich entsprechende Ansprüche besser durchsetzen lassen. In seiner Prüfung kam der Bundesrat zum Schluss, dass bereits das geltende DSG eine umfassende Regelung der Problematik kennt. Sie erlaubt der betroffenen Person, widerrechtlich bearbeitete Daten löschen zu lassen. Das Recht auf Löschung wird nunmehr in Art. 25 Abs. 1 Bst. c VE-DSG ausdrücklich garantiert. Durch diese Erwähnung möchte der Bundesrat erreichen, dass das Gesetz für die betroffenen Personen verständlicher ist. Gemäss Art. 23 Abs. 2 Bst. b VE DSG[157] liegt eine Persönlichkeitsverletzung vor, wenn Daten entgegen der ausdrücklichen Willenserklärung durch die betroffene Person bearbeitet werden (wie dies auch schon der bestehende Art. 12 Abs. 2 Bst. b DSG festhält). Art. 23 Abs. 2 Bst. b VE-DSG verleiht der betroffenen Person das Recht, dem Verantwortlichen eine konkrete Datenbearbeitung explizit zu untersagen, ohne dass hierbei spezifische Voraussetzungen erfüllt sein müssten (opt-out). Art. 8 Bst. d E-SEV 108 verlangt dies explizit.[158]

---

[155] Vorentwurf zum Datenschutzgesetz.

[156] Social Media-Bericht 2013, Ziff. 4.3.3, S. 27f.; vgl. auch Interpellation Munz 15.3657 Recht auf Vergessen für Internet -Nutzerinnen und –Nutzer.

[157] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, S. 37, sowie Rosenthal David, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20. Februar 2017, Rz. 67, S. 24.

[158] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, S. 68.

Neu ist die Bestimmung in Art. 19 lit. b VE-DSG. Danach sind Betroffene über jede Berichtigung, Löschung oder Vernichtung von Daten sowie über Verletzungen zu informieren. Diese Informationspflicht entfällt nur, wenn die Mitteilung nicht oder nur mit unverhältnismässigem Aufwand möglich ist.[159] Eine solche Pflicht kennen auch die europäischen Regelwerke (Art. 16 Abs. 5 Richtlinie 2016/680 und Art. 19 EU-DSGVO). Die Informationspflicht stellt sicher, dass Daten nicht durch Dritte weiter bearbeitet werden, denen die Daten ohne Kenntnis der betroffenen Person übermittelt worden sind.[160]

### 5.2.3 Empfehlungen der guten Praxis

Der Vorentwurf zum DSG sieht in Art. 8 die Ausarbeitung von Empfehlungen der guten Praxis vor. Nach Art. 8 Abs. 3 VE-DSG publiziert der EDÖB solche nicht verpflichtenden Empfehlungen, um die Anwendung der Vorschriften über den Datenschutz zu konkretisieren. Dies gilt insbesondere für die Transparenz der Datenbearbeitung, die Rechte der betroffenen Person und die Pflichten des für die Bearbeitung Verantwortlichen sowie des Auftragsbearbeiters.

Die Empfehlungen der guten Praxis können in wichtigen Bereichen wie dem Cloud Computing oder den sozialen Netzwerken die Rechtslage präzisieren. Der EDÖB kann die Empfehlungen sowohl für den öffentlichen Sektor als auch für den Privatsektor erlassen. Interessierte Kreise können die Empfehlungen des Beauftragten ergänzen oder eigene Empfehlungen der guten Praxis ausarbeiten und diese dem EDÖB zur Genehmigung vorlegen. Sind sie mit den Datenschutzvorschriften vereinbar, genehmigt er sie (Abs. 2). Dieser Mechanismus soll konzertierte und breit abgestützte Branchenlösungen fördern, denn er ermöglicht einer Branche, selbst aktiv zu werden. Dies gilt auch für die Branche der Social Media-Plattformen.[161]

## 5.3 Beeinträchtigung von Individualinteressen durch Dritte

### 5.3.1 Verletzungen der persönlichen und wirtschaftlichen Ehre

Der Social Media-Bericht 2013 analysierte die strafrechtlichen (Art. 173-178 StGB), zivilrechtlichen (Art. 28f. ZGB) und lauterkeitsrechtlichen (Art. 3 Abs. 1 lit. a UWG) Vorgaben für Äusserungen in sozialen Netzwerken.[162] Er kam zum Schluss, dass die praktischen Probleme des Ehr- und Persönlichkeitsschutzes primär bei der Rechtsdurchsetzung liegen, falls die Urheber rechtswidriger Äusserungen nicht identifizierbar sind.

In den vergangenen Jahren hat sich verschiedentlich gezeigt, dass eine erfolgreiche Rechtsdurchsetzung gelingen kann. Ein Beispiel findet sich im Jahresbericht der KOBIK 2014: Auf einer Pornografie-Videoplattform wurden Videos von Gästen einer Badeanstalt veröffentlicht, ohne dass die Betroffenen davon wussten. Grösstenteils wurden weibliche Brüste und Hinterteile in den Fokus gerückt und mit ehrverletzenden und sexistischen Kommentaren beschrieben. Nachdem sich eine Geschädigte an die Medien gewandt hatte, wurden mehreren Anzeigen wegen Ehrverletzungsdelikten eingereicht. Mit der Unterstützung der KOBIK gelang es der zuständigen Kantonspolizei, den Hersteller und Profilbesitzer in Zusammenarbeit mit den Plattformbetreibern zu identifizieren und den Täter festzunehmen.[163]

---

[159] Rosenthal David, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet in: Jusletter 20. Februar 2017, S. 24, Rz. 68.

[160] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, S. 65.

[161] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, Ziff. 8.1.2.5, S. 53.

[162] Social Media-Bericht 2013, Ziff. 4.4.1, S. 36ff.

[163] Jahresbericht KOBIK 2014, Ziff. 2.4; S. 14; https://www.cybercrime.admin.ch/dam/data/kobik/Berichte/2015-03-26/jb-2015-d.pdf.

Unter Hinweis auf ein Urteil des Bezirksgerichtes Lenzburg zu „Rachepornos im Internet“ und einem gefälschten Facebook-Profil wurde am 2015 im Nationalrat ein Postulat zum Schutz der Persönlichkeitsrechte im digitalen Raum eingereicht.[164] In seiner Antwort vom 1. Juli 2015 verwies der Bundesrat auf den Social Media-Bericht 2013, die DSG-Revision, das Programm Jugend und Medien, die Revision des FMG und die Abklärungen zur zivilrechtlichen Verantwortlichkeit von Plattformbetreibern und Providern. Ein weiterer Bericht zur Thematik sei derzeit nicht notwendig. Darüber hinaus habe der Bund bereits auf den Umstand reagiert, dass die Strafverfolgung im Internet aus technischen Gründen schwierig ist: Das nBÜPF schaffe eine gesetzliche Grundlage für den Einsatz von besonderen Informatikprogrammen, mit welchen auch der verschlüsselte Fernmeldeverkehr überwacht werden kann (vgl. vorne Ziff. 3.5). Auch auf staatsvertraglicher Ebene verfolge der Bund diese Strategie (z.B. im Rahmen des 2012 in Kraft getretenen Europaratskonvention über die Cyberkriminalität).

Das Problem der auf die Person zielenden Schmähungen und Entblössungen hat sich in jüngster Vergangenheit gerade in sozialen Netzwerken tendenziell verschärft. Besonders problematisch sind etwa Kommentare in Blogs oder auf Newsplattformen[165] sowie Äusserungen im Kurznachrichtendienst Twitter. Diese haben zu verschiedenen Urteilen schweizerischer Gerichte geführt.[166]

Zu Konflikten kommt es auch nach angriffigen Einträgen auf Bewertungsportalen, beispielsweise bei negativen von Äusserungen von Arbeitnehmern über ihren (früheren) Arbeitgeber. Auch abschätzige Bewertungen von Kunden über Dienstleister (z.B. Hotels, Anwälte) oder Produkte werfen immer wieder rechtliche Fragen auf und können zu juristischen Schritten der kritisierten Anbieter führen. In diesem Zusammenhang hat der EGMR 2015 deutlich gemacht, dass die Meinungsfreiheit der Bewertenden zu respektieren ist. Die Allgemeinheit habe ein berechtigtes Interesse an Kommentaren über die Fähigkeiten von Personen, die einen Beruf öffentlichen Vertrauens (z.B. den Anwaltsberuf) ausüben. Sie müssten damit leben, dass sie von jedermann beurteilt werden, mit dem sie professionelle Kontakte hatten. Das Recht auf Achtung des Privat- und Familienlebens (Art. 8 EMRK) verlange vom Staat auch nicht, dass er die Identifizierbarkeit der Verfasser solcher auf die beruflichen Fähigkeiten zielenden Postings sicherstelle. Die Situation sei hier nicht mit gravierenden Übergriffen (wie etwa dem sexuell motivierten „Grooming“ von Minderjährigen) zu vergleichen.[167]

### 5.3.2 Cyberbullying und Cyberstalking

Der Bundesrat resümierte im Social Media-Bericht 2013, dass das Schweizer Recht zwar keine spezifische Cyberstalking- oder Cyberbullying-Bestimmung kennt, dieses Verhalten aber unter die geltenden strafrechtlichen (Art. 173-178 StGB) und zivilrechtlichen (Art. 28f. ZGB) Normen subsumiert werden kann. Die Hauptschwierigkeit sah der Bundesrat auch hier im Bereich der Rechtsdurchsetzung.[168]

---

[164] 15.3407 „Schutz der Persönlichkeitsrechte“, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153407.

[165] Meili Andreas/Galfano Michèle, Medienrechtliche und medienethische Schranken für Online-Leserkommentare - Eine Übersicht mit Fallbeispielen, in: medialex Jahrbuch 2016, S. 38-44, Ziff. 1ff.; Bundesgerichturteil 5A_1009/2015 vom 22.11.2015.

[166] Vgl. dazu etwa Bähler Regula, Tweet und Retweet: mitgegangen, mitgefangen – aber nicht immer: Medienethische und rechtliche Annäherung an das Medium Twitter im Umfeld von Ehrverletzungen, in: medialex Newsletter 2/2017; Prazeller Markus/Hug David, Twitter und Persönlichkeitsschutz - Bemerkungen zu den Urteilen des Bundesgerichts betreffend die Berichterstattung zum «Kristallnacht-Tweet» (5A_975/2015 und 5A_195/2016 vom 4. Juli 2016), in: Jusletter 24. Oktober 2016.

[167] EGMR-Zulässigkeitsentscheid „Kucharczyk c. Polen“ (Beschwerde N° 72966/13) vom 24.11.2015.

[168] Social Media-Bericht 2013, Ziff. 4.4.2.3, S. 39.

#### 5.3.2.1 Cyberbullying und Cybermobbing

Der Bundesrat hat in seiner Stellungnahme zur – letztlich abgelehnten[169] – Motion Schmid-Federer 12.4161 „Nationale Strategie gegen Cyberbullying und Cybermobbing“[170] ausgeführt, dass er die Problematik seit mehreren Jahren intensiv verfolgt. Im Anschluss an das Programm Jugend und Medien (vgl. oben Kap. 3.2) sei zu evaluieren, ob und inwieweit Handlungsbedarf besteht.

Nach Abschluss des Programms „Jugend und Medien“ hat die Kommission für Wissenschaft, Bildung und Kultur des Ständerates 2015 die Schaffung einer nationalen Strategie gegen Cyberbullying und Cybermobbing verworfen. Das Förder- und Präventionsprogramm habe sich bewährt und Cybermobbing sei als zentrales Problem berücksichtigt worden. Insbesondere der Schutz der Kinder und Jugendlichen vor sozialem und kriminellem Fehlverhalten wurden dabei schwerpunktmässig behandelt. Im Bereich der Prävention konnten in den Kantonen bereits einige Erfolge festgestellt werden.[171] Mittlerweile existiert ein breites Angebot an Beratung.[172]

Eine Notwendigkeit zur Einführung von strafrechtlichen Normen verneinte die Kommission. Die strafrechtlichen Bestimmungen reichten aus, um die Täter wirkungsvoll bestrafen zu können.[173]

In einem 2016 publizierten Aufsatz zum Cyberbullying hat der Thurgauer Staatsanwalt Brun festgehalten, es sei sinnvoller, sich eher auf eine Stärkung prospektiver Opfer zu konzentrieren als auf weitere strafrechtliche Massnahmen. Der Autor verweist auf die zentrale Bedeutung der Förderung von Selbstbewusstsein und Zivilcourage bei Kindern und Jugendlichen.[174]

Zum Schutz der Kinder sieht Art. 8 Abs. 1 EU-DSGVO vor, dass die Verarbeitung personenbezogener Daten eines Kindes nur rechtmässig ist, sofern das Kind das sechzehnte Lebensjahr vollendet hat bzw. nur, wenn elterliche Zustimmung vorliegt. Den Mitgliedstaaten steht es gemäss dieser Bestimmung jedoch offen, durch nationale Rechtsvorschriften eine niedrigere Grenze vorzusehen, die aber zwingend nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf.[175] Die Altersfrage war heftig umstritten, da viele Kinder schon vor dem dreizehnten Altersjahr ein Profil bei einem Online-Dienst haben. Kritiker warnen davor, dass dadurch Kindern und Jugendlichen eine legale Nutzung der Plattformen erschwert wird.[176]

#### 5.3.2.2 Cyberstalking

Hinsichtlich Cyberstalking hat der Bundesrat in seiner Stellungnahme zum Postulat Feri 14.4204 „Bekämpfung von Stalking in der Schweiz verbessern“ festgehalten, dass es neben gesetzgeberischen Verbesserungen auch Massnahmen zur Unterstützung für Betroffene und zur Inverantwortungnahme

---

[169] Beschluss des Nationalrates vom 5.3.2014 sowie des Ständerates vom 8.9.2015 (AB 2015 S 734: https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=34928.)

[170] Motion Schmid-Federer 12.4161, „Nationale Strategie gegen Cyberbullying und Cybermobbing“; abrufbar unter: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20124161.

[171] Bericht der Kommission für Wissenschaft, Bildung und Kultur vom 22. Juni 2015 zur Motion Schmid-Federer 12.4161 „Nationale Strategie gegen Cyberbullying und Cybermobbing https://www.parlament.ch/centers/kb/Documents/2012/Kommissionsbericht_WBK-S_12.4161_2015-06-22.pdf.

[172] Jugend und Medien, Zukünftige Ausgestaltung des Kinder- und Jugendmedienschutzes der Schweiz, 13. Mai 2015, Bericht des Bundesrates in Erfüllung der Motion Bischofberger 10.3666 „Effektivität und Effizienz im Bereich Jugendmedienschutz und Bekämpfung von Internetkriminalität, S. 92 https://www.bsv.admin.ch/dam/bsv/de/dokumente/kinder/berichte-vorstoesse/BRBjugendundmedien.pdf.download.pdf/bundesratsberichtjugendundmedien.pdf.

[173] Bericht der Kommission für Wissenschaft, Bildung und Kultur vom 22. Juni 2015 zur Motion Schmid-Federer 12.4161 „Nationale Strategie gegen Cyberbullying und Cybermobbing https://www.parlament.ch/centers/kb/Documents/2012/Kommissionsbericht_WBK-S_12.4161_2015-06-22.pdf.

[174] Brun Marcel, Cyberbullying – aus strafrechtlicher Sicht, in: recht 2016, S. 20.

[175] Art. 8 Abs. 1 EU-DSGVO.

[176] http://www.thetimes.co.uk/tto/news/world/europe/article4641159.ece; http://www.politico.eu/?s=age+16+facebook; https://www.heise.de/newsticker/meldung/Neue-EU-Datenschutzregeln-Facebook-erst-ab-16-Jahren-3044585.html.

von Tatpersonen braucht. Der Bundesrat stellte in seiner Stellungnahme eine Übersicht zu international und national erfolgreichen Praxismodellen in Aussicht. Die Kompetenz zur Prävention und Bekämpfung von Stalking liege aber bei den Kantonen. Ausserhalb gesetzgeberischer Kompetenzen komme dem Bund nur eine untergeordnete Rolle zu.[177] Der Nationalrat unterstützte im März 2015 die Forderung des Postulats, der Bundesrat solle in einem Bericht erfolgreiche nationale und internationale Massnahmen im Kampf gegen Stalking zusammenzustellen.[178]

Im Oktober 2015 schickte der Bundesrat verschiedene Änderungen im Zivil- und Strafrecht in die Vernehmlassung. In seinem erläuternden Bericht zum Vorentwurf des Bundesgesetzes über die Verbesserung des Schutzes gewaltbetroffener Personen hielt er fest, die Wirksamkeit der zivilrechtlichen Gewaltschutznorm von Art. 28*b* ZGB sei zu verbessern und zivilprozessuale Hürden seien abzubauen. So sollen die Gerichtskosten im Entscheidverfahren wegfallen und keine Schlichtungsverfahren mehr durchgeführt werden müssen (Art. 114 Bst. g und Art. 198 Bst. a$^{bis}$ VE-ZPO).[179] Die entsprechende Vernehmlassung wird zurzeit ausgewertet, gleichzeitig werden Botschaft und Entwurf zuhanden des Bundesrates erstellt.[180]

Ein vom Bundesgericht am 2. Dezember 2015 gefälltes Urteil verdeutlicht, dass die strafrechtlichen Bestimmungen betreffend Stalking auch bei Facebook-Einträgen greifen.[181]

### 5.3.3 Identitätsdiebstahl und andere Gefahren böswilliger Manipulation

Die durch das Parlament angenommene Motion Comte (14.3288) verlangt, dass der Missbrauch einer Identität eine strafbare Handlung für sich wird.[182] Im Rahmen der Totalrevision des Bundesgesetzes über den Datenschutz (DSG) hat der Bundesrat eine neue Bestimmung im Strafgesetzbuch vorgeschlagen und am 21. Dezember 2016 in die Vernehmlassung gesandt.

Gemäss dem vorgeschlagenen Art. 179$^{decies}$ StGB soll Identitätsmissbrauch zwecks Erlangung eines unrechtmässigen Vorteils künftig verboten werden: „Wer die Identität einer anderen Person ohne deren Einwilligung verwendet, um dieser zu schaden oder sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen, wird, auf Antrag, mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.“ [183] Der Nachteil für den Betroffenen muss eine gewisse Schwere erreichen und kann materieller oder immaterieller Natur sein.[184]

### 5.3.4 Beobachtungen von Äusserungen in sozialen Medien (Social Media Monitoring)

Der Social Media-Bericht 2013 führte zum Phänomen des Social Media Monitoring aus, dass der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) auf seiner Internetseite Empfehlungen für einen datenschutzkonformen Einsatz von Social Media Monitoring abgegeben hat.[185] Der EDÖB empfiehlt, die Bearbeitung von Personendaten auf ein Minimum zu beschränken und die Daten

---

[177] Postulat Feri 14.4204 Bekämpfung von Stalking in der Schweiz verbessern; https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20144204.

[178] Beschluss des Nationalrats zum Postulat Feri vom 20.3.2015; https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=33752.

[179] Erläuternder Bericht zum Vorentwurf des Bundesgesetzes über die Verbesserung des Schutzes gewaltbetroffener Personen vom Oktober 2015, https://www.bj.admin.ch/dam/data/bj/sicherheit/gesetzgebung/gewaltschutz/vn-ber-d.pdf.

[180] Die im Vernehmlassungsverfahren eingegangenen Stellungnahmen der Kantone, der Parteien und weiterer Verbände sind abrufbar unter https://www.bj.admin.ch/bj/de/home/sicherheit/gesetzgebung/gewaltschutz.html.

[181] BGE 141 IV 437.

[182] 14.3288 Motion Comte „Identitätsmissbrauch. Eine strafbare Handlung für sich“ https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20143288.

[183] Vorentwurf abrufbar unter: https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/vorentw-d.pdf

[184] Vgl. dazu die Ausführungen im Erläuternden Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, Ziff. 8.2.11, S. 93f.; https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/vn-ber-d.pdf.

[185] Social Media-Bericht 2013, Ziff. 4.4.4.2, S. 42.

so rasch wie möglich zu löschen oder zu anonymisieren. Gemäss EDÖB müssten die Nutzenden von sozialen Netzwerken darüber in Kenntnis gesetzt werden, dass Monitoring betrieben wird. Falls die betroffene Person nicht über die Bearbeitung informiert worden und dies auch aus den Umständen nicht ersichtlich wird, verstösst diese Handlung gemäss EDÖB gegen die datenschutzrechtlichen Bestimmungen.[186]

Auch die DSG-Revision greift diese Thematik auf. Nach Art. 13 VE-DSG muss der für die Bearbeitung Verantwortliche die Betroffenen über jede Art von Beschaffung der Daten informieren. Art. 20 VE-DSG besagt, dass jede Person vom Verantwortlichen Auskunft verlangen darf, ob Daten über sie bearbeitet werden. Die Vorschrift listet eine Reihe von Informationen auf, die der Verantwortliche in jedem Fall mitzuteilen hat (z.B. über den Bearbeitungszweck und die Aufbewahrungsdauer). Bei automatisierten Einzelentscheidungen sieht Art. 15 VE-DSG eine Informations- und Anhörungspflicht vor. Weiter sind in Art. 8 und 9 VE-DSG die Empfehlungen der guten Praxis normiert und in Art. 18 VE-DSG wird der für die Datenbearbeitung Verantwortliche verpflichtet, angemessene Massnahmen zu treffen, welche das Risiko von Persönlichkeitsverletzungen oder der Grundrechte vermindern und ihnen vorbeugen. Art. 18 VE-DSG verlangt Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen.[187]

### 5.3.5 Verletzungen des Urheberrechts auf Social Media-Plattformen

Die Vorgaben des Urheberrechts sind für durchschnittliche Nutzer sozialer Netzwerke wenig greifbar. In den vergangenen Jahren hat sich denn auch gezeigt, dass es auf Social Media-Plattformen immer wieder zu Verletzungen des geistigen Eigentums (Rechte der Urheber und der Interpreten) kommt. Der unzulässige Upload geschützter Werke scheint sich allerdings auf wenige Plattformen zu konzentrieren[188] und die schweizerischen Hosting Provider scheinen das Problem über die Selbstregulierung weitgehend im Griff zu haben.[189]

## 5.4 Beeinträchtigung von Gemeininteressen

### 5.4.1 Rassistische und andere diskriminierende Äusserungen („hate speech“)

Die Problematik hasserfüllter, hetzerischer, rassistischer und diskriminierender Äusserungen in sozialen Netzwerken hat sich in den vergangenen Jahren zugespitzt (vgl. dazu vorne Ziff. 2.5.2.3 zur Empfehlung der Parlamentarischen Versammlung des Europarats zu Diskriminierung und Hass im Internet). Sie beschäftigt auch die schweizerische Strafjustiz immer wieder.[190]

Diskriminierende Äusserungen von Usern sind nicht zuletzt ein Problem auf Plattformen, welche durch Medienschaffende betreut werden. Aus medienethischer Sicht ist die Erklärung der Rechte und Pflichten der Journalistinnen und Journalisten wesentlich.[191] Pflicht 8 verlangt die Achtung der Menschenwürde und den Verzicht auf diskriminierende Anspielungen. Der Schweizer Presserat hat in seiner Rolle als Selbstkontrollgremium daran erinnert, dass diese Pflicht auch beim redaktionellen Umgang mit Leserbriefen oder Online-Kommentaren von Aussenstehenden zu berücksichtigen ist. Er mahnt die professionellen Medienschaffenden zu grosser Aufmerksamkeit. Je aufgeheizter die Stimmung in der Bevölkerung sei, desto strikter sei auf die Publikation offen oder auch nur latent diskriminierender Beiträge zu verzichten. Aus diesem Grund stellte der Presserat 2016 einen Verstoss gegen Pflicht 8

---

[186] Datenschutzkonformes Social Media Monitoring, https://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00692/index.html?lang=de.

[187] Vernehmlassungsvorlage zum Datenschutzgesetz https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutz-staerkung/vorentw-d.pdf.

[188] Vgl. simsa Umfrage 2015 Code of Conduct Hosting; http://simsa.ch/_Resources/Persistent/2be6be4bbea4d7d7ee569211184b0631b499ab71/Auswertung-Umfrage-CCH-2016.pdf.

[189] Medienmitteilung des IGE vom 2. März 2017, Modernisierung des Urheberrechts: Kompromiss in der AGUR12 II”; https://www.ige.ch/fileadmin/user_upload/Urheberrecht/d/AGUR12_II_Medienmitteilung_20170302_DE.pdf.

[190] Vgl. etwa BGE 141 IV 108 S. 111.

[191] http://presserat.ch/21690.htm.

des Medienkodexes durch die Tageszeitung „Tribune de Genève“ fest. Deren Online-Forum erhält täglich mehr als 500 Beiträge aus der Leserschaft, welche von Moderatoren vorgängig kontrolliert werden. Dennoch hatte die Zeitung zwei diskriminierende und hasserfüllte Kommentare gegen Asylsuchende und gegen den Islam toleriert. Der Presserat erinnerte daran, dass gegen offenkundig gravierende Diskriminierungen der Kommentierenden einzuschreiten ist.[192]

In seiner Stellungnahme zur Interpellation Masshardt 14.3969 „Mit Medienkompetenz gegen Hasskampagnen“ [193] hat der Bundesrat bekräftigt, dass der Verbreitung rassistischer Äusserungen durch Jugendliche im Internet mit präventiven Massnahmen zu begegnen ist. Die Medienkompetenzen müssen verbessert sowie der respektvolle Umgang mit Mitmenschen, Kulturen und Religionen in einem übergeordneten Rahmen gefördert werden. In diesem Zusammenhang ist wertvoll, dass in den letzten Jahren in der Schule sowie in der ausserschulischen Jugendarbeit zahlreiche Projekte umgesetzt worden sind (so z.B. im Bereich der Förderung des besseren Verständnisses der Situation und Lebensgewohnheiten von jungen Muslimen in der Schweiz und im Rahmen der Jugendverbände oder der Fanarbeit in Bezug auf Sportveranstaltungen). Diese Massnahmen werden sodann durch die Fachstelle für Rassismusbekämpfung (FRB) sowie mit Mitteln des Kinder- und Jugendförderungsgesetzes (KJFG; SR 446.1) unterstützt.

Im Übrigen existiert mit dem Europäischen Rahmenübereinkommen zum Schutz nationaler Minderheiten ein rechtlich verbindliches multilaterales Abkommen des Europarats, das nationalen Minderheiten das Diskriminierungsverbot, die Meinungs-, Glaubens-, Gewissens-, Versammlungs- und Vereinigungsfreiheit garantiert. Das Übereinkommen garantiert des Weiteren besondere Rechte für Minderheiten (bspw. das Recht des Gebrauchs der eigenen Sprache und das Recht auf ungehinderten Kontakt mit Personen derselben ethnischen, kulturellen, religiösen oder sprachlichen Identität) über nationale Grenzen hinaus. Die Schweiz ist dem Rahmenübereinkommen 1998 beigetreten.[194] Der Bundesrat hat sich in seinem Bericht „Quatrième rapport du Gouvernement suisse sur la mise en oevre de la Convention-cadre du Conseil de l`Europe pour la protection des minorités nationales“ vom Februar 2017 zu den aktuellsten Entwicklungen geäussert.[195]

### 5.4.2 Sexuelle Ausbeutung und sexueller Missbrauch, Pornografie

Die Schweiz hat das Übereinkommen des Europarates zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch vom 25.10.2007 (sog. Lanzarote Konvention) am 18. März 2014 ratifiziert. Es ist für die Schweiz am 1. Juli 2014 in Kraft getreten. Gleichzeitig mit der Ratifizierung der Lanzarote-Konvention wurden einzelne Bestimmungen des StGB angepasst. Namentlich werden Kinder neu bis zur Vollendung des 18. Altersjahres vor der Mitwirkung an sexuellen Darstellungen geschützt (Art. 197 Abs. 4 und 5 StGB), der Konsum von harter Pornografie wird neu unter Strafe gestellt (Art. 197 Abs. 5 StGB) und der Strafrahmen wurde punktuell angehoben. Art. 9 Abs. 2 der Konvention verpflichtet alle Vertragsparteien, den privaten Sektor (u.a. im Bereich der Informations- und Kommunikationstechnologien) zu ermutigen, sich an der Ausarbeitung und Umsetzung von Massnahmen zum Schutz vor sexueller Ausbeutung und sexuellem Missbrauch von Kindern zu beteiligen. Eine Selbstregulierung der Branchen oder gemeinsam von Staat und privatem Sektor zu treffende Vorkehren sollen dazu beitragen, dass das Übereinkommen auch in sozialen Netzwerken beachtet wird.[196]

---

[192] Presserat Stellungnahme 8/2016 vom 2.5.2016 (X. c. „Tribune de Genève“); http://www.presserat.ch/_08_2016.htm.

[193] Interpellation Masshardt Nadine 14.3969 vom 26.09.2014 „Mit Medienkompetenz gegen Hasskampagnen“; https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20143969.

[194] https://www.edi.admin.ch/edi/de/home/fachstellen/frb/internationales/europarat/schutz-nationaler-minderheiten.html.

[195] https://www.eda.admin.ch/content/dam/eda/fr/documents/aktuell/news/4e-rapport-minorites-Suisse-15022017_FR.pdf.

[196] s. 0.311.40 Übereinkommen des Europarates zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch, abrufbar unter: https://www.admin.ch/opc/de/classified-compilation/20121286/.

Die Konvention bezweckt den Schutz von Kindern auch vor modernen Formen sexueller Ausbeutung. Zu den Delikten, deren Bestrafung die Konvention anstrebt, gehört auch das sog. Grooming.[197]

Im Rahmen der hängigen Revision des FMG ist eine Bestimmung geplant, welche die Fernmeldedienstanbieterinnen verpflichtet, qualifiziert pornografische Inhalte[198] gemäss der von KOBIK geführten Listen zu sperren (s. oben Ziff. 3.3).

In weiteren Projekten hat der Bundesrat Massnahmen zur Verhinderung von Pornografie (insbesondere von Pornografie mit Kindern) initiiert oder unterstützt (z.B. die Förderung der Medienkompetenz, das Projekt Jugend und Medien und weitere Sensibilisierungsprogramme).[199]

### 5.4.3 Gefährdung der öffentlichen Ordnung durch Massenmobilisierung

Eine Standesinitiative des Kantons Bern verlangte 2014, dass die Anonymität von Organisatoren aufgehoben werden kann, falls mittels sozialer Netzwerke zu Grossanlässen und Demonstrationen aufgerufen wird.[200]

Die sicherheitspolitische Kommission des Ständerats beantragte, der Standesinitiative keine Folge zu geben. Gleichzeitig verlangte sie in ihrem Postulat 14.3672 „Demonstrationen und Grossanlässe: Bekanntgabe von Internetadressen“ vom Bundesrat einen Bericht zur Frage, wie der Inhalt der Standesinitiative allenfalls umgesetzt werden könnte.[201]

Der Bundesrat liess 2014 in seiner Stellungnahme verlauten, dass eine präventive Aufhebung der Anonymität nicht mit dem Grundsatz der Verhältnismässigkeit vereinbar sei. Eine Unvereinbarkeit sei insbesondere dann anzunehmen, wenn der Aufruf zu einer Demonstration oder einem anderen Anlass keine Aufforderung zu Verbrechen oder sonstigen Gewalttätigkeiten enthalte. Zudem wies der Bundesrat auf die Schwierigkeiten hin, eine derartige Regelung gegenüber Providern mit Sitz im Ausland durchzusetzen. Von der ins Auge gefassten Regelung würde auch eine prohibitive Wirkung ausgehen, welche die verfassungsrechtlich garantierte Versammlungsfreiheit erheblich beschränken würde.[202]

In seinem vom Ständerat verlangten Bericht „Demonstrationen und Grossanlässe: Bekanntgabe von Internetadressen“ analysierte der Bundesrat im September 2015 die Möglichkeiten, wie sie sich gemäss den damaligen Entwürfen zur Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) und des neuen Nachrichtendienstgesetzes (NDG) präsentierten. Der Bundesrat wies darauf hin, dass die Polizeihoheit bei den Kantonen liegt. Es sei daher primär Sache der Kantone, in ihren Gesetzen bei Bedarf neue Instrumente zum Ausbau der polizeilichen (Ermittlungs-) Tätigkeit einzuführen. Dabei sei dem Verhältnismässigkeitsprinzip angemessen Rechnung zu tragen. Bestehe das Bedürfnis nach einer gewissen Rechtsvereinheitlichung, so bleibe es den Kantonen unbenommen, die notwendigen Regelungen mittels interkantonaler Vereinbarungen vorzusehen.[203]

---

[197] http://www.humanrights.ch/de/internationale-menschenrechte/europarat-abkommen/sexuelle-ausbeutung/.

[198] Vgl. Art. 197 Abs. 4 und 5 StGB.

[199] Vgl. Stellungnahme des Bundesrates zur Motion Tornare, 13.3087 Cyberkriminalität; https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20133087.

[200] Fertig mit den anonymen Aufrufen zu Demonstrationen und Grossanlässen ohne Übernahme von Verantwortung, Standesinitiative des Kantons Bern 14.305: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20140305.

[201] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20143672.

[202] Stellungnahme des Bundesrates vom 29.10.2014: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20143672.

[203] Bericht des Bundesrates vom 16.9.2015 in Erfüllung des Postulats 14.3672 der Sicherheitspolitischen Kommission des Ständerates vom 1. September 2014. Demonstrationen und Grossanlässe. Bekanntgabe von Internetadressen. https://www.parlament.ch/centers/eparl/curia/2014/20143672/Bericht%20BR%20D.pdf.

## 5.5 Menschen mit besonderen (Schutz-)Bedürfnissen

### 5.5.1 Kinder und Jugendliche

Wie im Social Media-Bericht 2013 aufgezeigt, sind die Risiken für Kinder und Jugendliche in den sozialen Netzwerken vielfältiger Art. Sie gehen über die unter Ziff. 5.2 bis 5.3 beschriebenen, tendenziell alle Nutzenden betreffenden Beeinträchtigungen von Individualinteressen hinaus. Insbesondere die nicht jugendfreien und jugendschädlichen Inhalte, aber auch die Kontaktaufnahme mit Dritten (bspw. aus sexuellen Motiven) sind problematisch.[204]

In seinem Bericht zur zukünftigen Ausgestaltung des Kinder- und Jugendmedienschutzes der Schweiz vom 13. Mai 2015 hat der Bundesrat die Chancen und Risiken digitaler Medien für Kinder und Jugendliche eingehend dargestellt.[205] Hinsichtlich der Chancen stehen folgende Aspekte im Vordergrund: Information und Bildung (u.a. Zugang zu Ratgebern, Umgang mit neuen Technologien und Training von Problemlösungsstrategien), Vernetzung, Unterhaltung und Kreativität sowie Identitätsbildung (u.a. durch Erfahrungsaustausch mit Gleichgesinnten).[206]

Der Bericht nimmt eine umfassende Risikoanalyse vor. Ausgehend von Erhebungen im In- und Ausland systematisiert und priorisiert der Bericht die möglichen Problemlagen für Kinder und Jugendliche. Dabei unterscheidet er vier Arten von Problemlagen[207]:

1. **Gefahren durch standardisierte Medieninhalte** (Kinder als Rezipienten vorgefertigter Medieninhalte, welche die Heranwachsenden verstören oder belasten): Gewalthaltige, bedrohliche und hasserfüllte Inhalte / pornografische oder unerwünschte sexuelle Inhalte / verzerrte oder irreführende Informationen (z.B. zu Drogen, Anorexie, Selbstschädigungen) / kommerzielle Risiken (z.B. Schleichwerbung).

2. **Gefahren durch individualisierte Kontakte mit Anbietern** (Kinder als Marktteilnehmer und Vertragspartner, welche u.a. in die Irre geführt werden können): Druckausübung (z.B. durch Inkasso), Drohung mit vertraglichen Sanktionen durch Anbieter / Erotik-Spams / Micro-Payments, In-App Käufe, Gewinnspiele, Abofallen, Betrug, Irreführung / exzessive Nutzung (gefördert durch Flatrates, Bonuspunkte und Rabatte) / Intransparenz hinsichtlich der Verwendung oder Weitergabe eigener Daten.

3. **Gefahren durch individualisierte Kontakte des Kindes mit Anderen** (Kinder als Teilnehmer individueller Kommunikationsprozesse mit Bekannten und Unbekannten): Kind als Opfer von Belästigung, Schikane, Einschüchterung und Cyberbullying / Anzügliche Botschaften von Kommunikationspartnern, Kontaktnahme durch Pädokriminelle / Anstiftung zu Selbstschädigungen oder gesellschaftlichem bzw. kriminellem Fehlverhalten / Gruppendruck und reziproker Druck (Social Games) / Ausspionieren und Sammeln persönlicher Daten durch den Kommunikationspartner.

4. **Problematische Handlungen des Kindes** (Kinder als Akteure, die ungeeignete Inhalte produzieren und verbreiten bzw. Andere verletzen, bedrängen und beleidigen): Belästigung oder Einschüchterung Anderer (u.a. durch Cyberbullying) / Sexuelle Belästigung Anderer, Erstellen und Veröffentlichen pornografischen Materials / Veröffentlichung problematischer Inhalte und Aufforderung zur Nachahmung (z.B. zu Suizid oder Anorexie) / Illegale Uploads urheberrechtlich geschützter Werke, schädliche

---

[204] Social Media-Bericht 2013, Ziff. 4.7.1.1, S. 51.

[205] Jugend und Medien: Zukünftige Ausgestaltung des Kinder- und Jugendmedienschutzes der Schweiz - Bericht des Bundesrates in Erfüllung der Motion Bischofberger 10.3466 «Effektivität und Effizienz im Bereich Jugendmedienschutz und Bekämpfung von Internetkriminalität», Ziff. 3.3, S. 19ff.; http://www.jugendundmedien.ch/fileadmin/user_upload/1_Medienmitteilungen_Aktuellmeldungen/Bundesratsbericht_Jugend_und_Medien.pdf.

[206] Bericht Jugend und Medien 2015, Ziff. 3.3, S. 19.

[207] Vgl. die Tabelle im Bericht Jugend und Medien 2015, Ziff. 3.3, S. 20.

Downloads, Hacking, Glücksspiel / Exzessive Nutzung (selbst gesetzter Leistungsdruck, Vernachlässigung alternativer Aktivitäten) / Problematische Formen der Selbstdarstellung (Drogen, politische Einstellung, sexuelle Orientierung) und des Umgangs mit Daten Dritter.

Der Bericht hält fest, dass sich der bisherige Jugendmedienschutz auf den Schutz der Heranwachsenden vor standardisierten Medieninhalten (oben Ziff. 1) konzentriert hat. Das Spektrum möglicher Gefährdungen habe sich in den letzten Jahren aber massiv erweitert. Angesichts des veränderten Nutzungsverhaltens sei neu auch Problemlagen zu begegnen, die sich aus der Rolle von Kindern und Jugendlichen als Marktteilnehmende, Kommunikationsteilnehmende und Akteure (Ziff. 2-4) ergeben.

Nicht alle der identifizierten Risiken erforderten jedoch ein Handeln des Gesetzgebers. Aufgrund seiner Schutzpflichten müsse der Staat nur dort regulieren, wo schwerwiegende, fortwirkende negative Auswirkungen auf die körperliche und seelische Gesundheit der Heranwachsenden zu erwarten sind. In allen anderen Bereichen seien die Interessen des Kinder- und Jugendmedienschutzes mit den Freiheitsrechten Dritter in Einklang zu bringen.[208]

Zu diesem Zweck hat der bundesrätliche Bericht die Frage vertieft, welche der geschilderten Problemlagen prioritär zu behandeln sind. Dabei berücksichtigte er nicht nur die Eintrittswahrscheinlichkeit und die Schadenshöhe der jeweiligen Risiken (Risiko-Management-Perspektive), sondern auch die Steuerungswirkung regulatorischer Eingriffe.

Bei vielen der vorne aufgezeigten Problemlagen lasse sich eine ausreichende Steuerungswirkung primär durch Medienkompetenz (erzieherischer Jugendschutz) erzielen. Dies gilt für Handlungen von Heranwachsenden als Akteure (Ziff. 4) und als Marktteilnehmer (Ziff. 2; ausgenommen der Intransparenz bezüglich der Verwendung oder Weitergabe eigener Daten), teilweise auch für das Verhalten als Kommunikationsteilnehmer (Ziff. 3: Gruppendruck).

Prioritär zu behandeln seien drei Problembereiche[209]:

- Generell verbotene bzw. für bestimmte Altersgruppen ungeeignete Medieninhalte;
- Beeinträchtigende Mitteilung im Rahmen der Individualkommunikation (Cyberbullying, Cybermobbing, Grooming, Sexting u.a.);
- Intransparente und daher hinsichtlich ihrer Folgen nur schwer abschätzbare Bearbeitung persönlicher Daten.

Beim Kinder- und Jugendmedienschutz gebe es Schnittstellen zum Persönlichkeits-, Daten- und Konsumentenschutz. Die dort zuständigen Behörden, Aufsichtsinstanzen und Selbstkontrollstellen müssten systematische Formen der Zusammenarbeit entwickeln.

Fragen der Regulierung werden gegenwärtig im Rahmen der unter Federführung des BSV angelaufenen Vorarbeiten für eine Vernehmlassungsvorlage zum Schutz der Jugend vor ungeeigneten Inhalten in Film, Computerspielen und auf Online-Plattformen vertieft (vgl. oben Ziff. 3.2).

---

[208] Bericht Jugend und Medien 2015, Ziff. 3.4.1, S. 22ff.

[209] Vgl. die Tabelle im Bericht Jugend und Medien 2015, Ziff. 3.3, S. 20.

### 5.5.2 Arbeitnehmende

Der Social Media-Bericht 2013 widmete sich auch den mit sozialen Netzwerken zusammenhängenden Problemen für künftige oder bestehende Arbeitsverhältnisse.[210] Diese betreffen etwa den Zugriff des Arbeitgebers auf persönliche Daten von Kandidaten für eine offene Stelle.

Die vorne geschilderte Revision des Datenschutzrechts und der mit ihr verbundene Ausbau der Kontrolle über die eigenen Personendaten (Ziff. 5.2) ist geeignet, auch die Situation von Stellenbewerbern oder Arbeitnehmern verbessern. So erleichtern es datenschutzfreundliche Voreinstellungen, das Recht auf Löschung und wohl auch die vorgesehenen Empfehlungen der guten Praxis den Stellenbewerbern, die Angaben in Social Media besser vor den Recherchen durch potenzielle Arbeitgeber zu schützen.

### 5.5.3 Menschen mit Behinderung

Im Social Media-Bericht 2013 wurde aufgezeigt, dass soziale Netzwerke ein grosses Potential zur gesellschaftlichen Inklusion von Menschen mit Behinderungen bergen.[211] Der heutige Stand der Technik ermöglicht es Menschen mit einer physischen, geistigen oder psychischen Beeinträchtigung, sich besser am gesellschaftlichen Leben zu beteiligen und effektiver von ihren Informations- und Kommunikationsrechten Gebrauch zu machen. Voraussetzung ist allerdings, dass die Plattformanbieter die Zugänglichkeit und Nutzung ihrer Angebote barrierefrei gestalten. Dies bedeutet, dass sie für Menschen mit Behinderung in derselben Weise zugänglich und nutzbar sind wie für Menschen ohne Behinderung.

#### 5.5.3.1 Rechtliche Entwicklungen

Seit dem 15. Mai 2014 ist die Schweiz an das Übereinkommen über die Rechte von Menschen mit Behinderungen (UNO-BRK)[212] gebunden. Die Konvention verlangt den vollen und gleichberechtigten Genuss jeglicher Form von Kommunikation. Gemäss Art. 2 UNO-BRK umfasst Kommunikation eine Vielzahl von Elementen: Sprachen, Textdarstellung, Brailleschrift, taktile Kommunikation, Grossdruck, leicht zugängliches Multimedia sowie schriftliche, auditive, in einfache Sprache übersetzte, durch Vorleser zugänglich gemachte sowie ergänzende und alternative Formen, Mittel und Formate der Kommunikation, einschliesslich leicht zugänglicher Informations- und Kommunikationstechnologie. Diese Umschreibung ist auch auf Social Media anwendbar. Plattformen müssen behindertengerecht aufgebaut werden.

Art. 9 Abs. 2 lit. b UNO-BRK verpflichtet die Vertragsstaaten geeignete Massnahmen zu ergreifen um sicherzustellen, dass private Anbieter von öffentlich zugänglichen oder bereitgestellten Einrichtungen und Diensten alle Aspekte des barrierefreien Zugangs berücksichtigen.[213] Die Absicht ist, dass nicht zwischen privatrechtlichen oder öffentlich-rechtlichen Leistungen unterschieden wird. Ausschlaggebend für die geforderte Barrierefreiheit ist der Umstand, dass eine Leistung an die Öffentlichkeit gerichtet ist.[214]

Art. 21 UNO-BRK regelt das Recht auf freie Meinungsäusserung, Meinungsfreiheit und Zugang zu Informationen. Bst. c verpflichtet die Vertragsstaaten dazu, private Dienstleister dringend aufzufordern, ihre Dienste in Formaten zur Verfügung zu stellen, die für Menschen mit Behinderungen zugänglich und nutzbar sind. Art. 30 UNO-BRK normiert weiter die Teilhabe am kulturellen Leben sowie an Erho-

---

[210] Social Media-Bericht 2013, Ziff. 4.6.2, S. 54ff.

[211] Social Media-Bericht 2013, Ziff. 4.6.3, S. 56f.

[212] SR 0.109.

[213] CRPD, General Comment No. 2 (2014), N 13; Trenk-Hintenberger Peter, in: Kreutz Marcus/Lachwitz Klaus/Trenk-Hinterberger Peter (Hrsg.), Die UN-Behindertenrechtskonvention in der Praxis, Köln, 2013, N 5 und 7 zu Art. 9 UNO-BRK, S. 132 f.

[214] Darunter zu verstehen sind Dienste, die an einen unbestimmten Personenkreis gerichtet sind.

lung, Freizeit und Sport. Die Staaten achten dieses Recht und haben die Verpflichtung, alle Handlungen zu unterlassen, die dieses Recht beeinträchtigen könnten. Kulturelle und freizeitliche Inhalte müssen in einer barrierefreien Form angeboten werden. Dazu gehört der Zugang zum Internet und zu den sozialen Netzwerken.[215]

Am 2. Dezember 2016 wurde die EU-Richtlinie 2016/2102 vom 26. Oktober 2016 über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen im Amtsblatt veröffentlicht.[216] Zweck dieser Richtlinie ist die Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten zu den Barrierefreiheitsanforderungen für Websites und mobile Anwendungen öffentlicher Stellen. Die Mitgliedstaaten der EU müssen die Richtlinie bis zum 23. September 2018 umsetzen.[217]

#### 5.5.3.2 Umsetzung

In der Schweiz wurden verschiedene Massahmen ergriffen, welche die Umsetzung der Anforderungen der UNO-BRK und des Bundesgesetzes über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen (Behindertengleichstellungsgesetz, BehiG; SR 151.3) bezwecken.

Am 20. Juni 2014 hat der Bundesrat einen Massnahmenkatalog bezüglich der Barrierefreiheit der Bundes-Websites verabschiedet.[218] Darauf aufbauend entstand der Aktionsplan E-Accessibility 2015-2017. Die Departemente und Ämter sollen darin unterstützt werden, Instrumente bereitzustellen und Empfehlungen im Zusammenhang mit der E-Accessibility zu erarbeiten. Konkret müssen etwa Webseiten, elektronische Dokumente und Applikationen so ausgestaltet werden, dass sie z.B. mit Vorleseprogrammen gelesen werden können. Die Massnahmen sollen bis Ende 2017 mit der Unterstützung der 2014 auf drei Jahre gegründeten Fachstelle E-Accessibility umgesetzt werden.[219]

Weiter hat der Bundesrat im März 2016 die Strategie „Digitale Schweiz“ verabschiedet. Ein Kernanliegen dieses Projekts ist die Chancengleichheit und Partizipation aller Einwohnerinnen und Einwohner. Ziel ist ein chancengleicher, kostengünstiger, barriere- und diskriminierungsfreier Zugang zu einer qualitativ hochstehenden Netzwerkinfrastruktur und zu innovativen Inhalten, Diensten und Anwendungen.[220] In diesem Zusammenhang fordert der Aktionsplan e-Inclusion 2016-2020 des Netzwerks „Digitale Inklusion Schweiz“ die Verbesserung der Zugänglichkeit (E-Accessibility) und der Benutzerfreundlichkeit (Usability) von Webseiten und Online-Angeboten. Es werden Massnahmen verlangt, welche die Zugänglichkeit von Webseiten und allgemein von Informations- und Kommunikationstechnologien öffentlicher und privater Anbieter verbessern, sowie die stete und kohärente Umsetzung des gesamtschweizerischen Accessibility-Standards für Internetangebote (eCH-Standard) unterstützen.[221]

Ein Bericht des Eidgenössischen Büros für die Gleichstellung von Menschen mit Behinderungen (EBGB) zur Entwicklung der Behindertenpolitik vom 11. Januar 2017 fordert die verbesserte Zugänglichkeit zu neuen Informations- und Kommunikationsdienstleistungen. Programme und Projekte zur

---

[215] Kreutz Marcus/Lachwitz Klaus/Trenk-Hinterberger Peter (Hrsg.), Die UN-Behindertenrechtskonvention in der Praxis, Köln 2013, S. 312.

[216] Richtlinie (EU) 2016/2102 des Europäischen Parlaments und des Rates vom 26. Oktober 2016 über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen, ABl. L 327 vom 2.12.2016, S. 1; abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L2102&from=DE.

[217] Richtlinie (EU) 2016/2102, vor allem Art. 1 und Art. 12 (Umsetzung).

[218] Vgl. Medienmitteilung des EDI: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-53417.html.

[219] Mehr dazu Interdepartementale Arbeitsgruppe Barrierefreiheit IDA BF, Aktionsplan E-Accessibility 2015–2017 vom 16. Juli 2015 - Umsetzung des Massnahmenpakets Internet-Barrierefreiheit vom 20.6.2014, abrufbar unter http://www.news.admin.ch/NSBSubscriber/message/attachments/41220.pdf.

[220] Strategie „Digitale Schweiz“, BBl 2016 3987, Ziff. 3; abrufbar unter https://www.admin.ch/opc/de/federal-gazette/2016/3985.pdf.

[221] Mehr dazu: e-Inclusion Schweiz - Aktionsplan 2016 -2020, Informations- und Kommunikationstechnologien für eine integrative Gesellschaft, http://www.einclusion.ch/de/e-inclusion-ch/aktionsplan.html, unter anderem S. 3 und 4.

Förderung der Gleichstellung sollen sichergestellt und die beim Bund erarbeiteten Erfahrungen und Instrumente an andere Behörden und Private weitergegeben werden.[222]

#### 5.5.3.3 Studien und Barrierefreiheit in der Schweiz

Zur Nutzung sozialer Netzwerke durch Menschen mit Behinderungen gibt es in der Schweiz keine spezifischen Studien. Immerhin hat die Stiftung „Zugang für alle" im Jahr 2016 die Schweizer Accessibility Studie[223] publiziert, welche sich mit der Barrierefreiheit bestimmter Webseiten beschäftigt. Resultat der Studie war, dass ein grosses Verbesserungspotenzial für Private und kantonale sowie kommunale Webseiten besteht.

Auch einige Internetseiten des Bundes entsprechen nicht dem Standard, den sie gemäss den Richtlinien für die Gestaltung von barrierefreien Internetangeboten (P028)[224] zu erfüllen haben. Für die kantonalen und kommunalen Internetangebote gilt der Accessibility-Standard eCH-0059, Version 2.0, [225] welcher einheitliche Kriterien festhält, nach denen sich auch Private richten können. Die erwähnten Richtlinien entsprechen nur am Rande den Bedürfnissen der Menschen mit einer kognitiven Beeinträchtigung. Um ihren Bedürfnissen gerecht zu werden, hat die Stiftung „Zugang für alle" zusammen mit der Fachhochschule Nordwestschweiz den unverbindlichen Leitfaden „Einfach Surfen" erarbeitet, welcher sich an alle richtet, die an der Entwicklung einer Webseite beteiligt sind.[226]

#### 5.5.3.4 Deutsche Studie „Web 2.0/barrierefrei"

Die deutsche Studie „Web 2.0/barrierefrei", welche 2012 durch die „Aktion Mensch" [227] in Zusammenarbeit mit der Stiftung „Digitale Chancen" [228] herausgebracht wurde, befasst sich mit der Nutzung des Internets durch Menschen mit Behinderungen.[229] Resultate dieser Studie zeigten z.B., dass Wikipedia das bekannteste Internetangebot für gehörlose und schwerhörige Internetnutzer ist. Am häufigsten genutzt werden Wikis (61%), Fotos (60%) und Videos (47 %). Die selbständige Nutzung des Internets durch Blinde war eher gering. Die häufigsten Nutzungsarten sind Wikis lesen (85%), als Benutzer registrieren (80%), Kommentare schreiben (60%) sowie Podcasts hören (60%).

#### 5.5.3.5 Australische Studie „Sociability: Social Media for People with Disability"

Gemäss einer australischen Studie von 2012[230] , welche einzelne soziale Netzwerke auf ihre Zugänglichkeit getestet hat, sind einige Webseiten über gewisse Endgeräte einfacher zu bedienen als andere. Menschen mit einer Sehbehinderung oder blinde Personen orientieren sich beispielsweise besser auf der mobilen Seite von Facebook (m.facebook.com), da diese auf die primären Anwendungen reduziert ist. LinkedIn schneidet in dieser Studie besonders gut ab und gilt als generell benutzbar. Kritisiert wird der automatische Untertitel-Generator auf YouTube, der noch zu viele Fehler macht. Twitter gilt als

---

[222] EDI, Bericht zur Entwicklung der Behindertenpolitik vom 11. Januar 2017, S. 28; https://www.newsd.admin.ch/newsd/message/attachments/46888.pdf.

[223] Schweizer Accessibility-Studie 2016, Bestandesaufnahme der Zugänglichkeit bedeutender Schweizer Internetangebote, Eine Studie der Schweizerischen Stiftung zur behindertengerechten Technologienutzung <<Zugang für alle>>; abrufbar unter http://www.access-for-all.ch/ch/77-aktuell/518-schweizer-accessibility-studie-2016.html.

[224] Mehr zu den Richtlinien des Bundes unter: https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/prozesse-methoden/p028-richtlinien_bund_gestaltung_barrierefreie_internetangebote.html.

[225] Öffentlich-rechtliche Rahmenvereinbarung über die E-Government-Zusammenarbeit in der Schweiz (2016-2019), vom Bundesrat am 18. November 2015 verabschiedet und durch die Plenarversammlung der Konferenz der Kantonsregierungen am 18. Dezember 2015 genehmigt; https://www.egovernment.ch/de/umsetzung/offentlich-rechtliche-rahmenvereinbarung-uber-die-e-governme/.

[226] http://einfachsurfen.ch.

[227] Deutschlands grösste Förderorganisation im sozialen Bereich und Soziallotterie: https://www.aktion-mensch.de/.

[228] https://www.digitale-chancen.de/index.cfm/lang.

[229] Berger Andreas/Caspers Tomas/Croll Jutta/Hofmann Jörg/Kubicek Herbert/Peter Ulrike/Ruth-Janneck Diana/Trump Thilo, Web 2.0 / barrierefrei, Eine Studie zur Nutzung von Web 2.0 Anwendungen durch Menschen mit Behinderung, Hrsg. Aktion Mensch, Bonn, 2010; abrufbar unter http://publikationen.aktion-mensch.de/barrierefrei/Studie_Web_2.0.pdf.

[230] Media Access Australia (Hrsg.), Sociability: Social Media for People with a Disability, Ultimo NSW, 2012, abrufbar unter: http://www.mediaaccess.org.au/web/social-media-for-people-with-a-disability.

relativ unzugänglich, obwohl der Dienst ausschliesslich auf kurze Textnachrichten ausgerichtet ist. Gemäss dieser Studie gelten Weblogs (Blogs) als gut zugänglich, obwohl dies wiederum nach Behinderung und Inhalt variiert. Auch Skype hat gut abgeschnitten.

#### 5.5.3.6 Schlussfolgerungen

Ausländische Untersuchungen legen die Vermutung nahe, dass die Zugänglichkeit einzelner sozialer Netzwerke für schweizerische Behinderte mangelhaft ist. Die Barrierefreiheit von Social Media für schweizerische Nutzende wurde allerdings noch nicht systematisch untersucht. Eine Studie über die Nutzung von Social Media durch Menschen mit Behinderungen in der Schweiz könnte dazu beitragen, aktuelle Probleme und Bedürfnisse besser zu erkennen und anschliessend zielgerichtete Verbesserungen in die Wege zu leiten.

## 5.6 Durchsetzung des Rechts

### 5.6.1 Allgemeines

Einträge auf sozialen Plattformen können diverse Vorschriften des Straf- und Zivilrechts verletzen (s. Ziff. 5.3 und 5.4. oben). Vertieft zu diskutieren ist an dieser Stelle insbesondere die Problematik, dass die für eine Rechtsverletzung Verantwortlichen in der Praxis oft nicht zur Rechenschaft gezogen werden können und dass Social Media-Plattformen ihren Sitz hauptsächlich im Ausland haben, mithin nicht ausschliesslich schweizerisches Recht anwendbar ist bzw. oft auf das Instrument der Rechtshilfe verwiesen wird.[231]

Der Bundesrat hat im Social Media-Bericht 2013 in Aussicht gestellt, den gesetzgeberischen Handlungsbedarf für eine Regelung der Verantwortlichkeit von Internet-Dienstleistern erneut zu prüfen.[232] In der Folge hat er am 11. Dezember 2015 den Bericht über die zivilrechtliche Verantwortlichkeit von Providern vorgelegt (vgl. vorne Kap. 4.2).[233]

### 5.6.2 Providerverantwortlichkeit für fremde Inhalte

Wie im Social Media-Bericht 2013 ausgeführt, hat das Bundesgericht die zivilrechtliche Verantwortlichkeit (Art. 28 Abs. 1 ZGB) der „Tribune de Genève“ bejaht, welche auf ihrer Website als Hosting-Providerin den Speicherplatz für Blogs angeboten hatte. Dem Zivilkläger stehe es sogar frei, ausschliesslich gegen einen Beteiligten vorzugehen, welcher bei der Publikation nur eine untergeordnete Rolle gespielt hatte.[234]

2015 hat das Bundesgericht seine Rechtsprechung präzisiert: Aus Art. 28 ZGB lasse sich keine Haftung für fremdes Verhalten herleiten. Ein Mitwirken durch passives Verhalten setze die Verletzung einer Pflicht zum Handeln voraus. Eine ungenutzte Möglichkeit zu handeln genüge nicht. Nötig sei eine Rechtspflicht, die das Persönlichkeitsrecht verletzenden Äusserungen zu verhindern bzw. ihnen ein Ende zu setzen.[235] Das Bundesgericht gelangte somit zu den gleichen Schlüssen wie der Bundesrat in seinem Bericht über die zivilrechtliche Verantwortlichkeit der Provider.

2015 entschied die Grosse Kammer des Europäischen Gerichtshofs für Menschenrechte (EGMR) über die zivilrechtliche Verantwortlichkeit eines kommerziellen Internet-Nachrichtenportals für extreme,

---

[231] Vgl. Bundesgerichtsurteil 1B_185/2016, 1B_186/2016, 1B_188/2016 vom 16.11.2016.

[232] Social Media-Bericht 2013, Ziff. 7.2.4.2, S. 75.

[233] Die zivilrechtliche Verantwortlichkeit von Providern, Bericht des Bundesrates vom 11. Dezember 2015; abrufbar unter https://www.ejpd.admin.ch/dam/data/bj/aktuell/news/2015/2015-12-110/ber-br-d.pdf.

[234] Bundesgerichturteil 5A_792/2011 vom 14.1.2013 E. 6.2 (Tribune de Genève).

[235] BGE 141 III 513 E. 5.3.

als Hassrede und Gewaltaufruf zu qualifizierende Kommentare seiner Nutzer. Die Pflicht des Portalbetreibers zur Bezahlung einer Entschädigung an den Kläger verletzte das Recht auf freie Meinungsäusserung nicht.[236]

In einem Urteil von 2016 verneinte der EGMR hingegen die zivilrechtliche Verantwortlichkeit eines nicht-kommerziellen Plattformbetreibers für Kommentare, die vulgär und beleidigend (nicht aber als Hassrede oder Gewaltaufruf zu qualifizieren) waren und sich gegen ein Unternehmen (nicht aber eine natürliche, durch die Menschenwürde geschützte Person) richteten.[237] Diese Rechtsprechung bestätigte der EGMR 2017 im Falle diffamierender Vorwürfe gegen eine Einzelperson in den Kommentarspalten des Blogs einer kleinen Nichtregierungsorganisation.[238]

### 5.6.3 Verfolgung der Verfasser rechtswidriger Einträge auf Plattformen

Obwohl Einträge auf Social Media-Plattformen die Vorschriften des Straf- oder Zivilrechts zu respektieren haben, ist es oft schwierig, die verantwortlichen Verfasser eines rechtswidrigen Beitrages zur Rechenschaft zu ziehen. Dies weil sich die Identifizierung des Verfassers vielfach als schwierig erweist. Den Strafverfolgungsbehörden bleibt oft nur der Weg mittels Zugriff auf sog. IP-Adressen die Identität festzustellen. Von zentraler Bedeutung bleibt zudem die enge und direkte Zusammenarbeit der Polizei- und Strafverfolgungsbehörden mit Social Media-Anbietern.

Der Bundesrat ist sich dieser Problematik seit längerem bewusst. In seiner Stellungnahme zur Motion Schwaab 14.3905, „Identifizierung der Verfasser von Hassnachrichten im Internet gewährleisten“ [239] anerkannte er die wichtige Rolle der IP-Adressen für die Identifikation der Verfasser rechtswidriger Inhalte. Das eigentliche Problem sei die Internationalität des Internets: Die meisten strafbaren Inhalte, die im Internet in der Schweiz entdeckt oder gemeldet werden, befinden sich auf ausländischen Servern. Die Schweizer Behörden können somit nicht direkt dagegen vorgehen. Der Bundesrat erachtet aus diesem Grund die grenzüberschreitende Zusammenarbeit mit den Strafverfolgungsbehörden und den Nachrichtendiensten als wichtiges Instrumentarium. Sie erfolgt nach dem Gesetz über die internationale Rechtshilfe in Strafsachen (IRSG, SR 351.1), dem Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS; SR 120) und nach internationalen Übereinkommen zur Beseitigung jeglicher Form von Rassendiskriminierung (SR 0.104) sowie dem Übereinkommen des Europarates über Cyberkriminalität (SR 0.311.43). Die internationalen Bezüge lassen die Einführung einer auf die Schweiz beschränkten Identifikationspflicht nach Ansicht des Bundesrats wenig wirkungsvoll erscheinen, weil sie mit Durchsetzungsproblemen behaftet sein dürfte. Der Nationalrat teilte diese Sichtweise und wies die Motion im Dezember 2014 ab.[240]

Zwei parlamentarische Vorstösse vom 15. Dezember 2016 befassen sich mit der schwierigen Ermittlung von Userinnen und Usern, welche auf internationalen Social Media-Plattformen wie Facebook rechtswidrige Inhalte veröffentlicht haben.[241] Auslöser der Motionen war ein Urteil des Bundesgerichts vom 16. November 2016. Im Zusammenhang mit einem diffamierenden Eintrag auf Facebook entschied das Bundesgericht, dass nur zur Herausgabe von Daten verpflichtet werden kann, wer Inhaber oder Besitzer der Daten ist oder zumindest die Kontrolle über die Daten hat. Im vorliegenden Fall hielt das Bundesgericht fest, die für ein Ehrverletzungsverfahren verlangten Daten (Identität, Zugangsdaten

---

[236] EGMR-Urteil „Delfi AS c. Estland“ (Beschwerde N° 64569/09) vom 16.6.2015 (Grosse Kammer).

[237] EGMR-Urteil „Magyar Tartalomszolgáltatók Egyesülete c. Ungarn“ (Beschwerde N° 22947/13) vom 2.2.2016.

[238] EGMR-Zulässigkeitsentscheid „Pihl c. Schweden“ (Beschwerde N° 74742/14) vom 7.2.2017.

[239] Motion Schwaab 14.3905, „Identifizierung der Verfasser von Hassnachrichten im Internet gewährleisten“; abrufbar unter: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20143905.

[240] Beschluss des Nationalrats vom 12.12.2014; https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=29840#votum1.

[241] Motion Levrat, 16.4082 Den Strafverfolgungsbehörden den Zugang zu Daten von sozialen Netzwerken erleichtern; https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164082); sowie die gleich lautende Motion Schwaab 16.4080: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164080

sowie die IP-Adresse des Kontoinhabers) seien von Facebook Irland und nicht von Facebook Schweiz herauszuverlangen.[242]

Im Anschluss an dieses Urteil verlangten die beiden Motionen, dass international tätige Social Media-Unternehmen künftig über eine Vertretung in der Schweiz verfügen müssten, sofern diese für Schweizer Konsumenten Dienstleistungen anbieten und deren Personendaten bearbeiten.[243] Diese Unternehmen sollten – ohne dass ein Rechtshilfeersuchen an einen andern Staat notwendig wäre – den schweizerischen Behörden Daten liefern können.

In seiner Stellungnahme vom 15. Februar 2017 führt der Bundesrat aus, dass er die momentane Lage ebenfalls für unbefriedigend hält und deshalb auf internationaler Ebene nach einer gangbaren und justiziablen Lösung sucht. Der in der Motion aufgezeigte Weg sei allerdings nicht erfolgversprechend. Die zwangsweise Durchsetzung der Herausgabepflicht lasse sich kaum umsetzen, wenn das Unternehmen einer Anordnung nicht nachkommt und die Daten im Ausland gespeichert sind. Die Daten müssen hierbei mittels Rechtshilfe herausverlangt werden. Auf internationaler Ebene sind Bestrebungen zu einer Lösungsfindung in Gange. Das Cybercrime-Komitee des Europarates arbeitet an Vorschlägen, damit die Strafverfolgungsbehörden innert nützlicher Frist an elektronische Rand- oder Verkehrsdaten gelangen können. Der Bundesrat sei daran, Massnahmen für eine schnellere Datenherausgabe ergebnisoffen zu prüfen und dabei die Grundsätze der staatlichen Souveränität und Territorialität sowie der Rechtshilfe in Strafsachen und des Datenschutzes sorgfältig zu berücksichtigen.[244]

Die Motion 16.4082 wurde im März 2017 vom Ständerat an die zuständige Kommission zur Vorprüfung überwiesen.[245]

### 5.6.4 Weitere Aspekte der Rechtsdurchsetzung im grenzüberschreitenden Bereich

#### 5.6.4.1 Europäisches Zentrum für Bekämpfung von Cyberkriminalität

Das Europäische Zentrum zur Bekämpfung von Cyberkriminalität (EC 3) wurde 2013 in Den Haag eröffnet[246]. Das Zentrum soll u.a. Erfahrungen und Information bündeln, strafrechtliche Ermittlungen unterstützen und EU-weite Lösungen fördern.[247] Wie aus dem ersten Jahresbericht des EC 3 hervorgeht, unterstützt es verschiedene grosse Polizeioperationen gegen Kindsmissbrauch. Auch ausserhalb der EU hat EC3 gemeinsam mit anderen Mitgliedstaaten und Kooperationspartnern erhebliche Anstrengungen gegen illegale Tätigkeiten von Pädophilen unternommen, die sich an der sexuellen Ausbeutung von Kindern im Internet mit Hilfe sogenannter versteckter Dienste beteiligen. EC3 wirkt an zahlreichen Operationen und Ermittlungen mit, welche die Herstellung und Verbreitung von Kindsmiss-

---

[242] Zum Sachverhalt und ausführlicher Begründung s. Bundesgerichtsurteil 1B_185/2016, 1B_186/2016, 1B_188/2016 vom 16.11.2016 (BGE-Publikation vorgesehen).

[243] Motion Levrat, 16.4082 Den Strafverfolgungsbehörden den Zugang zu Daten von sozialen Netzwerken erleichtern; https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164082); sowie die gleich lautende Motion Schwaab 16.4080: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164080.

[244] Stellungnahmen des Bundesrates zu den erwähnten Motionen Levrat 16.4082 und Schwaab, 16.4080 vom 15.02.2017. https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164082

[245] Beschluss des Ständerats zum Ordnungsantrag Levrat vom 9. März 2017: https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=39503.

[246] s. auch Pressemitteilung der Europäischen Kommission vom 28.3.2012 “EU-Zentrum zur Bekämpfung der Cyberkriminalität und zum Verbraucherschutz beim elektronischen Geschäftsverkehr”, abrufbar unter: http://europa.eu/rapid/press-release_IP-12-317_de.htm.

[247] Pressemitteilung der Europäischen Kommission „Europäisches Zentrum zur Bekämpfung der Cyberkriminalität: Eröffnung am 11. Januar“; abrufbar unter: http://europa.eu/rapid/press-release_IP-13-13_de.htm.

brauchsmaterial über bestimmte Internet-Plattformen betreffen. Hierbei leistet das Zentrum bei Ermittlungen operative und analytische Unterstützung.[248] Das EC3 arbeitet in diesem Bereich auch mit dem Bundesamt für Polizei (fedpol) zusammen.[249]

#### 5.6.4.2 „Trusted Flaggers"

Im internationalen Kontext kämpfen die Social Media-Plattformen seit einiger Zeit gegen Propagandavideos mit Gewaltdarstellungen des Islamischen Staates (IS) an. Die Nutzer können solche Inhalte der Plattform melden, worauf diese den Inhalt prüft und gegebenenfalls löscht. Einigen Nutzern räumen die sozialen Netzwerke einen besonderen Status ein, nämlich als „Trusted Flaggers". Melden diese ein Gewaltvideo, so wird ihr Antrag privilegiert behandelt und das Video sehr rasch gelöscht, sofern tatsächlich ein Verstoss gegen die Nutzungsbedingungen der jeweiligen Plattform vorliegt.

Seit Mitte 2016 gehört bei Youtube auch fedpol zu diesen „Trusted Flaggers" und meldet regelmässig Fälle von Gewalt- und Propagandavideos, insbesondere im Bereich des jihadistischen Terrorismus. Gemeldet werden jeweils Inhalte, welche nach Schweizer Recht strafbar sind. Fedpol ist bezüglich Gewaltdarstellungen und Verbreitung terroristischer Propaganda auch mit Facebook und Twitter in Kontakt.[250] Die direkte Zusammenarbeit zwischen Polizei- und Strafverfolgungsbehörden und Social Media-Anbietern ist von zentraler Bedeutung für die Kriminalitätsbekämpfung, u.a. auch mit dem Ziel, bei Ermittlungen schneller an die benötigten Informationen zu gelangen. Es ist wünschenswert, dass fedpol im Rahmen seiner bisherigen Ressourcen weiterhin als „Trusted Flagger" agiert und auch bei weiteren Netzwerken diesen Status erhält.

### 5.6.5 Löschung und Sperrverfügungen

#### 5.6.5.1 Löschung problematischer Inhalte auf der Plattform

Das Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (URG; SR 231.1) befindet sich derzeit in Revision. Am 2. Dezember 2016 hat der Bundesrat vom Ergebnis der Vernehmlassung über die Teilrevision Kenntnis genommen. Das zuständige EJPD wird dem Bundesrat bis im Sommer 2017 einen Vorschlag für das weitere Vorgehen unterbreiten.[251] Urheberrechtsverletzungen im Internet können enorme Schäden verursachen. Sie geschehen auch auf Social Media-Plattformen (vgl. vorne Ziff. 5.3.5). Das System, das anlässlich der Revision eingeführt werden soll, setzt in erster Linie auf die Unterstützung der Anbieterinnen abgeleiteter Kommunikationsdienste (Hosting Provider im weitesten Sinn) bei der Rechtsdurchsetzung. Gemäss dem Take down-Prinzip sind sie gehalten, verletzende Inhalte von ihren Servern zu entfernen. Schaffen sie mit einem beherbergten Angebot eine besondere Gefahr von Urheberrechtsverletzungen sollen sie das erneute Anbieten über ihre Server verhindern (Stay down).[252]

In *Deutschland* wird davon ausgegangen, dass es einer Verbesserung der Rechtsdurchsetzung in Social Media bedarf, um strafbare Inhalte wie Volksverhetzung, Beleidigungen, Verleumdung oder Störung des öffentlichen Friedens durch Vortäuschen von Straftaten unverzüglich zu entfernen.[253] Gemäss dem Bundesjustizminister werden von den durch Nutzer gemeldeten strafbaren Inhalten auf

---

[248] First Year Report European Cybercrime Center EC3, S. 15, https://www.europol.europa.eu/publications-documents/european-cybercrime-center-ec3-first-year-report.

[249] s. Jahresbericht fedpol 2015, S. 34, https://www.fedpol.admin.ch/dam/data/fedpol/publiservice/publikationen/berichte/jabe/jabe-2015-d.pdf.

[250] Bühler Stefan, So stoppt der Bund Jihad-Videos, NZZ am Sonntag vom 14.8.2016; abrufbar unter https://www.nzz.ch/nzzas/nzz-am-sonntag/kampf-gegen-terrorismus-so-stoppt-der-bund-jihad-videos-ld.110858.

[251] Medienmitteilung des Bundesrates vom 2.12.2016; abrufbar unter: https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2016/2016-12-022.html.

[252] Medienmitteilung des IGE vom 2.3.2017; abrufbar unter: https://www.ige.ch/fileadmin/user_upload/Urheberrecht/d/AGUR12_II_Medienmitteilung_20170302_DE.pdf

[253] Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz, Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz NetzDG), S. 2, abrufbar: https://netzpolitik.org/wp-upload/2017/03/1703014_NetzwerkDurchsetzungsG.pdf.

Twitter lediglich 1% und auf Facebook 39% (Youtube 90%) gelöscht.[254] Aufgrund dieser Tatsache hat der Minister den Entwurf für ein Netzdurchsetzungsgesetz (NetzDG) ausarbeiten lassen, welcher am 14. März 2017 anlässlich einer Pressekonferenz vorgestellt wurde.[255] Damit die sozialen Netzwerke Beschwerden, insbesondere jene von Benutzern in Zusammenhang mit Hasskriminalität, rascher bearbeiten, werden im Gesetzesentwurf gesetzliche Compliance-Regeln eingeführt. Die Regelung besteht u.a. darin, für soziale Netzwerke eine gesetzliche Pflicht zur Berichterstattung über den Umgang mit Hasskriminalität, sowie ein wirksames Beschwerdemanagement und die Benennung eines inländischen Zustellungsbevollmächtigten einzuführen. Nach dem ursprünglichen Entwurf sollten Verstösse gegen diese Organisationspflichten mit einer Busse gegen das Unternehmen und die Aufsichtspflichtigen geahndet werden können.[256] Die Bussen können bis zu fünf Millionen Euro betragen, bzw. bis zu 50 Millionen Euro für Unternehmen.[257]

Das Bundeskabinett hat am 5. April den Gesetzesentwurf des Bundesjustizministeriums zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken auf Kritik hin in leicht veränderter Form zum Referentenentwurf beschlossen. Soziale Netzwerke müssen gemäss diesem abgeänderten Entwurf nun doch keine proaktiven Massnahmen gegen die erneute Speicherung rechtswidrigen Inhaltes treffen. Im Übrigen wurden die rechtswidrigen Inhalte um einige Straftatbestände wie bspw. Pornografie erweitert.[258]

#### 5.6.5.2 Sperren des Zugangs zu problematischen Inhalten durch Access-Provider

Im Rahmen der FMG Revision ist zur Bekämpfung der qualifizierten Pornografie die Einführung einer Bestimmung geplant, welche die Fernmeldedienstanbieter verpflichtet, den Zugang zu qualifiziert pornografischen Inhalten gemäss den durch die KOBIK geführten Listen zu sperren (vgl. Ziff. 3.3).[259]

Zugangssperren sind auch im Entwurf für ein neues Bundesgesetz über Geldspiele (Geldspielgesetz; BGS) vorgesehen.[260] Art. 84 Abs. 1 und 4 VE-BGS legen das Instrumentarium für die Bekämpfung nicht bewilligter Online-Spielangebote in den Grundzügen fest. Geplant ist die Führung von schwarzen Listen nicht bewilligter Spiel-Internetseiten. Die Internetzugangsprovider sollen verpflichtet werden, die auf diesen Listen geführten Websites zu sperren, sofern die Anbieter der Angebote im Ausland ansässig sind und nicht von sich aus ihr Angebot in der Schweiz unterbinden.

---

[254] Bundesministerium der Justiz und für Verbraucherschutz „Um die Unternehmen bei der Löschung strafbarer Inhalte noch stärker in die Pflicht zu nehmen, brauchen wir gesetzliche Regelungen“, Heiko Maas zum Gesetzesentwurf zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, http://www.bmjv.de/SharedDocs/Zitate/DE/2017/03132017_GE_Rechtsdurchsetzung_Soziale_Netzwerke.html;jsessionid=D058AAAA90B4E33625281119 18DFCFD7.1_cid297.

[255] https://netzpolitik.org/2017/netzwerkdurchsetzungsgesetz-maas-stellt-regulierungsplan-fuer-soziale-netzwerken-vor/.

[256] Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz, Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz NetzDG), S. 2, abrufbar: https://netzpolitik.org/wp-upload/2017/03/1703014_NetzwerkDurchsetzungsG.pdf.

[257] Süddeutsche Zeitung, Maas will Hasskommentare mit hohen Bussgeldern bekämpfen, 14. März 2017, http://www.sueddeutsche.de/digital/gesetzentwurf-maas-will-hasskommentare-mit-hohen-bussgeldern-bekaempfen-1.3418827; http://www.bmjv.de/SharedDocs/Zitate/DE/2017/03132017_GE_Rechtsdurchsetzung_Soziale_Netzwerke.html;jsessionid=D058AAAA90B4E33625281119 18DFCFD7.1_cid297. Der Entwurf wurde in der deutschen Rechtslehre kontrovers beurteilt, vgl. etwa Wimmers Jörg/Heymann Britta, Zum Referentenentwurf eines Netzwerkdurchsetzungsgesetzes (NetzDG) – eine kritische Stellungnahme, in: Archiv für Presserecht (AfP) 2017, S. 93-102; Schulz Wolfgang, Comments on the Draft for an Act improving Law Enforcement on Social Networks (NetzDG); abrufbar unter https://www.hans-bredow-institut.de/de/aktuelles/stellungnahme-von-prof-dr-wolfgang-schulz-zum-netzwerkdurchsetzungsgesetz.

[258] http://www.cmshs-bloggt.de/tmc/netzwerkdurchsetzungsgesetz-netzdg/; http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_NetzDG.pdf?__blob=publicationFile&v=2. Zum Regierungsentwurf vgl. etwa Kubiciel Michael, Neuartige Sanktionen für soziale Netzwerke ? Der Regierungsentwurf zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, Juris vom 12.4.2017; abrufbar unter https://www.juris.de/jportal/portal/page/homerl.psml?nid=jpr-NLSFADG000217&cmsuri=%2Fjuris%2Fde%2Fnachrichten%2Fzeigenachricht.jsp.

[259] Abrufbar unter: https://www.bakom.admin.ch/bakom/de/home/das-bakom/organisation/rechtliche-grundlagen/bundesratsgeschaefte/fernmeldebericht-2014.html.

[260] https://www.bj.admin.ch/bj/de/home/wirtschaft/gesetzgebung/geldspielinitiative.html.

Angebote, die von der Schweiz aus betrieben werden, können durch ordentliche verwaltungs- oder strafrechtliche Verfahren aufgehoben werden. Die zuständigen Behörden können eine vorläufige Sperrung anordnen, weshalb das vorgesehene Instrumentarium für Angebote in der Schweiz nicht notwendig ist.[261]

Der Ständerat und im März 2017 auch der Nationalrat[262] haben der vom Bundesrat vorgeschlagenen Sperrung des Zugangs zu illegalen Online-Geldspielen zugestimmt.

# 6 Fazit (Zwischenergebnis)

In seinem Postulatsbericht vom 9. Oktober 2013 legte der Bundesrat die Antworten auf folgende Fragen vor:

- Wie ist die aktuelle Rechtslage in der Schweiz und international in Bezug auf die Social Media?
- Wo bestehen Lücken im Recht?
- Wie können sie geschlossen werden?
- Wie beurteilt der Bundesrat die Schaffung eines eigenen Social-Media-Gesetzes, das den Besonderheiten dieser neuen Kommunikationsplattformen Rechnung trägt?

Der Bundesrat kam damals zum Schluss, dass es angezeigt erscheine, in einigen Jahren eine erneute Standortbestimmung zur rechtlichen Basis für Social Media vorzunehmen. Mit dem vorliegenden Bericht wird dieser Auftrag erfüllt.

Verschiedene derzeit laufende Regulierungsvorhaben in der Schweiz sehen Bestimmungen zu Social Media vor. Der aktuelle Stand dieser Regulierungsvorhaben sowie die darin enthaltenen Regelungsvorschläge in Bezug auf Social Media stellen sich folgendermassen dar:

- Die vorgesehene Revision des DSG schafft die Voraussetzungen dafür, dass die Schweiz die modernisierte Datenschutzkonvention des Europarates (SEV 108) ratifizieren und die EU-Richtlinie über den Datenschutz (Datenschutz-Richtlinie 2016/680) im Bereich der Strafverfolgung übernehmen kann. Darüber hinaus ermöglicht sie eine Annäherung der schweizerischen Gesetzgebung an die Anforderungen der Datenschutz-Grundverordnung der Europäischen Union (EU-DSGVO 2016/679). Die DSG-Revision enthält verschiedene Aspekte, welche im Zusammenhang mit Social Media relevant sind, wie z.B. die Pflicht zum Datenschutz durch Technik (Privacy by Design, Privacy by Default), den Ausbau der Sorgfaltspflichten bei der Datenbearbeitung (Recht auf Vergessenwerden, bzw. Recht auf Löschung) und die Veröffentlichung von Empfehlungen der guten Praxis durch den EDÖB.
- Zur Verbesserung des Jugendmedienschutzes hat der Bundesrat das EDI damit beauftragt, bis Ende 2017 ein Gesetz auszuarbeiten, das Alterskennzeichnungen und Abgabebeschränkungen für Videos und Games schweizweit einheitlich regeln soll. Ferner wird das Projekt „Jugend und Medien“ weitergeführt, das unter anderem auch das Ziel verfolgt, Jugendliche im Umgang mit neuen Medien zu sensibilisieren.
- Die Revision des FMG sieht neben der oben unter Ziff. 4.4 erwähnten Abkehr von der generellen Meldepflicht für Fernmeldedienstanbieterinnen auch neue Vorgaben für eine Verbesserung des Konsumenten-, Kinder- und Jugendschutzes vor: So sollen Fernmeldedienstanbieterinnen verpflichtet werden können, beim Verkauf von Mobilfunk- und Internetabonnements für die Eltern eine Beratung über die Möglichkeiten zum Schutz von Kindern und Jugendlichen anzubieten. Eine Sperrpflicht ist für Internetseiten mit qualifiziert pornografischem Inhalt vorgesehen.

---

[261] Botschaft zum Geldspielgesetz vom 21. Oktober 2015, 7. Kapitel: Einschränkung des Zugangs zu in der Schweiz nicht bewilligten Online-Spielangeboten, BBl 2015 8472, abrufbar unter; https://www.admin.ch/opc/de/federal-gazette/2015/8387.pdf

[262] Beratung des Nationalrates vom 1.3.2017; https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=39312.

- Die Totalrevision des BÜPF, welche voraussichtlich anfangs 2018 in Kraft treten wird, begünstigt die Durchsetzung des Strafrechts auch im Social Media-Bereich. Der Bundesrat kann gestützt auf die revidierte Gesetzgebung Anbieterinnen abgeleiteter Kommunikationsdienste, welche Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten, dazu verpflichten, Angaben aufzubewahren und zu liefern, wie dies bereits für herkömmliche Fernmeldedienstanbieterinnen gilt. Das revidierte und vom Volk jüngst angenommene NDG knüpft an diese Auskunfts- und Überwachungspflichten nach BÜPF an und wird damit dem Nachrichtendienst künftig ermöglichen, Personen auch auf grösseren Social Media-Plattformen zwecks Wahrung wichtiger Landesinteressen zu identifizieren und zu überwachen.

Nach Abschluss der national und international laufenden Regulierungsvorhaben sind die Nutzenden von Social Media-Plattformen künftig besser geschützt und die berechtigten Interessen der Allgemeinheit besser verwirklicht. Die Vorhaben sind deshalb durch die federführenden Verwaltungseinheiten des Bundes weiter zu verfolgen und mit Nachdruck voranzutreiben.

# 7 Handlungsempfehlungen / Weiteres Vorgehen

Vor dem Hintergrund der aktualisierten Standortbestimmung kommt der Bundesrat zum Schluss, dass derzeit keine zusätzlichen Regulierungsaktivitäten in Bezug auf Social Media ausgelöst werden müssen.

Die systematische Beeinflussung der politischen Meinungs- und Willensbildung durch Falschmeldungen („Fake News“) und insbesondere deren automatische Erstellung und Verbreitung durch sog. „Social Bots“ sind zurzeit Gegenstand der politischen und medienrechtlichen Diskussion in der Schweiz. Von Seiten der Plattformbetreiber und privater Organisationen sind bereits selbstregulatorische Massnahmen gegen absichtlich produzierte Falschinformationen im Gange. Die Gefahr der Beeinflussung der demokratischen Meinungsbildung, welche von „Fake News“ und insbesondere von „Social Bots“ ausgeht, ist erkannt. Aufgrund der insgesamt noch unübersichtlichen Lage kann jedoch zum jetzigen Zeitpunkt nicht beantwortet werden, ob eine staatliche Regulierung angezeigt ist. Der Bundesrat setzt momentan auf die Selbstregulierung der Branche und beobachtet die internationalen und nationalen Entwicklungen auch künftig aufmerksam.

Im Zusammenhang mit der Meldung von problematischen Inhalten auf Social Media-Plattformen geniessen sog. „Trusted Flaggers“ einen besonderen Status. Melden diese der Plattform problematische Inhalte, werden die Meldungen privilegiert behandelt und die Inhalte unmittelbar gelöscht, sofern tatsächlich ein Verstoss gegen die geltenden Nutzungsbedingungen der jeweiligen Plattform vorliegt. Diese Form der Selbstregulierung greift in der Schweiz zurzeit hauptsächlich bei den Meldungen von Propaganda- und Gewaltvideos. In der Schweiz übernimmt diese Aufgabe das Bundesamt für Polizei fedpol. Es wäre sinnvoll, wenn fedpol diese Aktivitäten auch auf weitere Social Media-Plattformen ausdehnen könnte.

Im Rahmen der Revision des Datenschutzgesetzes hat der Bundesrat geprüft, ob für die betroffenen Personen ein Recht auf Mitnahme der Daten (Datenportabilität) eingeführt werden soll. Er kam dabei zum Schluss, dass die Umsetzung schwierig sei. Dies insbesondere, weil die Einführung eines solchen Rechts eine gegenseitige Abstimmung unter den Verantwortlichen hinsichtlich der Eignung über die verwendeten Datenträger und Informatikstandards verlangt. In der Vernehmlassungsvorlage zur Revision des Datenschutzgesetzes verweist der Bundesrat sodann auf die weitere Prüfung im Rahmen der Strategie „Digitale Schweiz“. Erste Eckwerte für eine Datenpolitik der Schweiz werden voraussichtlich bis Ende 2017 vorliegen. In diesem Zusammenhang wird auch zu prüfen sein, welcher Regelungsbedarf für eine Weiterverwendung von Personen-, Sachdaten und anonymisierten Daten besteht.

Ein relativ neues Phänomen sind die „Social Media-Stars“, welche Webvideos zu verschiedenen Themen verbreiten. Die Popularität und Professionalisierung dieser „Social Media-Stars“ nimmt zu. Soziale Netzwerke und Plattformen setzen sie häufig als Verbreitungskanäle für kommerzielle Werbebotschaften ein. Oft fehlt dabei eine klare Trennung zwischen Werbung und anderen Inhalten. Sie haben

sich lediglich an die allgemeinen Vorgaben des Lauterkeitsrechts zu halten. Anders als etwa in Deutschland gibt es in der Schweiz zurzeit praktisch keine spezifischen Deklarationsvorschriften für Werbung, die auch auf Social Media Anwendung finden. Das Transparenzgebot des RTVG ist heute gesetzlich einzig im Bereich des herkömmlichen Rundfunks anwendbar. Der Schutz der unverfälschten Meinungsbildung bei den Rezipienten spricht dafür, dass das Transparenzgebot in Zukunft auch auf sozialen Netzwerken zur Anwendung gelangt. Die Frage, welche Mindeststandards hinsichtlich des Jugendschutzes und der Kennzeichnung von Produkteplatzierungen künftig gelten sollen, wird gegenwärtig im Rahmen der laufenden Vorbereitungen für ein neu zu schaffendes Gesetz über elektronische Medien (GeM) diskutiert. Im Übrigen wird eine Harmonisierung mit den einschlägigen europäischen Regelwerken geprüft. Den laufenden Abklärungen sollte hier nicht vorgegriffen werden.

Im Zusammenhang mit Social Media bestehen weiterhin Schwierigkeiten bei der grenzüberschreitenden Rechtsdurchsetzung. Mit dem Urteil des Bundesgerichts Ende letzten Jahres hat die Brisanz dieser Thematik zugenommen. Im Anschluss an das Urteil wurden im Parlament zwei Vorstösse eingereicht (Mo. Levrat 16.4082 bzw. Mo. Schwaab 16.4080). Die auf internationaler Ebene bereits angelaufenen Bestrebungen, hierbei eine praxisgerechte Lösung zu finden, werden von der Schweiz unterstützt. Sie sind mit Nachdruck voranzutreiben.

# 8 Verzeichnisse

## 8.1 Verzeichnis der Abkürzungen

| Abkürzung | Definition |
|---|---|
| Abs. | Absatz |
| AfP | Archiv für Presserecht |
| AGUR | Arbeitsgruppe zur Optimierung der kollektiven Verwertung von Urheberrechten |
| App | Engl. *Application*, Anwendung |
| Art. | Artikel |
| Art. 3 lit. b | Artikel 3 Buchstabe b |
| BAKOM | Bundesamt für Kommunikation |
| BehiG | Bundesgesetz über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen (SR 151.3) |
| BFS | Bundesamt für Statistik |
| BJ | Bundesamt für Justiz |
| bspw. | beispielsweise |
| BGS | Bundesgesetz über Geldspiele |
| BSV | Bundesamt für Sozialversicherungen |
| BÜPF | Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (SR 780.1) |
| BV | Bundesverfassung (SR 101) |
| BWIS | Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (SR 120) |
| bzw. | beziehungsweise |
| ca. | zirka |
| CCH | Code of Conduct Hosting (der simsa) |
| CM/Rec | Empfehlung des Ministerkomitees des Europarats |
| d.h | das heisst |

| Abkürzung | Definition |
|---|---|
| DLM | Deutsche Landesmedienanstalten |
| DSG | Bundesgesetz über den Datenschutz (SR 235.1) |
| EDI | Eidgenössische Department des Innern |
| EDÖB | Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter |
| EJPD | Eidgenössische Justiz- und Polizeidepartement |
| EKR | Eidgenössische Kommission gegen Rassismus |
| EMRK | Konvention zum Schutze der Menschenrechte und Grundfreiheiten (SR 0.101) |
| E-SEV 108 | Entwurf des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarates, Sammlung Europäischer Verträge – Nr. 108 |
| etc. | et cetera |
| EU | Europäische Union |
| EU-DSGVO | EU-Datenschutz-Grundverordnung |
| FMG | Fernmeldegesetz (SR 784.10) |
| FRB | Fachstelle für Rassismusbekämpfung |
| GeM | Bundesgesetz über elektronische Medien |
| GS EFD | Generalsekretariat des Eidgenössischen Finanzdepartementes |
| IGE | Eidgenössisches Institut für Geistiges Eigentum |
| inkl. | inklusive |
| IS | Islamischer Staat |
| Kap. | Kapitel |
| KJFG | Kinder- und Jugendförderungsgesetz |
| KOBIK | Schweizerischen Koordinationsstelle zur Bekämpfung der Internetkriminalität |
| Lit. | Litera |
| Mio. | Millionen |

| Abkürzung | Definition |
|---|---|
| Mo. | Motion |
| Mrd. | Milliarden |
| NDG | Bundesgesetz über den Nachrichtendienst (SR 121) |
| Nr. | Nummer |
| OAS | Organisation Amerikanischer Staaten |
| OTT IP | Over The Top Internetprotokoll |
| PACE | Parlamentarische Versammlung des Europarates |
| RL | Richtlinie |
| RTVG | Bundesgesetz über Radio und Fernsehen (SR 784.40) |
| Rz. | Randziffer |
| S. | Seite |
| s. unten | siehe unten |
| SAJV | Schweizerische Arbeitsgemeinschaft der Jugendverbände |
| Seco | Staatssekretariat für Wirtschaft |
| SEV 108 | Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarates, Sammlung Europäischer Verträge – Nr. 108 |
| Simsa | Swiss Internet Industry Association |
| SMS | Short Message Service |
| sog. | Sogenannte |
| SR | Systematische Sammlung des Bundesrechts der Schweiz |
| SRG | Schweizerische Radio- und Fernsehgesellschaft |
| StGB | Schweizerisches Strafgesetzbuch (SR 311.0) |
| u.a. | unter anderem |

| Abkürzung | Definition |
|---|---|
| UNO-BRK | Übereinkommen über die Rechte von Menschen mit Behinderungen der Vereinten Nationen (SR 0.109) |
| üpA | übriges publizistisches Angebot (der SRG) |
| URG | Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (SR 231.1) |
| usw. | und so weiter |
| UVEK | Eidgenössisches Departement für Umwelt, Verkehrs, Energie und Kommunikation |
| UWG | Bundesgesetz gegen den unlauteren Wettbewerb (SR 241) |
| VE-DSG | Vorentwurf für zu einer Totalrevision des Bundesgesetzes über den Datenschutz vom 21.12.2016 |
| vgl. | vergleiche |
| VOD | Video-on-Demand |
| WCAG | Engl. *Web Content Accessibility Guidelines,* Richtlinien für barrierefreie Webgestaltung |
| z.B. | zum Beispiel |
| ZGB | Schweizerisches Zivilgesetzbuch (SR 210) |

## 8.2 Liste Parlamentarische Vorstösse 2013 - 2016

**Jugendschutz**

15.3723 Ip. Schmid-Federer Barbara — 19.06.2015 Erledigt
Kinder- und Jugendmedienschutz.
Umsetzung der Empfehlungen von Experten

15.1024 A. Amherd Viola — 20.03.2015 Erledigt
Jugendschutzprogramme

14.3969 Ip. Masshardt Nadine — 26.09.2014 Erledigt
Mit Medienkompetenz gegen Hasskampagnen

14.3868 Ip. Gilli Yvonne — 25.09.2014 Erledigt
Problematische Smartphone-Nutzung von Jugendlichen

14.3367 Mo. Amherd Viola — 08.05.2014 Im Rat
Sexting bekämpfen — noch nicht behandelt

13.4266 Ip. Amherd Viola — 13.12.2013 Im Rat
Handlungsbedarf bei Sexting — noch nicht behandelt

13.3087 Mo. Tornare Manuel — 14.03.2013 Erledigt
Cyberkriminalität

**Datenschutz, Schutz der Persönlichkeitsrechte**

16.3313 Po. Guhl Bernhard — 27.04.2016 Erledigt
Massnahmen gegen Gaffer prüfen, welche Einsätze behindern
oder Persönlichkeitsrechte verletzen

15.3657 Ip. Munz Martina — 18.06.2015 Erledigt
Recht auf Vergessen für Internet-Nutzerinnen und -Nutzer

15.3407 Po. Feri Yvonne — 05.05.2015 im Rat
Schutz der Persönlichkeitsrechte — noch nicht behandelt

14.4204 Po. Feri Yvonne — 11.12.2014 Angenommen
Bekämpfung von Stalking in der Schweiz verbessern

14.3963 Po. Müller-Altermatt Stefan — 26.06.2014 Im Rat
Wie verstecken sich Pädophile hinter dem Datenschutz? — noch nicht behandelt

14.3905 Mo. Schwaab Jean Christophe — 25.09.2014 Erledigt
Identifizierung der Verfasser von Hassnachrichten
im Internet gewährleisten

14.3782 Po. Schwaab Jean Christophe — 24.09.2014 Angenommen
Richtlinien für den "digitalen Tod"

14.3655 Po. Derder Fathi — 20.06.2014 Angenommen
Die digitale Identität definieren und Lösungen
für ihren Schutz finden

14.3288 Mo. Comte Raphaël — 21.03.2014 Angenommen
Identitätsmissbrauch. Eine strafbare Handlung für sich

| | |
|---|---|
| 14.404 Pa. Iv. Schwaab Jean-Christophe<br>Für wirklich abschreckende Sanktionen<br>bei Datenschutzverletzungen | 19.03.2014 Erledigt |
| 13.5380 Fra. Reimann Maximilian<br>Ungenügendes Instrumentarium zur Bekämpfung<br>der Cyberkriminalität | 18.09.2013 Erledigt |
| 13.4086 Mo. Grüne Fraktion<br>Nationales Forschungsprogramm "Alltagstauglicher Datenschutz<br>in der Informationsgesellschaft" | 05.12.2013 Im Rat noch<br>nicht behandelt |
| 13.3989 Po. Recordon Luc<br>Verletzungen der Persönlichkeitsrechte im Zuge des<br>Fortschritts der Informations- und Kommunikationstechnik | 27.09.2013 Angenommen |
| 13.3841 Mo. Rechsteiner Paul<br>Expertenkommission zur Zukunft der<br>Datenbearbeitung und Datensicherheit | 26.09.2013 Angenommen |
| 13.3726 Po. Schwaab Jean Christophe<br>Identitätsmissbrauch.<br>Eine Lücke im Strafrecht, die es zu füllen gilt? | 25.09.2013 Erledigt |
| 13.3492 Ip. Fraktion BD<br>Datenschutzbestimmungen für E-Government | 18.09.2013 Erledigt |
| 13.3215 Mo. Riklin Kathy<br>Rechtliche Verantwortlichkeit von Internetprovidern regeln | 19.06.2013 Erledigt |
| 13.3052 Mo. Schwaab Jean Christophe<br>Recht zur Sammelklage bei Datenschutzverletzungen,<br>insbesondere im Internet | 21.03.2013 Erledigt |
| SOZIALE NETZWERKE | |
| 15.3460 Ip. Mörgeli Christoph<br>Youtube-Aktivitäten des Bundes | 07.03.2013 Erledigt |
| 14.3193 Po. Vogler Karl<br>Verbesserung der polizeilichen Ermittlungen in sozialen Netzwerken | 06.05.2015 Erledigt |
| 14.305 Standesinitiative Bern<br>Fertig mit den anonymen Aufrufen zu Demonstrationen<br>und Grossanlässen ohne Übernahme von Verantwortung | 20.03.2014 Erledigt |
| 16.4082 Mo. Levrat Christian<br>Den Strafverfolgungsbehörden den Zugang zu Daten<br>von sozialen Netzwerken erleichtern | 15.12.2016 Im Rat noch<br>nicht behandelt |
| 16.4080 Mo. Schwaab Jean Christoph<br>Den Strafverfolgungsbehörden den Zugang zu Daten<br>von sozialen Netzwerken erleichtern | 15.12.2016 im Rat noch<br>nicht behandelt |

## 8.3 Literaturverzeichnis


Bähler Regula, Tweet und Retweet: mitgegangen, mitgefangen – aber nicht immer: Medienethische und rechtliche Annäherung an das Medium Twitter im Umfeld von Ehrverletzungen, in: medialex Newsletter 2/2017.

Berger Andreas/Caspers Tomas/Croll Jutta/Hofmann Jörg/Kubicek Herbert/Peter Ulrike/Ruth-Janneck Diana/Trump Thilo, Web 2.0 / barrierefrei, Eine Studie zur Nutzung von Web 2.0 Anwendungen durch Menschen mit Behinderung, Hrsg. Aktion Mensch, Bonn, 2010.

Bernet PR AG für Kommunikation, ZHAW Studie Social Media Schweiz 2016.

Bessi Alessandro/Ferrara Emilio, Social bots distort the 2016 U.S. Presidential election online discussion, in: First Monday 2016, Vol. 21, Number 11.

Bond Robert M./Fariss Christopher J./Jones Jason J/Kramer Adam D. I./Marlow Cameron/Settle Jamie E./Fowler James H., A 61-million-person experiment in social influence an political mobilization, in nature international weekly journal of science, 13. September 2012.

Brun Marcel, Cyberbullying – aus strafrechtlicher Sicht, in: recht 2016, S. 20.

Cappello Maja, in: Europäische Audiovisuelle Informationsstelle (Hrsg.), Editorial zu IRIS Newsletter 2017-3.

Cook David M/Waugh Benjamin/Maldini Abdipanah/Omid Hashemi, et al.. "Twitter Deception and Influence: Issues of Identity, Slacktivism, and Puppetry" Journal of Information Warfare Vol. 13 Iss. 1 (2014).

Egli Patricia/Rechsteiner David, Social Bots und Meinungsbildung in der Demokratie, in: Aktuelle Juristische Praxis AJP 2017, S. 249ff.

Fucík Jan, Zentrum gegen Terrorismus und hybride Gefahren nimmt die Arbeit auf, in: Europäische Audiovisuelle Informationsstelle (Hrsg.), IRIS 2017-3, S. 9.

Hwang Tim/Rosen Lea, Harder, Better, Faster, Stronger, CompProp Working Paper No. 1.

Keller Claudia, Werberecht, in: Staffelbach Oliver / Keller Claudia (Hrsg.), Social Media und Recht für Unternehmen, Zürich 2015.

Kind Sonja/Bovenschulte Marc/Ehrenberg Sillies Simone/Jetzke Tobias/Weide Sebastian, Social Bots - Thesenpapier zum öffentlichen Fachgespräch „Social Bots – Diskussion und Validierung von Zwischenergebnissen“ am 26. Januar 2017 im Deutschen Bundestag.

Kreutz Marcus/Lachwitz Klaus/Trenk-Hinterberger Peter, Die UN-Behindertenrechtskonvention in der Praxis, Köln 2013.

Latzer Michael/Just Natascha/Metreveli Sulkhan/Saurwein Florian, Internet-Anwendungen und deren Nutzung in der Schweiz. Themenbericht aus dem World Internet Project-Switzerland 2013, Universität Zürich, Zürich.

Meili Andreas/Galfano Michèle, Medienrechtliche und medienethische Schranken für Online-Leserkommentare - Eine Übersicht mit Fallbeispielen, in: medialex Jahrbuch für Medienrecht 2016, S. 38ff.

Prazeller Markus/Hug David, Twitter und Persönlichkeitsschutz - Bemerkungen zu den Urteilen des Bundesgerichts betreffend die Berichterstattung zum «Kristallnacht-Tweet» (5A_975/2015 und 5A_195/2016 vom 4. Juli 2016), in: Jusletter 24. Oktober 2016.

Rieder Pierre, Beschwerdemöglichkeit gegen Online-Inhalte der SRG – Die Neugestaltung der Aufsicht über das übrige publizistische Angebot der SRG, in: medialex Jahrbuch für Medienrecht 2016, S. 32ff.

Rosenthal David, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20. Februar 2017.

Schweizer Accessibility-Studie 2016, Bestandesaufnahme der Zugänglichkeit bedeutender Schweizer Internetangebote, Eine Studie der Schweizerischen Stiftung zur behindertengerechten Technologienutzung <<Zugang für alle>>.

Sociability: Social Media for People with a Disability, Hrsg: Media Access Australia, Ultimo NSW, 2012.

Trenk-Hintenberger in Kreutz et al., N 5 und 7 zu Art. 9 UNO-BRK (Kreutz Marcus/Lachwitz Klaus/Trenk-Hinterberger Peter, Die UN-Behindertenrechtskonvention in der Praxis, Köln, 2013

Wimmers Jörg/Heymann Britta, Zum Referentenentwurf eines Netzwerkdurchsetzungsgesetzes (NetzDG) – eine kritische Stellungnahme, in: Archiv für Presserecht (AfP) 2017, S. 93ff.

## 8.4 Gesetzesverzeichnis

Bundesgesetz vom 13. Dezember über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen (BehiG), SR 151.3.

Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1.

Fernmeldegesetz vom 30. April 1997 (FMG), SR 784.10.

Bundesgesetz vom 30. September 2011 über die Förderung der ausserschulischen Arbeit mit Kindern und Jugendlichen (KJFG), SR 446.1.

Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldewesens (BÜPF), SR 780.1.

Bundesgesetz vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (nBÜPF), SR …, BBl 2016 1991.

Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV), SR 101.

Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (BWIS), SR 120.

Bundesgesetz vom 25. September 2015 über den Nachrichtendienst (Nachrichtendienstgesetz, NDG), SR …; BBl 2015 7211.

Bundesgesetz vom 24. März 2006 über Radio und Fernsehen (RTVG), SR 784.40.

Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB), SR 311.0.

Bundesgesetz vom 9. Oktober 1992 über das Urheberrecht und verwandte Schutzrechte (URG), SR 232.1.

Bundesgesetz vom 19. Dezember 1986 gegen den unlauteren Wettbewerb (UWG), SR 241.

Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (ZGB), SR 210.

Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), SR 0.101.

Übereinkommen des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, SR 0.235.1.