Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rechtliche Basis für Social Media

Bericht des Bundesrates in Erfüllung des Postulats Amherd 11.3912 vom 29.September 2011

Zusammenfassung

Social Media oder soziale Netzwerke sind mehr oder weniger offene, interaktive und partizipative Plattformen, die es Nutzenden ermöglichen zu kommunizieren, Beziehungen aufzubauen und diese zu pflegen. Mit geringem Aufwand können Nutzende allein oder zusammen mit Dritten Inhalte generieren und diese anderen zugänglich machen sowie Inhalte von und über Dritte austauschen. Dabei kommt es zu einer Auflösung der Grenzen zwischen Autor/in, Produzent/in, Verbreiter/in und Nutzer/in sowie zwischen privater und öffentlicher Kommunikation. Social Media finanzieren sich überwiegend dadurch, dass von den Nutzenden eingegebene Daten an Firmen zu Werbezwecken weiterverkauft werden.

Auf die Frage von NR Amherd nach der aktuellen Rechtslage im Bezug auf Social Media stellt der Bericht internationale Standards und Empfehlungen dar. Vor diesem Hintergrund analysiert er die bestehenden schweizerischen Vorschriften. Er kommt zum Schluss, dass ein etwa dem Bereich Radio und Fernsehen vergleichbarer Bedarf für die Schaffung eines eigenen Spezialgesetzes bei Social Media gegenwärtig nicht besteht. Was die Vielzahl mit den neuen Kommunikationsgefässen verbundener Chancen und Gefahren betrifft, ergibt sich ein facettenreiches Gesamtbild. Aufgrund bisheriger Erfahrungen springen im schweizerischen Recht keine grösseren Regelungslücken ins Auge. Die oft allgemein gehaltenen Regelungen in bestehenden Gesetzen (z.B. DSG, StGB, ZGB, UWG) erlauben bei umsichtiger Anwendung eine angemessene Antwort auf die meisten Probleme, welche soziale Plattformen für einzelne Betroffene und die Allgemeinheit schaffen oder schaffen könnten.

Ob sich die bestehenden Vorschriften in der Praxis bewähren werden, ist allerdings ungewiss. Dies gilt in erster Linie für die Durchsetzung der bestehenden Rechtsansprüche im Konfliktfall, die angesichts der internationalen Ausrichtung der Plattformen, der oft anonymen Kommunikation und der mitunter schwierig zuzuordnenden Verantwortlichkeit verschiedener Beteiligter (Nutzer, Plattformbetreiber, Provider usw.) prekär sein dürfte. Die grenzüberschreitende Ausgangslage bringt es mit sich, dass der schweizerische Gesetzgeber vielerorts nur beschränkte Einflussmöglichkeiten hat. In einzelnen Bereichen scheint es allerdings nicht ausgeschlossen, dass gewisse Gesetzesanpassungen eine Verbesserung bringen könnten. Dies gilt etwa für einzelne Aspekte des Datenschutzes, des Jugendmedienschutzes und der Zuordnung der Verantwortlichkeit von Dienstleistern, die Zugang zu einem Netzwerk ermöglichen (Plattformbetreiber und Provider).

Verschiedene dieser Gebiete sind derzeit Gegenstand vertiefter Abklärungen, welche u.a. die Kommunikation auf sozialen Plattformen betreffen. Im Rahmen der Arbeiten zur Revision des Datenschutzgesetzes wird allfälliger gesetzgeberischer Handlungsbedarf auch im Bezug auf Social Media abgeklärt. Die Überprüfung der Wirksamkeit bestehender Vorkehren zum Schutz Jugendlicher erfolgt im Rahmen des nationalen Programms „Jugend und Medien“.

Daneben drängt sich auf, die Notwendigkeit spezifischer Vorschriften für die zivilrechtliche Verantwortung von Plattformbetreibern und Providern vertieft zu untersuchen. Sollte sich aus dieser Analyse Gesetzesänderungsbedarf ergeben, wird eine entsprechende Vernehmlassungsvorlage vorgelegt.

Die fernmelderechtliche Erfassung von Social-Media-Plattformen ist in der Vernehmlassungsvorlage zur Revision des Fernmeldegesetzes zu klären. Gemäss der aktuellen Planung wird die FMG-Revision vom Bundesrat in der laufenden Legislaturperiode in Auftrag gegeben.

Die verschiedenen Aktivitäten und Abklärungen betreffen wie erwähnt nicht ausschliesslich Social Media, sondern sind im Zusammenhang der gesamten Rechtsordnung zu sehen. Allerdings müssen sich die verschiedenen Aspekte auch hinsichtlich von Social Media zu einem inhaltlich kohärenten Gesamtbild zusammenfügen. Der Informationsfluss zwischen den beteiligten Amtsstellen muss daher gewährleistet sein. Ausserdem erscheint es angezeigt, eine erneute Standortbestimmung zur rechtlichen Basis für Social Media vorzunehmen, sobald die genannten Arbeiten abgeschlossen sind bzw. ihre Stossrichtung deutlicher erkennbar ist.

Inhalt

1 Einleitung: Postulat Amherd 11.3912

In ihrem Postulat[1] 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 Gesetze und Grundrechte auszuhebeln drohe. Dies betreffe insbesondere Regeln zum Datenschutz, gegen Rassismus oder allgemein den Schutz der Privatsphäre. Möglicherweise müsse dieser 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, der insbesondere Antworten auf die folgenden Fragen geben soll:

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

Der Bundesrat schrieb in seiner Stellungnahme vom 23. November 2011, es stelle sich die Frage, ob das bestehende Recht (insbesondere im DSG, ZGB, StGB und URG) die Probleme adäquat erfasse und die Verantwortlichkeiten der Beteiligten ausreichend kläre. Dies gelte etwa für den Schutz überforderter Nutzender vor unerwünschter Verwendung ihrer Daten und die oft mangelhafte Möglichkeit, ihre Daten von einer Social-Media-Plattform auf eine andere zu übertragen. Eine weitere, zentrale Problematik sei die Durchsetzung geltenden Rechts, denn die Betreiber von Social-Media-Plattformen sind häufig international tätig, und die nationale Gesetzgebung stosse daher an ihre Grenzen. Der Bundesrat erklärte sich zur Annahme des Postulats bereit.

Der vorliegende Bericht wurde unter Federführung des Bundesamtes für Kommunikation erstellt. Die Arbeiten erfolgten in Abstimmung mit dem Bundesamt für Justiz, der nationalen Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK, dem Bundesamt für Sozialversicherungen und dem Bundesamt für Gesundheit, ebenso wie mit der Expertengruppe zur Revision des Datenschutzgesetzes. Drei externe Expertengutachten (zu begrifflichen Fragen zu Social Media, zur Durchsetzung des Rechts im internationalen Kontext und durch in ihren Rechten verletzte Private) sind in den Inhalt des Berichts eingeflossen.

[1] http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113912.

2 Social Media (Soziale Netzwerke)

2.1 Begriff

„Social Media“ oder „soziale Netzwerke“[2] haben sich in den vergangenen Jahren dank Breitband-Internet weltweit stark verbreitet. Auch in der Schweiz werden soziale Netzwerke intensiv genutzt. 47% der Schweizer und Schweizerinnen loggen sich in Online-Communities oder privaten sozialen Online-Netzwerken ein, 22% nutzen berufliche Online-Netzwerke und 11% den Microblogging-Dienst Twitter[3]. Zwei Drittel der Schweizer Unternehmen, Behörden und Organisationen pflegen aktive Social-Media-Auftritte und nur 34% verfügen über keine Präsenz im Social Web[4]. Bei sozialen Netzwerken handelt sich um mehr oder weniger offene, interaktive und partizipative Plattformen, welche es Nutzenden ermöglichen, zu kommunizieren, Beziehungen aufzubauen und diese zu pflegen. Zudem können Nutzende sozialer Netzwerke mit geringem Aufwand Informationen und Inhalte von und über Dritte austauschen sowie selbst oder in Gemeinschaft mit anderen Inhalte generieren und diese anderen Nutzenden zugänglich machen. In der Schweiz produzieren und verbreiten mehr als eine Million Personen eigene Inhalte im Internet, wobei sich insbesondere das Hochladen von Fotos und Bewegtbildern grosser Beliebtheit erfreut[5].

Es gibt eine stetig zunehmende Anzahl verschiedener Formen von Social Media, welche – je nach der durch die Betreiber geschaffenen Architektur der jeweiligen Plattform und den Vernetzungsmöglichkeiten mit anderen Plattformen – unterschiedliche Möglichkeiten der Nutzung, Interaktion sowie Mitgestaltung der Plattform selbst eröffnen.

Social Media ermöglichen oftmals ungeplante Kooperationen, indem Nutzende die Inhalte anderer Nutzender als für sie relevant erkennen, aufgreifen, verbessern, verarbeiten und in neue Kontexte stellen. So können ohne vorhergehende Planung grosse Gemeinschaftswerke entstehen[6].

Für die meisten Nutzenden sozialer Netzwerke steht jedoch der Austausch privater Mitteilungen in einem kleinen Kreis von meist untereinander bekannten Personen im Vordergrund. Gleichzeitig werden dieselben sozialen Netzwerke aber oft auch für eine professionell betriebene, publizistische Kommunikation benutzt, mit dem Ziel, das Kaufverhalten von Konsumenten oder die öffentliche Meinungsbildung zu beeinflussen.

Als Hauptmerkmale sozialer Netzwerke werden zunehmend die Möglichkeiten zur Verschiebung von Grenzen gesehen, welche sich im Vergleich zu traditionellen Kommunikationskanälen und Medien insbesondere auf drei Bereiche beziehen:

2.1.1 Auflösung der Grenze zwischen Autor, Produzent, Verbreiter und Nutzer

Während bei traditionellen Medien meist eine klare Trennung zwischen Leistungserbringern (z.B. professionelle Redaktoren, Filmregisseure, Medienunternehmen) und Leistungsempfängern (Publikum) herrscht, können die Teilnehmer eines sozialen Netzwerks leicht zwischen der Produzenten- und Konsumentenrolle wechseln. Laien können einzeln oder gemeinsam Inhalte herstellen oder bestehende Inhalte Dritter verändern und über die Verbreitung an andere Nutzende entscheiden.

---

[2] Die beiden Begriffe werden für die Zwecke dieses Berichts synonym verwendet.

[3] Latzer M./Just N./Metreveli S./Saurwein F. (2012). Internet-Anwendungen und deren Nutzung in der Schweiz. Themenbericht aus dem World Internet Project – Switzerland 2011. Universität Zürich, Zürich, S. 16, 19.

[4] Bernet ZHAW Studie Social Media Schweiz 2012, S. 3ff.; zu finden unter: http://www.bernet.ch/socialmediastudie.

[5] Latzer M./Just N./Metreveli S./Saurwein F. (2012). Internet-Anwendungen und deren Nutzung in der Schweiz. Themenbericht aus dem World Internet Project – Switzerland 2011. Universität Zürich, Zürich, S. 17f.

[6] Aguiton C./Cardon D., S. 52.

2.1.2 Auflösung der Grenze zwischen privater und öffentlicher Kommunikation

Traditionell existieren für die private und die öffentliche Kommunikation getrennte Kanäle: Bei der privaten Kommunikation sind dem Sender der oder die Empfänger in der Regel bekannt (z.B. im persönlichen Gespräch, beim Brief- oder Telefonverkehr). Bei der öffentlichen Kommunikation sind dem Sender die Empfänger in der Regel nicht genau bekannt.

Viele Social Media Angebote erlauben Nutzenden den einfachen Wechsel zwischen privater und öffentlicher Kommunikation auf derselben Plattform. Dies wird dadurch verstärkt, dass traditionelle Massenmedien ebenfalls in sozialen Netzwerken präsent sind und Inhalten und Aktivitäten Nutzender zu einer massenmedialen Wirkung verhelfen können, wenn sie diese aufgreifen und verbreiten.

2.1.3 Auflösung der Grenze zwischen lokaler und entfernter Datenbearbeitung

Social Media erlauben Nutzenden, Daten und Inhalte nicht mehr an einem bestimmten physischen Ort ablegen zu müssen. Durch die Einspeisung von Daten und Inhalten in soziale Netzwerke werden diese für die Nutzenden überall dort verfügbar, wo sie Zugang zu dem entsprechenden Netzwerk haben. Die Speicherung von Inhalten auf Servern Dritter führt zu einer höheren Flexibilität und Effizienz bei der Nutzung, geht aber oft auch mit einem gewissen Kontrollverlust über die (personenbezogenen) Daten und Inhalte einher.

2.2 Kategorisierung sozialer Netzwerke

Aufgrund der Vielfalt der Plattformen und deren unterschiedlicher Funktionen und Komplexität sowie deren kontinuierlicher Entwicklung und Veränderung, ist eine klare Trennung in Kategorien kaum möglich. Zudem entziehen sich soziale Netzwerke einer einfachen Einordnung, weil sie weder eine reine Weiterentwicklung traditioneller Massenmedien noch ein Kommunikationsmittel für ausschliesslich individuelle Kommunikation darstellen[7]. Häufig werden Social Media in der Forschung nach folgenden Kriterien kategorisiert:

2.2.1 Funktionen von Social Media

Soziale Netzwerke werden häufig nach ihren Funktionen kategorisiert, wobei sie regelmässig mehrere Funktionen aufweisen. Es gibt in der Forschung verschiedene Kategorisierungen, welche zumindest zwischen inhalts- und beziehungsorientierten Funktionen unterscheiden.

2.2.1.1 Inhaltsorientierte Funktionen

- Informations- und Wissensmanagement:
  Erzeugen, Auffinden, Rezipieren, Verwalten und Austauschen von Meinungen, Wissen und Informationen z.B. Wikis, Social Bookmarking, Tagging, RSS, Blogosphären oder Special-Interest-Plattformen[8].

- Unterhaltung oder Erfahrung von virtuellen Welten:
  Austausch von Inhalten mit dem Zweck der Unterhaltung oder des Erlebens von virtuellen (Spiel-)Welten, z.B. YouTube, gewisse interaktive Online-Spiele etc.

2.2.1.2 Beziehungsorientierte Funktionen:

- Beziehungsmanagement: Pflege bestehender und Knüpfen neuer Beziehungen (z.B. auf Kontaktplattformen), Austausch und Verknüpfung von Menschen mit gleichen Interessen, z.B. Special-Interest Plattformen wie myspace für Musiker.

---

[7] Neuberger, Christoph, „Soziale Netzwerke im Internet. Kommunikationswissenschaftliche Einordnung und Forschungsüberblick“. In. Neuberger, Christoph; Gehrau, Volker (Hrsg): StudiVZ. Diffusion, Nutzung und Wirkung eines sozialen Netzwerks im Internet. Wiesbaden 2011, S. 34.

[8] Schmidt, Jan, „Was ist neu am Social Web? Soziologische und kommunikationswissenschaftliche Grundlagen“, in: Zerfass u.a. (Hrsg): Kommunikation, Partizipation und Wirkungen im Social Web, Bd. 1, Köln 2008, S. 71.

- Identitäts- und Reputationsmanagement: (Selektives) Präsentieren von Aspekten der eigenen Person, z.B. in persönlichen Blogs, Podcasts, etc.

2.2.2 Partizipationsmöglichkeiten bei Social Media

Eine weitere Möglichkeit zur Kategorisierung bietet sich anhand der technischen Möglichkeiten zur Partizipation der Nutzenden sozialer Netzwerke. Dabei wird einerseits der Grad der Mitgestaltung der ausgetauschten Inhalte als Kriterium betrachtet. Diese kann von der blossen Möglichkeit der Bewertung oder Kommentierung bis hin zur Erschaffung oder Veränderung von Inhalten reichen. Andererseits wird auch der Grad der Öffentlichkeit der Kommunikation als Kriterium herangezogen, welche von rein individueller bis hin zu öffentlich vernetzter Massenkommunikation rangieren kann.

2.2.3 Erlösmodelle sozialer Netzwerke

Soziale Netzwerke sind nicht dem Gesetz der Knappheit unterworfen, sondern funktionieren genau umgekehrt: Der Wert eines Produktes oder einer Dienstleistung steigt mit der Anzahl der Nutzenden. Man spricht dann von Netzwerkeffekten[9]. In Angeboten sozialer Netzwerke sind Netzwerkeffekte für verschiedene Akteure zu beobachten. Mit steigender Mitgliederzahl wächst für alle Nutzenden die Wahrscheinlichkeit, auf der Plattform Gleichgesinnte zu treffen; auch nimmt die Attraktivität für Programmierer zu, Applikationen für diese Plattform bereitzustellen; und für Werber erhöht sich die Wahrscheinlichkeit, eng umgrenzbare Zielgruppen über die Plattform ansprechen zu können. Aus diesen Gründen setzen soziale Netzwerke häufig zunächst auf eine Strategie, bei der sie schnell sehr viele Nutzende gewinnen können, ohne bereits nennenswerte Umsätze zu generieren. Diese Nutzenden versuchen sie an sich zu binden, um ihre Abwanderung zu anderen Netzwerken zu verhindern oder zu erschweren.

Aufgrund der Skaleneffekte dieser Netzwerke und Foren sind Anreize zur Übernahme von und Verschmelzungen mit anderen Medien gross, um möglichst profitabel operieren zu können. Dies kann – zumindest für eine begrenzte Zeit – zu dominanten Positionen einzelner weniger Plattformen führen.

Die Erlösmodelle von Social Media lassen sich in nicht-kommerzielle und kommerzielle Formen einteilen. Aus den Anfängen des Internets besteht eine Tradition der kostenlosen Nutzung von Inhalten. Es gibt auch heute noch viele Social Media, die nicht kommerziell agieren, sondern sich in erster Linie dem Community-Gedanken verpflichtet fühlen. Da Nutzende diese Netzwerke häufig als Gemeinschaftswerk verstehen, dem sie eine gewisse Loyalität zollen, sind sie oft auch bereit, über Spenden den Unterhalt der jeweiligen Plattform mit zu finanzieren. Eine weitere Form der nicht-kommerziellen Finanzierung von Social Media erfolgt über die öffentliche Hand, da es im öffentlichen Interesse liegen kann, für besondere Zielgruppen wie Kinder und Jugendliche spezielle Angebote an sozialen Netzwerken aufzubauen.

Zu den kommerziellen Erlösmodellen von Social Media gehören insbesondere die Finanzierung über Nutzungsgebühren und über Werbung. Bei der Finanzierung über Werbung handelt es sich überwiegend um Werbeanzeigen, die dynamisch den jeweiligen Inhalten auf dem Bildschirm angepasst werden, um die Aufmerksamkeit der Nutzenden anzuziehen. In weit geringerem Umfang wird statische Werbung verwendet. Da Nutzende sozialer Netzwerke ein Profil mit Angaben zu ihrer Person erstellen, stehen relativ viele Informationen über sie zur Verfügung. Die eingegebenen Daten werden an Firmen zu Werbezwecken weiterverkauft. Durch die Erstellung von Profilen ist eine exakte Zielgruppenansprache möglich. Abgerechnet wird entweder pro 1000 Einblendungen der Werbung oder nach dem *Cost per Click* Verfahren, wo der Werbende nur dann bezahlt, wenn die Angesprochenen auf seine Anzeige geklickt haben. Die Zielgruppen von spezialisierten Plattformen[10] werden dabei finan-

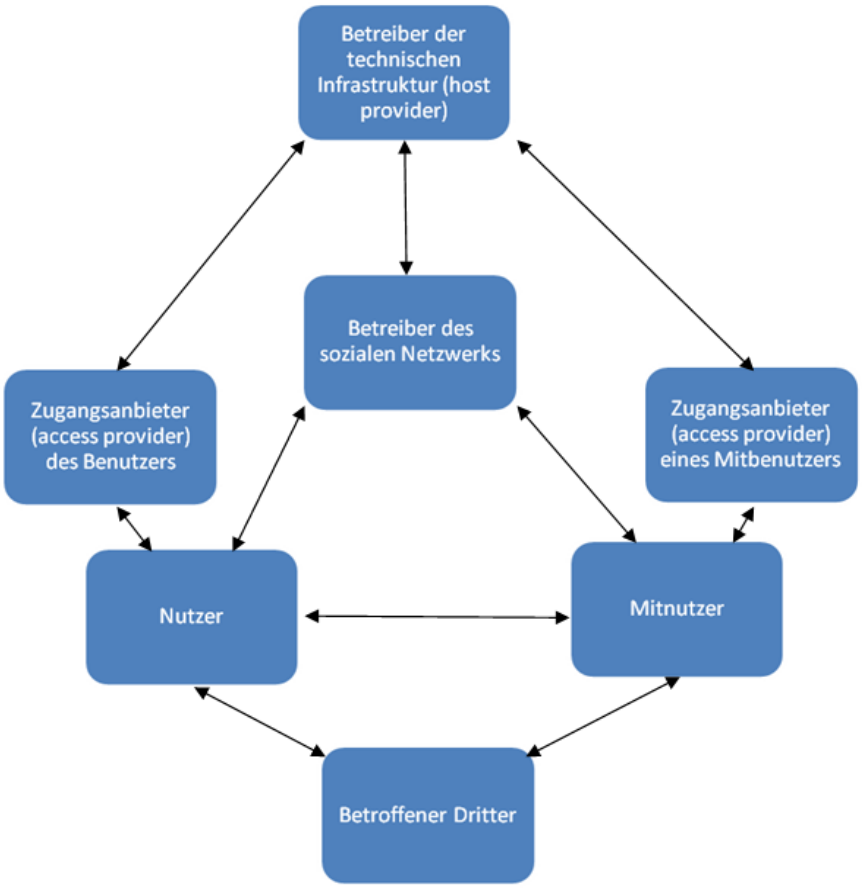
[9] Von Rimscha M. Björn, „Geschäftsmodelle für Social Media“ in: Grimm, Petra; Zöllner, Oliver (Hrsg): Schöne neue Kommunikationswelt oder Ende der Privatheit? Stuttgart 2012, S. 303 f.

[10] Bspw. auf die Arbeitswelt ausgerichtete Plattformen wie Xing oder LinkedIn

ziell höher bewertet. Nutzende „bezahlen“ also die kostenlose Nutzung der Dienstleistungen, die ihnen Social Media zur Verfügung stellen, mit ihren persönlichen Daten.

2.3 Rollen im Zusammenhang mit der Nutzung sozialer Netzwerke

Es gibt viele verschiedene an sozialen Netzwerken Beteiligte mit je verschiedenen Rollen. Dabei ist vorauszuschicken, dass die unterschiedlichen Rollen in der Praxis nicht immer klar voneinander abgegrenzt sind. Die Übergänge zwischen den Funktionen sind oft fliessend.[11] So können die Betreiber von Plattformen auch als Hosting-Provider agieren. Für eine erste Übersicht lässt sich aber von folgender, vereinfachender Einteilung ausgehen:



2.3.1 Betreiber von Social-Media-Plattformen (Plattformbetreiber)

Betreiber sozialer Netzwerke (Plattformbetreiber) stellen Nutzenden einen Rahmen zum Austausch selbst kreierter oder aufgegriffener Inhalte zur Verfügung. Viele der in der Schweiz stark genutzten Plattformen haben ihren Sitz im Ausland. Zu den bekannteren *ausländischen* Plattformbetreibern gehören etwa Facebook, YouTube und Twitter. Es gibt allerdings auch *inländische* Plattformbetreiber. Dazu gehören etwa die Anbieter von Blogs, welche mitunter für problematische Beiträge vor schweizerischen Gerichten belangt werden (z.B. die SRG[12] oder bestimmte Zeitungsverlage[13]).

---

[11] Vgl. dazu schon die Ausführungen zu den verschiedenen Beteiligten an der Internet-Kommunikation im Bericht der Expertenkommission „Netzwerkkriminalität“, EJPD 2003, S. 27ff.

[12] Vgl etwa den Konflikt um einen ehrenrührigen Kommentar im Blog zur Fernsehsendung Alpenfestung (BGE 136 IV 145).

[13] Vgl etwa den Konflikt um den persönlichkeitsverletzenden Beitrag eines Politikers auf einer von der Tribune de Genève betriebenen Blogplattform (BGer 5A_792/2011 vom 14.1.2013).

Durch die Architektur und das Design der Plattform entscheiden Betreiber über die Möglichkeiten der Interaktion sowie der Verbreitung von Inhalten. Sie bestimmen auch, inwieweit Nutzende private, teilöffentliche oder öffentliche Kommunikationsräume schaffen und Inhalte zwischen diesen Räumen austauschen können. Über „Content-Rankings“ und Verlinken auf Inhalte Dritter können die Betreiber die Aufmerksamkeit der Nutzenden auf bestimmte Inhalte lenken. Zudem bestimmen die Betreiber, welche Daten sie von Nutzenden erheben, welche Ansprüche sie an ausgetauschten Daten und Inhalten erwerben und wie sie diese ökonomisch verwerten.

Die meisten Plattformbetreiber machen Nutzenden Vorschriften für den Umgang mit anderen Nutzenden oder unbeteiligten Dritten sowie für die Herstellung, Verwendung oder Verbreitung von Inhalten. Über die Nutzungsbestimmungen können die Betreiber vorgeben, welche Inhalte oder Verhaltensweisen unerwünscht oder unerlaubt sind. Sie üben aber in der Regel eine im Vergleich zu traditionellen Medien geringere redaktionelle Kontrolle aus. Während bei den traditionellen Medien Inhalte in der Regel von einem Redaktions-Gremium im Vorfeld (ex-ante) selektioniert werden, gibt es bei sozialen Netzwerken meist eine ex-post-Kontrolle, wobei Inhalte, welche den Nutzungsbestimmungen widersprechen oder auf Kritik anderer Nutzender stossen, im Nachhinein entfernt werden können („Notice-and-Take-down“). Gewisse Plattformen überlassen es den Nutzenden, diese Regeln selber zu definieren und verweisen auf deren Selbstverantwortung und Organisationsfähigkeit.

2.3.2 Technische Dienstleister (wie Hosting- und Access-Provider)

Kommunikation über soziale Netzwerke ist auf eine technische Infrastruktur angewiesen. Es gibt Plattformbetreiber, welche die anfallenden Daten auf ihren eigenen Servern speichern. Viele Plattformbetreiber nehmen aber die Dienste Dritter in Anspruch, welche ihnen gegen Entgelt technische Infrastruktur (Speicherplatz, Rechenkapazität, Übermittlungskapazität) für die automatisierte Aufschaltung von Daten zur Verfügung stellen (oft: **Hosting-Provider**). Wie die meisten der im schweizerischen Markt stark vertretenen Plattformbetreiber hat auch die Mehrzahl der Hosting-Provider ihren Sitz im Ausland. Sie haben in der Regel keine eigene redaktionelle Verantwortung, sind aber technisch je nach Konstellation[14] in der Lage, auf ihren Computern gespeicherte und als unerwünscht erkannte Inhalte zu *löschen*.

Die Verbindung zwischen den Computern der Social Media-Nutzenden und den Servern mit dem Datenmaterial der Plattformen wird durch Zugangsdienstleister hergestellt (**Access-Provider**). Sie haben einen Vertrag mit den Nutzenden. Schweizerische Nutzende nehmen in der Regel die Dienste eines in der Schweiz ansässigen Access-Providers in Anspruch. Ein bekannter Access-Provider ist die Swisscom. Access-Provider sind typischerweise nicht in der Lage, unerwünschte Inhalte zu löschen (da sie nicht auf ihren Servern gespeichert sind). Denkbar ist allerdings, dass sie gezielt den Zugang zu bestimmten Inhalten blockieren (*Sperrung*).

2.3.3 Nutzende und Mitbenutzende

Es sind im Wesentlichen die Nutzenden, welche für die Erstellung von Inhalten sorgen („user generated content“) oder auf Inhalte anderer verweisen. Dazu benötigen sie sowohl die technische Unterstützung durch den Access-Provider als auch den Zugang zu der entsprechenden Social Media-Plattform. In der Regel können sie darüber entscheiden, an wen sich ihre Kommunikation richtet, d.h. ob sie ihre Inhalte mit der breiten Öffentlichkeit teilen wollen oder nur mit einem ausgewählten Kreis von Personen. Dabei bewegen sie sich im Rahmen der von Betreibern der Plattform vorgegebenen technischen Möglichkeiten und inhaltlichen Vorgaben.

Aus Sicht der Betreiber haben Nutzende eine (Mit-)Verantwortung für die Art und Weise wie sie miteinander umgehen und auch für die Inhalte, welche sie in sozialen Netzwerken einer breiteren Masse zugänglich machen. Oftmals ist die Haftung Nutzender für Aktivitäten, welche gesetzliche Grundlagen

[14] Mitunter kann der Hosting-Provider auf einem von ihm vermieteten Server nicht einzelne Inhalte löschen, sondern lediglich den Strom ausschalten oder Harddisks physisch ausbauen, was oft unverhältnismässig sein dürfte.

oder Rechte Dritter verletzen, nicht klar geregelt oder den Nutzenden nicht bekannt. Dies kann zu Risiken für die handelnden und die betroffenen Nutzenden führen.

2.3.4 Betroffene Dritte

Von den Aktivitäten in Social Media können auch Dritte betroffen sein, die selbst nicht in den entsprechenden Netzwerken aktiv sind. Dies ist etwa dann der Fall, wenn Inhalte, die Dritte betreffen, aus Social Media in die Massenmedien transportiert werden oder Netzwerkmitglieder ohne Einholung einer Erlaubnis Daten über Dritte in sozialen Netzwerken verwenden.

2.3.5 Traditionelle (Massen-) Medien und andere Mediendienste

Die traditionellen Medien verhelfen Social Media oft zu Aufmerksamkeit, neuen Mitgliedern und mehr Werbeeinnahmen. Social Media wiederum dienen den traditionellen Medien zunehmend als Lieferanten von Inhalten und Neuigkeiten.

Diese Verknüpfungen tragen dazu bei, dass die Grenzen zwischen privater und öffentlicher Kommunikation für die Nutzenden sozialer Netzwerke häufig nur schwer erkennbar sind. Viele herkömmliche Medien haben eine eigene Social Media Präsenz oder sind mit grossen sozialen Netzwerken wie z.B. Facebook verbunden oder verlinkt.

Weitere „Bindeglieder" sind Suchmaschinen, welche Nutzende auf Inhalte in traditionellen Medien, aber auch in sozialen Netzwerken verweisen. Auch ökonomische Kooperationen, insbesondere in Bezug auf Austausch und Auswertung von Nutzerdaten zu Werbezwecken etc., kommen vor.

2.4 Vorbemerkungen zur rechtlichen Einbindung der an Social Media Beteiligten

2.4.1 Aus der Verfassung fliessende Rechte und Pflichten

Für die Kommunikation über soziale Netzwerke sind in der Schweiz (und soweit ersichtlich auch im Ausland) bislang keine spezifischen gesetzlichen Regeln erlassen worden. Dennoch findet die Nutzung von Social Media nicht in einem rechtsfreien Raum statt.

Den an der Kommunikation Beteiligten (Nutzende, aber auch Plattformbetreiber und Provider) garantiert die Rechtsordnung auf höchster Normstufe Schutz vor staatlichen Eingriffen. So gewährleisten die schweizerische Verfassung und die Europäische Menschenrechtskonvention die ungehinderte Kommunikation (Art. 16, 17, 21, 22, 23, 34 BV sowie Art. 10 und 11 EMRK) und die Wirtschaftsfreiheit (Art. 27 BV). Die durch diese Grundrechte garantierten Freiheiten sind nicht absolut, sondern können vom Staat eingeschränkt werden. Dabei haben die Behörden strenge Voraussetzungen zu beachten. Gemäss Art. 36 BV bedürfen Einschränkungen von Freiheitsrechten einer gesetzlichen Grundlage, müssen einem öffentlichen Interesse oder dem Grundrechtsschutz Dritter dienen und verhältnismässig sein. Absolut verboten sind Eingriffe in den Kerngehalt der Grundrechte, wie etwa die systematische Zensur von Kommunikationsinhalten durch den Staat (Art. 17 Abs. 2 BV).

Im Hinblick auf die Kommunikation mittels sozialer Medien durch Private binden den Staat zwei Verpflichtungen: Zum einen darf er die Grundrechte selber nicht verletzen, zum anderen muss er die Rechte Privater vor unzulässigen Einschränkungen durch andere Private schützen.

Die Nutzung sozialer Netzwerke bringt neben Chancen auch verschiedene Gefahren für die Rechte von Einzelpersonen sowie für das Gemeinwohl mit sich. Zum Schutz von Grundrechten Dritter bzw. von öffentlichen Interessen (wie der Sicherheit oder der Volksgesundheit[15]) muss der Staat bestimmte rechtliche Vorkehren treffen. So hat er etwa Instrumente zum Schutz vor Verletzungen des Privat- und Familienlebens (Art. 13 BV, Art. 8 EMRK) des Einzelnen zur Verfügung stellen. Zu denken ist etwa an

[15] Zu denken ist etwa an Vorkehren gegen Alkohol- und Tabakwerbung oder gegen den Missbrauch von Betäubungsmitteln.

den Erlass von Gesetzesbestimmungen zum Schutz vor ehrenrührigen oder entblössenden Publikationen.

Besonderen Schutz verdienen Kinder und Jugendliche. So verlangt die UNO Kinderrechtskonvention den Schutz von Kindern vor allen Formen der Ausbeutung, welche ihr Wohl beeinträchtigen (Art. 36) und sichert ihnen Schutz vor rechtswidrigen Beeinträchtigungen ihrer Ehre und ihres Rufes zu (Art.16)[16]. Der Europäische Gerichtshof für Menschenrechte (EGMR) verlangt vom Staat, dass er wirksame Schritte unternimmt, wenn das Privatleben eines Jugendlichen durch unsittliche Veröffentlichungen im Internet (Publikation einer anstössigen Kontaktanzeige) tangiert wird[17].

Auch aus der Medienfreiheit fliessen Pflichten für den Staat. So hat er geeignete Vorkehrungen zu treffen gegen den Missbrauch der Meinungsmacht durch (ökonomisch) mächtige private Akteure.

2.4.2 Rechte und Pflichten im geltenden Gesetzesrecht

2.4.2.1 Beachtung der allgemeinen gesetzlichen Vorgaben

Die verfassungsrechtlichen Vorgaben werden auf Gesetzesstufe konkretisiert. Das Schweizer Gesetzesrecht enthält verschiedene Vorschriften, die die Rechte der Betroffenen näher definieren oder begrenzen. Diese Vorschriften gelten nicht nur für die Kommunikation in sozialen Netzwerken, sondern z.B. auch für Äusserungen über herkömmliche Kanäle wie Zeitungen, Radio, Briefe oder Telefongespräche. Zu denken ist etwa an Regeln im Straf-, Zivil- (Persönlichkeitsschutz) oder Datenschutzrecht. Die entsprechenden Vorschriften und ihre Tragweite für die sozialen Medien werden hinten in diesem Bericht unter Ziff. 4 näher erläutert.

2.4.2.2 Spezifische Regulierung von Plattformbetreibern im Fernmelderecht?

Für bestimmte Anbieter oder Transporteure von Informationen kennt das schweizerische Recht Spezialregeln. Dies gilt etwa für die Veranstalter herkömmlicher Radio- und Fernsehprogramme, die den Vorschriften im Radio- und Fernsehgesetz (RTVG) unterworfen sind.

Besondere Vorschriften für das Erbringen von Fernmeldediensten, das heisst für den fernmeldetechnischen Transport (Übertragung) von Informationen für Dritte (auch von Radio- und Fernsehprogrammen), finden sich im Fernmeldegesetz (FMG). Wer einen Fernmeldedienst erbringt, muss sich beispielsweise beim Bundesamt für Kommunikation melden (Art. 4 FMG), organisatorische Anforderungen erfüllen (Art. 6 FMG), das Fernmeldegeheimnis wahren (Art. 43 FMG), an Schlichtungsverfahren teilnehmen (Art. 12c FMG), transparente Preise haben (Art. 12a FMG), Spam bekämpfen (Art. 45a FMG) und zahlreiche weitere Pflichten einhalten. Das FMG datiert aus einer Zeit, in der die Erbringung von Fernmeldediensten noch vom Besitz oder zumindest vom autorisierten Zugang zu einem spezifischen, diesem Zweck dienenden Netz abhängig war. Durch die technologische Entwicklung ist diese enge Bindung zwischen Netz und Diensten aufgehoben worden. Heute gelten völlig andere technische Bedingungen (z.B. Internet, Smartphones). Dienste können auf verschiedenste Weise und ohne das aktive Zutun der Netzbetreiber erbracht werden, was ganz neue Geschäftsmodelle (z.B. Finanzierung über Werbung) möglich gemacht hat.

Nach geltendem Recht bietet Fernmeldedienste an, wer zwischen mindestens zwei anderen Parteien Informationen transportiert (Art. 3 Bst. b FMG). Betreiber von Social Media-Plattformen tun dies in aller Regel nicht, sondern sind eine dieser Parteien, zwischen denen Informationen transportiert werden. Es gibt aber Ausnahmefälle, wo die Plattformbetreiber für den Transport von Informationen zwischen Dritten zumindest mitverantwortlich sind, so dass nach heute geltender Definition allenfalls ein Fernmeldedienst vorliegen würde. Ein Beispiel hierfür sind Nachrichten, die ein Facebook-Mitglied z.B. mit

---

[16] Übereinkommen über die Rechte des Kindes, abgeschlossen in New York am 20. November 1989, in Kraft getreten für die Schweiz am 26. März 1997 (UNO Kinderrechtskonvention), SR 0.107.

[17] EGMR-Urteil „K.U. c. Finnland“ (Beschwerdenr. 2872/02) vom 2.12.2008: Unberechtigte Weigerung der finnischen Justiz, den Provider zur Herausgabe der fraglichen Daten zu verpflichten.

dem Facebook-Messenger einem anderen Facebook-Mitglied schickt. Abgesehen von der Schwierigkeit, nationales Fernmelderecht gegenüber global tätigen Plattformbetreibern ohne Sitz in der Schweiz mit den heutigen Instrumenten durchzusetzen, sind viele der geltenden fernmelderechtlichen Regeln auf ihre Aktivitäten nicht zugeschnitten.

3 Potenzial und Risiken sozialer Netzwerke

3.1 Allgemeines

Aufgrund der zunehmenden Präsenz sozialer Netzwerke im Alltagsleben vieler Menschen sind sie Gegenstand der Diskussion und Beobachtung durch Private, Staaten und multilaterale Organisationen. So haben sich etwa der Europarat und die Europäische Union in den vergangenen Jahren vermehrt mit ihrem Potenzial und ihren Risiken befasst.

3.2 Potenzial sozialer Netzwerke

Soziale Netzwerke erlauben Privaten Inhalte einfach, kostengünstig und schnell selber zu produzieren und zu vertreiben. Sie bieten Möglichkeiten zur Unterhaltung, zum kulturellen und politischen Austausch und zur Generierung von Einkommen. Überdies können sie zur politischen Aktivierung und Mobilisierung der Bevölkerung beitragen. So erhalten immer mehr Einzelpersonen neue Möglichkeiten zur Teilnahme am öffentlichen Diskurs[18].

Der *Europäische Gerichtshof für Menschenrechte* hat unterstrichen, das Internet sei heutzutage eines der wichtigsten Mittel zur Äusserung und zur Beschaffung von Informationen gerade über politische oder andere allgemein interessierende Fragen.[19]

Der *Europarat* hat eine Reihe von Empfehlungen an seine 47 Mitgliedstaaten erarbeitet, die dem Einzelnen helfen sollen, das Internet und die neuen Kommunikationsdienste (inklusive sozialer Netzwerke), zur besseren Wahrnehmung seiner Grundrechte zu nutzen[20]. Zu diesem Zweck soll etwa die Medienkompetenz[21] der Bevölkerung gefördert werden. Um das Bewusstsein aller Akteure bezüglich ihrer Verantwortung gegenüber den Bürgern zu stärken und sie zu einer besseren Zusammenarbeit zu bewegen, arbeitet der Europarat im Bereich Internet und neue Medien vermehrt auch mit der Wirtschaft und der Zivilgesellschaft zusammen[22].

Die Empfehlung des Europarats über den Menschenrechtsschutz in sozialen Netzwerken[23] betont die Förderung der Informations-, Meinungs- und Versammlungsfreiheit durch soziale Netzwerke und deren vielfältige Möglichkeiten zur Verbesserung der Teilnahme des Einzelnen am politischen, sozialen und kulturellen Leben. In einer Empfehlung zur Medienvielfalt wies der Europarat überdies ausdrücklich darauf hin, dass die Mitgliedstaaten die Entwicklung sozialer Netzwerke unterstützen sollten, um den Medienpluralismus und Räume für den Dialog zu fördern[24].

---

[18] Quantitative Angaben finden sich etwa in Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zürich 2012, S. 130f.

[19] EGMR-Urteil „Ahmet Yildirim c. Türkei“ (N° 3111/2010) vom 18.12.2012 zur EMRK-widrigen Sperre der Plattform Google Sites.

[20] http://www.coe.int/t/dghl/standardsetting/media/doc/cm_EN.asp.

[21] „Medienkompetenz“ meint die Fähigkeit, Medien auszuwählen und zu nutzen, Medieninhalte zu verstehen und kritisch zu bewerten, die Medienwirtschaft zu verstehen und Medieneinflüsse zu erkennen sowie in vielfältigen Kontexten kommunizieren und Transaktionen tätigen zu können.

[22] Vgl. z.B. die in Zusammenarbeit mit Internetdiensteanbietern und Online-Spiele-Herstellern erarbeiteten Menschenrechts-Richtlinien: http://hub.coe.int/de/human-rights-guidelines-for-internet-service-providers-and-online-games-providers/.

[23] Empfehlung CM/Rec(2012)4 des Ministerkomitees über den Menschenrechtsschutz in sozialen Netzwerken vom 04.04.2012 (Europarats-Empfehlung zu sozialen Netzwerken).

[24] Empfehlung CM/Rec(2007)2 betreffend Medienpluralismus und Vielfalt der Medieninhalte. Der Europäische Gerichtshof für Menschenrechte führte diese Empfehlung etwa in seinem Urteil „Centro Europa 7 S.R.L. & Di Stefano c. Italien“ (N° 38433/09) vom 7.6.2012 (Ziff. 72, 134) an, welcher den ungenügenden Medienpluralismus Italiens zum Gegenstand hatte.

Um das Funktionieren eines unabhängigen und pluralistischen Mediensystems in der Informationsgesellschaft zu gewährleisten, hat der Europarat ein Konzept für einen neuen umfassenden Medienbegriff erarbeitet, der es erlauben soll, die Grundprinzipien, welche hinter der traditionellen Medienregulierung stehen, in angepasster und abgestufter Form auch auf neue Medien, wie etwa soziale Netzwerke, anwenden zu können[25].

Auch die *Organe der EU* befassen sich mit dem vielseitigen Potenzial sozialer Netzwerke. So wird etwa der grosse Nutzen sozialer Plattformen für die Verwirklichung der Menschenrechte, die politische Partizipation[26] und die unabhängige Medienberichterstattung[27] hervorgehoben. Ebenso werden der innovative und kreative Gehalt sozialer Netzwerke als auch ihre Bedeutung für die Wirtschaft betont[28] und die Förderung der kreativen Nutzung dieser Medien gefordert[29].

3.3 Risiken sozialer Netzwerke

Durch die dominante Position einiger weniger globaler Plattformen können allerdings auch Risiken entstehen, wie etwa dass die Informations- und Meinungsvielfalt reduziert und die Marktdominanz eines sozialen Netzwerkes für politische oder wirtschaftliche Zwecke missbraucht wird. Überdies bergen die über soziale Netzwerke verbreiteten Inhalte verschiedene Gefahren für individuelle und allgemeine Interessen (ausführlich dazu das 4. Kapitel dieses Berichts).

Die *Europarats-Empfehlung* zu sozialen Netzwerken verortet die Risiken sozialer Netzwerke vor allem in Bereichen wie der möglichen diskriminierenden Verwaltung sozialer Plattformen, den Gefahren für Kinder und Jugendliche und dem mangelhaften Schutz der Privatsphäre sowie dem ungenügenden Datenschutz.

Auch der *Europäische Wirtschafts- und Sozialausschuss (EWSA)* bezeichnet den mangelhaften Schutz der Privatsphäre sowie von Kindern und Jugendlichen als ein wesentliches Problem sozialer Netzwerke[30]. Er empfiehlt die Einführung von Selbst- oder Ko-Regulierungsbestimmungen durch die EU-Institutionen, welche bei mangelnder Umsetzung in verbindliche Vorschriften umzuwandeln sind. Aufgrund der dynamischen Entwicklung sozialer Netzwerke fordert der EWSA die Formulierung allgemeiner, technologisch neutraler Vorschriften für die Regulierung der Plattformen und befürwortet die umfassende Förderung der digitalen Kompetenz der Bevölkerung und den Kompetenzausbau von Internet-Hotlines zur Überwachung des unsachgemässen Umgangs mit sozialen Netzwerken.

---

[25] Empfehlung CM/Rec(2011)7 zu einem neuen Medienbegriff.

[26] Gemeinsame Mitteilung Menschenrechte und Demokratie im Mittelpunkt auswärtigen Handelns, KOM(2011) 886 endgültig, S. 14, 20f. oder auch Stellungnahme des Ausschusses der Regionen „Universaldienst im Bereich der elektronischen Kommunikation“ und „künftige Netze und das Internet“, ABl. C vom 28.5.2009, S. 41 sowie Empfehlung EU-Parlament zur Stärkung Sicherheit und Grundfreiheiten im Internet, (2008/2160(INI), ABl. C 117 E vom 6.5.2010, S. 206.

[27] Entschliessung des Europäischen Parlaments vom 07. 09.2010 zu Journalismus und neuen Medien – Schaffung eines europäischen öffentlichen Raums, ABl. 308 E vom 25.10.2011, S. 55.

[28] Stellungnahme „Das Internet der Dinge“ ABl. C 77 vom 31.3.2009 S. 60 oder Mitteilung „Bericht über die digitale Wettbewerbsfähigkeit Europas Hauptergebnisse der i2010-Strategie 2005-2009“, KOM(2009) 390 endgültig, S. 10.

[29] Schlussfolgerung zur Förderung des Kreativitäts- und Innovationspotenzials junger Menschen, 2012/C 169/01, S. 2. Siehe auch Mitteilung „Bericht über die digitale Wettbewerbsfähigkeit Europas Hauptergebnisse der i2010-Strategie 2005-2009“, KOM(2009) 390 endgültig, S. 12. oder Stellungnahme „Eine digitale Agenda für Europa“, 2011/C 15/07, S. 38.

[30] Stellungnahme „Verantwortlicher Umgang mit sozialen Netzwerken und Verhinderung der durch soziale Netzwerke verursachten Probleme“, ABl. C 351 vom 15.11.2012, S. 31.

4 Aktuelle Rechtslage im Bereich sozialer Netzwerke

4.1 Vorbemerkung

Wie oben aufgezeigt, können soziale Netzwerke in der modernen Kommunikationsgesellschaft von grossem Nutzen sein. Gleichzeitig birgt ihre Nutzung jedoch auch Risiken, die teils rechtlicher Natur sind. Im Folgenden werden verschiedene spezifische Probleme sozialer Netzwerke für die Interessen der Nutzenden, anderer indirekt Beteiligter oder der Allgemeinheit erörtert. Weiter werden ausgewählte Lösungsansätze zu diesen Problemen im Ausland oder im internationalen Recht dargestellt und die aktuelle Rechtslage in der Schweiz analysiert.

4.2 Diskriminierende Verwaltung sozialer Netzwerke

4.2.1 Problematische Zutrittsbedingungen und Verweigerung des Zutritts

4.2.1.1 Ausgangslage

Die Nutzung sozialer Netzwerke setzt oft die Angabe von Informationen über die eigene Person (wie etwa Name oder E-Mailadresse) voraus. Umfang und Inhalt der eingeforderten Informationen können je nach Plattform variieren. Aufgrund des üblichen Geschäftsmodells (Vermarktung von Kundendaten) und dem Interesse an inhaltlichen Kontrollmöglichkeiten über die innerhalb des Netzwerks stattfindende Kommunikation, sind viele Plattformbetreiber an wahrheitsgetreuen Angaben über die Identität der Nutzenden interessiert. Zwar umgehen Interessierte mitunter die von den Betreibern aufgestellten Regeln zur Angabe von Informationen über ihre Person; die Mehrheit der Nutzenden dürfte aber wahrheitsgetreue Angaben über die eigene Identität auf Social-Media-Plattformen machen. Die Preisgabe dieser Angaben kann u.a. dann ein Problem sein, wenn es an Transparenz bezüglich der weiteren Bearbeitung der betroffenen Daten fehlt.

Die Registrierdaten können auch Informationen über zukünftige Nutzende enthalten, welche Rückschlüsse auf Aspekte ihrer Identität zulassen, die Plattformbetreiber zur Verweigerung des Zutritts veranlassen könnten. Dies wäre insbesondere dann problematisch, würde ein solcher Ausschluss auf der Zugehörigkeit Nutzender zu einer bestimmten Gruppe basieren (definiert etwa durch Merkmale wie Rasse, Nationalität, politische Gesinnung, Religion, sexuelle Neigung, Geschlecht etc.).

Denkbar ist auch der Ausschluss unliebsamer Einzelpersonen oder bestimmter Unternehmen aus anderen, bspw. wirtschaftlichen Interessen. Da die Geschäftsmodelle der meisten sozialen Netzwerke von einer möglichst hohen Mitgliederzahl profitieren, wird die Verweigerung einer Mitgliedschaft jedoch eher die Ausnahme darstellen.

4.2.1.2 Lösungsansätze im Ausland oder internationalen Recht

Die Europarats-Empfehlung zu sozialen Netzwerken warnt vor diskriminierenden Praktiken in sozialen Netzwerken, wie etwa dem möglichen Ausschluss Nutzender von der Plattform.

4.2.1.3 Rechtslage in der Schweiz

Aus dem Prinzip der Vertragsfreiheit fliesst das Recht Privater grundsätzlich frei zu bestimmen, ob, mit wem und zu welchem Inhalt sie einen Vertrag eingehen wollen[31]. Gemäss Schweizer Recht entscheiden Plattformbetreiber grundsätzlich frei, welche Vertragspartner sie akzeptieren. Die Vertragsfreiheit hat jedoch Grenzen. So kann in bestimmten Fällen ein Anbieter verpflichtet sein, Verträge mit Interessenten abzuschliessen (so genannter Kontrahierungszwang).

Ausdrücklich geregelt wurde der Kontrahierungszwang in Art. 261bis StGB, demzufolge sich strafbar macht, wer eine von ihm angebotene Leistung, die für die Allgemeinheit bestimmt ist, einer Person oder einer Gruppe von Personen wegen ihrer Rasse, Ethnie oder Religion verweigert (bspw. wenn ein Plattformbetreiber eine Interessengemeinschaft aufgrund ihres ethnischen Hintergrunds ausschlies-

[31] Schwenzer Ingeborg, Schweizerisches Obligationenrecht Allgemeiner Teil, 6. Aufl., Bern 2012, S. 171f.

sen würde). Ähnlich untersagt Art. 6 des Bundesgesetzes über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen (BehiG, SR 151.3) öffentliche Dienstleistungen anbietende Privaten, Behinderte auf Grund ihrer Behinderung zu diskriminieren. Betroffene können bei einem Gericht eine Entschädigung beantragen (Art. 8 Abs. 3 BehiG). Darüber hinaus ermöglicht das Gesetz Behindertenorganisationen gesamtschweizerischer Bedeutung eine Zivilklage zur Feststellung einer Diskriminierung (Art. 9 Abs. 3 Bst. a BehiG).

Pflichten zum Vertragsschluss lassen sich aus dem zivilrechtlichen Persönlichkeitsschutz (Art. 28, 28a Abs. 1 Ziff. 2 ZGB) sowie dem Verbot sittenwidriger Schädigung (Art. 41 Abs. 2 OR) ableiten[32]. Voraussetzung ist, dass die anbietende Partei zum Normalbedarf[33] gehörende Waren oder Dienstleistungen allgemein und öffentlich anbietet, der nachfragenden Partei aufgrund der starken Machtstellung des Anbieters zumutbare Ausweichmöglichkeiten fehlen und der Anbieter keine sachlich gerechtfertigten Gründe für die Verweigerung des Vertragsabschlusses anzugeben vermag[34].

Auch das Kartellrecht[35] beschränkt die Vertragsfreiheit, allerdings nur jene marktbeherrschender Unternehmen. Zunehmend nutzen auch Unternehmen Social Media Angebote, dies insbesondere zu Werbezwecken und für den Kundenkontakt. Würde ein soziales Netzwerk etwa im Werbemarkt eine marktbeherrschende Stellung einnehmen, so könnte eine Zugangsverweigerung gegenüber interessierten Unternehmen als Verweigerung einer Geschäftsbeziehung (Art. 7 Abs. 2 Bst. a KG) allenfalls im Widerspruch zum Kartellrecht stehen.

Aus der Analyse ergibt sich, dass Private beim Abschluss von Verträgen (bzgl. Vertragspartner, Inhalt etc.) weitreichende Freiheiten im Schweizer Recht geniessen. Begrenzt wird diese Freiheit durch das Gesetz allerdings dann, wenn einer Partei auf dem Markt eine besondere Machtstellung zukommt oder der Vertragsabschluss aufgrund gewisser Eigenschaften der Gegenpartei verweigert wird. In diesen Fällen kann der Vertragsabschluss rechtlich erzwungen werden.

4.2.2 Zensur von Inhalten durch Betreiber sozialer Netzwerke

4.2.2.1 Ausgangslage

Viele Betreiber sozialer Netzwerke sehen in ihren Nutzungsbedingungen Verhaltensregeln für die Kommunikation auf ihrer Plattform sowie eine Liste bestimmter generell verbotener Inhalte vor. Untersagt sind üblicherweise pornografische, rassistische, diskriminierende, verletzende oder übermässig gewalttätige Inhalte. Soziale Netzwerke, welche weltweit angeboten werden, gestalten ihre Inhaltskontrolle häufig so aus, dass diese den Rechtsordnungen der meisten Länder im Hinblick auf illegale Inhalte gerecht wird. Dies kann dazu führen, dass gewisse Inhalte auch in Ländern gelöscht werden, in welchen sie rechtlich unproblematisch wären.

Die Kontrollmethoden sind unterschiedlicher Natur. So können verdächtige Inhalte von Nutzenden gemeldet und anschliessend vom Betreiber untersucht und allenfalls gelöscht werden. Zudem setzen Betreiber häufig Filtersoftware ein, welche Inhalte automatisch zensiert. Auch die endgültige Löschung von Nutzerkonten infolge von Verstössen ist möglich. Alle diese Methoden können dazu führen, dass grundsätzlich harmlose Inhalte gelöscht werden (beispielsweise das Foto einer stillenden Mutter). Problematisch ist dies insbesondere in Fällen, in denen die veröffentlichten und geteilten Inhalte weder illegal noch sozialschädlich sind oder in begrenzten Benutzergruppen geteilt werden.

---

[32] Schwenzer Ingeborg, Schweizerisches Obligationenrecht Allgemeiner Teil, 6. Aufl., Bern 2012, S. 179.

[33] Güter und Leistungen, die heute praktisch jedermann zur Verfügung stehen und im Alltag in Anspruch genommen werden. Siehe BGE 129 III 35 E. 6.3.

[34] BGE 129 III 35 E. 6.3.

[35] Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen vom 06.10.1995 (KG), SR 251.

4.2.2.2 Lösungsansätze im Ausland oder internationalen Recht

Die Europarats-Empfehlung zu sozialen Netzwerken fordert, dass Nutzende über die redaktionellen Kriterien der Inhaltskontrolle der Plattformen sowie über den Umgang mit scheinbar illegalen oder unerwünschten Inhalten und Verhaltensformen transparent informiert werden und dass die eingesetzten Kontrollmechanismen nicht zu unzulässigen Einschränkungen der Meinungs- und Informationsfreiheit führen. In seiner Erklärung über die Achtung der Meinungs-, Versammlungs- und Vereinigungsfreiheit im Zusammenhang mit privat betriebenen Internetplattformen warnt der Europarat überdies vor der Gefahr, dass Internetdiensteanbieter als Konsequenz politischen Drucks die Kommunikationsgrundrechte ihrer Kunden einschränken könnten und weist die Mitgliedstaaten auf die Schwere der sich daraus möglicherweise ergebenden Grundrechtseinschränkungen hin. Überdies fordert der Europarat, dass Nutzende über den Einsatz von Inhaltsfiltern im Internet informiert und ihnen Abklärungs- und Anfechtungsrechte im Hinblick auf den Einsatz von Filtern eingeräumt sowie gegebenenfalls die Kontrolle über die Filterung von Inhalten ermöglicht werden[36].

4.2.2.3 Rechtslage in der Schweiz

Wer Inhalte Dritter übermittelt, geniesst innerhalb bestimmter rechtlicher Grenzen Freiheit zum Entscheid darüber, welche Inhalte er übertragen will und welche nicht. Spezifische Grenzen ziehen das Radio- und Fernsehgesetz und das Fernmeldegesetz, welche bestimmte Übertragungspflichten vorsehen. Plattformbetreiber sind diesen Vorschriften allerdings üblicherweise nicht unterworfen. Darüber hinaus können sich wettbewerbsrechtliche Fragen stellen: Bei Privaten mit marktbeherrschender Stellung kann die Weigerung gewisse Inhalte zu transportieren Dritte in der Ausübung oder Aufnahme des Wettbewerbs unrechtmässig behindern, falls das marktbeherrschende Unternehmen keine sachlichen Gründe (bspw. Widerrechtlichkeit oder Sittenwidrigkeit der zu übertragenden Inhalte, Platzmangel etc.) für die Ablehnung anzugeben vermag (Art 7 Kartellgesetz, KG). Kommt einem sozialen Netzwerk eine marktbeherrschende Stellung zu und vermag dieses aus jenem Grund weitgehend willkürlich über die Übertragung von Inhalten zu entscheiden, so fragt sich, ob sich allenfalls – analog zu den inhaltlichen Pflichten von Programmveranstaltern in Radio und Fernsehen oder zu den Übertragungspflichten von Programmen durch Fernmeldedienstanbieter – Verpflichtungen hinsichtlich der Übermittlung von Inhalten rechtfertigen liessen. Eine gesetzliche Verpflichtung von Plattformbetreibern, gewisse Inhalte zu übertragen, beschränkt deren Grundrechte (z.B. die Wirtschaftsfreiheit) und bedarf der üblichen Rechtfertigungsgründe (Art. 36 BV).

In bestimmten Konstellationen können auch das Urheberrecht (d.h. das Urheberpersönlichkeitsrecht) oder der zivilrechtliche Persönlichkeitsschutz (Art. 28 ZGB) gegen die Löschung bestimmter Inhalte sprechen.

Der Staat kann die Kommunikationsgrundrechte auch mittelbar einschränken, indem er Private in deren Ausübung hemmt. So ist denkbar, dass eine strenge Inhaltskontrolle durch einen Plattformbetreiber indirekt auch auf den Staat zurückzuführen ist. Insbesondere eine unklare Rechtslage in Form unbestimmter Gesetzesvorschriften kann dazu führen, dass Private sich nicht darüber im Klaren sind, welche Äusserungen rechtlich zulässig sind und welche nicht[37]. So kann eine unklare Regelung der Haftung von Providern und von Plattformbetreibern bezüglich ihrer Verantwortung für durch Dritte verbreitete illegale Inhalten dazu führen, dass die Unternehmen in Zweifelsfällen auch rechtlich unproblematische Beiträge löschen, um befürchteten rechtlichen Problemen aus dem Weg zu gehen.

---

[36] Empfehlung CM/Rec(2008)6 zur Wahrung der Meinungs- und Informationsfreiheit im Hinblick auf Internetfilter.

[37] Müller Jörg Paul/Schefer Markus, Grundrechte in der Schweiz, 4. Aufl., Bern 2008, S. 376.

4.3 Beeinträchtigung weiterer Individualinteressen durch Plattformbetreiber

4.3.1 Grundproblem: Mangelhafte Kontrolle der Nutzenden über ihre Daten

4.3.1.1 Ausgangslage

Aus datenschutzrechtlicher Sicht ist insbesondere die ungenügende Kontrolle der Nutzenden über ihre Daten ein zentrales Problem[38]. Die Erscheinungsformen dieses Kontrollmangels sind vielfältig:

Der Umfang der Autonomie der Nutzenden bezüglich der Verwendung ihrer Daten hängt nicht nur vom Entscheid ab, ob sie einem sozialen Netzwerk überhaupt beitreten und welche Informationen sie dort über sich preisgeben.[39] Von grosser Bedeutung ist die von den Plattformbetreibern angebotene Software. Sie beschränkt die Kontrolle der Nutzenden über ihre Daten regelmässig durch mangelhafte Voreinstellungen zum Schutz der Privatsphäre. Problematisch ist auch die Möglichkeit Dritter, welche Zugang zu anderen Nutzerprofilen haben, Texte und Fotos ohne vorherige Einwilligung des Profileigentümers auf diesen zu platzieren oder Inhalte von zugänglichen Nutzerprofilen ungefragt herunterladen zu können.

Nutzenden wird die Kontrolle über ihre Daten auch durch weitreichende Einwilligungserfordernisse für die Datenbearbeitung entzogen und erschwert. Die häufige Einführung neuer Anwendungen und Dienste und regelmässige Änderungen der Nutzungsbedingungen und Datenschutzerklärungen führen überdies dazu, dass sich Nutzende laufend neu informieren müssen, um über aktuelle Datenbearbeitungsmethoden orientiert zu sein. Informationen über die Verwendung von Profil- und Bewegungsdaten sind regelmässig nur schwer auffindbar und häufig fehlt es an einer transparenten Aufklärung der Nutzenden über den Zweck der Datenbearbeitung, die allfällige Datenweitergabe an Dritte oder einfachen Mechanismen zur Geltendmachung von Auskunfts- und Berichtigungsansprüchen.

Auch der Datenschutz von Personen, die soziale Netzwerke nicht nutzen, ist meistens nur mangelhaft gewährleistet. So erlauben bestimmte Netzwerkbetreiber (namentlich Facebook) Nutzenden ihre Kontakte aus Telefon- und E-Mailadresslisten sowie Instant-Messenger-Diensten auf ihr Nutzerprofil zu laden (Freundefinder-Funktion). Dies ermöglicht es Plattformbetreibern festzustellen, welche der übermittelten Kontakte noch nicht Mitglieder des Netzwerkes sind. Üblicherweise benutzt die Plattform die angegebenen Adressen mit Einwilligung des Mitglieds, um (vom Empfänger unerbetene) Einladungen und Werbung an Nichtmitglieder zu versenden.

Zu einer weiteren Einschränkung der Kontrolle führt die Einräumung weitreichender Befugnisse an den Plattformbetreiber in den Allgemeinen Geschäftsbedingungen (AGB), denen Nutzende üblicherweise zustimmen müssen, um den Dienst verwenden zu können. Besteht eine Knappheit an sozialen Netzwerken oder ist die Nutzung alternativer Plattformen aufgrund ihrer niedrigen Mitgliederzahl wenig interessant, so sind vom Plattformbetreiber diktierte, einschränkende Nutzungsbedingungen besonders problematisch. So sehen viele Netzwerke eine weitreichende *Einräumung von Nutzungsrechten an den Nutzerdaten* vor. Die Löschung von Inhalten durch die Nutzenden ändert an diesem Umstand in der Regel nichts und kann von diesen als endgültiges Entfernen ihrer Inhalte (die Daten auf dem Server des Netzwerkbetreibers umfassend) fehlinterpretiert werden.

Zu welchen Nachteilen die ungenügende Kontrolle über die Daten führen kann, illustriert ein Beispiel aus der Beratungspraxis des EDÖB: Der Organisator eines grösseren Anlasses wählte als primären

---

[38] Vgl. dazu den Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9.12.2011 (BBl 2012 335, 350). Eine von der Stiftung Warentest durchgeführte Studie, welche zehn häufig genutzte soziale Netzwerke auf Kriterien wie „Organisation und Transparenz", „Umgang mit Nutzerdaten", „Datensicherheit", „Nutzerrechte", „Jugendschutz" und „Mängel in den AGB" untersuchte, wies auf diverse Mängel in den betreffenden Bereichen hin. Insbesondere die Ergebnisse der U.S.-amerikanischen Plattformen Facebook, LinkedIn und Myspace, aber auch deutscher Netzwerke wie Xing oder Stayfriends fielen schlecht aus. Siehe Stiftung Warentest „Datenschutz bei Onlinenetzwerken", 2010; zu finden unter: http://www.test.de/Soziale-Netzwerke-Datenschutz-oft-mangelhaft-1854798-0/.

[39] So geben etwa 38% der Internetnutzenden in der Schweiz an, dass sie auf die Veröffentlichung persönlicher Angaben in sozialen Netzwerken verzichten. Siehe Studie des Bundesamtes für Statistik „Internet in den Schweizer Haushalten. Ergebnisse der Erhebung Omnibus IKT 2010", S. 47, 85.

Kommunikationskanal ein soziales Netzwerk, doch löschte der Plattformbetreiber den Netzwerkauftritt kurz vor dem Veranstaltungstermin. Da der Organisator ausserhalb des Netzwerks keine Kontaktinformationen zu den Teilnehmern besass, konnte er diese nicht mehr über den definitiven Ablauf des Anlasses informieren. Beim Plattformbetreiber hatte der Organisator trotz seines bezahlten Auftritts keinen direkten Ansprechpartner beim. Er musste sein Anliegen über das allgemeine Kontaktformular darlegen, was keine rechtzeitigte Orientierung der Teilnehmenden mehr erlaubte.

4.3.1.2 Lösungsansätze im Ausland oder internationalen Recht

Die Europarats-Empfehlung zu sozialen Netzwerken fordert, dass Plattformbetreiber die Transparenz der Datenbearbeitung erhöhen, für jede Datenbearbeitung die informierte Einwilligung der Betroffenen einholen und Nutzende aufklären, wann ihre Kommunikation privat oder öffentlich ist. Überdies soll Nutzenden geholfen werden, die Einstellungen sozialer Netzwerke zu verstehen. Sie sollen bewusst entscheiden, in welchem Umfang ihre Daten für Dritte zugänglich sind („opt in", „multi-layered access"). Betreiber sozialer Netzwerke sollen die Sammlung und Verarbeitung der Daten von Nichtmitgliedern (etwa E-Mailadressen oder biometrische Daten) unterlassen und datenschutzfreundliche Privatsphäreeinstellungen sowie eine datenschutzfreundliche Netzwerksoftware einsetzen. Überdies sollen Nutzende Inhalte über Dritte nur mit deren Einwilligung veröffentlichen können.

Der Vorschlag des Konsultativkomitees zur Revision der Europaratskonvention vom 28.1.1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SR 0.235.1) hebt u.a. hervor, dass soziale Netzwerke und Blogs besonderer Beachtung bedürfen[40]. So sollen die Nutzerrechte ausgebaut werden und Datenbearbeiter ihre Dienste, Produkte und Arbeitsvorgänge schon in der Entwicklung datenschutzkonform ausgestalten. Auch sollen die nationalen Datenschutzbehörden gestärkt und die Mitgliedsstaaten des Europarats verpflichtet werden, diesen angemessene personelle, technische und finanzielle Unterstützung zukommen zu lassen, sodass sie ihrer Aufgabe autonom und effizient nachgehen können[41].

Im Rahmen der Reform der EU Richtlinie 95/46/EG zum Schutz personenbezogener Daten[42] (sie soll zu einer in den EU-Staaten direkt anwendbaren Verordnung führen), sind verschiedene Vorschriften zur Verbesserung der Kontrolle der Nutzenden über ihre Daten vorgesehen. Die vorgeschlagenen Normen umfassen strenge Einwilligungserfordernisse in die Datenverarbeitung zu genau festgelegten Zwecken sowie umfassende Informations- und Auskunftspflichten unter besonderer Berücksichtigung der Position von Kindern. Der Verordnungsentwurf sieht den Datenschutz durch Technik, datenschutzfreundliche Voreinstellungen (privacy by design & privacy by default), den Grundsatz der Datensparsamkeit sowie die zeitliche Beschränkung der Datenspeicherung vor[43].

4.3.1.3 Schutz vor Persönlichkeitsverletzung durch Datenbearbeitung im Schweizer Datenschutzrecht

Die von Nutzenden in sozialen Netzwerken bereitgestellten Inhalte sind regelmässig als Personendaten[44] im Sinne des Bundesgesetzes über den Datenschutz (DSG, SR 235.1) zu qualifizieren. Häufig

---

[40] Modernisation of Convention 108, T-PD-BUR(2012)01Rev2_en, S. 4.

[41] Abridged Report of the Consultative Committee of Convention 108, T-PD (2012) RAP 29 Abr_en, S. 22 (Art. 5), 24ff. (Art. 7, 7^{bis}, 8, 8^{bis}), 29 (Art. 12^{bis}).

[42] Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, S. 31.

[43] Art. 6 Abs. 1 Bst. a, Art. 7, 11, 14, 15, 23 Vorschlag EU Datenschutz-Grundverordnung, KOM(2012) 11 endgültig; vgl. dazu etwa Caspar Johannes, Soziale Netzwerke und Einwilligung der Nutzer, in: digma 2013/2, S. 60ff.

[44] Personendaten sind gemäss Art. 3 Bst. a DSG alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Bestimmbar ist die Person gemäss BGE 138 II 346 E. 6.1., wenn sie zwar allein durch die Daten nicht eindeutig identifizierbar ist, aus den Umständen bzw. dem Kontext einer Information oder aufgrund zusätzlicher Informationen jedoch auf sie geschlossen werden kann (z.B. wenn aus Angaben über Liegenschaften der Eigentümer ausfindig gemacht werden kann).

handelt es sich sogar um besonders schützenswerte Personendaten[45] oder um Persönlichkeitsprofile, welche einen weitergehenden Schutz geniessen als gewöhnliche Personendaten. Das Datenschutzgesetz schützt natürliche und juristische Personen u.a. vor widerrechtlichen Persönlichkeitsverletzungen durch die Bearbeitung von Personendaten durch Private (Art. 12 DSG). Betreiber sozialer Netzwerke fallen somit grundsätzlich in den Anwendungsbereich des Gesetzes. Da die Betreiber oftmals ihren Sitz im Ausland haben, werden die zivilrechtlichen Ansprüche bezüglich der Zuständigkeit gemäss internationalen Übereinkommen46 oder den Bestimmungen der Art 129ff des Bundesgesetzes über das Internationale Privatrecht47 beurteilt. Weiter ist zu beachten, dass gemäss bundesgerichtlicher Rechtsprechung[48] der EDÖB bei Systemfehlern einen Sachverhalt nur abklären kann, wenn die Datenbearbeitungen überwiegende Anknüpfungspunkte zur Schweiz haben.

In sozialen Netzwerken sind verschiedene Verletzungen der allgemeinen datenschutzrechtlichen Bearbeitungsgrundsätze (Art. 12 Abs. 2 DSG) denkbar. Einige Beispiele:

- Informiert der Betreiber eines sozialen Netzwerks bei der Beschaffung personenbezogener Daten nicht darüber, dass er diese an Dritte verkaufen wird, damit jene sie zu Marketingzwecken verwenden können, oder macht er nicht transparent, dass er die Daten selbst zu Werbezwecken auswerten und verwenden wird, so liegt üblicherweise ein Verstoss gegen die Grundsätze der Zweckbindung (Art. 4 Abs. 3 DSG) sowie der Erkennbarkeit (Art. 4 Abs. 4 DSG) der Datenbearbeitung vor. Gibt der Betreiber des sozialen Netzwerks die Daten an Dritte weiter, so sind diese für die Datenbearbeitung ebenso an den Bearbeitungszweck gebunden, welcher bei der Erhebung der Daten angegeben wurde[49]; überdies ist die Bekanntgabe von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen an Dritte ohne Rechtfertigungsgrund widerrechtlich (Art. 12 Abs. 2 Bst. c DSG).

- Die Grundsätze der Verhältnismässigkeit und Zweckbindung der Datenbearbeitung (Art. 4 Abs. 2 und Abs. 3 DSG) können verletzt sein, wenn Betreiber sozialer Netzwerke mehr Daten sammeln, bearbeiten und aufbewahren als für die von ihnen angegebenen Bearbeitungszwecke erforderlich ist. Überdies scheint der Grundsatz der Verhältnismässigkeit der Datenbearbeitung bedeutsam, wenn besonders schützenswerte Personendaten (etwa bezüglich Rassenzugehörigkeit, Intimsphäre oder religiöser und politischer Ansichten; Art. 3 Bst. c DSG) für Marketingzwecke verwendet werden.

- Werden die Daten eines sozialen Netzwerks Gegenstand eines Datendiebstahls oder Datenlecks, weil der Plattformbetreiber die ihm zumutbaren technischen oder organisatorischen Schutzmassnahmen nicht getroffen hat, so liegt üblicherweise eine Verletzung des Grundsatzes der Datensicherheit (Art. 7 Abs. 1 DSG) vor. Aus dem Grundsatz der Datensicherheit und dem Grundsatz von Treu und Glauben (Art. 4 Abs. 2 DSG) lässt sich u.U. eine Informationspflicht des Plattformbetreibers über Datenlecks und Datendiebstähle ableiten[50].

- Die Datenbearbeitungsgrundsätze binden auch Nutzende. Laden sie etwa Kontakte aus Telefon- und E-Mailadresslisten oder Instant-Messenger-Diensten auf eine soziale Plattform, so ergibt sich aus den Grundsätzen der Zweckbindung und Erkennbarkeit (Art. 4 Abs. 3 und 4 DSG), dass der Plattformbetreiber und die Veröffentlicher der Kontaktdaten die betroffenen Personen über diese Datenbeschaffung und ihren Zweck informieren müssen, sofern dies nicht aus den Umständen ersichtlich ist.

---

[45] Besonders schützenswert sind gemäss Art. 3 Bst. c DSG Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten und Tätigkeiten, über die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe sowie administrative oder strafrechtliche Verfolgung und Sanktionen.

[46] Z.B. Lugano-Übereinkommen vom 30. Oktober 2007 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (LugÜ), SR 0.275.12.

[47] SR 272; IPRG.

[48] Vgl. BGE 138 II 346 E. 3.

[49] BSK-DSG, Maurer-Lambrou Urs/Steiner Andrea, 2. Aufl., Basel 2006, Art. 4, S. 83 Rz. 16.

[50] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, S. 82 N. 16.

- Das DSG sieht zwar keinen besonderen Schutz von Kindern vor. Die Einhaltung bestimmter Bearbeitungsgrundsätze, wie etwa des Grundsatzes der Erkennbarkeit oder des Grundsatzes von Treu und Glauben, wird bei der Bearbeitung personenbezogener Daten von Kindern jedoch mehr Sorgfalt erfordern als dies üblicherweise bei der Bearbeitung personenbezogener Daten von Erwachsenen der Fall ist.

4.3.1.4 Rechtfertigung – insbesondere Einwilligung in die Datenbearbeitung

Eine persönlichkeitsverletzende Datenbearbeitung kann durch ein überwiegendes privates oder öffentliches Interesse, durch Gesetz oder die Einwilligung des Verletzten gerechtfertigt sein (Art. 13 Abs. 1 DSG). Gemäss Bundesgericht ist eine Rechtfertigung der Bearbeitung von Personendaten entgegen den allgemeinen Bearbeitungsgrundsätzen zwar nicht generell ausgeschlossen. Rechtfertigungsgründe können im konkreten Fall aber nur mit grosser Zurückhaltung bejaht werden[51].

Bei der Bearbeitung von Daten durch Plattformbetreiber steht der Rechtfertigungsgrund der Einwilligung der Betroffenen im Vordergrund. Um die Dienste sozialer Netzwerke in Anspruch nehmen zu können, geben Nutzende üblicherweise datenschutzrechtlichen Zustimmungserklärungen in Allgemeinen Geschäftsbedingungen (AGBs) ab. Damit willigen sie grundsätzlich in die vom Betreiber in den AGBs beschriebene Datenbearbeitung ein. Es können sich allerdings Fragen der Gültigkeit und des Umfangs dieser Einwilligung stellen.

Probleme können etwa vorliegen, wenn die Urteilsfähigkeit (Art. 16 ZGB) einer Person im Hinblick auf den Vertragsinhalt fraglich erscheint, dies beispielsweise bei *Kindern*, die personenbezogene Daten über sich preisgeben. Urteilsunfähige Kinder werden im Umfang der elterlichen Sorge von ihren Eltern vertreten. Es ist davon auszugehen, dass die Eltern grundsätzlich für sie in bestimmte Formen der Datenbearbeitung einwilligen können (bspw. die Veröffentlichung des Fotos eines Kleinkindes in einem sozialen Netzwerk[52]).

Urteilsfähige Kinder können zwar selbständig handeln, soweit es um höchstpersönliche Rechte (Art. 19c Abs. 2 ZGB) wie die bei der Bearbeitung ihrer Personendaten tangierten Persönlichkeitsrechte geht. Sie können grundsätzlich ohne Zustimmung der Eltern persönlichkeitsrechtlich Informationen über sich selber preisgeben (Einzelheiten hinten unter Ziff. 4.6.1.3). Damit die Einwilligung eines urteilsfähigen Kindes in eine persönlichkeitsverletzende Datenbearbeitung gültig ist, sollte der Datenbearbeiter die nötigen Informationen allerdings so formulieren und darstellen, dass dieses sie verstehen und nachvollziehen kann. Überdies kann eine Einwilligung in Anbetracht der häufig ändernden Verwendungszwecke der Nutzerdaten sowie der z.T. schwierigen Verständlichkeit von Datenschutzerklärungen und der fraglichen Überschaubarkeit der Konsequenzen gewisser Datenbearbeitungen auch inhaltliche Grenzen haben.

Aufgrund der üblichen Länge und des Sprachstils von AGBs, verzichten Nutzende beim Eingehen eines Vertragsverhältnisses häufig auf deren Lektüre. Wurden datenschutzrechtliche Zustimmungserklärungen in AGBs aufgenommen und lesen Nutzende letztere beim Vertragsschluss nicht (Globalübernahme), so wird ihre Einwilligung für ungewöhnliche, geschäftsfremde Klauseln grundsätzlich nicht wirksam sein, wenn auf diese nicht besonders hingewiesen wurde[53]. Unklare AGB-Klauseln sind im Zweifel zu Lasten des Verwenders auszulegen. Führt die Auslegung einer Nutzungsbedingung zu keinem klaren Ergebnis, so ist sie in dem für die Nutzenden günstigsten Sinne auszulegen.

---

[51] Siehe BGE 138 II 346 E. 7.2 mit Verweis auf BGE 136 II 508 E. 5.2.4.

[52] Zur menschenrechtlichen Problematik solcher Aufnahmen vgl. den Sachverhalt des EGMR-Urteils „Reklos & Davourlis c. Griechenland“ (Beschwerdenr. N° 1234/05) vom 15.1.2009.

[53] BSK-DSG, Rampini Corrado, 2. Aufl., Basel 2006, Art. 13, S. 194 Rz. 13 sowie Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, S. 112 N. 90.

Eine Einwilligung in eine persönlichkeitsverletzende Datenbearbeitung liegt nur vor, wenn sie gültig ist und nicht widerrufen wurde[54]. Gültig ist sie nur, wenn sie vor der Bearbeitung, auf der Grundlage angemessener Information und freiwillig (d.h. ohne Täuschung, Drohung oder Zwang) erteilt wurde[55]; bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss sie überdies ausdrücklich sein (Art. 4 Abs. 5 DSG). Bei sozialen Netzwerken spielen in diesem Zusammenhang insbesondere Form und Inhalt der Nutzerinformation eine Rolle. Diese muss klar, sachlich, korrekt, einfach zugänglich, gut erkennbar und nicht irreführend sein[56].

Sollen gewöhnliche Personendaten bearbeitet werden, so kann die Einwilligung konkludent erfolgen bzw. sich aus dem Verhalten der betroffenen Person ergeben, bspw. wenn diese ihre Daten in einem sozialen Netzwerk selbst zugänglich macht[57]. Die Zustimmung hat jedoch umso klarer zu sein, je sensibler die zu bearbeitenden Personendaten sind[58]. Im Internet sollte ein Mausklick zur Bestätigung einer datenschutzrechtlichen Einwilligungserklärung, wie er für die Nutzung der meisten sozialen Netzwerke erforderlich ist, den Formansprüchen an eine ausdrückliche Einwilligung genügen[59].

Willigen Nutzende in die Nutzungsbedingungen von sozialen Netzwerken ein, so akzeptieren sie – sofern sie angemessen informiert wurden – auch die konkrete Funktionsweise des Dienstes und somit beispielsweise auch, dass Dritte ohne vorherige Anfrage Inhalte über sie und auf ihrem Profil veröffentlichen. Soweit die Aktivitäten Dritter nicht gegen geltendes Recht verstossen (bspw. in Form von Ehrverletzungen, Verletzungen des Rechts am eigenen Bild oder Wort, Verletzungen des Berufsgeheimnisses etc.), können sich Nutzende dagegen kaum wehren. Als mögliche Reaktion käme in Betracht, auf eine Mitgliedschaft in sozialen Netzwerken mit derart offenen Kommunikationsformen zu verzichten oder unangenehme Inhalte im eigenen Profil zu löschen. Löschungen sind in Fällen eines grossen Interesses der Netzwerkgemeinschaft an einem bestimmten Inhalt allerdings nur bedingt nützlich, wenn dieser bereits mehrfach kopiert und verlinkt wurde.

4.3.1.5 Allgemein zugängliche Personendaten

Allgemein zugänglich sind Personendaten, wenn eine unbestimmte Zahl von Personen diese ohne wesentliche Hindernisse in Erfahrung bringen kann. Geben Nutzende in sozialen Netzwerken Daten über sich selbst preis, liegt in der Regel keine Persönlichkeitsverletzung vor, falls sie die Daten mit Wissen und Willen allgemein zugänglich gemacht und deren Bearbeitung nicht ausdrücklich untersagt haben (Art. 12 Abs. 3 DSG). Dies gilt auch für die grenzüberschreitende Bekanntgabe von Personendaten in Länder mit unangemessenem Datenschutzniveau (Art. 6 Abs. 2 Bst. f DSG).

Über die Zugänglichkeit von Informationen können Nutzende auf der Grundlage der angebotenen Nutzungseinstellungen grundsätzlich selber entscheiden. In den meisten sozialen Netzwerken werden verschiedene Kommunikationsformen mit unterschiedlich weitreichender Privatsphäre angeboten, womit Individual- bis hin zu Massenkommunikation möglich ist. Werden Nutzende angemessen über die verschiedenen möglichen Kommunikationsformen und deren Privatheit informiert, so lässt sich anhand der von ihnen gewählten Kommunikationsform abschätzen, ob private Kommunikation beabsichtigt war oder Informationen allgemein zugänglich gemacht wurden.

Auch die Bearbeitung allgemein zugänglich gemachter Personendaten kann eine Persönlichkeitsverletzung darstellen, wenn die Daten zu Zwecken bearbeitet werden, für welche sie nach den Umstän-

---

[54] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, S. 386 N. 3.

[55] Äusserst kritisch bezüglich Facebooks Datenschutzerklärung: Baeriswyl Bruno, Kleingedrucktes unter der Lupe - Die Allgemeinen Geschäftsbedingungen (AGB) von Sozialen Netzwerken versprechen keinen Datenschutz, in: digma 2010 S. 56, 59 und Caspar Johannes, Soziale Netzwerke und Einwilligung der Nutzer, in: digma 2013/2, S. 63f.

[56] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, S. 106 N. 75.

[57] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, S. 108 N. 79.

[58] BBl 2003 2127f.

[59] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, S. 108 N. 78.

den bei objektiver Betrachtung nicht allgemein zugänglich gemacht wurden[60]. Dies ist für im Internet allgemein zugänglich gemachte Daten insbesondere wegen ihrer leichten Auffindbarkeit von Bedeutung[61]. Wenn eine Person ihre Fotos in einem sozialen Netzwerk öffentlich zugänglich macht, so darf diese grundsätzlich wohl jeder sehen, die ungefragte Verwendung der Bilder für die Werbekampagne eines Unternehmens wird jedoch nicht zulässig sein. Problematisch ist die Verwendung solcher Bilder auch im Rahmen herkömmlicher journalistischer Medienberichterstattung.[62]

Vor diesem Hintergrund stellt sich die Frage, ob das ungefragte Herunterladen und Speichern von Inhalten aus fremden Nutzerprofilen vom Veröffentlichungszweck noch gedeckt ist, in jedem Einzelfall wieder neu. Grundsätzlich gilt in jedem Fall, dass sich andere Netzwerkmitglieder ebenso an die Bearbeitungsgrundsätze des Datenschutzgesetzes zu halten haben wie die Plattformbetreiber.

4.3.1.6 Spezialproblem Übertragung umfassender Nutzungsrechte an den Plattformbetreiber

Ist die unbeschränkte Aufbewahrung und Verwendung sämtlicher durch Nutzende in sozialen Netzwerken veröffentlichter Inhalte ausdrücklich Gegenstand des Vertrages zwischen Nutzenden und Plattformbetreibern geworden, so fragt sich, ob ein Vertrag diesen Inhalts gültig ist. Es ist nicht ausgeschlossen, dass ein solcher Vertrag im Einzelfall als persönlichkeitsrechtswidriges Rechtsgeschäft qualifiziert werden könnte (Art. 19 Abs. 2 und Art. 20 Abs. 1 OR; Art. 27 Abs. 2 ZGB), zumal die in sozialen Netzwerken veröffentlichten und später verknüpften Daten häufig besonders schützenswert sind oder Persönlichkeitsprofile darstellen und das Verhältnis von Leistung und Gegenleistung Fragen aufwirft (Angebot einer Kommunikationsinfrastruktur durch die Plattformbetreiber versus Übertragung weitreichender Nutzungsrechte an Personendaten der Nutzenden)[63]. In diesem Zusammenhang wirkt sich allerdings wesentlich aus, dass Nutzende einen beachtlichen Einfluss darauf haben, welche ihrer Daten in sozialen Netzwerken publiziert werden.

4.3.1.7 Weitere Schutzinstrumente der schweizerischen Rechtsordnung

Neben dem Datenschutzgesetz enthält die schweizerische Rechtsordnung weitere Instrumente zum Schutz gegen intransparente Methoden der Datenerhebung, -bearbeitung und –bekanntgabe durch Betreiber sozialer Netzwerke. In Betracht kommen beispielsweise die privatrechtlichen Möglichkeiten der **Vertragsanfechtung** bei Vorliegen eines wesentlichen Irrtums (Art. 23ff. OR) oder einer absichtlichen Täuschung (Art. 28 OR)[64].

Überdies kann etwa die Verwendung missbräuchlicher allgemeiner Geschäftsbedingungen (AGB) ein unlauteres Geschäftsgebaren darstellen (Art. 8 Bundesgesetz vom 19.12.1986 gegen den unlauteren Wettbewerb [**UWG**], SR 241). Mit der neusten Änderung des UWG ist seit dem 1.7.2012 jede den Grundsatz von Treu und Glauben verletzende Verwendung von AGB unlauter, wenn sie zum Nachteil der Kundschaft ein erhebliches und ungerechtfertigtes Missverhältnis zwischen den vertraglichen Rechten und Pflichten verursacht[65]. Die Neufassung strich das in Art. 8 UWG bisher geltende Erfordernis der Irreführung (Nachweis der Täuschungsgefahr), so dass nun eine offene Inhaltskontrolle von

---

[60] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, S. 381 N. 76.

[61] BSK-DSG, Rampini Corrado, 2. Aufl., Basel 2006, Art. 12, S. 187f. Rz. 18.

[62] Als Organ der institutionalisierten Selbstkontrolle im Journalismus hat der Schweizer Presserat die Medienschaffenden mehrmals zur Zurückhaltung bei der Verwendung von im Internet publizierten Informationen Privater gemahnt. Wer Bilder auf einem Blog oder einer anderen für jedermann zugänglichen Plattform veröffentliche, willige nicht einfach in deren Weiterverbreitung durch ein anderes Medium ein. Medienschaffende müssten auch dann den Schutz des Privatlebens sorgfältig gegen das Informationsinteresse der Öffentlichkeit abwägen; vgl. etwa Presserats-Stellungnahme Nr. 43/2010 vom 1.9.2010: Internet und Privatsphäre; www.presserat.ch/28340.htm.

[63] Schwenzer Ingeborg, Schweizerisches Obligationenrecht Allgemeiner Teil, 6. Aufl., Bern 2012, S. 256f.

[64] Siehe zu diesen Rechtsbehelfen Schweizer Alex, Data Mining – ein rechtliches Minenfeld. Rechtliche Aspekte von Methoden des Customer Relationship Management (CRM) wie Data Mining, digma 2001 S. 108, 111-114.

[65] AS 2011 4910.

AGB für den Konsumentenverkehr möglich ist.[66] Im Hinblick auf die AGBs von Social Media Anbietern fragt sich etwa, ob Klauseln vor dem neuen Art. 8 UWG standhalten würden, welche die einseitige Anpassung der Nutzungsbedingungen durch den Plattformbetreiber ohne Frist oder persönliche Mitteilung erlauben.

Der wiederholte, nicht gerechtfertigte Verstoss gegen die Bearbeitungsgrundsätze des Datenschutzgesetzes könnte überdies unlauter im Sinne der Generalklausel von Art. 2 UWG sein, falls sich der Datenbearbeiter durch die DSG-Verletzung einen Wettbewerbsvorsprung gegenüber seinen Konkurrenten zu verschaffen vermag[67]. Zu denken ist beispielsweise an Personendaten, welche datenschutzwidrig aus sozialen Netzwerken erhoben, bearbeitet und zu Werbezwecken verkauft werden.

4.3.1.8 Würdigung

Gesamthaft lässt sich festhalten, dass das geltende schweizerische Recht mit seinen offen formulierten Schutzvorschriften einen relativ umfangreichen Schutz vor den in sozialen Netzwerken üblichen problematischen Datenbearbeitungen ermöglicht. Es sind allerdings verschiedene, auch für Social Media relevante, Schwierigkeiten zu erkennen, die einem wirksamen Datenschutz im Wege stehen. Sie liegen etwa in der oft mangelnden Erkennbarkeit problematischer Datenbearbeitungen, der enormen Zunahme von Datenbearbeitungen mit internationalem Bezug (was Ermittlung und Durchsetzung stark erschwert; vgl. dazu hinten Kap. 5) und der verhältnismässig geringen Wahrscheinlichkeit von Sanktionen. Hinzu kommt, dass Nutzende ihre einklagbaren Rechte kaum wahrnehmen und der EDÖB in Anbetracht der Vielzahl relevanter Sachverhalte an die Grenzen seiner Ressourcen stösst[68].

Verbesserungspotenzial gäbe es auch etwa durch vermehrte datenschutzfreundliche Voreinstellungen (*privacy by design* und *privacy by default*) und eine verständlichere Formulierung von Datenschutzerklärungen. Im Evaluationsbericht zum DSG hat der Bundesrat eine Vertiefung des Konzepts *Privacy by Design*), die Förderung datenschutzfreundlicher Technologien sowie Massnahmen zur Verbesserung der Datenkontrolle und –herrschaft in Aussicht gestellt.[69]

4.3.2 Erstellen und Bewirtschaften von umfassenden Nutzerprofilen (Data Mining)

4.3.2.1 Ausgangslage

Nutzende geben zu Zwecken ihrer Registrierung, durch ihre Aktivitäten in sozialen Netzwerken, wie auch durch die mit der Internetnutzung entstehenden Metadaten (Verbindungsdauer, grobe geografische Herkunft der IP-Adresse, Verweildauer und Bewegungen auf der Webseite, etc.) umfassende Informationen über sich preis. So erlaubt beispielsweise die Platzierung des Facebook-„like“-Buttons auf Webseiten Dritter Facebook, Angaben über die Besucher dieser Webseiten zu erhalten.

Bei vielen Plattformbetreibern ist unklar, wie die gesammelten Daten verwendet werden. Die Zusammenführung sämtlicher Informationen, welche die Benutzung sozialer Netzwerke hinterlässt, kann zur Erstellung aussagekräftiger, aber auch fehleranfälliger Profile führen. Verkauft der Plattformbetreiber die Datenpakete an Dritte, so können sie die Profile als Grundlage für Angebote von Dienstleistungen und Waren nutzen. Dies ist nicht nur wegen der wirtschaftlichen Instrumentalisierung der Daten problematisch, sondern auch wegen des Diskriminierungspotenzials.

---

[66] Durch das Streichen des Tatbestandsmerkmals der Irreführung wollte der Gesetzgeber den Weg für eine offene Inhaltskontrolle bereiten (BBl 2009 6178).

[67] Weber Rolf/Volz Stephanie, Online Marketing und Wettbewerbsrecht, Zürich 2011, S. 65f.

[68] Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9.12.2011 (BBl 2012 341-345, 349).

[69] Bericht über die Evaluation des Bundesgesetzes über den Datenschutz vom 9.12.2011, Ziff. 5.2.2 (BBl 2012 350)

4.3.2.2 Lösungsansätze im Ausland oder internationalen Recht

Die Empfehlung des Ministerkomitees des Europarats über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling[70] befasst sich mit der Beobachtung, Sammlung und Übereinstimmung personenbezogener Daten im Internet und verlangt umfassende Schutzrechte der Betroffenen. Soziale Netzwerke sind eine wichtige Quelle für derartige Datenbearbeitungen. Als problematisch identifiziert der Europarat die mangelnde Transparenz der Profilerstellung, deren Diskriminierungspotenzial gegenüber den Betroffenen sowie den ungenügenden Schutz von Kindern vor derartigen Datensammlungen. Gefordert wird auch, dass der Zugang zu Waren und Dienstleistungen (und zu Informationen darüber) möglich ist, ohne dass für die Erbringung der Dienstleistung oder Warenlieferung nicht erforderliche personenbezogene Daten preisgegeben werden müssen. Anbieter von Diensten der Informationsgesellschaft sollen zudem sicherstellen, dass die Informationen über ihre Dienste ohne Erstellung eines Profils zugänglich sind.

Artikel 20 des Vorschlags zu einer EU-Datenschutz-Grundverordnung[71] beabsichtigt natürliche Personen (unter Berücksichtigung gewisser Ausnahmen) vor der automatisierten Verarbeitung ihrer Daten zu schützen, welche die Analyse oder Voraussage bestimmter Merkmale ihrer Person oder Lebenssituation bezwecken. Schutzvoraussetzung ist, dass die Bearbeitung die Betroffenen in massgeblicher Weise beeinträchtigt oder ihnen gegenüber rechtliche Wirkungen entfaltet. Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, sollen Betroffene gemäss Art. 19 Abs. 2 des Vorschlags das Recht erhalten, unentgeltlich Widerspruch einzulegen.

Die U.S.-amerikanische Behörde für Verbraucherschutz und Wettbewerbsrecht (Federal Trade Commission FTC) hat die Internetindustrie zur Einrichtung einer „Do-Not-Track"-Option aufgefordert. Diese soll Konsumenten die Entscheidung überlassen, welche Informationen über ihre Online-Aktivitäten geteilt werden sollen, als auch mit wem und zu welchem Zweck (im Vordergrund stehen hier Massnahmen des direkten Marketing) [72].

Der Trans Atlantic Consumer Dialogue (TACD)[73] erliess eine Resolution zu sozialen Netzwerken[74]. Gefordert wird der Erlass von Gesetzen, die u.a. vorsehen, dass soziale Netzwerke den Zugang zu ihren Diensten nicht von der Zustimmung der Nutzenden zur Verwendung ihrer Daten zu Marketingzwecken abhängig machen. Zudem soll die ausdrückliche Einwilligung der Nutzenden in die Datensammlung zu Marketingzwecken zwingend sein und Kinder unter 16 Jahren sowie Webseiten, die mehrheitlich von diesen besucht werden, grundsätzlich von Werbemassnahmen ausgenommen sein.

4.3.2.3 Rechtslage in der Schweiz

Die Ansammlung und Zusammenführung der durch Nutzeraktivitäten entstehenden Daten führt in vielen Fällen zu der Erstellung von Persönlichkeitsprofilen i.S.v. Art. 3 Bst. d DSG. Das Datenschutzgesetz stellt besondere Anforderungen an die Bearbeitung von Persönlichkeitsprofilen (Art. 4 Abs. 5, Art. 11a Abs. 3 Bst. a, Art. 12 Abs. 2 Bst. c, Art. 14 DSG).

---

[70] Empfehlung CM/Rec(2010)13.

[71] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endgültig.

[72] Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, FTC Report March 2012; zu finden unter: http://www.ftc.gov/opa/2012/03/privacyframework.shtm . Der Bericht über den Schutz der Privatsphäre von Konsumenten im Internet enthält Empfehlungsrichtlinien für die Internetindustrie. Gefordert wird u.a. auch, dass Unternehmen ihre Internetdienste so entwickeln, dass ein hoher Schutz der Privatsphäre automatisch vorgesehen ist (privacy by design) und Konsumenten umfassend über Zweck, Umfang und Art der Datenverwendung aufgeklärt werden.

[73] Der TACD ist ein Forum U.S.-amerikanischer sowie europäischer Verbraucherverbände, das Verbraucherschutzempfehlungen für die U.S. Regierung und die Europäische Union erarbeitet; siehe: http://www.tacd.org/.

[74] Resolution on Social Networking of May 2010, Doc No. Infosoc 43-09; zu finden unter: http://tacd.org/index.php?option=com_docman&task=cat_view&gid=83&Itemid=40.

Erstellen Plattformbetreiber durch Datenverknüpfung Persönlichkeitsprofile, so mag infolge mangelnder Erkennbarkeit dieser Verknüpfung der Grundsatz von Treu und Glauben (Art. 4 Abs. 2 DSG) verletzt sein. Überdies kommt hier die Informationspflicht des Inhabers einer Datensammlung gegenüber den Betroffenen bei der Beschaffung von Persönlichkeitsprofilen (Art. 14 DSG) zum Tragen. Auch die Übertragung von Nutzerdaten an Facebook durch die Einbettung des „like-Buttons" auf Webseiten Dritter kann mangels Aufklärung der Webseitenbesucher über die erfolgende Datenübertragung gegen den Grundsatz der Erkennbarkeit verstossen (Art. 4 Abs. 4 DSG). Überdies vermag die Angabe sehr allgemeiner Bearbeitungszwecke zum Zeitpunkt der Datenerhebung, wie beispielsweise die Erstellung und Bearbeitung von Nutzerprofilen „zu Marketingzwecken", dem Zweckbindungsgrundsatz (Art. 4 Abs. 3 DSG) nicht zu genügen. Nutzenden ist zum Zeitpunkt der Datenbeschaffung häufig nicht ausreichend bewusst, wozu ihre zu Nutzerprofilen zusammengefügten Daten später verwendet werden.

Die Sammlung einer Vielzahl von Personendaten und deren Zusammenstellung zu Persönlichkeitsprofilen kann auch im Konflikt mit dem Grundsatz der Verhältnismässigkeit der Datenbearbeitung (Art. 4 Abs. 2 DSG) stehen. Überdies kann auch der Grundsatz der Datenrichtigkeit (Art. 5 DSG) im Zusammenhang mit der Erstellung von Persönlichkeitsprofilen betroffen sein: Das automatisierte Sammeln, Zusammenführen und Auswerten von Daten führt zum Verlust des ursprünglichen Kontexts, in welchem die Daten entstanden sind, und kann u.U. in Falschaussagen resultieren[75].

Relevant ist insbesondere, dass die Einwilligung der Betroffenen bei Persönlichkeitsprofilen ausdrücklich zu sein hat (Art. 4 Abs. 5 DSG). Dies erhöht die Anforderungen an die Informationen über die Erstellung, Verwendung und Weitergabe von Persönlichkeitsprofilen, insbesondere wenn diese in AGBs enthalten sind. Die Ausdrücklichkeit einer Einwilligung dürfte beispielweise dann zweifelhaft sein, wenn bestimmte ungewöhnliche Bearbeitungszwecke oder Bekanntgaben an Dritte nicht besonders hervorgehoben werden. Eine ausdrückliche Einwilligung ist erforderlich, wenn die Bearbeitung von Persönlichkeitsprofilen entgegen den Bearbeitungsgrundsätzen oder die Bekanntgabe von Persönlichkeitsprofilen an Dritte durch die Einwilligung der Betroffenen gerechtfertigt werden soll (Art. 13 Abs. 1 i.V.m. Art. 4 Abs. 5 DSG). Dies ist im Zusammenhang mit sozialen Netzwerken von besonderer Bedeutung, da deren Geschäftsmodelle üblicherweise auf dem Verkauf von Nutzerprofilen basieren, was als Datenbekanntgabe an Dritte zu qualifizieren ist.

Einen besonderen Schutz von Kindern vor der Erstellung und Bearbeitung von Persönlichkeitsprofilen kennt das DSG nicht. Hier sind allerdings wieder die Besonderheiten der Einwilligung in die Bearbeitung der Personendaten eines Kindes zu berücksichtigen (siehe vorne Kap. 4.3.1.3.). Es existiert auch kein grundsätzliches Verbot, gegenüber Kindern unter 16 Jahren oder auf diese ausgerichteten Webseiten werbend tätig zu werden.

Das **Fernmeldegeheimnis** in Art. 43 FMG und Art. 321ter StGB schützt die Vertraulichkeit der Telekommunikation. Es kann aber in aller Regel nicht vor dem Erstellen von Persönlichkeitsprofilen schützen. Nur in den Ausnahmefällen, in denen Plattformbetreiber zwischen mehreren Nutzenden Informationen transportieren, würde das Fernmeldegeheimnis diese Nutzenden davor schützen, dass die Daten ihres Fernmeldeverkehrs an Dritte weitergegeben und für die Erstellung von Nutzerprofilen verwendet werden.

4.3.3 Fehlendes Recht auf Vergessenwerden

4.3.3.1 Ausgangslage

Die mangelhafte Kontrolle Nutzender über ihre Daten in sozialen Netzwerken manifestiert sich auch in der Schwierigkeit, Benutzerkonten unwiderruflich zu löschen. Meistens umfasst die Abmeldung eines Kontos nur die Deaktivierung eines Profils, wobei die Daten auf dem Server des Plattformbetreibers weiterhin aufbewahrt werden. Die endgültige Löschung sämtlicher Inhalte ist zwar oft, aber nicht im-

[75] Schweizer Alex, Data Mining – ein rechtliches Minenfeld. Rechtliche Aspekte von Methoden des Customer Relationship Management (CRM) wie Data Mining, in: digma 2001 S. 108, 109.

mer möglich. Sie gestaltet sich ausserdem sehr kompliziert, sodass der Vorgang Nutzende abschrecken oder von diesen nicht verstanden werden kann. Überdies können aktive Nutzende viele Informationen und Inhalte auf anderen Seiten und Profilen des Netzwerks hinterlassen. Diese allumfassend zu löschen, ist in der Praxis kaum möglich.

Der Nutzen einer allfälligen Löschung des Ursprungsprofils wird auch dadurch geschmälert, dass es auf gewissen Plattformen möglich ist, Daten aus Nutzerprofilen Dritter herunterzuladen und zu speichern. Dies kann zu einer Unzahl privater Datensammlungen führen. Auch wenn Nutzende ihr Ursprungsprofil löschen, können ihre Daten so an einem anderen Ort gespeichert bleiben. Darüber hinaus haben Dritte weitere Möglichkeiten für eine Datenarchivierung (bspw. durch screenshots) und eine allfällige spätere Wiederveröffentlichung.

4.3.3.2 Lösungsansätze im Ausland oder internationalen Recht

Die Europarats-Empfehlung zu sozialen Netzwerken sowie der Vorschlag zu einer EU-Datenschutz-Grundverordnung[76] sehen unter gewissen Voraussetzungen das Recht auf Vergessenwerden, die Löschung personenbezogener Daten sowie die Unterlassung jeglicher weiteren Datenverbreitung vor.[77] Im Besonderen wird das Recht von Kindern auf Vergessenwerden und Datenlöschung vorgesehen[78].

Auch der Entwurf zur Änderung des Deutschen Telemediengesetzes sieht ein Recht auf Löschung von Nutzerkonten in sozialen Netzwerken und sämtlicher von Nutzenden generierter Inhalte vor[79].

4.3.3.3 Rechtslage in der Schweiz

Beim Recht auf Vergessenwerden in sozialen Netzwerken handelt es sich grundsätzlich um den Anspruch, dass Inhalte, welche Nutzende sozialer Netzwerke veröffentlicht haben, wieder gelöscht werden. Löschansprüche können sich aus dem Datenschutzgesetz sowie dem zivilrechtlichen Persönlichkeitsschutz ableiten lassen.

Das **Datenschutzrecht** untersagt die Bearbeitung von personenbezogenen Daten gegen den ausdrücklichen Willen einer Person (Art.12 Abs. 2 Bst. b DSG). Da die Aufbewahrung und Archivierung von Personendaten Gegenstand eines ausdrücklichen Bearbeitungsverbots sein kann, lässt sich mithilfe des Widerspruchsrechts grundsätzlich auch eine umfassende oder teilweise Löschung von Personendaten verlangen[80]. Auch kann die Einwilligung gemäss Art. 13 Abs. 1 DSG, mittels welcher persönlichkeitsverletzende Datenbearbeitungen gerechtfertigt werden, grundsätzlich widerrufen werden. Der Widerruf ist allerdings nur für zukünftige, nicht für abgeschlossene Datenbearbeitungen wirksam[81]. Wurde also in eine zeitlich unbeschränkte Aufbewahrung von Daten eingewilligt, kann diese Einwilligung grundsätzlich für die zukünftige Datenspeicherung widerrufen werden.

Verstossen Dritte ohne Rechtfertigungsgrund gegen die Bearbeitungsgrundsätze des Datenschutzgesetzes, so kann sich aus Art. 15 Abs. 1 DSG ein Anspruch auf Löschung der betroffenen Daten ergeben. Zu denken ist hier etwa an Fälle, in denen andere Nutzende die Personendaten der Betroffenen in sozialen Netzwerken publizieren, ohne dass dies für die Betroffenen erkennbar war (Art. 4 Abs. 2 und 4 DSG). Möglich ist auch, dass sie besonders schützenswerte Personendaten oder Persönlichkeitsprofile einer Person ohne Rechtfertigung anderen Netzwerkmitgliedern oder Drittunternehmen

---

[76] Art. 17 Vorschlag EU Datenschutz-Grundverordnung, KOM(2012) 11 endgültig.

[77] Vgl. dazu Treyer Tobias, Das „Recht auf Vergessen“ im digitalen Zeitalter, in: medialex 2013, S. 61f.

[78] Art. 17 Abs. 1 Vorschlag EU Datenschutz-Grundverordnung, KOM(2012) 11 endgültig. Siehe auch die Erklärung des Europarats zum Schutz der Würde, Sicherheit und Privatsphäre von Kindern im Internet.

[79] Gesetzesentwurf Änderung Telemediengesetz, 17/6765.

[80] Rosenthal David / Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, S. 362 N. 32.

[81] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, S. 118ff. N. 104ff.

bekanntgegeben (Art. 12 Abs. 2 Bst. c DSG), Personendaten einer Person zu einem anderen als bei deren Beschaffung ersichtlichen Zweck bearbeiten (beispielsweise indem in sozialen Netzwerken in einem bestimmten Forum oder zu einem bestimmten Thema getätigte Äusserungen in einem zweckfremden Kontext wiederverwendet werden)[82] oder Personendaten gegen den ausdrücklichen Willen der Betroffenen bearbeiten (Art. 12 Abs. 2 Bst. b DSG).

Auch aus dem **zivilrechtlichen Persönlichkeitsschutz** (Art. 28 ZGB) lassen sich Argumente für einen Löschanspruch ableiten, die allerdings von einer Abwägung der auf dem Spiel stehenden Interessen abhängen bzw. von der Frage, ob Rechtfertigungsgründe vorliegen, welche die Widerrechtlichkeit einer Persönlichkeitsverletzung aufheben. Art. 28 ZGB umfasst verschiedene Teilgehalte. Ein Recht auf Vergessenwerden kann mittels Berufung auf den Schutz der seelischen Integrität, der Privatsphäre, der Ehre, des Rechts am eigenen Bild, Namen oder Wort geltend gemacht werden. Art. 28 ZGB untersagt Dritten, Inhalte aus dem Geheim- oder Privatbereich oder Fotos einer Person ohne deren Einwilligung (oder andere gültige Rechtfertigungsgründe) zu beschaffen oder zu publizieren. Art. 28a Abs. 1 Ziff. 2 ZGB gibt Betroffenen den Anspruch, eine bestehende Verletzung zu beseitigen, womit grundsätzlich auch eine Löschung von persönlichkeitsverletzenden Inhalten im Internet erwirkt werden kann. Veröffentlichen Nutzende in sozialen Netzwerken Inhalte über sich selbst und werden diese anschliessend von Dritten bearbeitet, so ist zu beachten, dass eine für einen bestimmten Zweck erteilte Einwilligung nicht auch andere Verwendungszwecke umfasst[83]. Zivilrechtlich problematisch ist es beispielsweise, wenn von einer Person gemachte Äusserungen für Falschzitate genutzt werden[84], von einer Person publizierte Fotos ohne deren Einwilligung in einem anderen Zusammenhang oder zweckfremd verwendet werden[85] oder der Name einer Person persönlichkeitsverletzend genutzt wird[86]. Auch ist davon auszugehen, dass eine einmal erteilte Einwilligung widerrufen werden kann, wobei auch hier das Bestehen eines Löschanspruchs vom Ergebnis der konkreten Interessenabwägung abhängt[87].

Für das Bestehen eines allfälligen Löschanspruchs spielt auch eine Rolle, in welcher Form der Betroffene Inhalte publiziert hat (private oder öffentliche Kommunikation?), welcher Natur diese Inhalte sind (fallen sie in den Geheim-, Privat- oder Öffentlichkeitsbereich?) und um was für eine Person es sich bei dem Betroffenen handelt. Wurden die Inhalte von den Betroffenen selbst allgemein zugänglich gemacht (i.S.v. Art. 12 Abs. 3 DSG), so wird diesem Umstand im Rahmen der Interessenabwägung bezüglich eines geltend gemachten Löschanspruchs zugunsten des Plattformbetreibers Rechnung zu tragen sein (Art. 13 Abs. 1 DSG; Art. 28 Abs. 2 ZGB). Je persönlichkeitsrelevanter die Daten, desto schwerer wird jedoch das Interesse des Betroffenen an einer Löschung wiegen, selbst wenn er diese zu einem anderen Zeitpunkt selbst publiziert hat. Handelt es sich bei den Betroffenen um absolute oder relative Personen der Zeitgeschichte[88] oder um Amtsträger, so kann ein schutzwürdiges Informationsinteresse der Allgemeinheit einer Löschung von Inhalten entgegenstehen. Mit entsprechendem Zeitablauf kann ein Anspruch auf Vergessenwerden allerdings auch für sie wieder aufleben[89]. Sollen Personendaten, welche veröffentlicht wurden als der Betroffene noch im Kindesalter war, gelöscht werden, ist ein Eingriff in dessen Persönlichkeit aufgrund der besonderen Schutzbedürftigkeit und zum

---

[82] Dies könnte die Grundsätze der Zweckbindung und der Datenrichtigkeit (Art. 4 Abs. 3 und 5 DSG) betreffen.

[83] BSK-ZGB I, Meili Andreas, 4. Aufl., Basel 2010, Art. 28, S. 269 Rz. 48.

[84] Schweizer Michael, Das Recht am Wort nach Art. 28 ZGB, in: medialex 2011 S. 197, 199.

[85] BSK-ZGB I, Meili Andreas, 4. Aufl., Basel 2010, Art. 28, S. 260 Rz. 20 mit dem Hinweis, dass in der Praxis digitale und herkömmliche Bildretouchen, Fotomontagen und eigentliche Bildmanipulationen, wie auch die Verwendung von Archivbildern in einem ganz anderen Zusammenhang als zum Zeitpunkt der Herstellung der Fotografie, immer wieder zu Problemen führen.

[86] BSK-ZGB I, Meili Andreas, 4. Aufl., Basel 2010, Art. 28, S. 320 Rz. 1.

[87] BSK-ZGB I, Meili Andreas, 4. Aufl., Basel 2010, Art. 28, S. 259 Rz. 48.

[88] Sportler, Politiker, Künstler, Wirtschaftsführer und andere Prominente etwa sind absolute Personen der Zeitgeschichte; relative Personen der Zeitgeschichte sind Personen, welche durch ein bestimmtes Ereignis das Interesse der Öffentlichkeit auf sich ziehen. Siehe BSK-ZGB I, Meili Andreas, 4. Aufl., Basel 2010, Art. 28, S. 271 Rz. 52.

[89] Siehe bspw. BGE 109 II 353 E. 3 sowie BSK-ZGB I, Meili Andreas, 4. Aufl., Basel 2010, Art. 28, S. 271 Rz. 52.

Teil eingeschränkten Einsichtsfähigkeit von Kindern grundsätzlich wohl schneller zu bejahen als wenn Daten Erwachsener betroffen sind.

Ein weiteres Problem, welches dem Recht auf Vergessenwerden zuzuordnen ist, ist der digitale Nachlass bzw. der Umgang mit den von Verstorbenen im Internet hinterlassenen Daten. Das Erb-, Personen- und Datenschutzrecht bieten hier nur eine lückenhafte Lösung[90].

Aus der Analyse ergibt sich, dass das geltende Recht in gewissem Umfang ein Recht auf Vergessenwerden garantiert, welches allerdings durch entgegenstehende Interessen (bspw. Informationsinteresse der Allgemeinheit, Verhältnismässigkeit der einem Plattformbetreiber auferlegten Massnahmen etc.) in grundsätzlich sinnvoller Weise beschränkt wird.[91]

Trotz Vorliegen gewisser rechtlicher Möglichkeiten zur Entfernung gewisser Inhalte mag es sich allerdings als äusserst kompliziert erweisen, deren umfassende Löschung in sozialen Netzwerken zu erwirken. Dieses Problem spitzt sich zu, wenn eine Vielzahl Dritter die betroffenen Inhalte bereits heruntergeladen oder weiterverwendet hat.

Im Evaluationsbericht zum DSG hat der Bundesrat eine Präzisierung des Rechts auf Vergessenwerden in Erwägung gezogen.[92]

4.3.4 Auffindbarkeit von Daten aus Nutzerprofilen in Suchmaschinen

4.3.4.1 Ausgangslage

Mittels Metadaten, welche in Webseiten eingebaut werden, können die Suchroboter von Suchmaschinen aufgefordert werden, bestimmte Inhalte und Seiten nicht in ihrem Index oder Zwischenspeicher aufzunehmen. Betreiber sozialer Netzwerke können den Zugriff von Suchmaschinen auf Nutzerdaten folglich gestalten. Problematisch sind soziale Netzwerke, die Nutzenden die Entscheidungsbefugnis darüber entziehen, ob die von ihnen in sozialen Netzwerken bereitgestellten Daten in internen oder externen Suchmaschinen auffindbar sind.

4.3.4.2 Lösungsansätze im Ausland oder internationalen Recht

Die Empfehlung des Europarats zum Schutz der Menschenrechte mit Bezug auf Suchmaschinen[93] verlangt ein Recht Nutzender Suchmaschinenbetreiber zur umgehenden Löschung ihrer persönlichen Daten auffordern zu können, falls diese in Kopien bereits gelöschter originaler Webseiten weiterhin von Suchmaschinen gespeichert werden. Zudem soll Nutzenden ein Recht zukommen, von Suchmaschinenbetreibern die Löschung und Korrektur der über sie bearbeiteten Daten zu verlangen. Die Europarats-Empfehlung zu sozialen Netzwerken fordert, dass Nutzenden die Möglichkeit einer informierten Entscheidung über die Indexierung ihrer Daten sowie das Recht zur Entfernung ihrer Daten in Suchmaschinenzwischenspeichern einzuräumen ist.

Auch der Entwurf zur Änderung des deutschen Telemediengesetzes fordert, dass Nutzerkonten und nutzergenerierte Inhalte in externen Suchmaschinen nur nach vorheriger Einwilligung der Nutzenden auffindbar sind[94].

---

[90] Hierzu ausführlich Studer Melanie/Schweizer Matthias/Brucker-Kley Elke, Sterben und Erben in der digitalen Welt, in: Jusletter 17.12.2012.

[91] Nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte gibt die EMRK den Betroffenen keinen Anspruch auf Löschung rechtswidriger Medienpublikationen aus Online-Archiven. Es sei nicht Sache der Justiz, alle Spuren unrechtsmässiger Veröffentlichungen zu beseitigen: EGMR-Urteil „Wegrzynowski & Smolczewski c. Polen“ (Beschwerdenr. 33846/07) vom 16.7.2013, Ziff. 65.

[92] Bericht zur Evaluation des Bundesgesetzes über den Datenschutz vom 9.12.2011, Ziff. 5.2.2 (BBl 2012 350).

[93] Empfehlung CM/Rec(2012)3 zum Schutz der Menschenrechte mit Bezug auf Suchmaschinen.

[94] Gesetzesentwurf Änderung Telemediengesetz, 17/6765.

4.3.4.3 Rechtslage in der Schweiz

Erlauben soziale Netzwerke den Zugriff von Suchmaschinen auf Personendaten der Netzwerkmitglieder, so liegt eine Datenbekanntgabe im Sinne des Datenschutzgesetzes (Art. 3 Bst. e und f DSG) vor, auf welche die Datenbearbeitungsgrundsätze anwendbar sind. Der Grundsatz der Erkennbarkeit der Datenbeschaffung (Art. 4 Abs. 4 DSG) gewährt Betroffenen ein Recht über die Zugänglichkeit ihrer in sozialen Netzwerken veröffentlichten Personendaten für Suchmaschinen informiert zu werden, sofern diese nicht aus den Umständen ersichtlich ist.

In Anbetracht der Vielzahl der in sozialen Netzwerken veröffentlichten Daten und deren oft sehr persönlichem Charakter, dürften häufig besonders schützenswerte Personendaten oder Persönlichkeitsprofile vorliegen. In den überwiegenden Fällen wird folglich mangels Vorliegen anderer Rechtfertigungsgründe (Art. 13 Abs. 1 DSG) die Einholung einer ausdrücklichen Einwilligung (Art. 4 Abs. 5 DSG) in die Suchmaschinenzugänglichkeit von Nutzerdaten erforderlich sein. Aus dem Zweckbindungsgrundsatz folgt, dass Dritte - in diesem Fall Suchmaschinenbetreiber - grundsätzlich auch an den bei der Datenbeschaffung vorliegenden Bearbeitungszweck gebunden sind[95].

Umgehen Suchmaschinenbetreiber einschränkende Angaben der Betreiber sozialer Netzwerke an Suchroboter bezüglich der Zugriffsmöglichkeiten auf Nutzerdaten, sammeln diese Daten dennoch und machen sie öffentlich zugänglich, so ist dieses Vorgehen aufgrund der Heimlichkeit[96] der Datenbeschaffung allenfalls als unrechtmässig (Art. 4 Abs. 1 DSG) zu qualifizieren.

4.3.5 Probleme der Bilderkennung

4.3.5.1 Ausgangslage

Auf soziale Netzwerke hochgeladene Fotos mit erkennbaren Personen und diesen zugeordneten Benutzerprofilen können der Entwicklung und Verbesserung von Gesichtserkennungs-Software dienen. Diese kann Personen auf später veröffentlichten Fotos mit den gesammelten Daten abgleichen und einem Benutzerprofil zuordnen. Laden Dritte Bilder, auf welchen andere Netzwerkmitglieder abgebildet sind, auf eine Plattform, so kann eine derartige Software die Verbindung der Abgebildeten mit einem angemeldeten Profil vorschlagen („tag-suggest“)[97]. Überdies kann Gesichtserkennungs-Software an Anonymität interessierte Personen (z.B. auf einer Dating-Webseite) identifizieren oder dank des Fotos auf der sozialen Plattform und dem dazugehörigen Namen mit ihrem Lebenslauf auf einer Firmenwebseite in Verbindung bringen.

In eine ähnliche Richtung geht die automatische Wiedererkennung von anderen auf Bildern enthaltenen Informationen basierend auf Umrissen, Farben oder Oberflächenstruktur der dargestellten Objekte (*content based image retrieval*). Die Funktion kann Gebäude oder spezifische Gegenstände identifizieren und möglichweise zu der geografischen Lokalisierbarkeit einer Fotosituation führen, die Offenlegung von Adressen, Stalking oder andere schädliche oder illegale Handlungen zur Folge haben.

4.3.5.2 Lösungsansätze im Ausland oder internationalen Recht

In Erfüllung der Forderungen des irischen Datenschutzbeauftragten stellte Facebook seine Gesichtserkennungssoftware innerhalb der Europäischen Union ein[98]. Der Kompromiss war Teilergebnis einer allgemeinen Überprüfung der Vereinbarkeit der Dienste des Unternehmens mit dem Datenschutzrecht Irlands und der Europäischen Union. Laut EDÖB gilt die Einigung auch für die Schweiz.

---

[95] Rosenthal David /Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, S. 95 N. 47.

[96] Die heimliche Datenbeschaffung verstösst grundsätzlich gegen die Grundsätze von Treu und Glauben sowie der Erkennbarkeit der Datenbearbeitung (Art. 4 Abs. 2 und 4 DSG).

[97] Person A prüft also zum Beispiel die von Person B erstellten Fotos mit einem Bilderkennungsprogramm, erkennt Person C und benennt sie auf dem Foto.

[98] Report of Re-Audit Facebook Ireland Ltd of the Data Protection Commissioner from 21.09.2012; zu finden unter: http://dataprotection.ie/viewdoc.asp?DocID=1233&m=f.; Driessen Benedikt / Dürmuth Markus, Anonymität und Gesichtserkennung, in: digma 2013, S. 54.

Die Europarats-Empfehlung zu sozialen Netzwerken verlangt, dass Technologien, welche einen entscheidenden Einfluss auf die Privatsphäre Nutzender haben (da sie beispielsweise auf der Bearbeitung sensibler oder biometrischer Daten basieren, wie etwa Gesichtserkennungssoftware), einen erhöhten Datenschutz garantieren und nicht ohne Einwilligung der Nutzenden eingesetzt werden sollen.

Die Art. 29-Datenschutzgruppe, ein unabhängiges Beratungsgremium der Europäischen Kommission, befasste sich in einer Stellungnahme zur Gesichtserkennung bei Online- und Mobilfunkdiensten[99] mit den datenschutzrechtlichen Risiken dieser Technologie und erliess Empfehlungen an die Datenbearbeiter bezüglich der Einholung gültiger Einwilligungen der Betroffenen sowie der Verschlüsselung der übertragenen Daten und deren sicheren Aufbewahrung.

4.3.5.3 Rechtslage in der Schweiz

Damit Gesichtserkennungssoftware in sozialen Netzwerken überhaupt zur Anwendung gelangen kann, müssen in einem ersten Schritt Fotos auf einer derartigen Plattform veröffentlicht werden. Als Teilgehalt von Art. 28 Abs. 1 ZGB schützt das Recht am eigenen Bild den Einzelnen vor der widerrechtlichen Verwendung seines eigenen Erscheinungsbildes[100]. Ohne vorgängige oder nachträgliche Einwilligung darf grundsätzlich niemand abgebildet und eine bestehende Aufnahme nicht veröffentlicht werden; überdies umfasst die Einwilligung in die Aufnahme eines Fotos nicht jede denkbare folgende Veröffentlichung, sondern grundsätzlich nur jene, welche bei der Erstellung des Bildes für den Betroffenen ersichtlich war[101].

Auch das Datenschutzrecht, dessen privatrechtliche Bestimmungen den allgemeinen Persönlichkeitsschutz ergänzen und konkretisieren[102], schützt davor, dass Bilder einer Person[103] ohne deren Kenntnis veröffentlicht werden. Der Grundsatz der Erkennbarkeit der Datenbeschaffung (Art. 4 Abs. 4 DSG) verlangt, dass es für die Abgebildeten zumindest aus den Umständen ersichtlich ist, wenn Bilder von ihnen in sozialen Netzwerken veröffentlicht werden. Überdies garantiert der Grundsatz der Zweckbindung, dass Personendaten nur zu dem Zweck bearbeitet werden, welcher bei der Beschaffung feststand. Die Veröffentlichung von Fotos einer Person in sozialen Netzwerken ist somit mangels Rechtfertigung (Art. 13 Abs. 1 DSG) nur zulässig, wenn bei Aufnahme der Fotografie ersichtlich war, dass diese in einem sozialen Netzwerk veröffentlicht werden soll.

Wurden Fotos von Personen in sozialen Netzwerken veröffentlicht, so ist deren Analyse und Verbindung mit Nutzerprofilen durch Gesichtserkennungssoftware nur zulässig, wenn die Betroffenen über diese Form der Verwendung informiert waren[104], was in keinem Fall auf jene Fotos zutreffen wird, welche Dritte ohne Einwilligung der Betroffenen veröffentlicht haben. Regelmässig werden Fotografien als besonders schützenswerte Personendaten zu qualifizieren sein (Art. 3 Bst. c DSG), was dementsprechend erhöhte Datenschutzanforderungen zur Folge hat[105]. Grundsätzlich verstösst die Anwendung einer automatischen Gesichtserkennungssoftware verbunden mit der Funktion des „tag-suggest“ wohl auch gegen den Grundsatz der Verhältnismässigkeit der Datenbearbeitung (Art. 4 Abs. 2 DSG).

Fraglich ist, wie die Situation zu qualifizieren ist, in der eine Person ihre eigenen Fotos wissentlich und willentlich in einem sozialen Netzwerk veröffentlicht und ihr Profil mittels Nutzungseinstellungen allge-

---

[99] Art. 29-DSG Stellungnahme 00727/12/DE WP 192.

[100] Bächli Marc, Das Recht am eigenen Bild, Basel 2002, S. 69.

[101] Es sein denn, es liegt ein gültiger Rechtfertigungsgrund i.S.v. Art. 28 Abs. 2 ZGB vor. Eine Schranke findet das Recht am eigenen Bild etwa an berechtigten Publikationsinteressen (Meinungsfreiheit gemäss Art. 10 EMRK); vgl. zur entsprechenden Strassburger Rechtsprechung Zeller Franz, Das eigene Bild und sein begrenzter Schutz, in: digma 2013/2, S. 50ff.

[102] Schweizer Michael, Recht am Wort, Bern 2012, S. 209.

[103] Unter den Personendatenbegriff des Datenschutzgesetzes fallen auch Bilder von Personen, sofern sich diese einer Person zuordnen lassen; folglich sind auch Fotografien erfasst.

[104] Dies ergibt sich aus den Anforderungen an die Einwilligung gemäss Art. 28 Abs. 2 ZGB bzw. Art. 13 Abs. 1 DSG sowie aus den Grundsätzen von Treu und Glauben sowie der Zweckbindung der Datenbearbeitung gemäss Art. 4 Abs. 2 und 3 DSG.

[105] Siehe Art. 4 Abs. 5, Art. 11a Abs. 3 Bst. a, Art. 12 Abs. 2 Bst. c sowie Art. 14 DSG.

mein zugänglich gemacht hat (Art. 12 Abs. 3 DSG). Werden allgemein zugänglich gemachte Personendaten zu Zwecken bearbeitet, für welche sie nach den Umständen bei objektiver Betrachtung nicht zugänglich gemacht wurden, so kann dennoch eine Persönlichkeitsverletzung vorliegen[106]. In Anbetracht der relativen Neuartigkeit des Einsatzes von Gesichtserkennungssoftware, können Zweifel daran bestehen, ob eine Person, die ihre Fotos allgemein zugänglich macht, sie auch zu Zwecken einer derartigen Bearbeitung veröffentlicht hat. Auch in diesem Fall müsste das Vorliegen einer Einwilligung in die konkrete Bearbeitung geprüft werden[107].

Was die automatische Wiedererkennung von Merkmalen und Gegenständen auf Bildern durch Softwareprogramme anbelangt, so sind diese Informationen als Sachdaten zu qualifizieren. Sachdaten sind immer dann Personendaten im Sinne des Datenschutzgesetzes, wenn sie mit einer Person in Verbindung gebracht werden können. Als Beispiele sind etwa Grundstücke oder Motorfahrzeuge zu nennen[108]. In diesem Fall geniessen auch sie datenschutzrechtlichen Schutz.

4.3.6 Probleme der Geolokalisierung (Ortungstechnologie)

4.3.6.1 Ausgangslage

Gewisse soziale Netzwerke bieten Dienste an, welche Nutzende (deren Daten üblicherweise über Smartphones übermittelt werden) unter Verwendung von Ortungstechnologien wie GPS oder WLAN, orten und mit gewünschten lokalitätsbezogenen Informationen versorgen. Gewisse soziale Netzwerke spezialisieren sich sogar gänzlich auf derartige Geolokalisierungsdienste[109]. Je nach Kommunikationsverhalten der Nutzenden können Plattformbetreiber eine Vielzahl von Daten mit den erhobenen Geodaten verbinden. So wissen sie unter Umständen nicht nur ungefähr wo sich Nutzende aufhalten, sondern möglicherweise sogar in welchem Gebäude (Bsp.: Kino, Restaurant etc.), mit wem, was sie dort tun und wie es ihnen gefällt.

Die Verbindung solcher Ortungsdienste mit sozialen Netzwerken kann dazu führen, dass Nutzende bewusst oder unbewusst Informationen über ihre Aufenthaltsorte und dortigen Aktivitäten mitteilen, die Aussenstehende für von Nutzenden nicht beabsichtigte Zwecke verwenden können. Schädliches Verhalten wie Identitätsdiebstahl, Cybermobbing, Cyberstalking oder Cybergrooming können durch derartige Technologien erleichtert werden. Überdies können lokalitätsbezogene Daten Dritte darüber in Kenntnis setzen, wo sich Betroffene aufhalten und wo diese leben und somit etwa die Vornahme von Einbrüchen begünstigen[110].

4.3.6.2 Lösungsansätze im Ausland oder internationalen Recht

Die Art. 29-Datenschutzgruppe[111] befasste sich in einer Stellungnahme vom Mai 2011 mit den datenschutzrechtlichen Risiken von Geolokalisierungsdiensten[112]. Zentrales Thema ist die Einwilligung der Nutzenden, welche gemäss der Stellungnahme ungültig ist, wenn sie auf der zwingenden Annahme von AGBs beruht oder lediglich die Möglichkeit des „Opt-out“ besteht. Geolokalisierungsdienste sollten grundsätzlich ausgeschaltet sein mit der Möglichkeit des „Opt-in“ für die Nutzenden. Auf ungewöhnliche Bearbeitungszwecke sollen Nutzende explizit aufmerksam gemacht werden, bspw. auf die Erstellung von Profilen oder die Vornahme des Behavioural Targeting. Werden Nutzende über Änderungen des Bearbeitungszwecks oder eine Datenweitergabe informiert, so soll ihr Schweigen nicht als Einwilligung gewertet werden dürfen. Endgeräte sollen Nutzende durch ein Warnsymbol darauf hinweisen,

---

[106] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, S. 381 N. 76.

[107] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, S. 383 N. 84.

[108] BSK-DSG, Belser Urs, 2. Aufl., Basel 2006, Art. 3, S. 64 Rz. 5. In diesem Sinne auch BGE 138 II 346 E. 6.2.

[109] Siehe etwa Foursquare (https://foursquare.com/) oder Friendticker (http://en.friendticker.com/).

[110] Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zürich 2012, S. 162f.

[111] http://www.edps.europa.eu/EDPSWEB/edps/lang/de/Cooperation/Art29

[112] Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten vom 16.05.2011, 881/11/DE WP 185.

wann ein Geolokalisierungsdienst in Betrieb ist und Diensteanbieter auch ohne Veränderungen der Dienstleistung die Einwilligung Nutzender regelmässig erneut einholen. Auch sollen die Aufbewahrungsfristen zweckgemäss kurz ausgestaltet werden und Nutzende ein Recht auf Information in lesbarem Format sowie auf Änderung und Löschung ihrer Daten haben.

4.3.6.3 Rechtslage in der Schweiz

Geodaten stellen Personendaten im Sinne der Datenschutzgesetzgebung dar, wenn eine Verknüpfung mit einer natürlichen oder juristischen Person besteht oder mit vernünftigem Aufwand hergestellt werden kann[113]. Durch die Ortung von Personen zugeordneten mobilen Endgeräten und das Zusammenfügen von Sach- und Personendaten können überdies Persönlichkeitsprofile oder besonders schützenswerte Personendaten entstehen[114], an deren Bearbeitung das Datenschutzgesetz erhöhte Anforderungen stellt. Die datenschutzrechtlichen Risiken der Geolokalisierungsdienste sozialer Netzwerke werden grundsätzlich von den Bearbeitungsgrundsätzen des Datenschutzgesetzes erfasst.

So gelangt beispielsweise der Grundsatz der *Verhältnismässigkeit* (Art. 4 Abs. 2 DSG) zur Anwendung, wenn mehr Daten gesammelt und verknüpft werden als für den Bearbeitungszweck erforderlich ist – allenfalls bedingt der Verhältnismässigkeitsgrundsatz sogar die Anonymisierung geokodierter Daten[115].

Der Grundsatz der *Zweckbindung* (Art. 4 Abs. 3 DSG) erfasst Abänderungen des Bearbeitungszwecks, wenn Plattformbetreiber die erhobenen Personendaten aufgrund ihrer Nützlichkeit im Nachhinein für neue Zwecke verwenden. Die Generierung von gewöhnlichen Personendaten, Persönlichkeitsprofilen oder besonders schützenswerten Personendaten mittels Verknüpfung von Geo- und weiteren in sozialen Netzwerken veröffentlichten Daten müssen für die Betroffenen erkennbar sein[116] und die Betreiber sozialer Netzwerke haben bei der Datenverknüpfung in angemessenem Umfang die Schaffung unrichtiger Daten zu vermeiden (Art. 5 Abs. 2 DSG).

Es stellt sich auch hier, wie bei vielen von sozialen Netzwerken angebotenen Diensten, das Problem der oft mangelnden Aufklärung Nutzender über Umfang, Weitergabe, Art und Zweck der Verarbeitung ihrer lokalitätsbezogenen Daten, womit auch Zweifel an der Wirksamkeit und Gültigkeit ihrer *Einwilligung* einhergehen können[117].

Art. 45b des Fernmeldegesetzes (FMG) regelt die Geolokalisierung für die Kunden von Anbieterinnen von Fernmeldediensten. Sie ist in drei Fällen erlaubt: erstens wenn dies für die Fernmeldedienste oder ihre Abrechnung erforderlich ist, zweitens nach Einwilligung der Kunden und drittens in anonymisierter Form. Anbieterinnen von Social Media sind aber wohl in der Mehrzahl nicht gleichzeitig Anbieterinnen von Fernmeldediensten (vgl. vorne Ziff. 2.4.2.2), sodass Art. 45b häufig nicht anwendbar sein wird.

4.3.7 Übermässige Bindung der Nutzenden an ein soziales Netzwerk

4.3.7.1 Ausgangslage

In den Wirtschaftswissenschaften wird es als „lock-in-Effekt“ bezeichnet, wenn es einem Unternehmen durch grosse Investitionen in die Zusammenarbeit mit einem Partnerunternehmen besonders erschwert wird, sich von dieser Zusammenarbeit wieder zu lösen. Das Partnerunternehmen kann diese Lage ausnützen, um besonders ungünstige Bedingungen für die Zusammenarbeit vorzuschreiben.

---

[113] BBl 2006 7851f.

[114] Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zürich 2012, S. 48f., 55f.

[115] Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zürich 2012, S. 47.

[116] Hier greifen die Grundsätze von Treu und Glauben sowie der Erkennbarkeit der Datenbearbeitung sowie die Informationspflicht des Inhabers einer Datensammlung bei der Beschaffung von Persönlichkeitsprofilen oder besonders schützenswerten Personendaten (Art. 4 Abs. 2 und 4 sowie Art. 14 DSG).

[117] Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zürich 2012, S. 65.

Die Nutzenden sozialer Netzwerke können in einer ähnlichen Lage sein, wenn sie so viel Zeit und Aufwand in ihren Auftritt auf einer sozialen Plattform investiert haben, dass ihnen ein Wechsel undenkbar erscheint. Dann kann die Plattform die Nutzungsbedingungen verschlechtern, ohne dass die Nutzenden darauf reagieren und zu einer Konkurrenzplattform wechseln.

Das kann etwa der Fall sein, wenn wichtige Bilder, Filme, Musik, Texte oder andere Daten der Nutzenden durch die Plattform gespeichert werden. Es kann auch sein, dass Nutzende über eine Plattform derart viele Personen erreichen (zum Beispiel bei einem persönlichen youtube-Kanal oder bei einem Blog), dass sie nur unter Mitnahme dieser Kontakte zu einer anderen Plattform wechseln würden.

Ein Wechsel der Plattform kann auch dann undenkbar sein, wenn Nutzende Nachrichten untereinander nur über die Plattform austauschen können und ohne die Plattform ihre Kontaktmöglichkeit verlieren würden. Andererseits kann es in diesem Fall auch der Wunsch der übrigen Nutzenden sein, dass sie nur über die Anonymität der Plattform kontaktiert werden können und z.B. ihre E-Mail-Adresse vom Plattformbetreiber geheim gehalten wird. Den Interessen solcher Nutzenden würde eine Mitnahme der Kontaktmöglichkeiten beim Wechsel der Plattform nicht entsprechen. Dieser Zielkonflikt lässt sich aber auflösen, wenn Nutzende beim Verlassen der Plattform die Kontaktmöglichkeit zu denjenigen anderen Nutzenden mitnehmen können, welche dies wünschen.

Einige Plattformen bieten Nutzenden die Mitnahme von gespeicherten Dateien an. Grundsätzlich sollte diese Datenportierung zwischen verschiedenen Plattformen möglich sein, denn nur dann sinkt für die Nutzenden der Aufwand für einen Plattformwechsel auf ein erträgliches Mass.

4.3.7.2 Lösungsansätze im Ausland oder internationalen Recht

Die Europarats-Empfehlung zu sozialen Netzwerken verlangt die einfache Datenübertragbarkeit zu einem anderen Anbieter in einem gängigen elektronischen Format.

Auch der Vorschlag zur EU Datenschutz-Grundverordnung sieht ein Recht auf Datenübertragbarkeit vor[118]. Werden personenbezogene Daten elektronisch in einem strukturierten gängigen elektronischen Format bearbeitet, so sollen die betroffenen Personen das Recht haben, eine Kopie der bearbeiteten Daten in einem weiter verwendbaren strukturierten gängigen Format zu verlangen. Haben die Betroffenen die personenbezogenen Daten selbst zur Verfügung gestellt, so sollen sie das Recht haben, diese in einem gängigen elektronischen Format in ein anderes System zu überführen, ohne dass sie der Datenbearbeiter dabei behindert.

4.3.7.3 Rechtslage in der Schweiz

Im schweizerischen Recht existiert keine Norm, die soziale Netzwerke verpflichtet, ihren Nutzenden beim Verlassen der Plattform diejenigen Daten mitzugeben, die diese auf der Plattform veröffentlicht oder gespeichert haben. Eine solche Norm könnte einer übermässigen Bindung der Nutzenden an bestimmte Plattformen entgegenwirken.

Einen hierzu vergleichbaren Zweck hat die bestehende Regelung der Nummernportabilität im Fernmelderecht. Sie erlaubt es Kundinnen und Kunden, ihre Telefonnummer zu behalten, wenn sie die Telefonanbieterin oder die Wohnadresse wechseln. Wer die Anbieterin wechselt, kann seine Telefonnummer zur neuen Anbieterin mitnehmen und sich so den Aufwand ersparen, allen seinen Kontakten eine neue Telefonnummer mitzuteilen. Sie oder er ist darum eher bereit, zu einer neuen Anbieterin zu wechseln.

Allerdings ist der Markt für soziale Netzwerke noch sehr in Bewegung. Die Bindung der Nutzenden an eine bestimmte Plattform ist schon aus diesem Grund noch nicht so ausgeprägt wie in einem reifen

---

[118] Art. 18 Vorschlag EU Datenschutz-Grundverordnung, KOM(2012) 11 endgültig.

Markt. Erst in einem solchen reifen Markt spielt das Halten der vorhandenen Kundschaft für die Unternehmen eine wichtigere Rolle. Ob die Unternehmen aus diesem Wunsch heraus, die vorhandene Kundschaft von einem Wechsel abzuhalten, auch deren Daten zurückbehalten werden, bleibt abzuwarten. In der Praxis zeigt sich heute, dass viele der auf verbreiteten sozialen Netzwerken vorhandenen Kundendaten bereits mitgenommen werden können. Eine spezielle Pflicht zur Datenfreigabe erscheint angesichts dieser vorhandenen freiwilligen Angebote heute noch nicht erforderlich. Dies gilt umso mehr, als sich bei der Umsetzung dieser Pflicht Fragen stellen: Welche Daten stehen Nutzenden zur Mitnahme zu? Auch Daten, die vom Betreiber mit anderen Daten kombiniert wurden, um nützlicher zu sein (z.B. die Kennzeichnung des Nutzenden auf durch Dritte veröffentlichten Fotos)? Auch Daten, die mit Programmen des Betreibers erstellt wurden? In welchem Format sind welche Daten mitzugeben?

Wie sich dieses Thema in Zukunft entwickeln wird, ist heute noch nicht absehbar. Es ist daher angezeigt, die zukünftige Entwicklung zu beobachten und allenfalls zu einem späteren Zeitpunkt rechtliche Vorschriften zu erlassen (siehe dazu Ziff. 7.2.4.4).

4.4 Beeinträchtigung von Individualinteressen durch Dritte

4.4.1 Ehrverletzungen und widerrechtliche Verletzungen der Persönlichkeit

4.4.1.1 Ausgangslage

Auch in sozialen Netzwerken kommt es zu ehrverletzenden Werturteilen oder falschen Tatsachenbehauptungen[119]. So wurden in der Schweiz bereits Urteile wegen Beschimpfungen in sozialen Netzwerken gefällt[120]. Beeinträchtigungen des gutes Rufs durch soziale Medien lassen sich nicht einfach mit Ehrverletzungen in herkömmlichen Medien (wie in Zeitungen) vergleichen. Im Ausland ist erkannt worden, dass die Online-Kommunikation über neue Kanäle wie Blogs oder Twitter eine besondere Belastungsprobe für die Wirksamkeit der bestehenden rechtlichen Instrumente zum Schutz des Ansehens bedeutet. [121]

Für die Betroffenen sind neue, schwer zu kalkulierende Risiken entstanden. So können in vielen sozialen Netzwerken Inhalte auf Nutzerprofilen Dritter ohne Einholung derer vorherigen Einwilligung platziert werden, was eine Kontrolle des eigenen Profils erschwert. Durch die einfache, sofortige und uneditierte Übertragung von Inhalten in sozialen Netzwerken und der für die Nutzenden häufig ausgeprägten Sozialrelevanz ihrer Kontaktgruppen, kann der Schaden ehrverletzender Werturteile oder falscher Tatsachenbehauptungen durch Dritte gross sein.

Ein weiteres Phänomen, welches zu negativen Beeinträchtigungen des guten Rufs der Betroffenen führen kann, sind beispielsweise die Gruppeneinladungen auf Facebook. Wird ein Dritter durch einen Facebook-Freund zu einer Gruppe eingeladen, wird er unabhängig von seiner Zustimmung automatisch deren Mitglied. Er wird zwar sofort von dieser Einladung benachrichtigt und kann umgehend aus der Gruppe austreten. Bis zu diesem Zeitpunkt kann je nach Profil der Gruppe und Identität des Eingeladenen jedoch bereits ein Rufschaden entstanden sein.

4.4.1.2 Lösungsansätze im Ausland oder internationalen Recht

Eine mögliche Massnahme zum Schutz gegen unrichtige öffentliche Tatsachenbehauptungen ist das Recht auf Gegendarstellung. Es sollte nach der Empfehlung des Europarats über das Recht auf Ge-

---

[119] So weist etwa KOBIK im Jahresbericht 2011 auf eine Zunahme der Ehrverletzungsdelikte bei ihren Meldungseingängen sowie den Umstand hin, dass Kriminelle hierzu vermehrt soziale Netzwerke als Tatwerkzeug nutzen. Siehe Jahresbericht 2011 Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK, S. 6.

[120] Vgl. etwa den Entscheid des Kreisgerichtes St. Gallen vom 9.5.2011 (Beschimpfung über Facebook); http://wifimaku.com/pages/viewpage.action?pageId=5669650

[121] Aus der neueren ausländischen Literatur vgl. etwa Ladeur Karl-Heinz/Gostomzyk Tobias, Der Schutz von Persönlichkeitsrechten gegen Meinungsäusserungen in Blogs, Neue Juristische Wochenschrift NJW 2012, S. 710ff.; Richardson Megan, Honour in a Time of Twitter, Journal of Media Law 2013, S. 45ff.

gendarstellungen in der neuen Medienumgebung[122] auf sämtliche Kommunikationsmittel anwendbar sein, die der periodischen Vermittlung redaktionell kontrollierter Inhalte an die Öffentlichkeit dienen, unabhängig davon, ob diese off- oder online publiziert werden. Bleiben bestrittene Inhalte in elektronischen Archiven öffentlich zugänglich und wurde ein Gegendarstellungsrecht gewährt, so soll ein Link die betroffenen Inhalte mit der Gegendarstellung verbinden.

Das Europäische Parlament und der Europäische Rat forderten die Mitgliedstaaten auf, Massnahmen zur Gewährleistung des Rechts auf Gegendarstellung in Online-Medien vorzusehen[123]. Die EU-Kommission hielt 2011 in ihrem Bericht über die Umsetzung der Empfehlung fest, dass die Einführung eines Rechts auf Gegendarstellung in Onlinemedien in den EU-Mitgliedstaaten sehr uneinheitlich ausfalle[124]und forderte eine Verbesserung der Wirksamkeit der Systeme.

4.4.1.3 Rechtslage in der Schweiz

Der strafrechtliche (Art. 173-178 StGB) sowie der zivilrechtliche Ehrenschutz (Art. 28f. ZGB) sind grundsätzlich auch auf die Tätigkeiten in sozialen Netzwerken anwendbar. Der wirtschaftliche Ehrenschutz des Art. 28 ZGB wird durch Art. 3 Abs. 1 lit a UWG ergänzt.

Als besonderes Instrument kennt das ZGB ein Recht auf Gegendarstellung gegenüber Tatsachenbehauptungen in periodisch erscheinenden Medien, welche sich an die Öffentlichkeit richten oder dieser zugänglich sind (Art. 28g – 28l ZGB). Der Gesetzgeber hat den Medienbegriff bewusst offen formuliert, weshalb das Gegendarstellungsrecht auch gegenüber neuen Medienformen zum Tragen kommt und nicht von der Technik der Verbreitung abhängt. [125] Ob Nutzerprofile in sozialen Netzwerken als periodisch erscheinende Medien qualifiziert werden können, hängt von der konkreten Nutzung der jeweiligen Plattform bzw. dem Publikationsverhalten des Profilbesitzers ab. So werden etwa regelmässig aufdatierte Weblogs von Journalisten als periodisch erscheinende Medien im Sinne des ZGB eingestuft werden können, während dies bei Diskussionsforen zweifelhaft ist .[126]

Die praktischen Probleme beim Vorgehen gegen ehrenrührige oder persönlichkeitsverletzende Beiträge in sozialen Netzwerken scheinen primär bei der *Rechtsdurchsetzung* zu liegen, falls Urheber einer Ehrverletzung nicht identifizierbar und die Ermittlungen auf den Kooperationswillen von Plattformbetreibern und Providern angewiesen sind. Besonders schwierig ist ein rasches Vorgehen gegenüber Publikationen auf ausländischen Plattformen.[127] (Bei schweizerischen Tatbeteiligten wird die Rechtsdurchsetzung hingegen dadurch erleichtert, dass Beseitigungs- und Feststellungsbegehren gegen sämtliche an der Persönlichkeitsverletzung Mitwirkenden gestellt werden können.[128])

Rechtliche Instrumente sind auch weitgehend wirkungslos, wenn sich die verletzenden Inhalte unüberschaubar schnell und weitläufig verbreitet haben: Selbst wer seine Persönlichkeitsrechte vor Ge-

---

[122] Empfehlung Rec(2004)16 über das Recht auf Gegendarstellung in der neuen Medienumgebung.

[123] Empfehlung des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über den Schutz Minderjähriger und den Schutz der Menschenwürde und über das Recht auf Gegendarstellung im Zusammenhang mit der Wettbewerbsfähigkeit des europäischen Industriezweiges der audiovisuellen Dienste und Online-Informationsdienste, ABl. L 378 vom 27.12.2006, S. 72.

[124] Bericht der Kommission über die Anwendung der Empfehlung des Rates vom 24. September 1998 zum Jugendschutz und zum Schutz der Menschenwürde und der Empfehlung des Europäischen Parlamentes und Rates vom 20. Dezember 2006 über den Schutz Minderjähriger und den Schutz der Menschenwürde und über das Recht auf Gegendarstellung im Zusammenhang mit der Wettbewerbsfähigkeit des europäischen Industriezweigs der audiovisuellen Dienst und Online-Informationsdienste – Schutz der Kinder in der digitalen Welt –, KOM(2011) 556 endgültig, S. 10.

[125] BGE 113 II 369 E. 3 S. 371.

[126] Vgl. etwa Barrelet Denis/Werly Stéphane, Droit de la communication, Bern 2011, N 1683.

[127] Dazu etwa Schneider-Marfels Karl-Jascha, Facebook, Twitter & Co: „Imperium in imperio“, Jusletter vom 20. Februar 2012.

[128] Vgl etwa das Urteil zu einer von Tribune de Genève betriebenen Blogplattform (BGer 5A_792/2011 vom 14.1.2013).

richt erfolgreich durchgesetzt hat, muss damit rechnen, dass der rechtswidrige Inhalt anderswo auftaucht.[129]

4.4.2 Cyberbullying und Cyberstalking

4.4.2.1 Ausgangslage

Eine besondere Erscheinungsform der Persönlichkeitsverletzung ist das Cyberbullying oder Cybermobbing[130], d.h. die Verbreitung diffamierender Texte, Bilder oder Filme unter Einsatz moderner Kommunikationsmittel (Handy, Chat, soziale Netzwerke, Videoportale, Foren oder Blogs), um Personen zu verleumden, lächerlich zu machen oder zu belästigen[131], wobei die Angriffe grundsätzlich wiederholt oder über einen längeren Zeitraum hinweg erfolgen[132].

Cyberstalking ist die Nutzung elektronischer Kommunikationsmittel, wie etwa sozialer Netzwerke, um Dritte zu bedrängen. Unter Stalking versteht man die wiederholte Verfolgung oder Belästigung einer Person. Dies kann etwa in Form von Beobachtung, Ausforschung oder Kontaktaufnahmen erfolgen. Häufig finden Stalkinghandlungen zwischen Personen statt, die sich bereits kennen oder einander nahe standen. Die in sozialen Netzwerken von Nutzenden selbst zur Verfügung gestellten Daten können neben Online-Belästigungen überdies dazu genutzt werden, um die Adressen potenzieller Opfer ausfindig zu machen, ihre Lebensgewohnheiten zu studieren und sie physisch zu verfolgen.

Die Phänomene des Cyberstalking sowie des Cyberbullying beschränken sich nicht auf soziale Netzwerke, finden jedoch vermehrt auch in diesen statt und unterliegen dort besonderen Umständen[133]. Die Möglichkeit der Nutzung sozialer Netzwerke unter einem Pseudonym bietet Angreifern Raum für anonymes Handeln, was die Belästigung oder Demütigung Dritter erleichtert. Derartige Verletzungshandlungen können in sozialen Netzwerken zudem so vorgenommen werden, dass sie auch für Aussenstehende sichtbar sind, was den Schaden für die Opfer vergrössert.

4.4.2.2 Lösungsansätze im Ausland oder internationalen Recht

Die Europarats-Empfehlung zu sozialen Netzwerken fordert den Austausch von „best practices“ zur Prävention gegen Cyberbullying (und Cybergrooming). Überdies sollen Plattformbetreiber wirksame Beschwerdemechanismen zur Verfügung stellen und eingehende Beschwerden sorgfältig betreuen.

Die Sensibilisierungskampagne „klicksafe“ im Auftrag der Europäischen Kommission zur Förderung der Medienkompetenz im Umgang mit dem Internet und neuen Medien informiert im Internet u.a. auch

---

[129] Ladeur Karl-Heinz/Gostomzyk Tobias, Der Schutz von Persönlichkeitsrechten gegen Meinungsäusserungen in Blogs, Neue Juristische Wochenschrift NJW 2012, S. 713.

[130] Die beiden Begriffe werden in diesem Bericht synonym verwendet.

[131] Eine in den Kantonen Wallis, Thurgau und Tessin zwischen November 2010 und Juni 2012 mit 960 SchülerInnen – 49% davon weiblich, bei einem Durchschnittsalter von 13,5 Jahren – durchgeführte Studie belegt, dass die Anzahl an Cybermobbingopfern und -tätern zwar sehr niedrig ist, weist aber auch auf eine Steigung der Vorfälle zwischen 2010 und 2012 hin. Siehe: Unveröffentlichte Zahlen aus der netTEEN-Studie (Perren S. & Sticca F., 2012. Jacobs Center for Productive Youth Development, Universität Zürich). Überdies scheint Cybermobbing unter Jugendlichen regelmässig eng mit traditionellen Mobbingformen verbunden zu sein, da Onlineopfer und -täter meistens auch offline betroffen bzw. tätig sind. Siehe: Perren Sonja, Professionswissen für Lehrerinnen und Lehrer – Grundlagen für die Aus- und Weiterbildung von Lehrerinnen und Lehrern, Hrsg.: H.U. Grunder, K. Kansteiner-Schänzlin, H.Moser, S. 15.

[132] Bericht des Bundesrates vom 26.05.2010 „Schutz vor Cyberbullying“; zu finden unter: http://www.ejpd.admin.ch/ejpd/de/home/dokumentation/info/2010/ref_2010-06-02.html.

[133] KOBIK hielt im Jahresbericht 2011 fest, dass Meldungen wegen Drohungen und Nötigungen zugenommen hätten und hierzu vermehrt soziale Netzwerke genutzt werden. Ebenso stellte sie fest, dass 30 der unter den Kategorien „Ehrverletzungsdelikte, Drohung und Nötigung“ gemeldeten Fälle Cyberbullying betrafen, wobei keine Angaben dazu gemacht wurden, ob diese in sozialen Netzwerken oder per E-Mail erfolgten. (Siehe Jahresbericht KOBIK, S. 6). Gemäss einer internen Mitteilung von KOBIK zum Jahresbericht 2011 wurden neun der gemeldeten Ehrverletzungen mithilfe/in sozialen Netzwerken begangen und fanden drei Vorfälle in der Deliktskategorie „Drohung, Nötigung, Erpressung“ in sozialen Netzwerken statt. Diese markante Zunahme bestätigte sich 2012 allerdings nicht und stellt nach Einschätzung von KOBIK keinen erkennbaren Trend dar (Jahresbericht KOBIK 2012, S. 9).

über die Phänomene Cybermobbing und Cyberbullying, erläutert das geltende Recht und gibt allgemeine Ratschläge für ein sinnvolles Vorgehen der Betroffenen[134].

Südkorea versuchte folgenreichen Vorfällen von Cyberbullying sowie Fairnessbedenken im Zusammenhang mit politischen Wahlen[135] mit einer Identitätspflicht in sozialen Netzwerken zu begegnen[136]. Der Entscheid des südkoreanischen Verfassungsgerichts über die Verfassungswidrigkeit der Identitätspflicht[137], unzählige Hacker-Angriffe auf die Server der Anbieter der betroffenen Webseiten und der Diebstahl persönlicher Daten von Millionen Südkoreanern führten dazu, dass die Koreanische Communications Commission beschloss, das System der Identitätsverifizierung bis 2014 wieder abzuschaffen[138]. Eine Lizenzpflicht für Nachrichtenportale mit mehr als 50‘000 Nutzenden wurde im Juni 2013 in Singapur eingeführt.[139]

4.4.2.3 Rechtslage in der Schweiz

Das Schweizer Recht enthält keine spezifische Cyberstalking- oder Cyberbullying-Bestimmung. Dennoch erfassen das geltende Straf- und Zivilrecht viele jener Handlungen, welche den beiden Begriffen zugeordnet werden können, wenn sie mithilfe elektronischer Kommunikationsmittel verübt werden. Der vom Bundesrat zum Cyberbullying verfasste Bericht hält denn auch fest, dass zum heutigen Zeitpunkt keine Anhaltspunkte vorliegen, wonach das bestehende strafrechtliche Instrumentarium nicht ausreichen würde[140].

Auf die den Begriffen Cyberstalking oder Cyberbullying zuzuordnenden Handlungen sind etwa der strafrechtliche (Art. 173-178 StGB) sowie der zivilrechtliche Ehrenschutz (Art. 28f. ZGB) anwendbar. Neben den Ansprüchen aus Art. 28a ZGB können Betroffene zum Schutz vor Persönlichkeitsverletzungen in Form von Gewalt, Drohung oder Nachstellungen auch bei einem Gericht geltend machen, Dritten sei der Kontakt mit ihnen – was elektronische Kommunikation explizit umfasst – zu verbieten (Art. 28b Abs. 1 Ziff. 3 ZGB).

Weiteren Schutz vermögen die Artikel 135 (Gewaltdarstellungen), 143bis (Unbefugtes Eindringen in ein Datenverarbeitungssystem), 144bis (Datenbeschädigung), 156 (Erpressung), 179^{novies} (Unbefugtes Beschaffen von Personendaten), 180 (Drohung), 181 (Nötigung), 197 (Pornografie) und 198 (Sexuelle Belästigungen) des Strafgesetzbuches zu gewähren.

Auch hier liegen die hauptsächlichen Schwierigkeiten wieder im Bereich der Rechtsdurchsetzung, wobei die Ermittlung der Identität der Täterin oder des Täters dadurch erleichtert sein sollte, dass je-

---

[134] Siehe http://www.klicksafe.de/themen/kommunizieren/cyber-mobbing/ .

[135] Einführung eines Systems zur Zwangsidentifizierung von Personen, welche sich auf Webseiten oder Internetforen für oder gegen politische Kandidaten und Kandidatinnen äussern im Public Officials Election Act (POEA) im Jahr 2005.

[136] Siehe Bericht des UN-Sonderberichterstatters für die Förderung und den Schutz des Rechts auf freie Meinungsäußerung zu Südkorea vom 21.03.2011, A/HRC/17/27/Add.2 sowie Länderbericht zu Südkorea der OpenNet Initiative; zu finden unter: http://www.access-controlled.net/profiles/.

[137] Das Südkoreanische Verfassungsgericht erklärte die Pflicht zur Identitätspreisgabe als verfassungswidrig: „South Korea’s real-name net law is rejected by court“, 23.08.2012; zu finden unter: http://www.bbc.co.uk/news/technology-19357160.

[138] Siehe etwa Kate Jee-Hyung Kim, Lessons Learned from South Korea’s Real-Name Policy, 17.01.2012, zu finden auf: http://www.koreaittimes.com/story/19361/lessons-learned-south-koreas-real-name-verification-system sowie Real-name Internet law on way out, Korea Joonang Daily, 30.12.2011; zu finden unter: http://koreajoongangdaily.joinsmsn.com/news/article/article.aspx?aid=2946369.

[139] Vgl. etwa NZZ Nr. 123 vom 31.5.2013, S. 5: Lizenzpflicht für Onlinemedien – Singapur verschärft die Aufsicht über Nachrichtenportale im Internet.

[140] Bericht des Bundesrates vom 26.05.2010 „Schutz vor Cyberbullying“. Abgelehnt hatte der Bundesrat auch die in der Motion Freysinger 10.4054 geforderte Einführung eines neuen Mobbing-Straftatbestandes für das Arbeitsumfeld, da das geltende Recht die fraglichen Handlungen bereits weitgehend reguliere und die Einführung einer weiteren Strafnorm keinen zusätzlichen Nutzen bringe in Anbetracht dessen, dass diese den zentralen Problemen der Beweisbarkeit sowie der Hemmung Betroffener gegen das betreffende Verhalten rechtlich vorzugehen, auch nicht begegne. Siehe http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20104054. Auch der Nationalrat lehnte die Einführung des Mobbing-Straftatbestandes mit 130 zu 33 Stimmen bei 11 Enthaltungen ab.

ne/r häufig aus dem sozialen Umfeld der Betroffenen (Schule, Arbeitsplatz etc.) stammt. KOBIK stellte 2012 einen Rückgang von Meldungen wegen strafbarer Handlungen gegen die Ehre fest. Ein Grund dafür könnte der bewusstere Umgang mit Social Media aufgrund der vermehrten Mediatisierung von Cyberbullying-Fällen sein. [141]

4.4.3 Identitätsdiebstahl und andere Gefahren böswilliger Manipulation

4.4.3.1 Ausgangslage

In vielen sozialen Netzwerken ist der *Identitätsdiebstahl* einfach. Im Bereich der Internetkriminalität nehmen Identitätsdiebstahl- und missbrauch in sozialen Netzwerken zu, wobei diese häufig der Begehung vermögensrechtlicher Delikte dienen[142]. Überdies kann der Identitätsdiebstahl der Rufschädigung oder sonstigen Verletzungen der Persönlichkeit oder Ehre Dritter dienen. Nutzende legen ein Profil mit dem Namen einer bekannten Person an und profitieren von deren Berühmtheit oder schädigen deren Ruf durch bösartiges Verhalten. Gleichermassen können Profile im Namen einer Person aus dem persönlichen Umfeld eröffnet werden, um dieser zu schaden, indem man sie lächerlich macht oder in ihrem Namen illegale oder schädliche Inhalte verschickt.

Auch die Erstellung einer *Fantasieidentität* in sozialen Netzwerken kann Nutzenden Vorteile einbringen, welche diesen bei Preisgabe ihrer wahren Identität nicht zuteil kämen. So können sie sich in Kontaktkreise einschleusen, zu denen sie ansonsten keinen Zugang hätten oder Online-Freundschaften mit Personen schliessen, welche sie bei Kenntnis ihrer echten Identität anders behandeln würden.

Gestohlene oder erfundene Identitäten können zu verschiedenen böswilligen Zwecken genutzt werden, wie etwa zwecks Sammlung von Informationen zur illegalen Verwendung sowie Grooming, Cyberstalking, Cyberbullying, Phishing, Spamming oder auch zur Verbreitung von Computerviren.

4.4.3.2 Lösungsansätze im Ausland oder internationalen Recht

Die Europarats-Empfehlung zu sozialen Netzwerken fordert die Einrichtung angemessener Beschwerdemechanismen gegen böswilliges Verhalten in sozialen Netzwerken mit besonderem Fokus auf den Identitätsdiebstahl. Mitgliedsstaaten sollen Plattformbetreiber verpflichten, die wirksamsten Sicherheitsmassnahmen einzusetzen, um Personendaten vor dem unrechtmässigen Zugriff Dritter zu schützen. Dies soll die Verschlüsselung der Kommunikation zwischen Nutzenden und der Webseite des Plattformbetreibers umfassen. Überdies sollen Plattformbetreiber Nutzende über Verletzungen der Sicherheitsvorkehrungen informieren, damit diese präventive Massnahmen ergreifen können, wie etwa einen Passwortwechsel.

Die EU-Kommission schlägt die Errichtung eines EU-Zentrums zur Bekämpfung der Cyberkriminalität vor[143], welches sich unter anderem dem Schutz von Nutzerprofilen sozialer Netzwerke vor digitalem Missbrauch widmen soll, um gegen den Identitätsdiebstahl im Internet vorgehen zu können[144].

4.4.3.3 Rechtslage in der Schweiz

Erstellen Dritte in sozialen Netzwerken Nutzerprofile unter Verwendung eines rechtlich geschützten Namensund ohne Einwilligung der Berechtigten, verstossen sie üblicherweise gegen den zivilrechtlichen Namensschutz nach Art. 29 Abs. 2 ZGB. Die Vorschrift schützt Betroffene vor der unbefugten Namensanmassung durch Dritte. Sie erfasst den bürgerlichen und amtlichen Namen natürlicher Per-

---

[141] Jahresbericht KOBIK 2012, S. 9.

[142] ENISA Threat Landscape Report vom 28.09.2012, S. 21ff.; zu finden unter: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape.

[143] Mitteilung „Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität“, KOM(2012) 140 endgültig.

[144] Pressemitteilung der EU Kommission vom 28.03.2012 „EU-Zentrum zur Bekämpfung der Cyberkriminalität und zum Verbraucherschutz beim elektronischen Geschäftsverkehr“, IP/12/317.

sonen, aber auch Pseudonyme, Spitznamen, Kurzbezeichnungen, Akronyme und abgekürzte Namen, sofern diese im Verkehr als Name eines Namenträgers aufgefasst werden[145].

Eine Verletzung des Rechts am eigenen Bild gemäss Art. 28 ZGB dürfte vorliegen, wenn Unberechtigte Bilder einer anderen Person verwenden, um unter deren Identität ein Nutzerprofil einzurichten.

In sozialen Netzwerken, die auch der privaten Kommunikation dienen (wie etwa Facebook), kommt auch eine Verletzung der Geheim- oder Privatsphäre gemäss Art. 28 ZGB in Betracht, wenn Dritte sich in fremde Nutzerprofile einschleichen und damit private, ihnen nicht von den Betroffenen zugänglich gemachte, Kommunikation wahrnehmen. Unzulässig ist es auch, fremde oder in fremden Namen erstellte Nutzerprofile zu verwenden, um Dritte mittels vorgetäuschter Identität zu veranlassen, private Informationen preiszugeben.

Aus datenschutzrechtlicher Sicht kann das Beschaffen von Personendaten unter Angabe einer falschen Identität einen Verstoss gegen den Grundsatz der Erkennbarkeit der Datenbeschaffung sowie den Grundsatz von Treu und Glauben (Art. 4 Abs. 2 und 4 DSG) darstellen[146]. Veröffentlichen Dritte in einem unter fremden Namen errichteten Nutzerprofil besonders schützenswerte Personendaten der betroffenen Person, so verstösst dieses Vorgehen gegen Art. 12 Abs. 2 Bst. c DSG.

Hacken sich Dritte unbefugt in fremde Nutzerprofile ein, informieren sich dort über nicht frei zugängliche Informationen, verändern dortige Inhalte oder die Zugangspasswörter der Berechtigten, können die Straftatbestände des unbefugten Eindringens in ein Datenverarbeitungssystem (Art. 143bis StGB), der Datenbeschädigung (Art. 144bis StGB) und der unbefugten Beschaffung von Personendaten (Art. 179^{novies} StGB) zur Anwendung gelangen.

Unter Verwendung einer fremden Identität errichtete Nutzerprofile sowie Fantasieprofile können verschiedensten rechtswidrigen Zwecken dienen. Im Vordergrund stehen Vermögens- und Ehrverletzungsdelikte, wie auch etwa Nötigung oder Drohung (Art. 173-177, 146, 147, 156, 180, 181 StGB) sowie Persönlichkeitsverletzungen und Stalkinghandlungen (Art. 28, 28b Abs. 1 Ziff. 3 ZGB). Gegen Spamming schützt Art. 3 Abs. 1 Bst. o UWG, während Art. 144bis StGB die Datenbeschädigung sowie den Einsatz und die Verbreitung von Computerviren (auch) mittels sozialer Netzwerke erfasst.

Gegen Phishing und Malwareverbreitung auf .ch-Domains kann gemäss Art. 14f^{bis} der Verordnung vom 06. Oktober 1997 über die Adressierungselemente im Fernmeldebereich[147] (Blockierung eines Domain-Namens bei Missbrauchsverdacht) wirksam vorgegangen werden. Das kann im Einzelfall auch gegen die Verwendung fremder Identitäten von Nutzen sein.

Aus der Analyse ergibt sich, dass das materielle Recht die mit dem digitalen Identitätsmissbrauch verbundenen Tathandlungen weitgehend erfasst. Allerdings mag es in der Realität insbesondere bei professionellen Tätern schwierig sein, deren Identität zu ermitteln, um gegen sie vorgehen zu können.

4.4.4 Beobachtung von Äusserungen in sozialen Medien (Social Media Monitoring)

4.4.4.1 Ausgangslage

Firmen, Behörden, Organisationen und bestimmte Privatpersonen haben ein Interesse an Informationen zur Frage, was über sie in den sozialen Medien berichtet wird. Durch systematisches und kontinuierliches Beobachten können die interessierten Organisationen versuchen, die Kontrolle über ihre Darstellung (zurück) zu gewinnen. Zur Bewältigung des unstrukturierten Informationsflusses wird auf automatisierte Tools zurückgegriffen.

---

[145] BSK-ZGB I, Bühler Roland, 4. Aufl., Basel 2010, Art. 29, S. 321f. Rz. 4, 7, S. 325 Rz. 16.

[146] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, S. 81 N. 14, S. 99 N. 56.

[147] AEFV; SR 784.104.

Ein Problem des Social Media Monitoring ist es, dass es nicht nur die Inhalte der in Netzwerken verbreiteten Informationen erfasst, sondern auch Angaben über deren Autorinnen und Autoren. Die Beobachtenden erhalten Informationen über den echten Namen oder zumindest das Pseudonym der Autorinnen, mitunter auch über Alter, Geschlecht, Beruf, Arbeitgeber, Herkunftsgebiet sowie allenfalls weitere offen gelegte Angaben. Besonders heikel sind etwa Informationen über die Weltanschauung und politische Einstellungen.

4.4.4.2 Rechtslage in der Schweiz

Nicht jegliche technisch mögliche Bearbeitung von Daten in Netzwerken ist ohne weiteres vom Zweckbindungsgrundsatz gedeckt. Auch veröffentlichte Daten dürfen laut Datenschutzgesetz nicht einfach für andere Zwecke verwendet werden. Personendaten auf Social Media-Plattformen sind häufig nur an persönliche Freunde gerichtet oder sie werden nur in einem bestimmten Umfeld oder in einem bestimmten Zusammenhang veröffentlicht. Ohne transparente Information über ein Social Media Monitoring fehlt es den betroffenen Personen mindestens am verlangten Wissen über die Verwendung der Personendaten für das Monitoring. Die Mitglieder von Social-Media-Plattformen müssen mindestens aus den Umständen erkennen können, dass Monitoring Tools zum Einsatz kommen. Werden Personendaten über Dritte publiziert, fehlt es ohnehin am Wissen und Willen dieser dritten Personen. Aus diesen Gründen kann in vielen Fällen nicht davon ausgegangen werden, die betroffenen Personen hätten die Personendaten auf Social-Media-Plattformen im Sinne von Art. 12 Abs. 3 DSG allgemein zugänglich gemacht.

Der EDÖB hat auf seiner Website Empfehlungen für einen datenschutzkonformen Einsatz von Social Media-Monitoring abgegeben. [148] So soll sich die Bearbeitung von Personendaten auf das für die Auswertungszwecke nötige Minimum beschränken und sind diese so rasch wie möglich zu löschen oder zu anonymisieren. Nichtöffentliche personenbezogene Daten (insbesondere aus geschlossenen Benutzergruppen resp. Freundeskreisen) sollten nicht einbezogen werden. Das Monitoring sollte sich auf die Analyse von öffentlichen Meinungen und Kommentaren beschränken.

4.5 Beeinträchtigung von Gemeininteressen

4.5.1 Rassistische und andere diskriminierende Äusserungen („hate speech“)

4.5.1.1 Ausgangslage

Wie das Internet im Allgemeinen, so bieten auch soziale Netzwerke eine Plattform zur einfachen Verbreitung rassistischer Inhalte mittels Bildern, Texten und Videos[149]. Zudem können die Plattformen zur Organisation rassistischer Vereinigungen und zur Rekrutierung neuer Mitglieder genutzt werden.

Soziale Netzwerke können auch missbraucht werden, um Menschen auf der Grundlage anderer Merkmale als der Rasse zu diskriminieren, beispielsweise aufgrund ihrer sexuellen Orientierung, Herkunft, Religion, Behinderung, Lebensform, Sprache, sozialen Stellung, politischen oder weltanschaulichen Überzeugung sowie ihres Geschlechts oder Alters.

Die Kontrolle und somit auch Löschung rassistischer und diskriminierender Inhalte ist bei sozialen Netzwerken im Vergleich zu Webseiten insofern zusätzlich erschwert, als sich die Verbreitung von Inhalten und die Vernetzung von Personen in diesen Foren noch einfacher und schneller gestaltet als dies mittels Webseiten bereits möglich ist.

Beim Vorgehen gegen diskriminierende Äusserungen in sozialen Netzwerken kann sich auch das Problem stellen, dass die Rechtslage bezüglich rassistischer und anderswie diskriminierender Inhalte in verschiedenen Ländern unterschiedlich ist. Folglich können im Ausland Inhalte legal sein, welche in

---

[148] http://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00692/.

[149] Gemäss einer internen Mitteilung von KOBIK zum Jahresbericht 2011 wurden bei neun der rund 30 im Jahr 2011 gemeldeten Rassendiskriminierungen soziale Netzwerke als Tatwerkzeug/-ort benutzt.

der Schweiz strafbar sind[150]. Dies führt bei international zugänglichen Medien zu Schwierigkeiten im Umgang mit derartigen Inhalten, wobei grundsätzlich die Tendenz beobachtbar ist, dass Betreiber sozialer Netzwerke gewisse Seiten und Inhalte auf Antrag hin in jenen Ländern sperren, in welchen diese strafbar sind. So sperrte Twitter etwa das Nutzerkonto einer rechtsextremistischen Vereinigung, welche in Deutschland verboten worden war, für jene Twitter-Nutzenden, die in ihren Kontoeinstellungen Deutschland als ihr Land angeben[151].

4.5.1.2 Lösungsansätze im Ausland oder internationalen Recht

Das Zusatzprotokoll zum Übereinkommen über Cyberkriminalität des Europarats betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art vom 28. Januar 2003 ist u.a. ausdrücklich auf die Verbreitung rassistischer und fremdenfeindlicher Inhalte im Internet ausgerichtet. Das Übereinkommen des Europarats über die Cyberkriminalität vom 23. November 2001[152] trat für die Schweiz am 1. Januar 2012 in Kraft. Das Zusatzprotokoll wurde vom Bundesrat zwar genehmigt, ist für die Schweiz jedoch noch nicht in Kraft getreten.

Auf der Grundlage von § 18 des Jugendmedienschutz-Staatsvertrags[153] zwischen den deutschen Bundesländern wurde die Stelle „jugendschutz.net“ gegründet[154]. In Deutschland geht jugendschutz.net aktiv gegen rassistische und diskriminierende Inhalte im Internet und in sozialen Netzwerken vor. Überdies sensibilisiert die Organisation in der Öffentlichkeit mittels Präventionstagen, Fortbildungsreihen oder Publikationen, wie etwa der Broschüre „Klickt’s? Geh Nazis nicht ins Netz!“[155]. Dabei richtet sich ihre Arbeit insbesondere auch gegen die umfangreiche Nutzung sozialer Netzwerke durch Rechtsextreme. Eine weitere deutsche Plattform ähnlicher Ausrichtung ist auch etwa Netz-Gegen-Nazis.de[156].

Die von jugendschutz.net gegründete Initiative INACH (International Network Against Cyberhate)[157] geht transnational gegen die Verbreitung und Anstachelung zu Hass im Internet, insbesondere auch Mobbing in sozialen Netzwerken, vor. Das Netzwerk setzt sich aus Meldestellen verschiedener Staaten zusammen, welche Best-Practice-Strategien austauschen und auf die Löschung diskriminierender und strafbarer Inhalte und Webseiten im Internet hinarbeiten.

4.5.1.3 Rechtslage in der Schweiz

Art. 261bis StGB untersagt verschiedene Formen der Diskriminierung von Personen aufgrund ihrer Rasse, Ethnie oder Religion durch Private. Die Bestimmung erfasst grundsätzlich alle in sozialen Netzwerken denkbaren Kommunikationsformen, seien dies Fotos, Videos, Bilder oder Texte. Vorausgesetzt ist allerdings, dass die Kommunikation *öffentlich* erfolgt[158]. In der Rechtslehre[159] werden Äusserungen in sozialen Netzwerken als öffentlich betrachtet, falls sich der Adressatenkreis nicht auf Per-

---

[150] So geniesst sog. „hate speech“ etwa in den USA einen sehr viel weitergehenden Schutz als in den meisten Westeuropäischen Staaten. Siehe etwa den Entscheid des französischen Tribunal de Grande Instance de Paris LICRA v. Yahoo! vom 22.05.2000, in dem das französische Gericht den Verkauf von Nazi-Memorabilien auf der Auktionsseite Yahoos - was gemäss U.S. Recht zulässig, gemäss französischem Strafrecht jedoch verboten ist - für illegal erklärte.

[151] „Erste landesspezifische Sperre auf Twitter: Account von verbotener rechtsextremistischer Vereinigung in Deutschland gesperrt“; zu finden unter: https://netzpolitik.org/2012/erste-landesspezifische-sperre-auf-twitter-account-von-verbotener-rechtsextremistischer-vereinigung-in-deutschland-gesperrt/.

[152] SR 0.311.43.

[153] Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien vom 10. bis 27.09.2002, Bay.GVBI Nr. 5/2003, S. 147ff.

[154] http://www.jugendschutz.net/.

[155] http://www.jugendschutz.net/materialien/klickts.html.

[156] http://www.netz-gegen-nazis.de/.

[157] http://www.inach.net/index.php.

[158] Zur weiten Auslegung des Begriffs der Öffentlichkeit durch das Bundesgericht siehe etwa BGE 130 IV 111.

[159] Vgl. Fiolka Gerhard, Basler Kommentar Strafrecht II, 3. Aufl. Basel 2013, vor Art. 258 N. 25.

sonen begrenzt, die durch ein Vertrauensverhältnis verbunden sind (z.B. durch restriktive Einstellungen der Privatsphäre auf Facebook).

In der schweizerischen Gerichtspraxis ist es bereits zu verschiedenen Verurteilungen wegen rassistischer Äusserungen in sozialen Netzwerken gekommen.[160] Art. 261bis StGB erfasst allerdings nur Diskriminierungen aufgrund der Rasse, Ethnie oder Religion und folglich nicht sämtliche der im verfassungsrechtlichen Diskriminierungsverbot (Art. 8 Abs. 2 BV) aufgezählten Merkmale wie Geschlecht, Alter und Behinderung oder auch die sexuelle Orientierung. Einen gewissen Schutz bietet hier lediglich das Persönlichkeitsrecht (Art. 28f. ZGB), wenn eine Person in sozialen Netzwerken aufgrund anderer persönlichkeitsnaher Merkmale diskriminiert wird.

Auf Bundesebene gehen die Eidgenössische Kommission gegen Rassismus (EKR)[161] sowie die Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK)[162] gegen Rassismus im Internet vor. Wird die EKR auf rassistische Äusserungen in sozialen Netzwerken aufmerksam, so meldet sie diese der KOBIK, welche die Meldungen[163] nach einer ersten Prüfung und Datensicherung an die zuständigen Strafverfolgungsbehörden im In- und Ausland weiterleitet. Zudem wird KOBIK selbständig tätig, durchsucht das Internet nach strafrechtlich relevanten Inhalten und erstellt eingehende Analysen über die Internetkriminalität. Da die Betreiber vieler sozialer Netzwerke ihren Sitz im Ausland haben, gestaltet sich die Strafverfolgung häufig schwierig, insbesondere wenn es darum geht die unbekannte Identität eines Urhebers aufzudecken. Die Löschung mutmasslich strafbarer Inhalte stellt nach Auskünften von KOBIK in der Praxis grundsätzlich kein Problem dar. Die Verbreitung von Inhalten rassistischer oder anderswie diskriminierender Natur ist in den Nutzungsbedingungen vieler sozialer Netzwerke untersagt und bei entsprechenden Meldungen veranlassen die Betreiber grundsätzlich Löschungen.

4.5.2 Pornografie

4.5.2.1 Ausgangslage

Probleme mit der Verbreitung von Pornografie über soziale Netzwerke können sich wie auch sonst im Internet ergeben, wenn diese als harte Pornografie (d.h. nach Art. 197 Ziff. 3 StGB bspw. die Darstellung sexueller Handlungen mit Kindern [Synonym: Pädopornografie] oder Tieren) zu qualifizieren oder weiche Pornografie für Personen unter 16 Jahren zugänglich ist. Für die Zwecke des Berichts steht das Problem der Kinderpornografie (Pädopornografie) im Vordergrund.

Da kinderpornografische Inhalte grundsätzlich weltweit verboten sind, nutzen Täterkreise im Internet üblicherweise Verbreitungs- und Kommunikationskanäle, welche anonymer und geheimer als die klassischen sozialen Netzwerke operieren. Darstellungen des sexuellen Missbrauchs von Kindern werden über kommerzielle Webseiten verkauft oder in geschlossenen Gruppierungen oder Peer-to-Peer-Netzwerken getauscht[164]. Letzteres erlaubt den diskreten und anonymen Austausch von kinderpornografischem Material[165]. Die Veröffentlichung oder Verbreitung kinderpornografischer Inhalte auf durchlässigen Plattformen ist in der Praxis folglich wohl eher selten.

---

[160] So etwa wegen eines gegen eine dunkelhäutige Mitschülerin gerichteten Kommentars auf Facebook (Entscheid Nr.2010-32 in der Sammlung Rechtsfälle der Eidg. Kommission gegen Rassismus; http://www.ekr.admin.ch/dienstleistungen/00169/).

[161] http://www.ekr.admin.ch/aktuell/index.html.

[162] http://www.cybercrime.admin.ch/kobik/de/home.html .

[163] Der Anteil von Meldungen wegen Rassendiskriminierung betrug 2012 lediglich 0,78 Prozent des gesamten Meldungseingangs; Jahresbericht KOBIK 2012, S. 4.

[164] Information der Koordinationsstelle zur Bekämpfung der Internetkriminalität zum Thema Kinderpornografie, http://www.cybercrime.admin.ch/content/kobik/de/home/themen/kinderpornografie.html.

[165] Siehe Medienmitteilungen des Bundesamtes für Polizei „Trotz Rückgang der Verdachtsmeldungen: Kinderpornografie bleibt die meistgemeldete Kategorie bei KOBIK“ vom 03.04.2012, http://www.fedpol.admin.ch/content/fedpol/de/home/dokumentation/medieninformationen/2012/2012-04-03.html.

4.5.2.2 Lösungsansätze im Ausland oder internationalen Recht

Die auch für die Schweiz verbindliche Europaratskonvention über die Cyberkriminalität vom 23. November 2001 (SR 0.311.43) dient der internationalen Rechtsangleichung sowie der Verbesserung der Zusammenarbeit zwischen den Vertragsstaaten, was insbesondere in Anbetracht der häufig grenzüberschreitenden Internet-Sachverhalte von Bedeutung ist. Die Konvention enthält mit Art. 9 eine relativ umfassende Bestimmung zur Strafbarkeit von Taten mit Bezug zu Kinderpornografie.

Diverse Organisationen in verschiedenen Staaten widmen sich dem Auffinden und Löschen schädlicher und illegaler Inhalte im Internet. In England ist beispielsweise die Internet Watch Foundation tätig, welche u.a. auch kinderpornografischen Inhalten im Internet nachgeht[166].

Voraussichtlich wird in Folge des Beitritts der Schweiz zum Übereinkommen des Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch vom 25.10.2007 künftig auch der vorsätzliche Konsum harter Pornografie – was auch deren reine Betrachtung in sozialen Netzwerken ohne Download der Inhalte umfasst – strafbar sein[167].

4.5.2.3 Rechtslage in der Schweiz

Art. 197 StGB schützt Personen unter 16 Jahren vor jeglicher sowie Erwachsene vor der unaufgeforderten Konfrontation mit Pornografie. Überdies verbietet die Bestimmung harte Pornografie. Art. 197 StGB erfasst die meisten Handlungen und Tatobjekte, welche dazu führen können, dass weiche Pornografie über soziale Netzwerke an die falschen Adressaten gelangt oder harte Pornografie über soziale Netzwerke verbreitet oder aufgefunden wird. Werden pornografische Inhalte in sozialen Netzwerken – beispielsweise in Form eines YouTube Videos – ohne wirksame Zugangsbeschränkung veröffentlicht, so werden diese damit Personen unter 16 Jahren zugänglich gemacht. So reicht ein Warnhinweis auf einer Internetseite, der durch Anklicken verschwindet, beispielsweise nicht aus[168], ebenso wenig die Nutzungsbeschränkung einer Webseite mittels Passwort bei mangelnder Überprüfung des Alters[169].

Pornografische Inhalte – weiche Pornografie einbezogen – gehören zu jenen Inhalten, welche die meisten Plattformbetreiber üblicherweise in ihren Nutzungsbedingungen untersagen und im Falle deren Auftauchens dank relativ rigider „Notice-and-Take-down"-Funktionen und Filterprogrammen einfach und schnell löschen können. Die häufig internationalen Zusammenhänge bei der Verbreitung illegaler Pornografie stellen Strafverfolgungsbehörden insbesondere wegen der Unterschiede von Vorschriften und Massnahmen in den verschiedenen Rechtsordnungen vor grosse Herausforderungen. Die Anzahl an KOBIK gerichteter Meldungen wegen verbotener Pornografie (v.a. mit Kindern) ist konstant hoch. [170] Darüber hinaus betreibt KOBIK auf Bundesebene auch im Bereich der Kinderpornografie aktive Ermittlung, die verdachtsunabhängige Recherche eingeschlossen.

4.5.3 Gefährdung der öffentlichen Ordnung durch Massenmobilisierung

4.5.3.1 Ausgangslage

Soziale Plattformen haben das für eine demokratische Gesellschaft wertvolle Potenzial, einen wesentlichen Beitrag zur Meinungsbildung und zur Äusserung gerade für Minderheiten zu leisten. In bestimmter Konstellation sind sie geeignet, in kurzer Zeit grosse Menschenmengen zu mobilisieren.[171]

---

[166] http://www.iwf.org.uk/.

[167] BBl 2012 7618 sowie BBl 2012 7657.

[168] BGE 131 IV 64 E. 10.3.

[169] Bundesgerichtsurteil 6S.26/2005 E. 3.2.

[170] Der Anteil von Verdachtsmeldungen wegen verbotener Pornografie mit Kindern betrug 2012 annähernd einen Drittel des gesamten Meldungseingangs; Jahresbericht KOBIK 2012, S. 4.

[171] Zu den durch Social Media eröffneten Chancen für eine vielfältige und lebendige Kommunikation vgl. vorne Ziff. 3.2.

Dies kann in Extremfällen allerdings auch negative Folgen haben und die öffentliche Ordnung erheblich beeinträchtigen.

So wurde auf Facebook zur Teilnahme an einer Massenveranstaltung zum Thema „Tanz dich frei" aufgerufen, an der eine Minderheit von Gewaltbereiten im Mai 2013 in der Berner Innenstadt erheblichen Sachschaden verursachte. Als Privatklägerin im Strafverfahren stellte die Stadt unter anderem den Antrag, gegenüber dem Unternehmen Facebook sei anzuordnen, es müsse die Identifikationsdaten des fraglichen Facebook-Accounts herausgeben. [172]

4.5.3.2 Lösungsansätze im Ausland oder internationalen Recht

Die Probleme der Mobilisierung durch soziale Netzwerke lassen sich am Beispiel schwerer Ausschreitungen illustrieren, zu denen es am 21. September 2012 in der niederländischen Kleinstadt Haren gekommen war. Auslöser war ein Facebook-Eintrag einer Jugendlichen, die für eine Einladung zu ihrem 16. Geburtstag vergessen hatte, dies als private Party zu markieren. Darauf wurde über Twitter und Facebook ein sich rasend schnell verbreitender Aufruf zu einem «Projekt-X-Fest» publiziert, dem mehrere tausend Jugendliche folgten. Die ursprünglich friedliche Stimmung schlug – nicht zuletzt unter Alkoholeinfluss – in massive Aggression um, der die anwesenden Ordnungshüter wegen verschiedener Versäumnisse nicht gewachsen waren.

In einem im März 2013 veröffentlichten Bericht empfahl eine Untersuchungskommission u.a., die Behörden sollten sich Kenntnisse über die Funktionsweise sozialer Medien aneignen. Dank eines gezielten Monitorings der Plattformen sollten sie sich künftig in die Lage versetzen, derartige Gefahren für die öffentliche Ordnung rechtzeitig zu erkennen – ohne dabei Einzelpersonen systematisch zu überwachen – und in gute Bahnen zu lenken. So sollten sie die Betreiber sozialer Plattformen unverzüglich dazu anhalten, Aufrufe zu unrechtmässigen Aktivitäten zu entfernen. Darüber hinaus sollten die Betreiber gerade ihre jugendliche Kundschaft besser auf die Risiken hinweisen, welche die für Social Media typische Vermischung von privater und öffentlicher Kommunikation birgt.[173]

4.5.3.3 Rechtslage in der Schweiz

Weckt ein Aufruf bei einer bestimmten Person den Vorsatz zur Begehung einer konkreten Straftat (z.B. einer Sachbeschädigung), so kommt eine Bestrafung wegen Anstiftung zu diesem Delikt in Betracht (Art. 24 StGB). Der Anstiftende fällt in diesem Fall unter dieselbe Strafandrohung wie der Täter. Darüber hinaus bedroht das schweizerische Strafgesetzbuch die öffentliche Aufforderung zu Verbrechen oder zu einem Vergehen mit Gewalttätigkeit gegen Menschen oder Sachen (Art. 259 StGB) mit einer Freiheitsstrafe bis zu drei Jahren oder Geldstrafe. Der Aufruf muss sich nicht auf genau umrissene Taten beziehen und sich auch nicht an bestimmte Personen richten. Er muss aber nach der Gerichtspraxis eine gewisse Eindringlichkeit aufweisen, wobei eine eindeutige Aufforderung auch gegeben sein kann, wenn sich jemand fremde Botschaften zu Eigen macht („Retweeten") [174].

Nicht unter diese Strafnorm fällt hingegen der blosse Aufruf zur Teilnahme an einer unbewilligten Kundgebung. Dieser kann allerdings gegen kantonale oder kommunale Vorschriften[175] verstossen. Wie bei anderen Strafbestimmungen (z.B. der Rassendiskriminierungsnorm; vgl. oben Ziff. 4.5.1.3) stellt sich bei Art. 259 StGB das auf sozialen Plattformen jeweils die Frage, ob eine Äusserung als öffentlich oder als privat einzustufen ist.

---

[172] Medienmitteilung der Stadt Bern vom 12. Juni 2013: http://www.bern.ch/mediencenter/aktuell_ptk_sta/2013/06/strafanzeige/view?searchterm=tanz dich frei.

[173] Bericht der Kommission „Project X – Haren" vom 8.3.2013, S. 31ff.; in niederländischer Sprache abrufbar unter http://de.scribd.com/doc/129273298/Hoofdrapport-rellen-Haren.

[174] Fiolka Gerhard, Basler Kommentar Strafrecht II, 3. Aufl. Basel 2013, Art. 259 N. 12.

[175] Vgl. etwa Art. 8 des Reglements der Stadt Bern über Kundgebungen auf öffentlichem Grund http://www.bern.ch/leben_in_bern/stadt/recht/dateien/143.1/.

Wie etwa Ehrverletzungen können auch Aufforderungen nach Art. 259 unter die Sonderregelung über die Strafbarkeit der Medien (Art. 28 StGB)[176] fallen. Strafrechtlich verantwortlich ist nach dieser Vorschrift allein der Autor der öffentlichen Aufforderung (und lediglich ersatzweise – falls der Autor nicht ermittelt oder in der Schweiz nicht vor Gericht gestellt werden kann – der verantwortliche Redaktor oder die für eine Veröffentlichung verantwortliche Person).

Zur Verfolgung der Verfasser rechtswidriger Einträge auf Plattformen vgl. hinten Ziff. 5.2 und zu Sperr- und Löschmassnahmen vgl. Ziff. 5.4.

4.5.4 Gefährdung der öffentlichen Gesundheit

4.5.4.1 Ausgangslage

Soziale Netzwerke werden zum Austausch über Interessen verschiedenster Art genutzt. Dies kann je nach Thema und Motivation auch sozial- oder gesundheitsschädliche Auswirkungen auf Nutzende haben. So können Online-Foren, in denen sich interessierte Personen über Suizid, Magersucht oder Selbstverletzung austauschen, derartige Handlungen und Phänomene verherrlichen oder sogar anregen und befürworten. Dies kann zu einer Verharmlosung des Problems führen, bereits vorhandene selbstzerstörerische Neigungen verstärken und im schlimmsten Fall die Vornahme konkreter schädigender Handlungen fördern. Neben den Risiken bietet das Internet Betroffenen aber auch unterstützende Informationen für derartige Probleme[177].

Ein weiteres Problem stellen die im Internet zahlreich vorhandenen Online-Foren zum Informationsaustausch über Krankheiten, Medikamente und Behandlungsmethoden dar, deren Qualität nicht oder nur schwer überprüfbar ist. 44% der schweizerischen Wohnbevölkerung informieren sich im Internet über Gesundheitsthemen, wobei das Internet meistens zur komplementären Information neben dem Austausch mit Experten oder vertrauten Laien genutzt wird. Dabei geht man davon aus, dass die Nachfrage nach Gesundheitsinformationen im Internet sowie nach partizipativen Internetanwendungen steigen wird. Zwei von drei Personen, die sich mithilfe des Internets über Gesundheitsfragen informieren, mangelt es an Vertrauen in die dort aufgefundenen Informationen[178]. Für diesen Teil der Bevölkerung sind die Einrichtung von Kontrollen oder Zertifikaten im Online-Gesundheitsbereich vertrauensbildend. Für weniger misstrauische Nutzende bleibt das Risiko bestehen, dass sie sich auf Online-Portalen zu Gesundheitsfragen unsachlich oder falsch informieren, was im schlimmsten Fall negative Folgen für ihre Gesundheit haben kann.

4.5.4.2 Lösungsansätze im Ausland oder internationalen Recht

Die von den deutschen Bundesländern gegründete Stelle „jugendschutz.net“ informiert auch über Gefahren und Risiken im Zusammenhang mit jugendgefährdenden Portalen, welche Suizid, Magersucht und Selbstverletzungen verherrlichen oder fördern[179]. „Jugendschutz.net“ informiert Betroffene und Eltern, überprüft einschlägige Internetangebote und arbeitet auf die Entfernung problematischer Inhalte hin. Zudem sensibilisiert sie die Betreiber sozialer Netzwerke für das Thema und bietet Anbietern, die derartige Inhalte löschen wollen, zum Thema Essstörungen eine Ersatzwebseite, die auf Aufklärungsinitiativen und Beratungsstellen verweist[180].

Gestützt auf § 18 Abs. 1 des deutschen Jugendschutzgesetzes[181] kann die zuständige Bundesprüfstelle[182] Träger- und Telemedien, die geeignet sind, die Entwicklung von Kindern oder Jugendlichen

---

[176] Vgl. etwa Zeller Franz, Basler Kommentar Strafrecht II, 3. Aufl. Basel 2013, Art. 28 N. 65.

[177] Siehe etwa Arbeitsgemeinschaft Ess-Störungen (AES); zu finden unter: www.aes.ch.

[178] Zu diesen Informationen siehe: eHealth Suisse Bericht Öffentliches Gesundheitsportal, verabschiedet vom Steuerungsausschuss am 26.01.2012, S. 6,7,11.

[179] http://www.jugendschutz.net/selbstgefaehrdung/index.html.

[180] http://www.anaundmia.de/.

[181] Jugendschutzgesetz (JuSchG) vom 23.07.2002, BGBl. I S. 2730.

zu gefährden, auf eine Liste jugendgefährdender Medien setzen. Die Indizierungen der Prüfstelle umfassen u.a. auch Foren, welche Magersucht oder Selbstmord verherrlichen[183].

4.6 Rechtslage in der Schweiz

Der Austausch gleichgesinnter Privater über Suizidfantasien, Magersucht, Selbstverletzung etc. fällt grundsätzlich in den Schutzbereich der Meinungsfreiheit. Es gibt keine gesetzlichen Grundlagen, welche das Phänomen konkret ins Recht fassen würden, wenn dieses eine offensichtlich sozialschädigende Wirkung entfaltet. Grundsätzlich kann der Bund zum Schutz der Gesundheit der Bevölkerung informierend tätig werden. Das Bundesamt für Gesundheit BAG ist in vielen Bereichen aktiv, welche Schnittstellen mit den Themen Suizid, Magersucht und Selbstverletzung aufweisen. Bis zum jetzigen Zeitpunkt befasste sich das BAG jedoch nicht explizit mit durch Social Media möglicherweise geförderten gesundheitsschädigenden Handlungen.

Bisher gibt es keine Rechtsgrundlage, welche den Austausch Privater über Medikamente und Behandlungsmethoden einschränken würde, solange diese nicht werbend tätig werden[184]. Gemäss BAG wäre mehr Transparenz im Bereich Gesundheitsinformationen und Gesundheitsforen im Internet wichtig. Qualitätslabels für seriöse Gesundheitsinformation im Internet[185] beziehen sich bisher jedoch primär eher auf Webseiten als auf Social Media.

4.6.1 Manipulation der Meinungsbildung aus kommerziellen Überlegungen

4.6.1.1 Ausgangslage

Soziale Netzwerke können von Unternehmen dazu genutzt werden, um durch von ihnen bezahlte Akteure, welche als unabhängige Konsumenten auftreten, positive oder auch fehlleitende Informationen über ihre Waren oder Dienstleistungen zu verbreiten. Dabei können nur wenige Personen Aktivitäten grösserer Gruppen vortäuschen. Dies kann auch unter Einsatz gefälschter Blogs, sogenannten Flogs (fake blog) oder Sockpuppets (gefälschte Online-Identitäten) erfolgen, welche unabhängig erscheinen, jedoch nur zu Werbezwecken eröffnet wurden. Die beschriebenen Methoden können ebenso eingesetzt werden, um konkurrierende Unternehmen und ihre Angebote negativ darzustellen.

Weitere Probleme können sich auch aus dem Kommunikationsformat eines sozialen Netzwerkes ergeben. Wird Twitter beispielsweise zu Werbezwecken genutzt, so sind Texte auf 140 Zeichen beschränkt, womit der Transparenz über Urheber, Hintergrund, Ursache und Motivation einzelner Mitteilungen ein Platzproblem erwachsen kann.

4.6.1.2 Lösungsansätze im Ausland oder internationalen Recht

Auch in der EU reagiert man auf das Phänomen intransparenter Werbemethoden in sozialen Netzwerken[186]. Die EU-Verbraucherschutzrichtlinie[187], welche den Abschluss von Verträgen zwischen Un-

---

[182] http://www.bundespruefstelle.de/.

[183] Siehe etwa den Entscheid der Bundesprüfstelle zur Indexierung eines Magersucht-Blogs: BPjM-Entscheid Nr. 5601 vom 04.12.2008 – „Pro Ana"; zu finden unter: http://www.doerre.com/jugendschutz/20081204_bpjm_index.pdf.

[184] Art. 31f. Bundesgesetz vom 15.12.2000 über Arzneimittel und Medizinprodukte (HMG), SR 812.21 sowie Verordnung vom 17.10.2001 über die Arzneimittelwerbung (AWV), SR 812.212.5, welche in Art. 4 Bst. c als Fachwerbung für Arzneimittel Werbung mittels Einsatz von audiovisuellen Mitteln und anderen Bild-, Ton- und Datenträgern und Datenübermittlungssystemen, wie zum Beispiel im Internet, aufzählt.

[185] Wie z.B. die Qualitätslabels der Stiftung Health on the Net HON, www.hon.ch.

[186] In der Entschliessung zum Einfluss der Werbung auf das Verbraucherverhalten (2010/2052(INI)) (Ziff. 17) kritisiert das EU-Parlament neue Formen der Schleichwerbung im Internet, welche nicht von der Richtlinie über unlautere Geschäftspraktiken erfasst werden. Es bezieht sich hierbei auf kommerzielle Kommentare und Werbenachrichten von Unternehmen in Blogs, sozialen Netzwerken oder ähnlichen Foren, die den Anschein erwecken Meinungen unabhängiger Verbraucher zu sein. Das Parlament regt die Mitgliedstaaten an, Beobachter zur Überprüfung möglicher Schleichwerbung in derartige Foren einzuführen.

[187] Richtlinie 2011/83/EU über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG und der Richtlinie 1999/44/EG sowie zur Aufhebung der Richtlinie 85/577/EWG und der Richtlinie 97/7/EG.

ternehmen und Verbrauchern regelt, befasst sich mit der Erfüllung der Informationspflichten der Unternehmen in Anbetracht technischer Einschränkungen, wie etwa der beschränkten Anzahl von Zeichen auf kleinen Displays. Die Richtlinie formuliert Mindestanforderungen an die Informationspflicht und verlangt, dass Verbraucher auf andere Informationsquellen hingewiesen werden, beispielsweise in Form von gebührenfreien Telefonnummern oder Hypertext-Links zu der Webseite des Unternehmens. Die Regulierung ist im Zusammenhang mit sozialen Netzwerken insofern interessant, als sich gewisse Angebote, wie etwa Twitter, durch eine beschränkte Zeichenanzahl auszeichnen. Überdies loggen sich immer mehr Nutzende über mobile Kommunikationsmittel, in soziale Netzwerke ein, womit das Informations- und Platzproblem durch das benutzte Endgerät (z.B. Smartphone) entsteht.

Die U.S.-amerikanische Behörde für Verbraucherschutz und Wettbewerbsrecht (Federal Trade Commission; FTC) erliess Richtlinien zum Konsumentenschutz vor unlauterer oder täuschender Werbung[188], welche werbenden Parteien helfen sollen geltendes Recht[189] einzuhalten. Die Richtlinien fordern, dass finanzielle und materielle Verbindungen (Bezahlungen oder Geschenke) zwischen werbenden Parteien und für sie werbenden Dritten (insbesondere Blogger, Celebrities etc.) bei der Werbetätigkeit in sozialen Netzwerken aufzuzeigen sind (auch in sozialen Netzwerken mit beschränkter Zeichenanzahl wie etwa Twitter)[190].

4.6.1.3 Rechtslage in der Schweiz

Die Bestimmungen des Bundesgesetzes gegen den unlauteren Wettbewerb[191], welche die Werbetätigkeit unabhängig von bestimmten Produkten, Branchen oder Medien regulieren, sind auch auf das Internet und folglich ebenso auf wettbewerbsrelevante Tätigkeiten in sozialen Netzwerken anwendbar[192].

Die Generalklausel Art. 2 UWG erfasst getarnte Werbung bzw. die Täuschung oder Irreführung über den Werbecharakter von Wettbewerbshandlungen als unlauteres Verhalten[193]. Erhalten Private für positive Äusserungen über ein Unternehmen und dessen Angebot auf ihren Blogs oder Netzwerkprofilen von diesem kostenlose Produkte oder Bezahlungen und wird diese Tatsache nicht transparent dargestellt, kann dieses Verhalten unlauter i.S.d. Generalklausel von Art. 2 UWG sein[194], sofern das Verhalten objektiv geeignet ist, die Funktionsfähigkeit des betroffenen Marktes zu beeinflussen. Irreführende Werbung kann weiter auch von Art. 3 Abs. 1 lit. b und i UWG erfasst sein. Mit der letzten UWG-Revision wurde Art. 3 Abs. 1 lit. s UWG eingeführt[195], welcher verbindliche Informationspflichten zur Verbesserung der Transparenz im elektronischen Geschäftsverkehr vorsieht.

Werden bezahlte oder anderswie vergütete private Dritte durch ein Unternehmen instruiert ihren Auftritt in sozialen Netzwerken zu nutzen, um Konkurrenten des Unternehmens negativ darzustellen, kann Art. 3 Abs. 1 Bst. a UWG zur Anwendung gelangen, sofern das Vorgehen die Konkurrenz, ihre Waren, Werke, Leistungen, Preise oder Geschäftsverhältnisse durch unrichtige, irreführende oder

---

188 Guides Concerning the Use of Endorsements and Testimonials in Advertising, FTC 16 CFR Part 255; zu finden unter: http://www.ftc.gov/os/2009/10/091005revisedendorsementguides.pdf.

189 Insb. Section 5 Federal Trade Commission Act (15 U.S.C. 45) to the use of endorsements and testimonials in advertising; zu finden unter: http://www.ftc.gov/ogc/ftcact.shtm . Die FTC überwacht die Einhaltung der Richtlinien; im Falle eines Verstosses kann die Behörde eine Untersuchung vornehmen, ob die betroffene Praxis gegen geltendes Recht verstösst; siehe hierzu: http://www.ftc.gov/opa/2009/10/endortest.shtm.

190 Die Richtlinien empfehlen werbenden Parteien überdies, Blogger, Celebrities u.dgl., welche werbend für sie tätig werden, über die Eigenschaften des Produkts und die Rechtslage umfassend aufzuklären, um irreführenden Werbeaussagen vorzubeugen. Zudem sollen sie Werbeaussagen der von ihnen engagierten Dritten auf ihre Richtigkeit und Angemessenheit überprüfen. Für unwahre und fehlleitende Aussagen über ein Produkt haften die werbende Partei wie auch die für sie tätig werdenden Dritten.

191 Bundesgesetz vom 19.12.1986 gegen den unlauteren Wettbewerb (UWG), SR 241.

192 Jöhri Yvonne, Werbung im Internet, Zürich 2000, S. 59.

193 Jung Peter/Spitz Philippe (Hrsg.), Bundesgesetz gegen den unlauteren Wettbewerb, Bern 2010, S. 180f.; Weber Rolf/Volz Stephanie, Online Marketing und Wettbewerbsrecht, Zürich 2011, S. 52.

194 Weber Rolf/Volz Stephanie, Online Marketing und Wettbewerbsrecht, Zürich 2011, S. 71f.

195 BBl 2011 4910.

unnötig verletzende Äusserungen herabsetzt[196].Die Schwierigkeit dürfte in diesem Bereich insbesondere in der Erkennung des Werbecharakters privater Auftritte in sozialen Netzwerken sowie im Nachweis der Verbindung engagierter Privater mit einem bestimmten Unternehmen liegen.

4.6.2 Manipulation der öffentlichen (politischen) Meinungsbildung

4.6.2.1 Ausgangslage

Ähnliche Methoden wie im kommerziellen Sektor können auch im Bereich der öffentlichen Meinungsbildung eingesetzt werden, um den politischen Diskurs zu beeinflussen, was insbesondere im Vorfeld von Wahlen und Abstimmungen problematisch erscheint. Profile sozialer Netzwerke, Netzwerkgruppen oder Blogs werden genutzt, um für einen Kandidaten oder eine Kandidatin sowie konkrete Abstimmungsgegenstände zu werben unter dem Anschein der Unabhängigkeit. Das Phänomen ist unter dem Begriff „Astroturfing“ bekannt.

Überdies sind Softwareprogramme in Entwicklung, die es Einzelpersonen erlauben sollen, mehrere Benutzerkonten in Blogs, Internetforen und sozialen Netzwerken zu verwalten, um so fingierte Meinungsmehrheiten zu schaffen[197].

4.6.2.2 Rechtslage in der Schweiz

Die Wahl- und Abstimmungsfreiheit gemäss Art. 34 Abs. 2 BV schützt in beschränktem Umfang auch vor Einflussnahmen privater Akteure auf die freie Willensbildung. Insbesondere im Vorfeld eines Urnenganges treffen den Staat gewisse Schutzpflichten. Verbreiten Private kurz vor einem Abstimmungstermin Inhalte, welche offensichtlich falsch oder irreführend sind, so müssen die Behörden die Stimmberechtigten allenfalls über das Verhalten der Privaten aufklären oder gewisse Inhalte richtigstellen. Eine Wiederholung der Abstimmung ist möglich in Fällen, in denen es wahrscheinlich erscheint, dass das private Verhalten das Abstimmungsergebnis entscheidend beeinflusst hat und die Behörden ihrer Aufklärungspflicht nicht nachgekommen sind.

Folglich soll der Staat im Hinblick auf versteckte politische Werbung in sozialen Netzwerken nur dann eingreifen, wenn die Verschleierung der eigentlichen Hintergründe des Auftritts in sozialen Medien zu einer Irreführung der Stimmberechtigten führen kann und diese kurz vor dem Abstimmungstermin erfolgte. Abstimmungsergebnisse werden nur aufgehoben, wenn es wahrscheinlich erscheint, dass sie durch derartige intransparente Methoden entscheidend beeinflusst wurden. Ist ein solcher Einfluss nicht nachweisbar und fällt das fragliche Verhalten nicht in den unmittelbaren Zeitraum vor Wahlen oder Abstimmungen, so soll insbesondere der öffentliche Diskurs zur Richtigstellung falscher oder irreführender Äusserungen Privater führen[198].

4.6.3 Unzulässige Werbung für bestimmte Produkte oder Dienstleistungen

4.6.3.1 Ausgangslage

Zum Schutz bestimmter öffentlicher Interessen gibt es in der Schweiz verschiedene Werbeverbote, die auch durch Kommunikation in sozialen Netzwerken missachtet werden können. Sie betreffen etwa die Werbung für Tabak oder bestimmte Heilmittel.

Prekär ist etwa die Einhaltung der Regeln im Bundesgesetz über die gebrannten Wasser (SR 680; Alkoholgesetz [AlkG]). Die für die Einhaltung des Alkoholgesetzes zuständige Koordinationsstelle für

---

[196] Jung Peter/Spitz Philippe (Hrsg.), Bundesgesetz gegen den unlauteren Wettbewerb, Bern 2010, S. 226ff.

[197] „Security-Firma entwirft Tools zur Meinungsmache mit Kunstfiguren“, heise online vom 20.02.2011; zu finden unter: http://www.heise.de/newsticker/meldung/Security-Firma-entwirft-Tools-zur-Meinungsmache-mit-Kunstfiguren-1193436.html .

[198] Siehe zu diesem Abschnitt: Müller Jörg Paul/Schefer Markus, Grundrechte in der Schweiz, 4. Aufl., Bern 2008, S. 618f. sowie Häfelin Ulrich/Haller Walter/Keller Helen, Schweizerisches Bundesstaatsrecht, 8. Aufl., Zürich 2012, S. 443f. Rz. 1392ff.

Handel und Werbung [KHW][199] hat vermehrt Facebookauftritte zu beurteilen. Dabei stellt sich das Problem, dass die nicht produktbezogenen Beiträge oft nicht vom Administrator der Seite stammen, sondern auf dessen Aufforderung freiwillig von Nutzern ("Friends") gepostet werden.

4.6.3.2 Rechtslage in der Schweiz

Auf die Schweiz ausgerichtete Werbeauftritte in den sozialen Medien haben insbesondere die Werbebeschränkungen in Art. 42b des Alkoholgesetzes zu respektieren. Es enthält auch Vorschriften zum Schutz der Jugend. So untersagt Art. 42b Abs. 3 Bst. e AlkG die Werbung für gebrannte Wasser „an Veranstaltungen, an denen vorwiegend Kinder und Jugendliche teilnehmen oder die vorwiegend für diese bestimmt sind". Ob derartige Veranstaltungen auch in sozialen Netzwerken stattfinden könnten, ist bislang nicht geklärt.

In der Praxis verschafft die Eidg. Alkoholverwaltung den Werbevorschriften nicht nur mit Mitteln des Verwaltungsstrafrechts Nachachtung, sondern auch durch verwaltungsrechtliche Verfügungen. Deren Durchsetzung wirft bei Äusserungen in sozialen Medien verschiedene Fragen auf: Wem ist ein Eintrag auf einer Plattform zuzurechnen? Wie lässt sich der im Ausland ansässige kommerzielle Anbieter eines Auftritts in den sozialen Medien ins Recht fassen?

4.7 Besondere Schutzbedürfnisse

4.7.1 Kinder und Jugendliche

4.7.1.1 Ausgangslage

Die Risiken, welche sich für Kinder und Jugendliche in sozialen Netzwerken ergeben können, sind unterschiedlicher Natur und gehen über die oben beschriebenen, tendenziell alle Nutzenden betreffenden Beeinträchtigungen von Individualinteressen hinaus. Problematisch sind insbesondere nicht jugendfreie und jugendschädliche Inhalte oder Kontaktaufnahmen Dritter, insbesondere jene sexuell motivierter Natur[200]. Nicht alle Kinder und Jugendliche verfügen über die nötigen technischen Fähigkeiten und das Problembewusstsein, um sich vor Risiken im Zusammenhang mit problematischen Kontaktaufnahmen oder der Weitergabe persönlicher Daten zu schützen[201]. Überdies mangelt es den verantwortlichen Betreuungspersonen, wie Eltern oder Lehrpersonal, häufig auch an dem nötigen Erfahrungsschatz und Fachwissen, um Kinder und Jugendliche sinnvoll über die Risiken in sozialen Netzwerken informieren zu können. Ein weiteres Problem können Freundschaften in sozialen Netzwerken zwischen Schülern und Lehrkräften darstellen, da sie das Risiko einer unangemessenen Nähe in sich bergen. Überdies können derartige Netzwerk-Kontakte Einsichten in das Privatleben der Schüler bzw. Lehrkräfte ermöglichen, welche das Verhältnis im Schulalltag belasten.

Ein Problem der technischen Umsetzbarkeit eines effektiven Jugendschutzes in sozialen Netzwerken ist u.a. die Mangelhaftigkeit bisher entwickelter Systeme zur Altersverifikation. Diese können nicht

---

[199] Die KHW überprüft einzig Werbeauftritte, welche einen eindeutigen Bezug zur Schweiz aufweisen (z.B. durch Sprache, Währung oderVerbreitung des Produkts).

[200] So besagt eine aktuelle Studie, dass sexuelle Übergriffe über elektronische Medien unter Jugendlichen in der Schweiz weit verbreitet sind. 9,5% der Jungen und 28% der Mädchen behaupteten hiervon betroffen gewesen zu sein. So gilt denn auch als wichtige Unterkategorie der sexuellen Übergriffe ohne Körperkontakt die sogenannte Cyberviktimisierung. Die Angaben umfassen jedoch elektronische Medien im Allgemeinen, womit nicht ausschliesslich soziale Netzwerke, sondern beispielweise auch Handy- oder E-Mail-Kommunikation erfasst sein können. Siehe Optimus Studie „Sexuelle Übergriffe an Kindern und Jugendlichen in der Schweiz“, Februar 2012, S. 9, 29f., 96f.

[201] Gemäss der Studie EU Kids Online 2011, welche auf einer Datenerhebung in 25 europäischen Staaten beruht, wissen etwa 64% der Kinder und Jugendlichen zwischen 11 und 16 Jahren, wie man unerwünschte Nachrichten Dritter blockiert und 56%, wie man seine Privatsphäreeinstellungen in sozialen Netzwerken verändert. Diese Zahlen verweisen auf eine grosse Minderheit von Kindern und Jugendlichen, denen es an der nötigen Sachkenntnis zur Vornahme der betreffenden Schutzmassnahmen mangelt. Überdies haben 29% der 9-12 Jährigen und 27% der 13-16 Jährigen ihre Profile öffentlich eingestellt und gibt ein Fünftel davon in öffentlich zugänglichen Profilen Informationen wie Adressen oder Telefonnummern an. Siehe EU Kids Online Final Report, September 2011, S. 17.

sicherstellen, dass die Angabe und das tatsächliche Alter der sich registrierenden Nutzenden übereinstimmen[202].

4.7.1.2 Lösungsansätze im Ausland oder internationalen Recht

Die Europarats-Empfehlung zu sozialen Netzwerken fordert den besonderen Schutz von Kindern und Jugendlichen bei der Verwendung sozialer Netzwerke. Dazu sollen Anbieter präventive Schutzmassnahmen vorsehen, Meldesysteme für problematische Inhalte einrichten und gegen Cyberbullying und Cybergrooming vorgehen.

Zudem fordert der Europarat die Mitgliedstaaten auf, Möglichkeiten der Beseitigung oder Löschung der von Kindern im Internet erstellten Inhalte zu überprüfen, welche deren Würde, Sicherheit oder Privatsphäre schaden könnten[203] und deren Medienkompetenz auszubauen[204]. Überdies empfiehlt er die Schaffung eines geschützten Raums für Kinder im Internet, wozu insbesondere die Einführung eines paneuropäischen Labels für verantwortungsvolle Zertifizierungssysteme für Online-Inhalte führen soll[205]

Auch der Vorschlag zur EU Datenschutz-Grundverordnung [206] enthält spezifische Bestimmungen zum Schutz von Kindern. So soll die Verarbeitung personenbezogener Daten eines Kindes, dem Dienste der Informationsgesellschaft angeboten werden, bis zu dessen *vollendeten 13. Lebensjahr* nur unter Einwilligung der Eltern oder des Vormundes zulässig sein[207]. Gemäss Art. 11 hat die Aufklärung über die Datenverarbeitung in Form und Sprache kindergerecht zu erfolgen, sofern sich diese an Kinder richtet.

Unter dem Programm „Sicheres Internet“ 2009-2013[208] fördert die EU die Sensibilisierung der Öffentlichkeit, die Einrichtung eines Netzes öffentlicher Anlaufstellen für die Meldung illegaler und schädlicher Inhalte (Grooming, Cyberbullying etc.), Initiativen zur Selbstregulierung und die Einbeziehung von Kindern in die Schaffung eines sicheren Online-Umfelds sowie den Aufbau einer Wissensbasis zu neuen Trends bei der Nutzung von Online-Technologien und ihren Folgen für den Alltag von Kindern[209].

Ein Teilbestand des Programms ist die Förderung der *Selbstregulierung der Internetbranche*. In diesem Rahmen unterzeichneten 2009 die wichtigsten in Europa tätigen sozialen Netzwerke die „Safer Social Networking Principles for the EU“[210]. Die Prinzipien sehen unter anderem vor, dass Nutzerprofi-

---

[202] Gemäss Studie EU Kids Online 2011 geben 27% der 9-12 Jährigen in sozialen Netzwerken ein falsches Alter an und besitzen 38% der 9-12 Jährigen ein Profil in sozialen Netzwerken. Siehe EU Kids Online Final Report, September 2011, S. 18.

[203] Erklärung des Europarats zum Schutz der Würde, Sicherheit und Privatsphäre von Kindern im Internet.

[204] Empfehlung Rec(2006)12 über die Befähigung von Kindern zum Umgang mit den neuen Informations- und Kommunikationstechnologien.

[205] Empfehlung CM/Rec(2009)5 zum Schutz der Kinder gegen schädliche Inhalte und Verhaltensweisen und zur Förderung ihrer aktiven Beteiligung am neuen Informations- und Kommunikationsumfeld.

[206] Vorschlag EU Datenschutz-Grundverordnung, KOM(2012) 11 endgültig. Zu EU-Bestrebungen im Bereich des Kinderschutzes siehe auch die Mitteilung der Kommission „Europäische Strategie für ein besseres Internet für Kinder“, KOM(2012) 196 endgültig, mit umfassenden Forderungen und Empfehlungen der Kommission.

[207] Siehe Art. 8 Vorschlag EU Datenschutz-Grundverordnung, KOM(2012) 11 endgültig.

[208] Beschluss Nr. 1351/2008/EG des Europäischen Parlaments und des Rates vom 16. Dezember 2008 über ein mehrjähriges Gemeinschaftsprogramm zum Schutz der Kinder bei der Nutzung des Internets und anderer Kommunikationstechnologien, ABl. L 348 vom 24.12.2008, S. 118–127.

[209] Siehe http://europa.eu/legislation_summaries/information_society/internet/l24190d_de.htm sowie Mitteilung der Kommission „Zwischenbewertung des Mehrjahresprogramms der Union zum Schutz der Kinder bei der Nutzung des Internets und anderen Kommunikationstechnologien“, KOM(2012) 33 endgültig.

[210] Links zu den „Safer Social Networking Principles“ sowie den Umsetzungsberichten der EU-Kommission finden sich unter: http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm . Eine weitere Selbstregulierungsvereinbarung auf EU-Ebene ist die im Dezember 2011 gegründete “CEO Coalition to make the Internet a better place for kids“. Grundlagendokumente und Informationen über die Vereinbarung finden sich unter: http://ec.europa.eu/information_society/activities/sip/self_reg/index_en.htm .

le von Kindern automatisch als privat eingestellt sind und effiziente Bericht- und Löschmechanismen für problematische Inhalte und Kontaktaufnahmen vorgesehen werden. Zudem sollen einfach verständliche Informationen über Sicherheit und Privatsphäre in sozialen Netzwerken sowie gut entwickelte Privatsphäreeinstellungen angeboten werden. Auch soll die Kontaktaufnahme mit Kindern durch Fremde unterbunden werden und Benutzerprofile von Kindern über Suchmaschinen unzugänglich sein

4.7.1.3 Rechtslage in der Schweiz

Die im Bericht dargestellten allgemeinen Rechtsvorschriften, die dem Schutz vor den Risiken sozialer Netzwerke dienen können, wie etwa das Datenschutzrecht oder der zivilrechtliche und strafrechtliche Persönlichkeitsschutz, schützen auch Kinder und Jugendliche. Für Kinder sind insbesondere einschlägig die Schutzinstrumente gegen Cyberbullying und Cyberstalking (s. Ziff. 4.4.2), Identitätsdiebstahl (s. Ziff. 4.4.3.), Pornografie (s. Ziff. 4.5.2) sowie die im Bericht angesprochenen Gesundheitsrisiken sozialer Netzwerke (s. Ziff. 4.5.4).

Neben diesen allgemeinen Schutzvorschriften kennt die schweizerische Rechtsordnung aber auch eine Vielzahl von Bestimmungen, die sich spezifisch dem Schutz und der Förderung von Kindern und Jugendlichen widmen. So kommen die besonderen Bedürfnisse von Kindern in der Bundesverfassung sowie in diversen für die Schweiz verbindlichen internationalen Übereinkommen zum Ausdruck[211]. Auf Gesetzes- und Verordnungsstufe sind besondere Schutzvorschriften beispielsweise im Strafrecht[212], im Zivilrecht[213], in der Radio- und Fernsehgesetzgebung[214], im Arbeitsrecht[215] oder in der Lebensmittelregulierung (Alkoholabgabe)[216] vorgesehen. Auch im Bereich der Jugendförderung wurde der Bundesgesetzgeber tätig[217].

Darüber hinaus gibt es bislang keine bundesrechtlichen Jugendschutzbestimmungen, welche spezifisch auf die Regulierung sozialer Netzwerke ausgerichtet sind. Gewisse Vorschriften zum Schutz von Kindern und Jugendlichen greifen allerdings auch in sozialen Netzwerken, wie etwa das Werbeverbot für Tabak oder Alkohol gegenüber Jugendlichen[218] oder das Verbot Jugendlichen unter 16 Jahren Pornografie zugänglich zu machen.

Für den Schutz von Kindern und Jugendlichen genügen rechtliche Instrumente allein nicht. Eine wichtige Rolle spielt auch das Verhalten der Eltern. Im Rahmen ihrer elterlichen Sorge können sie den Umgang ihrer Kinder mit sozialen Netzwerken und ihren persönlichen Daten bestimmen, soweit die Kinder bezüglich ihrer Handlungen in sozialen Netzwerken nicht urteilsfähig sind oder ihre Urteilsfä-

---

[211] Siehe Art. 11, 19, 41, 62, 67, 123b BV. Im Bereich internationaler Verträge siehe etwa das Übereinkommen vom 20.11.1989 über die Rechte des Kindes, SR 0.107, inklusive Fakultativprotokolle, oder auch das Übereinkommen Nr. 182 vom 17.06.1999 über das Verbot und unverzügliche Massnahmen zur Beseitigung der schlimmsten Formen der Kinderarbeit, SR 0.822.728.2. Das Übereinkommen des Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch vom 25.10.2007 wurde vom Bundesrat und von der Bundesversammlung genehmigt; siehe BBl 2012 7571 bzw. BBl 2012 7653.

[212] Art. 5, 136, 187, 188, 195, 197, 213, 219, 220, 363f., 264f StGB; Bundesgesetz vom 20.06.2003 über das Jugendstrafrecht (JStG), SR 311.1; Schweizerische Jugendstrafprozessordnung vom 20.03.2009 (JStPO), SR 312.1.

[213] Art. 296ff., 307-317 ZGB.

[214] Art. 5, 13 RTVG sowie Art. 4, 16 RTVV.

[215] Jugendarbeitsschutzverordnung vom 28.09.2007 (ArGV 5), SR 822.115; Verordnung des WBF vom 4.12.2007 über gefährliche Arbeiten für Jugendliche, SR 822.115.2.

[216] Art. 11 Lebensmittel- und Gebrauchsgegenständeverordnung vom 23.11.2005 (LGV), SR 817.02.

[217] Bundesgesetz vom 30.09.2011 über die Förderung der ausserschulischen Arbeit mit Kindern und Jugendlichen (KJFG), SR 446.1; Verordnung vom 17.10.2012 über die Förderung der ausserschulischen Arbeit mit Kindern und Jugendlichen (KJFV), SR 446.11; Verordnung vom 11.06.2010 über Massnahmen zum Schutz von Kindern und Jugendlichen sowie zur Stärkung der Kinderrechte, SR 311.039.1.

[218] Art. 18 Verordnung vom 27.10.2004 über Tabakerzeugnisse und Raucherwaren mit Tabakersatzstoffen (TabV), SR 817.06 sowie Art. 4 Verordnung des EDI vom 23.11.2005 über alkoholische Getränke, SR 817.022.110.

higkeit zumindest zweifelhaft ist. Ob ein Kind urteilsfähig ist kann nicht abstrakt bestimmt, sondern nur im Hinblick auf eine konkrete Handlung beurteilt werden[219].

Betreffen die Handlungen eines urteilsfähigen Kindes dessen höchstpersönliche Rechte, so gelangt die elterliche Vertretungsmacht an ihre Grenzen[220]. Urteilsfähige Kinder üben jene Rechte, die ihnen um ihrer Persönlichkeit willen zustehen, selbstständig aus, soweit das Gesetz nicht die Zustimmung ihres gesetzlichen Vertreters verlangt (Art. 19c ZGB). Dies ist für die Tätigkeiten in sozialen Netzwerken von Bedeutung, da diese regelmässig jene Rechte Nutzender betreffen, die ihnen um ihrer Person willen zustehen. Urteilsfähige Kinder brauchen also grundsätzlich nicht die Zustimmung ihres gesetzlichen Vertreters, um persönliche Daten über sich selbst, wie etwa Fotos u.dgl., oder selbsterstellte Inhalte in sozialen Netzwerken zu veröffentlichen. Auch ist die Einwilligung des urteilsfähigen Kindes in eine Persönlichkeitsverletzung grundsätzlich gültig (Art. 13 Abs. 1 DSG; Art. 28 Abs. 2 ZGB).[221]

Mit dem 2010 vom Bundesrat lancierten nationalen Programm „Jugendmedienschutz und Medienkompetenz“ sollen Kinder und Jugendliche über die Chancen und Risiken im Online-Bereich sensibilisiert und Eltern, Lehrpersonen und weitere Erziehungsberechtigte mit geeigneten Massnahmen zur Begleitung von deren Internetaktivitäten befähigt werden. Social Media werden in diesem Zusammenhang berücksichtigt. Unter anderem zeigt die Website http://www.jugendundmedien.ch/de.html , Massnahmen zur Unterstützung von Eltern, Erziehungsberechtigten und Schulen auf.

Der Bundesrat hat 2011 im Evaluationsbericht zum DSG in Aussicht gestellt, Massnahmen zu einem verbesserten Datenschutz von Minderjährigen zu prüfen, welche dem Umstand Rechnung tragen, dass sie sich der Risiken der Verarbeitung personenbezogener Daten weniger bewusst sind als Erwachsene.[222]

4.7.2 Arbeitnehmende

4.7.2.1 Ausgangslage

International[223], aber auch in der Schweiz[224] werden im Zusammenhang mit sozialen Netzwerken häufig die Risiken der Offenlegung persönlicher Daten in Hinblick auf zukünftige Bewerbungsvorhaben diskutiert. Es ist bekannt, dass Arbeitgeber in Rekrutierungsprozessen Internetsuchmaschinen nutzen, um sich über potenzielle zukünftige Angestellte zu informieren. Oft ist Nutzenden nur unzureichend bewusst, dass die von ihnen einmal auf einer Plattform bereitgestellten Informationen je nach Privatsphäreeinstellung über externe Suchmaschinen auffindbar sind. Ausserdem können sich Arbeitgeber über die Nutzerprofile Dritter Zugang zu Informationen verschaffen, welche Bewerbende in sozialen Netzwerken preisgeben.

4.7.2.2 Lösungsansätze im Ausland oder internationalen Recht

Ein Gesetzesentwurf zur Änderung des deutschen Bundesdatenschutzgesetzes befasst sich mit dem zulässigen Umfang der Datenerhebung vor der Begründung eines Beschäftigungsverhältnisses (Bewerberdatenschutz)[225]. Der Entwurf verbietet Arbeitgebern Daten über Bewerbungskandidaten in so-

---

[219] BSK-ZGB I, Bigler-Eggenberger Margrith, 4. Aufl., Basel 2010, Art. 16, S. 177f. Rz. 14f.

[220] BSK-ZGB I, Schwenzer Ingeborg, 4. Aufl., Basel 2010, Art. 304/305, S. 1606 Rz. 6.

[221] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, S. 104 N. 70.

[222] Bericht zur Evaluation des Bundesgesetzes über den Datenschutz vom 9.12.2011, Ziff. 5.2.2 (BBl 2012 350)

[223] Siehe etwa die Stellungnahme „Verantwortlicher Umgang mit sozialen Netzwerken und Verhinderung der durch soziale Netzwerke verursachten Probleme“, 2012/C 351/07, S. 2, 7, 10.

[224] „Schweizer Konzerne überprüfen Bewerber im Internet“, Tagesanzeiger vom 02.05.2011, http://www.tagesanzeiger.ch/leben/gesellschaft/Schweizer-Konzerne-ueberpruefen-Bewerber-im-Internet/story/17153295?dossier_id=510.

[225] Gesetzesentwurf Beschäftigtendatenschutz, 17/4230.

zialen Netzwerken zu erheben, selbst wenn diese allgemein zugänglich sind (beispielsweise über externe Suchmaschinen). Professionelle Netzwerke (wie etwa Xing oder LinkedIn) sind von der Regel ausgeschlossen. Die Entwicklung des Vorhabens ist insbesondere vor dem Hintergrund der derzeitigen Revision des Europäischen Datenschutzrechts abzuwarten.

Seit Februar 2013 liegt dem U.S.-amerikanischen Kongress der Entwurf eines Gesetzes vor[226], welcher es Arbeitgebern, Hochschuleinrichtungen und lokalen Ausbildungsstätten verbietet, Angestellte, Bewerbungskandidaten, Studierende und Schüler um Benutzername, Passwort oder sonstige Zugangsmöglichkeiten zu ihren Konten auf sozialen Netzwerken oder zu ihren privaten E-Mailkonten zu bitten. Auch dürfen den Betroffenen keine Nachteile erwachsen, wenn sie die Preisgabe derartiger Informationen verweigern. In einigen U.S.-Bundesstaaten, etwa in Kalifornien, Maryland und Illinois, sind ähnliche Gesetzesvorschriften bereits in Kraft getreten[227].

4.7.2.3 Rechtslage in der Schweiz

Ob und in welchem Umfang sich Arbeitgeber in sozialen Medien über Bewerbungskandidaten informieren dürfen, ist in der Schweiz gesetzlich nicht ausdrücklich geregelt. Art. 328b OR erlaubt dem Arbeitgeber Daten über den Arbeitnehmer zu bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Dass sich die Vorschrift auf die Bewerbungsphase vor dem Bestehen eines Arbeitsverhältnisses erstreckt, wird vom Bundesgericht und einem gewichtigen Teil der Lehre bejaht, doch gibt es auch Gegenmeinungen[228]. Dadurch ergibt sich bereits aus dem Wortlaut der Norm eine sachliche Grenze bezüglich der Daten, welche der Arbeitgeber über einen Bewerbungskandidaten erheben darf. Private, nicht professionelle Nutzerprofile in sozialen Netzwerken mögen gewisse Informationen enthalten, welche Auskunft über die Eignung des Arbeitnehmers geben. Darüber hinaus enthalten private Nutzerprofile üblicherweise aber vor allem Informationen ausserhalb des Anwendungsbereichs von Art. 328b OR, da Angaben aus dem Privatbereich nur ausnahmsweise unter den Begriff der Daten über die Eignung des Arbeitnehmers fallen[229]. Da der Arbeitgeber bei deren Abruf unweigerlich alle Inhalte eines Nutzerprofils wahrnimmt, ist es äusserst fraglich, ob er gestützt auf Art. 328b OR einen Anspruch auf Einsicht in die privaten Netzwerkprofile von Bewerbungskandidaten haben kann. Ein Teil der Lehre ist denn auch der Auffassung, eine generelle Recherche im Internet mithilfe einer Suchmaschine oder in sozialen Netzwerken mit privater Ausrichtung verstosse gegen Art. 328b OR[230].

Verschafft sich der Arbeitgeber durch eine verbotene Handlung (etwa in Verletzung von Art. 143bis Abs. 1, Art. 179^{novies} oder Art. 181 StGB) Zugang zu einem privaten Nutzerprofil, so verletzt er neben den strafrechtlichen Bestimmungen auch den Grundsatz der Rechtmässigkeit der Datenbearbeitung (Art. 4 Abs. 1 DSG). Die Grundsätze von Treu und Glauben sowie der Erkennbarkeit der Datenbearbeitung (Art. 4 Abs. 2 und 4 DSG) wiederum untersagen eine heimliche Datenbeschaffung durch den Arbeitgeber. Ist ein Nutzerprofil privat und ein Arbeitgeber durch dessen Besitzer nicht zugelassen dieses zu sichten, so liegt überdies wohl eine Verletzung von Art. 12 Abs. 2 lit. b DSG vor, wenn sich der Arbeitgeber Zugang zu dem Profil verschafft. Erbittet sich der Arbeitgeber Zugang zu dem privaten Nutzerprofil eines Bewerbungskandidaten, so ist die Freiwilligkeit der Einwilligung des Bewerbungs-

---

[226] Social Networking Online Protection Act vom 06.02.2013, H.R.537.

[227] Kalifornien schützt private Online-Kommunikation vor Arbeitgebern und Unis, heise online (02.10.2012), http://www.heise.de/newsticker/meldung/Kalifornien-schuetzt-private-Online-Kommunikation-vor-Arbeitgebern-und-Unis-1721503.html .

[228] Siehe Urteil des BGer 2C_103/2008 vom 30. Juni 2008, E. 6.2. Für die Anwendung von Art. 328b OR auf die Bewerbungsphase: BSK-OR I, Portmann Wolfgang, 5. Aufl., Basel 2011, Art. 328b, S. 1952 Rz. 34ff. sowie Streiff Ullin/von Kaenel Adrian/Roger Rudolph, Arbeitsvertrag Praxiskommentar, 7. Aufl., Zürich 2012, Art. 328b, S. 580 N. 4. Dagegen Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, S. 731 N. 25.

[229] BSK-OR I, Portmann Wolfgang, 5. Aufl., Basel 2011, Art. 328b, S. 1947 Rz. 8; Streiff Ullin/von Kaenel Adrian/Roger Rudolph, Arbeitsvertrag Praxiskommentar, 7. Aufl., Zürich 2012, Art. 328b, S. 581f. N. 5.

[230] Egli Urs, Soziale Netzwerke und Arbeitsverhältnis, in: Jusletter 17.01.2011, Rz. 65ff.; Streiff Ullin/von Kaenel Adrian/Roger Rudolph, Arbeitsvertrag Praxiskommentar, 7. Aufl., Zürich 2012, Art. 328b, S. 597 N. 10.

kandidaten grundsätzlich in Frage zu stellen, da er die Nachteile einer Verweigerung befürchten könnte.

Fraglich ist, inwiefern die Recherche des Arbeitgebers von im Internet allgemein zugänglichen Daten (Art. 12 Abs. 3 DSG) – beispielsweise öffentliche Nutzerprofile in sozialen Netzwerken – rechtlich eingeschränkt ist. Es wird die Ansicht vertreten, eine Persönlichkeitsverletzung liege vor, wenn ein Arbeitgeber als Teilnehmer in einem Netzwerk privater Prägung allgemein zugängliche Daten über einen Bewerbungskandidaten recherchiert, die in keinem Zusammenhang mit dessen vergangener oder künftiger beruflichen Tätigkeit stehen. Liege bei einem Netzwerk wie Facebook der Fokus auf dem Privatleben, so würden Informationen durch den Arbeitgeber für Zwecke missbraucht, an die der Betroffene im Zeitpunkt der Veröffentlichung nicht gedacht habe.[231] Allerdings wird sich in der Praxis kaum je nachweisen lassen, ob ein Arbeitgeber mittels einfacher Websuche zugängliche Daten eingesehen hat. Bei beruflichen sozialen Netzwerken (z.B. XING, LinkedIn) ist davon auszugehen, dass diese vom Besitzer bewusst erstellt wurden, damit sich potenzielle Arbeitgeber über die dort veröffentlichten Daten informieren können. [232] Aber auch hier sind viele Informationen wiederum nur Mitgliedern des Netzwerkes zugänglich.

Für eine sinnvolle Lösung der in diesem Zusammenhang auftretenden Probleme sollten Plattformbetreiber ausreichende Privatsphäreeinstellungen anbieten, Arbeitgeber die Privatsphäre von Bewerbungskandidaten grundsätzlich achten und sich Nutzende sozialer Netzwerke ihrer Eigenverantwortung bei der Veröffentlichung von Daten bewusst sein. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte empfiehlt Nutzenden in seinen Erläuterungen zu Sozialen Netzwerken denn auch, sich vor der Veröffentlichung persönlicher Daten Gedanken darüber zu machen, ob sie mit diesen in einem späteren Bewerbungsgespräch konfrontiert werden wollen[233].

4.7.3 Menschen mit Behinderung

4.7.3.1 Ausgangslage

Die neuen Informations- und Kommunikationstechnologien (IKT), soziale Netzwerke mit einbezogen, eröffnen Menschen mit Behinderungen neue Möglichkeiten, am sozialen Leben teilzunehmen, sich zu informieren und auszutauschen. Voraussetzung dafür ist jedoch die barrierefreie Ausgestaltung des Internets bzw. der über das Internet angebotenen Informations-, Kommunikations- und Transaktionsdienstleistungen.

4.7.3.2 Lösungsansätze im Ausland oder internationalen Recht

Empfehlungen auf internationaler Ebene (Web Content Accessibility Guidelines WCAG 2.0 des World Wide Web Konsortiums) bezwecken, die Zugänglichkeit der IKT für Nutzende mit Behinderungen sicherzustellen[234]. Auch die Europarats-Empfehlung CM/Rec(2012)4 über den Menschenrechtsschutz in sozialen Netzwerken fordert die Betreiber sozialer Netzwerke auf, die Zugänglichkeit ihrer Dienste für Menschen mit Behinderung zu garantieren.

4.7.3.3 Rechtslage in der Schweiz

Eine rechtliche Verpflichtung, soziale Medien im Rahmen der Verhältnismässigkeit hindernisfrei anzubieten, besteht in der Schweiz für die Gemeinwesen. Dies ergibt sich allgemein aus dem Diskriminierungsverbot (Art. 8 Abs. 2 BV) und, spezifisch für den Bund, aus dem Behindertengleichstellungsgesetz[235], in dessen Geltungsbereich auch Dienstleistungen über das Internet fallen[236]. Privaten Anbie-

---

[231] So etwa Egli Urs, Soziale Netzwerke und Arbeitsverhältnis, in: Jusletter 17.01.2011, Rz. 66ff.

[232] Egli Urs, Soziale Netzwerke und Arbeitsverhältnis, in: Jusletter 17.01.2011, Rz. 70f.

[233] Siehe http://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00693/index.html?lang=de.

[234] http://www.w3.org/TR/WCAG/ .

[235] Bundesgesetz vom 13.12.2002 über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen (BehiG), SR 151.3.

ter/innen von Dienstleistungen, die grundsätzlich von jedermann beansprucht werden können, ist gemäss Art. 6 BehiG lediglich verboten, Behinderte wegen ihrer Behinderung zu diskriminieren. Eine Verpflichtung, internetbasierte Angebote barrierefrei anzubieten, lässt sich daraus nicht ableiten.

Angesichts der Bedeutung, die soziale Medien generell, als auch in Bezug auf die Förderung der Teilhabe von Menschen mit Behinderungen am gesellschaftlichen Leben haben, ist die Gewährleistung eines barrierefreien Zugangs zu Social-Media-Angeboten äusserst wünschenswert. Gesetzgeberische Massnahmen auf nationaler Ebene würden gerade bei den meist genutzten Social Media-Angeboten jedoch kaum greifen. Es erscheint aber sinnvoll, mit anderen Massnahmen und im Verbund mit zentralen Stakeholdern auf eine Beachtung der Accessibility-Standards hinzuwirken.

4.8 Postulat Amherd 12.3545 „Facebook Zugang für Kinder“

Das Postulat 12.3545[237] beauftragt den Bundesrat aufzuzeigen, mit welchen Massnahmen Kinder vor den schädlichen Auswirkungen von Social Media in der Schweiz geschützt werden können. Neben Anpassungen der Gesetzgebung sind Massnahmen zur Unterstützung von Eltern, Erziehungsberechtigten und Schulen aufzuzeigen. Weiter ist zu prüfen, ob es sinnvoll ist, die Profile von Kindern mit denen ihrer Eltern auf Facebook zu verknüpfen und welche Möglichkeiten elektronische Identitätsausweise wie die SuisseID in diesem Zusammenhang bieten. Befragungen haben ergeben, dass in der Schweiz nur sehr wenige unter 13-Jährige ein Profil bei einer sozialen Netzwerkplattform eingerichtet haben. [238]

Die Überlegungen von Facebook, die Alterslimite für die Nutzung unter 13 Jahre zu senken und die Profile von unter 13-Jährigen mit denen ihrer Eltern zu verknüpfen, könnten einen monetären Hintergrund haben, denn so kann eine neue Kundengruppe erschlossen werden, die insbesondere für den ständig wachsenden und auf Facebook beworbenen Spielemarkt von Interesse ist. Die Bindung an das Profil ihrer Eltern könnte bei Vertragsabschlüssen durch Kinder die (stillschweigende oder ausdrückliche) Zustimmung der Eltern zum Vertrag erwirken. Zum anderen ist es denkbar, dass Facebook durch Eigeninitiative einer staatlichen Regelung vorzugreifen und diese dadurch obsolet werden zu lassen versucht.[239]

Wie in Kap. 4.6.1.3 bereits dargestellt, schützen die allgemeinen Rechtsvorschriften, die dem Schutz vor den Risiken sozialer Netzwerke dienen können, auch Kinder und Jugendliche. Daneben gelten zahlreiche spezifische Bestimmungen zum Schutz und zur Förderung von Kindern und Jugendlichen, die ebenfalls in Social Media Anwendung finden.

Eine Bindung der Profile von Kindern an diejenigen ihrer Eltern ist aus verschiedenen Gründen problematisch. Sie setzt voraus, dass auch die Eltern ein Profil auf dieser Social-Media-Plattform haben und dieses bewirtschaften. Dies wäre für die betreffende Plattform selbst sicher von Vorteil, dürfte aber von vielen Eltern abgelehnt werden, die die Plattform aus welchen Gründen auch immer nicht nutzen möchten. Ausserdem könnte eine Verknüpfung der Profile von Eltern und Kindern eine Einschränkung der Persönlichkeitsrechte urteilsfähiger Kinder zur Folge haben.

---

[236] Für Internetdienstleistungen des Bundes schreibt Art. 10 der Verordnung vom 19.11.2003 über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen (BehiV), SR 151.31, vor, sämtliche Internetangebote, und somit Social Media, seien für Menschen mit Behinderungen zugänglich zu gestalten. Referenzstandard für die Webseiten des Bundes ist die Norm P028 - "Richtlinien des Bundes für die Gestaltung von barrierefreien Internetangeboten“. Siehe http://www.isb.admin.ch/themen/standards/alle/03237/ .

[237] http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20123545#

[238] In Deutschland scheint das Problem bei einem durchschnittlichen Alter von 12,7 Jahren für die erste Anmeldung ausgeprägter zu sein: Caspar Johannes, Soziale Netzwerke und Einwilligung der Nutzer, in: digma 2013, S. 62. Gemäss Dreyer, Stephan/Hasebrink, Uwe/Lampert, Claudia/Schröder, Hermann-Dieter, Entwicklungs- und Nutzungstrends im Bereich der digitalen Medien und damit verbundene Herausforderungen für den Jugendmedienschutz. In: Beiträge zur sozialen Sicherheit. Forschungsbericht Nr. 9/13, Kap. 2.4, S.27 (Publikation in Vorbereitung) kommt der Unterschied überwiegend dadurch zustande, dass in der Schweiz nur sehr wenige unter 13-Jährige ein solches Profil haben. Zudem scheinen die Schweizer Kinder und Jugendlichen deutlich seltener ihre Profile öffentlich einsehbar eingestellt zu haben.

[239] Siehe z.B. http://online.wsj.com/article/SB10001424052702303506404577444711741019238.html#.

Damit ein standardisierter elektronischer Identitätsnachweis für die Überprüfung des Alters etc. auf einer Social-Media-Plattform eingesetzt werden könnte, müsste diese in ihrem System die Voraussetzungen dafür schaffen und die Identitätsnachweise jeweils prüfen. Ob die SuisseID den Anforderungen von Facebook in diesem Zusammenhang genügen würde, kann heute nicht beantwortet werden.

4.9 Versuch einer Gesamtwürdigung der aktuellen Rechtslage

Was die im vorliegenden Kapitel 4 dargestellten gesetzlichen Regelungen für die verschiedenen durch Social Media aufgeworfenen Rechtsfragen betrifft, so ergibt sich ein ausgesprochen facettenreiches Gesamtbild. Verallgemeinernde Aussagen sind schwierig. Grob gesagt lässt sich aber aufgrund bisheriger Erfahrungen festhalten, dass die oft weit formulierten Regelungen des geltenden schweizerischen Gesetzesrechts im Konfliktfall so interpretiert und angewendet werden können, dass ausgewogenen Lösungen möglich sind. Grössere Regelungslücken springen nicht ins Auge.

Die bisherige Praxis schweizerischer Gerichte und Behörden ist allerdings noch spärlich. So fragt es sich, ob das bestehende Recht genügende Anreize für Betroffene schafft, sich aktiv für ihre Rechte einzusetzen. Verbesserungspotenzial dürfte es beispielsweise in verschiedenen datenschutzrechtlichen Aspekten geben (wie etwa den Ressourcen des EDÖB und der fehlenden Pflicht zu datenschutzfreundlichen Voreinstellungen; vgl. vorne Ziff. 4.3.1.5). Gerade technische Entwicklungen könnten dazu beitragen, dass die Bevölkerung bestehende Rechtsansprüche wirkungsvoller wahrnehmen kann.

Darüber hinaus bleibt in manchen Bereichen eine gewisse Unsicherheit, ob die Anwendung der allgemeinen Vorschriften auf die neuen Rechtsfragen in einem vor Gericht ausgetragenen Konflikt tatsächlich zu praktisch befriedigenden Ergebnissen führen wird. Diese Unsicherheit hat nicht zuletzt damit zu tun, dass die praktische Durchsetzung bestehender Rechtsansprüche im internationalen Umfeld sozialer Plattformen prekär sein kann.

5 Grundproblem: Durchsetzung des Rechts

5.1 Allgemeines

In Kapitel 4 wurde für die einzelnen Fragestellungen untersucht, ob das geltende schweizerische Recht (insbesondere im DSG, ZGB, UWG und StGB) die spezifischen rechtlichen Probleme sozialer Netzwerke adäquat erfasst.

Eine zentrale und an dieser Stelle zu vertiefende Problematik ist die Durchsetzung geltenden Rechts, denn die für eine Rechtsverletzung Verantwortlichen (z.B. die Verfasser rechtswidriger Beiträge auf einer sozialen Plattform) können oft nicht zur Rechenschaft gezogen werden. Es stellt sich mithin die Frage, ob das schweizerische Recht die Verantwortlichkeiten der Beteiligten ausreichend klärt.

Zudem sind die Betreiber sozialer Netzwerke häufig international tätig, weshalb die nationale Gesetzgebung wesensgemäss an ihre Grenzen stösst.

5.2 Verfolgung der Verfasser rechtswidriger Einträge auf Plattformen

5.2.1 Das Problem der Anonymität

Wie oben im 4. Kapitel aufgezeigt, können Einträge auf sozialen Plattformen eine Vielzahl verschiedener Vorschriften des Strafrechts (z.B. üble Nachrede, Pornografie, Rassendiskriminierung, öffentliche Aufforderung zu Verbrechen oder Gewalttätigkeit) oder des Zivilrechts (z.B. Persönlichkeitsschutz) verletzen. In der Rechtswirklichkeit gestaltet sich die Durchsetzung dieser Vorschriften oft schwierig. So lassen sich die verantwortlichen Verfasser möglicherweise rechtswidriger Beiträge nur zur Rechenschaft ziehen, wenn deren Identität bekannt ist. Dies ist nicht immer gegeben, da anonyme (oder unter einem Pseudonym veröffentlichte) Einträge in den Kommentarspalten von Blogs oder auf Plattformen wie Facebook an der Tagesordnung sind. Eine eindeutige Identifizierung ist in solchen Fällen schwierig bis unmöglich.

Mitunter können Strafverfolgungsbehörden in der Schweiz allerdings Spuren verfolgen, etwa durch Zugriff auf die sog. IP-Adressen, d.h. Internet-Netzwerkadressen, die der Internet-Benutzer normalerweise nicht zu Gesicht bekommt. Sie werden von den System-Betreibern in der Regel aufgezeichnet, wenn ein Benutzer beispielsweise eine Social-Media-Plattform benutzt oder eine E-Mail versendet. Ob

dieser Zugriff möglich und zulässig ist, hängt auch davon ab, wer die entsprechende Plattform betreibt.

5.2.2 Anonyme Beiträge auf Plattformen beruflicher Medienschaffender

Die schweizerische Rechtsordnung anerkennt seit langem, dass anonymen Publikationen durchaus nicht immer verwerfliche Motive zu Grunde liegen.[240] Das Strafgesetzbuch schützt die anonyme Publikation in erheblichem Umfang sogar ausdrücklich. Nach Art. 28a StGB und Art. 172 StPO dürfen alle Personen die Identität des Autors geheim halten, die sich beruflich mit der Veröffentlichung von Informationen im redaktionellen Teil eines periodisch erscheinenden Mediums befassen. Sie und ihre Hilfspersonen haben etwa das Recht, die von den Strafverfolgungsbehörden verlangte Herausgabe der IP-Adressen anonymer Autoren zu verweigern. Dieses Recht greift auch auf sozialen Plattformen wie Blogs, falls sie von professionellen Medienschaffenden betrieben werden. So akzeptierte das Bundesgericht die Weigerung der SRG, der Zuger Staatsanwaltschaft die IP-Adresse einer Person zu übermitteln, die in der Kommentarspalte des SRG-Blogs zur Fernsehsendung Alpenfestung unter falschem Namen einen angeblich ehrverletzenden Kommentar platziert hatte.[241] Kann der Autor nicht ermittelt oder in der Schweiz nicht vor Gericht gestellt werden, so kommt eine Bestrafung des verantwortlichen Redaktors (oder ersatzweise der für die Veröffentlichung verantwortlichen Person) wegen Nichtverhinderns einer strafbaren Veröffentlichung (Art. 322bis StGB) in Betracht.

5.2.3 Anonyme Beiträge auf anderen Plattformen

Anders ist die Situation bei Betreibern von Plattformen, die nicht beruflich als Medienschaffende tätig sind. Sie können durch die zuständigen Behörden zur Herausgabe der IP-Adressen tatverdächtiger Personen verpflichtet werden. Die entsprechenden Daten sind gemäss dem Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR 780.1) zu speichern. Das BÜPF verpflichtet neben allen Anbieterinnen von Fernmeldedienstleistungen auch Internet-Anbieterinnen (Art. 1 Abs. 2) dazu, die für die Teilnehmeridentifikation notwendigen Daten sowie die Verkehrs- und Rechnungsdaten während sechs Monaten aufzubewahren (Art. 15 Abs. 3) und diese dem Dienst für die Überwachung des Post- und Fernmeldeverkehrs auf Verlangen zuzuleiten (Art. 15 Abs. 1). Gemäss der heutigen Praxis und dem französischen Wortlaut des Artikels 1 werden dadurch aber nur Internet-Zugangs-Anbieter verpflichtet. Plattformbetreiber müssen nur vorhandene Daten herausgeben. Gemäss Art. 22 Abs. 4 des Entwurfs für ein revidiertes BÜPF[242] soll der Bundesrat Anbieter von Diensten, die sich auf Fernmeldedienste stützen und eine Einweg- oder Mehrwegkommunikation ermöglichen (Anbieter abgeleiteter Kommunikationsdienste) wie FDA zur Datenaufbewahrung verpflichten können. Wird eine Straftat über das Internet begangen, können Strafverfolgungsbehörden nach geltendem Recht auch ohne Gerichtsbeschluss die Identität des betreffenden Anschlussinhabers aufdecken und bei diesem beispielsweise eine Hausdurchsuchung vornehmen lassen. Aus diesem Grund hat das Bundesgericht 2010 die Bestrafung des Betreibers einer von ihm gehosteten Internetplattform wegen Begünstigung (Art. 305 StGB) bestätigt, der als Provider die IP-Adressen der anonymen Autoren angeblich ehrverletzender Kommentare vernichtet hatte und diese so der Strafverfolgung entziehen wollte.[243]

Schwieriger gestaltet sich die Rechtsdurchsetzung allerdings, wenn die IP-Adressen lediglich dem Betreiber einer ausländischen, nicht den Vorschriften des BÜPF unterworfenen Plattform bekannt sind. In diesem Fall sind die schweizerischen Behörden auf die Kooperation des ausländischen Plattformbetreibers angewiesen oder müssen den beschwerlichen Weg internationaler Rechtshilfe in Strafsachen beschreiten. Ausländische Betreiber einer Plattform sind mitunter nicht bereit, einen Inhalt zu löschen, willigen aber unter Umständen ein, den Strafverfolgungsbehörden auf deren Anfrage hin die IP-Adresse einer Person mitzuteilen, die z.B. eine rechtswidrige Äusserung verfasst hat.

---

[240] Vgl. etwa BGE 55 II 94 E. 1 S. 98.

[241] BGE 136 IV 145.

[242] BBl 2013 2789.

[243] Bundesgerichtsurteil 6B_766/2009 vom 8.1.2010.

5.2.4 Das Problem der örtlichen Zuständigkeit

Praktische Probleme bei der Verfolgung von Straftaten schafft gerade bei Social Media-Plattformen der Umstand, dass erst geklärt sein muss, welche Behörde für die Verfolgung überhaupt zuständig ist. Erst dann können die allenfalls nötigen internationalen Rechtshilfeersuchen (z.B. an Facebook) gestellt und mögliche Straftaten aufgeklärt werden. Da die auf internationalen Plattformen platzierten Äusserungen überall abrufbar sind, droht allerdings die Situation, dass sich weder eine kantonale Staatsanwaltschaft noch die Bundesanwaltschaft für die Verfahrenseröffnung als zuständig betrachtet. Aus diesem Grund gibt Art. 27 Abs. 2 StPO der Bundesanwaltschaft die Möglichkeit, bei ungeklärter Zuständigkeit ein Verfahren zu eröffnen. Wendet die Bundesanwaltschaft diese Bestimmung konsequent an, so können Straftaten auf sozialen Plattformen strafrechtlich verfolgt werden.

5.3 Verantwortlichkeit von Plattformbetreibern und Providern

5.3.1 Lösungsansätze im Ausland oder internationalen Recht

Die Verantwortlichkeit von Internetdienstleistern (Providern) ist im EU-Raum durch die Spezialregeln der *E-Commerce-Richtlinie (EC-RL)*[244] vorgegeben: Art. 12 EC-RL statuiert den Grundsatz, dass Internet-Zugangsanbieter und andere reine «Durchleitungsanbieter» (Access-Provider) für die Inhalte der von ihnen übermittelten Informationen nicht verantwortlich gemacht werden können. Nach Art. 14. EC-RL sind auch Provider, die fremde Inhalte auf ihren Rechnern speichern (Hosting-Provider) zumindest solange von einer Verantwortlichkeit ausgenommen, als ihnen die rechtswidrige Tätigkeit nicht bekannt ist. Haben sie Kenntnis, müssen sie die fraglichen Inhalte entfernen oder den Zugang zu ihr sperren.

Es besteht aber keine Pflicht, die übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach rechtswidrigen Inhalten zu forschen (Art. 15 EC-RL). Dass Provider keine Pflicht zur vorgängigen Überwachung aller bei ihnen gespeicherten oder durch sie zugänglich gemachten Inhalte treffen soll, hat auch der Europäische Gerichtshof (EuGH) anerkannt. Der EuGH hat sowohl bei Access-Providern[245] als auch bei Hosting-Providern[246] eine generelle Pflicht zur vorgängigen Filterung verneint.

Beschränkt sich der Provider allerdings nicht auf die automatisierte Verarbeitung der von seiner Kundschaft eingegebenen Informationen, sondern wählt er die übermittelten Informationen aus oder verändert er sie, so fällt das von Art 15 Abs. 1 EC-RL gewährte Privileg fehlender Haftung und fehlender Überwachungspflicht weg.[247] Eine solche aktive Rolle ist nicht bereits anzunehmen, wenn der Plattformbetreiber die Angebote auf seinem Server speichert, die Modalitäten für seinen Dienst festlegt, für diesen eine Vergütung erhält und seinen Kunden Auskünfte allgemeiner Art erteilt. Sie ist aber nach EuGH gegeben, wenn der Betreiber Hilfestellung leistet, beispielsweise für die Optimierung der Präsentation eines Inhalts oder dessen Bewerbung. [248]

Aus *menschenrechtlicher Optik* ist umstritten, ob und unter welchen Umständen ein Plattformbetreiber für rechtswidrige (z.B. persönlichkeitsverletzende) Kommentare von Nutzenden zivilrechtlich belangt und zur Bezahlung einer Genugtuungssumme verurteilt werden darf. Die Beschwerde eines verurteil-

---

[244] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), ABl. L 178 vom 17.7.2000, S. 1.

[245] EuGH-Urteil vom 24.11.2011, SABAM / Scarlet Extended, Rs. C-70/10 (Anordnung an Access-Provider zur Filterung und Sperrung von Filesharing-Dateien europarechtswidrig).

[246] EuGH-Urteil vom 16.2.2012, SABAM / Netlog NV, Rs. C 360/10 (Keine Pflicht für Hosting-Provider, die auf einer Plattform für ein soziales Netzwerk gespeicherten Inhalte allgemein zu überwachen und zwecks Verhinderung von Urheberrechtsverletzungen ein Filtersystem einzurichten)

[247] EuGH-Urteil vom 19.7.2011, L' Oréal / E-Bay, Rs. C-324/09, Slg. I-6011 (Haftung für Provider mit „aktiver Rolle")

[248] EuGH-Urteil vom 19.7.2011, L' Oréal / E-Bay, Rs. C-324/09, Slg. I-6011 Rz. 115f.

ten estnischen Newsportal-Betreibers wegen Verletzung der Meinungsfreiheit (Art. 10 EMRK) ist seit 2009 beim Europäischen Gerichtshof für Menschenrechte hängig. [249]

5.3.2 Rechtslage in der Schweiz

Wie im Ausland ist auch in der Schweiz unbestritten, dass die Urheber rechtswidriger Inhalte (Content Provider) auf Social Media juristisch verantwortlich sind, falls sie identifiziert und vor Gericht gestellt werden können. Für die Verantwortlichkeit der weiteren Beteiligten in der Kommunikationskette (z.B. der Hosting- und Access-Provider) kennt die Schweiz anders als die meisten europäischen Staaten keine spezifischen Regeln. Massgebend sind die allgemeinen Vorschriften über die straf- und zivilrechtliche Verantwortlichkeit. Es ist verschiedentlich kritisiert worden, wegen des Verzichts auf eine Spezialregulierung fehle die nötige Klarheit über die Rechtslage. So haben National- und Ständerat 2001 eine rechtssichere Regelung verlangt und eine entsprechende Motion überwiesen.

Daraufhin wurde eine Expertenkommission "Netzwerkkriminalität" eingesetzt. Gestützt auf deren Bericht schickte der Bundesrat 2004 einen Vorentwurf zur Änderung des Strafgesetzbuchs (StGB) beziehungsweise des Militärstrafgesetzes (MStG) in die Vernehmlassung. Dort wurde eine ausdrückliche Regelung der strafrechtlichen Verantwortlichkeit für Provider und Suchmaschinenbetreiber begrüsst, doch gab es Kontroversen über verschiedene Einzelheiten der vorgeschlagenen Regelung. 2008 beschloss der Bundesrat einen Verzicht auf eine Regelung der strafrechtlichen Verantwortlichkeit.

In der Folge hat der Bundesrat wiederholt festgehalten, eine Spezialregelung der Verantwortlichkeit von Access- und Hostingprovidern sei weder im Straf- noch im Zivilrecht angezeigt (vgl. Motion Riklin 09.4222 "Rechtliche Verantwortlichkeit von Internet-Providern", parlamentarische Initiative Hochreutener 08.418 "Mehr Rechtssicherheit bei Netzwerkkriminalität" und zuletzt Interpellation Stöckli 12.4202 "Swisscom. Umgang mit urheberrechtlich geschützten Inhalten").

- Im *strafrechtlichen* Bereich sind nach seiner Auffassung sachgerechte Lösungen möglich, welche auf dem Medienstrafrecht (Art. 28 StGB) und den allgemeinen Grundsätzen über Täterschaft und Teilnahme (Art. 24ff. StGB) beruhen.
- Bezüglich der *zivilrechtlichen* Verantwortlichkeit haften die Provider nach den gleichen Grundsätzen wie die Anbieter anderer Dienstleistungen. Schadenersatzpflichtig werden sie gemäss Obligationenrecht (OR), wenn sie einem anderen widerrechtlich Schaden zufügen, sei es mit Absicht oder aus Fahrlässigkeit (Art. 41 Abs. 1 OR).[250]

Noch nicht geklärt wurde bislang die Verantwortlichkeit der Betreiber von Social Media-Plattformen, welche sich nicht in die gängigen Providerkategorien einordnen lassen.[251] Plattformbetreiber spielen in der Regel eine aktivere Rolle als die reinen Hosting-Provider, welche ihrer Kundschaft lediglich das automatisierte Aufladen von Informationen auf ihrem Webserver ermöglichen. Sie haben einen engeren Bezug zu den kommunizierten Inhalten als jene Hosting-Provider, welche ausschliesslich Speicherplatz zur Verfügung stellen. Plattformbetreiber stellen Spielregeln für Gestaltung, Umfang und Inhalt des von den Nutzern generierten Inhalts auf. Anders als herkömmliche Hosting-Provider werden sie oft in der Lage sein, eine Überwachungsfunktion auszuüben und nötigenfalls gegen problematische Inhalte einzuschreiten. Der Verzicht auf eine gewisse Filterung durch zumindest stichprobeweise Kontrollmassnahmen bzw. auf rechtzeitiges Einschreiten gegen erkennbar rechtswidrige Inhalte könnte in ihrem Fall eher straf- und zivilrechtliche Konsequenzen haben. Der Umfang ihrer Pflichten ist bislang durch die Gerichte und die Wissenschaft[252] höchstens ansatzweise umrissen worden.

---

[249] Beschwerdenr.64569/09 “Delfi AS c Estland”; die Angelegenheit wurde der Regierung Estlands am 11.2.2011 vom Gerichtshof zur Stellungnahme unterbreitet.

[250] Stellungnahme des Bundesrates vom 5.3.2010 zur Motion 09.4222 – Rechtliche Verantwortlichkeit von Internet-Providern.

[251] Bianchi della Porta Manuel/Robert Vincent, Responsabilité pénale de l‘éditeur de médias en ligne participatifs, in: medialex 2009, S. 21f.

[252] Vgl. immerhin Bianchi della Porta Manuel/Robert Vincent, Responsabilité pénale de l‘éditeur de médias en ligne participatifs, in: medialex 2009, S. 19ff.

So lässt sich darüber streiten, ob und in welchem Masse die Plattformbetreiber bei Gedankenäusserungsdelikten unter die Sonderregeln des Medienstrafrechts fallen (Art. 28 StGB) und ob sie allenfalls eine subsidiäre Verantwortlichkeit für die Nichtverhinderung einer strafbaren Veröffentlichung (Art. 322bis StGB) trifft. Eines der Probleme ist der Umstand, dass auf vielen Plattformen sowohl an ein breites Publikum gerichtete als auch nichtöffentliche Inhalte zu finden sind. Auf solche Mischformen ist das heutige Medienstrafrecht kaum zugeschnitten. Anders als Presseverlage, Rundfunkveranstalter oder Betreiber einer einzelnen Website sind Betreiber sozialer Netzwerke nicht Medienunternehmen im herkömmlichen Sinn des Wortes.

In der Rechtsliteratur wird festgehalten, die aus Zeiten der Druckerpresse stammende medienstrafrechtliche Sondernorm (Art. 28 StGB) vermöge den heutigen Anforderungen der Online-Welt nicht mehr zu genügen. Deren Anwendungsbereich sei bei verschiedenen Delikten (z.B. der weichen Pornografie) und gerade bei Veröffentlichungen in den verschiedenen massenmedialen Anwendungen des Internet unklar. Die Strafbarkeitsgrenzen seien daher auf dem Wege der Gesetzesrevision zu klären.[253]

Der Bundesrat ist sich bewusst, dass Provider, Kunden, Behörden, aber auch die Justiz von klaren Rechtsregeln profitieren. Jede denkbare Gesetzesvorlage zur Verantwortlichkeit von Internet-Providern sowie zur Verfolgung von Rechtsverletzungen im Internet steht allerdings vor der Herausforderung, angesichts der Vielzahl von Akteuren und deren unterschiedlichen Bedürfnissen und Problemen, eine Lösung zu finden, die möglichst allen Ansprüchen gerecht wird. Dabei besteht nicht nur die Gefahr einer Überregulierung, sondern auch die Gefahr der Unterregulierung.

In seiner Antwort auf aktuelle parlamentarische Vorstösse (Motion Riklin 13.3215; Rechtliche Verantwortlichkeit von Internet-Providern regeln und Frage Glättli 13.5059, Haftbarkeit von Hosting-Providern, Blog- und Forenbetreibern) hat der Bundesrat anerkannt, dass sich in zivilrechtlicher Hinsicht ein gesetzgeberischer Handlungsbedarf ergeben kann: Das Bundesgericht hat sich mittlerweile erstmals mit der zivilrechtlichen Verantwortlichkeit von Hosting-Providern für rechtswidrige (persönlichkeitsverletzende) Inhalte befasst.[254] Es hat gegenüber einem Provider, der fremde Blogs auf eigenem Server zum Abruf bereit hält, ein Haftungsprivileg bei Beseitigungs- und Feststellungsansprüchen abgelehnt. Die Schweiz habe bislang keine Spezialregeln erlassen, weshalb die allgemeinen Regeln von Art. 28 ZGB anwendbar seien.[255] Allfällige unerwünschte Konsequenzen aus dieser Rechtslage habe nicht die Justiz zu korrigieren, sondern der Gesetzgeber.[256] Dabei verwies das Bundesgericht ausdrücklich auf den vorliegenden Bericht, der damals in Ausarbeitung war.

Die aktuelle Rechtsprechung deutet darauf hin, dass die Justiz die allgemeinen Regeln über die zivilrechtliche Verantwortlichkeit als unzureichend empfindet und in diesem Bereich auf eine Klärung durch den Gesetzgeber hofft. Die Äusserungen der Justiz und der Rechtswissenschaft[257] sowie die ausländischen Entwicklungen[258] legen nahe, einen gesetzgeberischen Handlungsbedarf im Zivilrecht vertieft zu prüfen. Der Bundesrat ist bereit, entsprechende Schritte in die Wege zu leiten (vgl. hinten Ziff. 7.2.4).

---

[253] Christian Schwarzenegger, Der Anwendungsbereich des Medienstrafrechts (Art. 28, 322bis StGB), in: Cavallo u.a. (Hrsg.), FS-Donatsch, Zürich 2012, S. 187.

[254] Urteil 5A_792/2011 vom 14. Januar 2013.

[255] Urteil 5A_792/2011 vom 14. Januar 2013, E. 6.1.

[256] Urteil 5A_792/2011 vom 14. Januar 2013, E. 6.3.

[257] Kernen Alexander, Volle Verantwortlichkeit des Host Providers für persönlichkeitsverletzende Handlungen seines Kunden, in: Jusletter 4. März 2013, Rz 20ff.; Bühlmann Lukas, Blog-Hoster sind mitverantwortlich für persönlichkeitsverletzende Blogbeiträge, in: Digitaler Rechtsprechungs-Kommentar Weblaw, 13. März 2013, Rz 10f.; Schoch Nik / Schüepp Michael, Provider-Haftung „de près ou de loin"?, in: Jusletter 13. Mai 2013, Rz. 43ff; Hürlimann Daniel, Replik: Das Leistungsschutzrecht für Presseverlage, in: Jusletter 13. Mai 2013, FN 30.

[258] So etwa die oben (Fn. 249) erwähnte, beim EGMR eingereichte Beschwerde N 64569/09 "Delfi AS c Estland" zur Pflicht eines Newsportals, wegen automatisierter Aufschaltung fremder rechtswidriger Inhalte (persönlichkeitsverletzende Kommentare) eine Genugtuungssumme zu bezahlen.

5.4 Löschungen und Sperrverfügungen

5.4.1 Löschen problematischer Inhalte auf der Plattform

Besteht bei einem gesetzlich verbotenen Inhalt auf einer Social Media-Plattform ein Anknüpfungspunkt zur Schweiz, kann die zuständige Strafverfolgungsbehörde Schritte zu dessen Löschung unternehmen. Als rechtliche Grundlage für eine Löschung in Betracht kommt etwa ein auf die Vorschriften über die Beschlagnahme (Art. 263 StPO) gestütztes Vorgehen, sofern der fragliche Inhalt im Rahmen des Strafverfahrens als Beweismittel dient oder anderweitig eingezogen wird. Zusätzlich kann fedpol gestützt auf Artikel 13e des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (SR 120) bei Verbreitung von Gewaltpropaganda über das Internet die Löschung der betreffenden Website verfügen, wenn das Propagandamaterial auf einem schweizerischen Server liegt. Befindet sich das Propagandamaterial auf einem ausländischen Server, kann fedpol den schweizerischen Providern empfehlen, die betreffende Website zu sperren. Im Bereich bestimmter Verstösse gegen Werbevorschriften (z.B. im Alkoholgesetz) kann die zuständige Verwaltungsbehörde (z.B. die Eidg. Alkoholverwaltung) darüber hinaus dem Recht mittels verwaltungsrechtlicher Verfügung Nachachtung verschaffen. Auch dort kann die Rechtsdurchsetzung gerade gegenüber Äusserungen aus dem Ausland mit Schwierigkeiten verbunden sein.

Bei der Löschung ist im Auge zu behalten, dass nach Möglichkeit lediglich unrechtmässige Inhalte entfernt und rechtmässige Äusserungen weiterhin zugänglich gemacht werden sollten. Andernfalls dürfte eine übertriebene und damit unverhältnismässige Beschränkung der Meinungsfreiheit (Art. 16 BV) vorliegen (s. auch vorne Ziff. 4.2.2).

Nach den Erfahrungen von KOBIK ist die Löschung rechtswidriger Inhalte einfach zu realisieren, wenn eine soziale Plattform nach entsprechender Meldung aus eigenem Antrieb tätig wird. Dazu gehöre etwa Facebook. Eine für die gesamte Branche geltende Selbstregulierung haben die Betreiber der Plattformen für soziale Netzwerke mit Sitz in der Schweiz bislang noch nicht geschaffen. Darauf haben bislang beispielweise auch die deutschen Plattformbetreiber[259] – wegen der grenzüberschreitenden Zusammenhänge – verzichtet.

Ansätze zu einer Selbstregulierung der Branche gibt es aber im Bereich der Hosting-Provider, welche Plattformbetreibern (und anderen Interessenten) Speicherplatz für das automatisierte Aufschalten ihrer Angebote zur Verfügung stellen. Nach dreijährigen Vorarbeiten hat 2013 eine Reihe grosser Schweizer Hosting-Anbieter[260] unter der Leitung des Branchenverbands Simsa einen "Code of Conduct"[261] erarbeitet. Dieser soll ihre Rolle bei der Verfolgung rechtswidriger Inhalte im Internet klären. Dabei geht es um Straftatbestände im Bereich Pornografie, Gewaltdarstellung, Rassismus und Ehrverletzung, aber auch um die Verletzung von Urheber- oder Persönlichkeitsrechten. Lässt sich der Betreiber einer Website oder sozialen Plattform nicht ermitteln oder reagiert er nicht auf Anfragen und scheint eine Strafanzeige nicht erfolgsversprechend, können Betroffene ihre Beanstandung an den Hosting-Provider richten. Gemäss dem Code of Conduct soll er die Vorwürfe an den Betreiber der beanstandeten Website (oder Plattform) weiterleiten und diesen dazu auffordern, die erhobenen Vorwürfe abzuklären und gegebenenfalls rechtswidrige Inhalte zu entfernen. In "eindeutigen Fällen" kann der Hosting-Provider gemäss dem Verhaltenskodex aber auch vorübergehend den Zugang zur betroffenen Website sperren.

Deutsche Untersuchungen haben gezeigt, dass Modelle der Selbstregulierung (und der vom Staat regulierten Selbstregulierung) gewisse Vorteile gegenüber staatlicher Fremdregulierung aufweisen, ihre Funktionsweise aber komplex und instabil ist. Die Selbstregulierung stösst namentlich dann an

---

[259] http://www.heise.de/newsticker/meldung/Selbstregulierung-von-Social-Networks-gescheitert-1857533.html.

[260] Dazu gehören gemäss laut Simsa die grössten Schweizer Hosting-Anbieter, nämlich Cyon, Green, Hostpoint, Metanet, Nine, Swisscom und Webland.

[261] Code of conduct hosting (CCH); http://static.simsa.ch/1362151411/130201_simsa_cch_public_web.pdf.

Grenzen, wenn es um das Verhalten externer, nicht dem Branchenverband angehörender (z.B. ausländischer) Anbieter geht.[262]

5.4.2 Sperren des Zugangs zu problematischen Inhalten durch Access-Provider

Lässt sich eine Löschung des problematischen Inhalts auf der betroffenen (meist ausländischen) Social Media-Plattform nicht oder nicht rechtzeitig realisieren, so kommt eine Sperre des Zugangs in Betracht. Im Bereich Kinderpornografie bzw. Kindsmissbrauch stellt KOBIK daher den schweizerischen Providern eine Liste mit Links ausländischer Websites zur Verfügung, die eindeutig rechtswidrige Inhalte aufweisen und trotz Löschungsantrag an die ausländischen Stellen weiterhin abrufbar sind. Gestützt auf ihre allgemeinen Geschäftsbedingungen sind die Provider dafür besorgt, dass ein Verbotshinweis von KOBIK anstelle des verbotenen Inhaltes erscheint. Diese auf Freiwilligkeit basierende Art der Zusammenarbeit zwischen Behörden und Privatwirtschaft hat sich bewährt. Jährlich werden dank dieser Zusammenarbeit hunderttausende von Aufrufen zu Internetseiten mit illegalem Inhalt durch die Internetdienstanbieter blockiert und somit die Rechte der Opfer bestmöglich gewahrt.

Darüber hinaus sind derartige Sperren durch schweizerische Strafverfolgungsbehörden in der Vergangenheit vereinzelt angeordnet worden, so durch einen Waadtländer Untersuchungsrichter wegen ehrverletzender Inhalte auf der Website „Appel au peuple".[263] In der Rechtsliteratur ist kritisiert worden, dass entsprechende Verfügungen im schweizerischen Gesetzesrecht über keine klare Rechtsgrundlage verfügen. [264]

Im Zusammenhang mit Sperrmassnahmen sind mögliche Kollateralschäden für ebenfalls blockierte rechtmässige Inhalte besonders sorgfältig im Auge zu behalten. Wird etwa der Zugriff auf bestimmte Domain-Namen verunmöglicht, so sind auch allfällige legale und erwünschte Angebote unter diesen Domain-Namen nicht mehr nutzbar.[265] Der Europäische Gerichtshof für Menschenrechte hat Ende 2012 in einem türkischen Fall[266] die als Reaktion auf eine einzelne problematische Website angeordnete Sperre der ganzen Plattform Google Sites beanstandet. Solche Sperrmassnahmen verlangen eine ausreichend präzise gesetzliche Grundlage. Der Rechtsrahmen muss laut Gerichtshof streng umrissen und die Kontrolle solcher Sperrmassnahmen durch die nationale Justiz besonders wirkungsvoll ausgestaltet sein – damit sich Willkür verhindern lässt.

In Anbetracht der bestehenden Rechtsgrundlagen und der gut funktionierenden Zusammenarbeit zwischen Behörden und Internetdienstanbietern hat der Bundesrat in seiner Antwort auf die Anfrage Schwaab (12.1128 – Zugang zu Inhalten im Internet. Grundsatz "Löschen statt Sperren") einen Bedarf zur Schaffung gesetzlicher Grundlagen verneint.

---

[262] Dreyer, Stephan/Hasebrink, Uwe/Lampert, Claudia/Schröder, Hermann-Dieter, Entwicklungs- und Nutzungstrends im Bereich der digitalen Medien und damit verbundene Herausforderungen für den Jugendmedienschutz. In: Beiträge zur sozialen Sicherheit. Forschungsbericht Nr. 9/13, (Publikation in Vorbereitung) Kap. 3.5, S. 38.

[263] Vgl. den Sachverhalt des Bundesgerichtsurteils 1B_242/2009 vom 21.10.2009.

[264] Schwarzenegger Christian, Sperrverfügungen gegen Access-Provider - über die Zulässigkeit polizeilicher Gefahrenabwehr durch Sperranordnungen im Internet, in: Arter Oliver/Jörg Florian (Hrsg.), Internet-Recht und Electronic Commerce Law, Bern 2003, S. 249ff.

[265] Rosenthal David, Internet-Provider-Haftung – ein Sonderfall? in: Peter Jung (Hrsg.), Aktuelle Entwicklungen im Haftungsrecht, Bern/Zürich/Basel/Genf, 2007, S. 158.

[266] EGMR-Urteil „Ahmet Yildirim c. Türkei" (Beschwerdenr. N°3111/2010) vom 18.12.2012 zur konventionswidrigen Sperre der Plattform Google Sites.

5.5 Probleme der Rechtsdurchsetzung im grenzüberschreitenden Bereich

Die Durchsetzung bestehender schweizerischer Rechtsvorschriften in sozialen Netzwerken wird u.a. dadurch wesentlich erschwert, dass es sich meistens um ausländische Plattformbetreiber und regelmässig um grenzüberschreitende Kommunikation handelt. In vielen Bereichen verfügt das Schweizer Recht über eine Regulierung der im Zusammenhang mit Social Media auftretenden Probleme. Häufig wäre Schweizer Recht auf grenzüberschreitende Sachverhalte auch anwendbar. Doch selbst das Vorliegen eines rechtskräftigen Urteils eines Schweizer Gerichts garantiert nicht, dass dieses im Ausland auch umgesetzt wird.

5.5.1 Rechtsdurchsetzung durch Ermittlungs- und Strafverfolgungsbehörden

5.5.1.1 Internationale Kooperation

In der Praxis hängt die Rechtsdurchsetzung wesentlich von der Bereitschaft des (ausländischen) Plattformbetreibers zur Zusammenarbeit ab. Diese Bereitschaft kann durch Interventionen der Strafverfolgungsbehörden gefördert werden. So haben gewisse Betreiber von Social-Media-Plattformen eigene Stellen geschaffen, an die sich gewisse ausländische Behörden mit ihren Anliegen wenden können, ohne ein Rechtshilfeverfahren einleiten zu müssen. [267]

Im Konfliktfall müssten die Strafverfolgungsbehörden nach den Regeln der internationalen Rechtshilfe vorgehen, was die Strafverfolgung erheblich verzögern kann. Angesichts der vielen grenzüberschreitenden Sachverhalte wird es oft keine Alternative zur internationalen Kooperation von Ermittlungsbehörden geben. [268] Ist beispielsweise im Ausland eine Strafverfolgung wegen eines auch dort strafbaren Verhaltens (z.B. Hacking oder Datendiebstahl) eröffnet, wird auch für die schweizerischen Strafverfolgungsbehörden der Informationsaustausch mit ihren ausländischen Kollegen einfacher.

Seit Inkrafttreten der Europaratskonvention über die Internetkriminalität (Cybercrime Convention, CCC) am 1. Januar 2012 ist nach den Ausführungen von KOBIK ein markanter Anstieg des kriminalpolizeilichen Informationsaustauschs festzustellen. [269] KOBIK leitet Angaben über auf ausländischen Servern gespeicherte unrechtmässige Inhalte via Interpol oder Europol den zuständigen Behörden weiter, damit die betroffenen Länder gemäss ihren jeweiligen Rechtsgrundlagen die Inhalte löschen und die Strafverfolgung aufnehmen können. Obwohl diese gemäss schweizerischem Recht verbotenen Inhalte in der Schweiz abgerufen werden können, hat KOBIK allerdings keinen direkten Einfluss auf die Löschung oder Sperrung von illegalen Inhalten im Ausland.

5.5.1.2 Grenzen von Massnahmen gegen ausländische Fernsehsendungen

Internationalrechtliche Grenzen sind allfälligen Sperrmassnahmen gezogen, wenn sie herkömmliche Fernsehprogramme betreffen. Für Massnahmen ist hier gemäss der für die Schweiz verbindlichen Europaratskonvention über grenzüberschreitendes Fernsehen (EÜGF) im Grundsatz ausschliesslich der Sendestaat zuständig.

Die Verbreitung eigentlicher Fernsehprogramme (d.h. zeitgleich ausgestrahlter [so genannt gestreamter] integraler, vom Veranstalter programmartig zusammengestellter audiovisueller Inhalte) über Social Media-Plattformen ist bislang eher selten. In sozialen Netzwerken wesentlich häufiger ist das Bereitstellung einzelner audiovisueller Inhalte zum Abruf (so genanntes Video On Demand bzw. nicht lineare Angebote). Für solche Angebote sieht das EU-Recht ebenfalls das Sendestaatsprinzip (bzw. Her-

---

[267] Gemäss Facebook wird jede behördliche Anfrage auf „ihre rechtliche Zulässigkeit und ihre Übereinstimmung mit unseren Nutzungsbedingungen sowie mit dem Gesetz“ geprüft. Für die erste Hälfte des Jahres 2013 weist Facebook aus, das Unternehmen habe bei 13 Prozent der schweizerischen Anfragen die Daten über bestimmte Nutzer weitergegeben. https://www.facebook.com/about/government_requests

[268] Dreyer, Stephan/Hasebrink, Uwe/Lampert, Claudia/Schröder, Hermann-Dieter, Entwicklungs- und Nutzungstrends im Bereich der digitalen Medien und damit verbundene Herausforderungen für den Jugendmedienschutz. In: Beiträge zur sozialen Sicherheit. Forschungsbericht Nr. 9/13 (Publikation in Vorbereitung) Kap. 4.2, S. 47.

[269] Jahresbericht KOBIK 2012, Ziff. 4, S. 20.

kunftslandsprinzip) vor. Die entsprechende Richtlinie 2010/13/EU über audiovisuelle Mediendienste ist bislang hinsichtlich von Abrufdiensten für die Schweiz nicht verbindlich. Es ist allerdings nicht ausgeschlossen, dass dies künftig einmal der Fall sein wird.

5.5.2 Rechtsdurchsetzung durch Private (z.B. zum Schutz ihrer Persönlichkeitsrechte)

Die Rechtsdurchsetzung bei problematischen Beiträgen auf sozialen Plattformen ist nicht nur für Behörden schwierig, sondern auch für Privatpersonen, die beispielsweise durch die Publikation von Bildern oder Texten in ihren Persönlichkeitsrechten verletzt sein können. [270] Hat ein Benutzer auf einer Social-Media-Plattform unzulässige Inhalte publiziert, welche die betroffene Person entfernt haben möchte, drängt sich in der Praxis folgende Vorgehensweise auf: Zunächst den Urheber der Verletzung kontaktieren, dann den Betreiber der Plattform kontaktieren und schliesslich, falls nötig, rechtliche Schritte prüfen und vornehmen. Ein solches Vorgehen hat in verschiedenen Fällen funktioniert.

5.5.2.1 Anwendbares Recht

Für die Rechtsdurchsetzung durch Private ist zunächst das im Konfliktfall anwendbare Recht von grosser Bedeutung. Die Nutzungsbedingungen von Social Media verweisen in ihren Rechtswahlklauseln üblicherweise auf das nationale bzw. lokale Recht des Anbieters (z.B. kalifornisches Recht), der in aller Regel seinen Sitz nicht in der Schweiz hat, selbst wenn Gruppengesellschaften des Anbieters hierzulande präsent sind. Auch als Gerichtsstand sehen die Nutzungsbedingungen üblicherweise die Zuständigkeit der staatlichen Gerichte am Sitz des Anbieters vor. Es stellt sich allerdings die Frage, inwieweit derartige Rechtswahl- und Gerichtsstandsklauseln durchsetzbar sind. Aus den zwingenden Bestimmungen des Schweizer Internationalen Privatrechts ergibt sich Folgendes:

Die Rechtswahl kann nur dort gelten, wo überhaupt ein Vertrag zustande gekommen ist. Zwar wird hierfür eine Benutzer-Registrierung typischerweise genügen, doch soweit eine Plattform die Rechte von "Nicht-Benutzern" verletzt, wird sich der Anbieter nicht auf die Rechtswahl in seinen Nutzungsbedingungen berufen können. Verletzt er beispielsweise die Persönlichkeit einer Person, wird letztere vor einem Schweizer Gericht nach den allgemeinen Regeln zur Bestimmung eines Gerichtsstands für Ansprüche aus unerlaubter Handlung in internationalen Sachverhalten klagen und gestützt auf die allgemeinen Regeln des internationalen Privatrechts Schweizer Recht zur Anwendung bringen können. Dasselbe gilt für Verletzungen des Lauterkeitsrechts. Hier bedarf es für die Anknüpfung des Schweizer Rechts einer Auswirkung auf den Schweizer Markt, für die es typischerweise genügt, dass ein Anbieter die fragliche Tätigkeit (auch) auf Schweizer Kunden ausrichtet (Art. 136 IPRG[271]). An die Bestimmungen des Lauterkeitsrechts (einschliesslich Art. 8 UWG, welcher den zulässigen Inhalt von AGB regelt) wird sich ein ausländischer Anbieter einer Social-Media-Plattform für Schweizer Kunden somit halten müssen, gleichgültig, was seine Nutzungsbedingungen vorsehen. Das gilt auch für den Datenschutz: Auch registrierte Benutzer können sich ungeachtet der Nutzungsbedingungen und einer darin enthaltenen Wahl ausländischen Rechts vor einem Schweizer Gericht darauf berufen, dass Datenschutzverletzungen nach DSG beurteilt werden, wenn sie dies möchten (Art. 139 IPRG).

Die Klauseln zum Gerichtsstand und zur Rechtswahl in den Nutzungsbedingungen spielen zweitens dort keine Rolle, wo das internationale Privatrecht, einschliesslich etwaiger völkerrechtlicher Verträge, den Gerichtsstand und das zwischen Benutzer und Anbieter anwendbare Vertragsrecht zwingend oder halbzwingend vorschreiben. Dies tut es mit Bezug auf den Schutz von Konsumenten auch im Falle von Verträgen, die ein solcher von der Schweiz aus über eine Webseite abschliesst, auch wenn sich der Anbieter im Ausland befindet. In solchen Fällen wird der Konsument mit Wohnsitz in der Schweiz Ansprüche gegenüber dem Anbieter grundsätzlich vor einem Schweizer Gericht geltend ma-

---

[270] Die Ausführungen unter Ziff. 5.5.2 basieren auf einem im Auftrag des Bundesamts für Kommunikation im Februar 2013 verfassten Text von David Rosenthal, Lehrbeauftragter für Informations- und Telekommunikationsrecht an der Universität Basel. Eine ausführlichere Version des Textes findet sich auf http://www.infosociety.admin.ch .

[271] Bundesgesetz vom 18. Dezember 1987 über das Internationale Privatrecht (IPRG), SR 291.

chen (Art. 15 Ziff. 1 Bst. c Lugano Übereinkommen[272]; Art. 114 Abs. 1 Bst. a IPRG), welches wiederum Schweizer (Vertrags-)Recht zur Anwendung bringen wird (Art. 120 IPRG).

5.5.2.2 Anerkennung und Vollstreckung der Ansprüche

Die Anwendbarkeit des schweizerischen Rechts und die Zuständigkeit schweizerischer Gerichte im Hinblick auf das Nutzungsverhältnis vermag allerdings für sich allein nicht zu garantieren, dass die Ansprüche gegen ausländische (insb. amerikanische) Social-Media-Anbieter in der Praxis tatsächlich vollstreckt werden können. Die Betroffenen müssten hierzu ein Anerkennungs- und Vollstreckungsverfahren vor den Gerichten im Land des betreffenden Anbieters führen. Selbst wenn die Anerkennung und Vollstreckung eines schweizerischen Gerichtsurteils im Ausland grundsätzlich möglich ist und teilweise durch internationale Übereinkommen erleichtert wird[273], bietet ein entsprechendes Verfahren dem Anbieter oft (erneut) die Möglichkeit, sich beispielsweise gegen die Zuständigkeit des Schweizer Gerichts (das typischerweise in Abweichung der vereinbarten Gerichtsstandsklausel entschieden haben wird) zu wehren. Dies kann die Anerkennung und Vollstreckung verhindern oder zumindest verzögern. Welche Möglichkeiten der Anbieter hierbei hat, hängt unter Umständen auch vom ausländischen Recht ab. Mitunter kann es für die Betroffenen sinnvoller sein, etwaige Ansprüche direkt vor Ort geltend zu machen und auf den Schutz des Schweizer Rechts zu verzichten.

In beiden Szenarien werden aber bereits die mit dem Rechtsweg verbundenen Kosten viele Betroffene abschrecken. Insgesamt sind gerichtliche Streitigkeiten aus dem Nutzungsverhältnis von Social-Media-Plattformen in der Schweiz eine Seltenheit.

Es gibt auch ausländische Social-Media-Plattformen, die gegen sie in der Schweiz ergangene Entscheide "freiwillig", d.h. auch ohne Vollstreckungsverfahren im Ausland, akzeptieren und erfüllen. Die meisten Betreiber untersagen in den Nutzungsbestimmungen der Plattform nicht nur "rechtswidrige" Inhalte (was natürlich auch Inhalte erfasst, die gegen das DSG verstossen), sondern allgemein die Verunglimpfung anderer Benutzer oder Dritter und gehen mitunter sogar weiter als das, was das Recht verbietet (s. vorne Ziff. 4.2.2). Die grösseren Betreiber haben eigene Teams, die sich mit solchen Beschwerden beschäftigen, weil sie jeden Tag zahlreiche davon erhalten.

Viele Betreiber wollen dabei selbst keine rechtliche Beurteilung vornehmen, sondern verlangen hierzu den vollstreckbaren Entscheid einer zuständigen Behörde im betreffenden Land. Wird dem Betreiber ein solcher Entscheid vorgelegt, so sperrt er die darin konkret benannten und als rechtswidrig erkannten Inhalte, auch ohne dass dieser Entscheid gegen den Betreiber selbst ergeht (d.h. der Betreiber eingeklagt wurde) oder hierfür der Rechtshilfeweg bemüht werden muss. In einem solchen Fall muss eine betroffene Person zwar den Rechtsweg beschreiten, aber sie kann den Aufwand in Grenzen halten: Es genügt, ein Verfahren in der Schweiz durchzuführen. Es gibt auch in diesen Fällen verschiedene Möglichkeiten, die vor allem von zwei Fragen abhängig sind: Liegt erstens ein strafrechtlich relevantes Verhalten vor (eine blosse Verletzung der Privatsphäre mag zwar rechtswidrig sein, ist aber meist nicht strafrechtlich relevant, d.h. mit Strafe bedroht, sondern kann "nur" vor einem Zivilgericht klageweise verfolgt werden), und ist zweitens der Urheber der Verletzung mit Sicherheit bekannt.

Handelt es sich um eine Persönlichkeitsverletzung durch einen unbekannten Urheber, ist es in der Schweiz an sich nicht möglich, vor einem Zivilgericht "gegen Unbekannt" zu klagen. In solchen Fällen muss daher formal gegen den Betreiber der Plattform geklagt werden, sofern es keine andere Person gibt, die an der Persönlichkeitsverletzung mitwirkt (z.B. der Verantwortliche für die Seite, auf welcher eine persönlichkeitsverletzende Bemerkung erscheint) und sofern der Betreiber nicht bereit ist, die verantwortliche Person zu benennen. So bietet das Persönlichkeitsschutzrecht in der Schweiz die Möglichkeit, gegen jeden zivilrechtlich vorzugehen, der an einer Persönlichkeitsverletzung "mitwirkt".

---

[272] Übereinkommen vom 30. Oktober 2007 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (LugÜ), SR 0.275.12.

[273] Z.B. gegenüber den EU-und EFTA-Staaten das oben erwähnte Lugano-Übereinkommen über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen.

Der Betreiber einer Social Media-Plattform (z.B. eines Blogs) gehört nach herrschender Auffassung dazu, selbst wenn er für die Publikation nur eine sekundäre Rolle gespielt hat.[274]. Anders als bei einem an sich kooperationswilligen Betreiber, der jedoch ein Gerichtsurteil oder eine Behördenverfügung in der Hand haben möchte, bevor er einen Inhalt sperrt, ist eine Klage gegen einen renitenten Betreiber in der Praxis meist nur dann wirklich sinnvoll, wenn dieser sich in der Schweiz oder in einem Land befindet, in welchem die Anerkennung und Vollstreckung eines Urteils aus der Schweiz einfach und rasch möglich ist.

Die betroffene Person kann auch am Sitz des Betreibers im Ausland klagen. Dies muss nicht unbedingt teurer sein als ein Vorgehen vor einem Schweizer Gericht, ist aber normalerweise nicht ohne anwaltliche Vertretung und damit Kostenaufwand möglich.

5.5.2.3 Vorsorglicher Rechtsschutz

Das geltende Recht sieht zur Wahrung der Persönlichkeitsrechte u.a. Begehren auf Beseitigung, Unterlassung, Feststellung, Genugtuung und Schadenersatz vor. Angesichts der Gefahr rascher Verbreitung persönlichkeitsverletzender Äusserungen besteht ein besonderes Bedürfnis nach raschem Rechtsschutz. In der Praxis ist die gerichtliche Anordnung vorsorglicher Massnahmen häufig. Sie sollen verhindern, dass ein verletzender Inhalt weiterhin online bleibt, während das normale Gerichtsverfahren läuft, das durch alle Instanzen durchaus mehrere Jahre in Anspruch nehmen kann. Daher wird zu Beginn des Verfahrens oder sogar noch vorher vorläufig die Entfernung des Inhalts verlangt bzw. ein einstweiliges Verbot der Publikation ausgesprochen. Das geschieht bei superprovisorisch ausgesprochenen Massnahmen in der Regel unverzüglich und allein gestützt auf die Ausführungen des Antragstellers, ohne Anhörung anderer betroffener Personen oder Dritter. Bei anderen vorsorglichen Massnahmen wird eine Anhörung durchgeführt, was einige Wochen dauern dürfte.

Im Rahmen eines Verfahrens für eine vorsorgliche Massnahme wird vereinfacht gesagt beurteilt, ob die Klage dringlich ist, ob sie vermutlich erfolgreich sein wird (also ob z.B. ein bestimmter Inhalt tatsächlich rechtswidrig ist), ob die Anordnung der vorsorglichen Massnahme im Hinblick auf die Folgen für den Beklagten für die Dauer des Verfahrens vertretbar ist (z.B. welche Nachteile die einstweilige Sperrung bzw. Löschung für den Beklagten haben könnte) und ob sonst ein nicht leicht (d.h. mit Geld) wieder gut zu machender Nachteil für den Kläger entstehen würde. Ist eine vorsorgliche Massnahme angeordnet worden, muss der Kläger innert einer gewissen Frist Klage gegen den Beklagten einleiten, da sonst die Massnahme verfällt.

Die Durchsetzung vorsorglicher Massnahmen ist im internationalen Verhältnis kompliziert und oftmals nur verzögert möglich. So sind etwa superprovisorische Verfügungen vom Anwendungsbereich des Lugano-Übereinkommens ausgenommen,[275] sodass sie nicht vom erleichterten Anerkennungs- und Vollstreckungsmechanismus dieses Übereinkommens profitieren. Vom Erlass vorsorglicher Massnahmen bis zur Durchsetzung im Ausland kann es mitunter Monate dauern.[276]

5.5.2.4 Weitere Aspekte eines wirkungsvollen Schutzes privater Interessen

Der wirkungsvolle Schutz privater Interessen ist in der Praxis nicht allein mit gerichtlichen Interventionen zu verwirklichen. So kann es selbst nach Entfernung eines Inhalts auf einer Plattform nötig sein, die Suchmaschinen zu bereinigen, weil die Suche nach wie vor einen Treffer ergibt (und die alte Seite möglicherweise im Zwischenspeicher abrufbar ist, falls die Zwischenspeicherung vom Betreiber der Seite nicht gesperrt wurde). Hilfe bietet hier eine oft angebotene Sonderfunktion, mit der dem Suchmaschinenroboter beantragt werden kann, eine bestimmte Seite vorzeitig erneut abzuscannen bzw.

---

[274] Vgl. etwa BGer 5A_792/2011 vom 14.1.2013 E. 6.2 (für den Betreiber der Blogplattform der Tribune de Genève); zustimmend etwa Fanti Sébastien, Remarques, in: medialex 2013, S. 80.

[275] EuGH-Urteil vom 21.5.1980 Denilauler / Couchet, Rs. C-125/79: vorsorgliche Massnahmen, die ohne Ladung oder vorherige Zustellung vollstreckt werden können, sind nicht zirkulationsfähig.

[276] Für ein illustratives Beispiel siehe Schneider-Marfels Karl-Jascha, Facebook, Twitter & Co: „Imperium in imperio“, in: Jusletter vom 20. Februar 2012.

sie aus dem Suchindex zu entfernen (es muss dazu die Internetadresse der betreffenden Seite eingegeben werden).

Ein weiteres Problem liegt darin, dass einmal veröffentlichte Inhalte (z.B. Videofilme) von anderen Benutzern aufgegriffen und ihrerseits weiterverbreitet werden ("viraler Effekt") können. Dies kann es einer betroffenen Person letztlich verunmöglichen, selbst bei bestehenden rechtlichen Ansprüchen und Instrumenten eine unerwünschte Publikation wirkungsvoll zu unterdrücken.

In bestimmten Konstellationen kann es sinnvoll sein, wenn eine verunglimpfte Person ihrerseits aktiv wird und sich für ihren Ruf wehrt. Dies kann die Bereitschaft des Plattformbetreibers fördern, gegen bestimmte rechtswidrige Inhalte entschlossen vorzugehen. Ein Grund dafür ist der Umstand, dass auch Betreiber üblicherweise kein Interesse an Negativschlagzeilen oder einer grossen Zahl wütender Benutzer haben und nicht als Plattformen etwa für Cybermobbing oder Rufmord erscheinen wollen. Sie werden daher bei öffentlichem Druck entsprechende Inhalte schon zum Schutz der eigenen Reputation rascher entfernen, während sie einen Fall, der keine öffentliche Aufmerksamkeit erregt, womöglich weniger speditiv und mit geringerer Priorität behandeln. Umgekehrt erhöht öffentliche Aufmerksamkeit auch den Druck auf das Opfer eines Angriffs und kann dafür sorgen, dass sich Inhalte erst recht unkontrolliert verbreiten.

6 Weitere, im Rahmen dieses Berichts nicht vertiefte Rechtsfragen

Neben den in Kap. 4 und 5 erwähnten Fragestellungen werfen die sozialen Medien unter unterschiedlichsten Blickwinkeln eine Reihe weiterer Fragen auf, die an dieser Stelle nicht vertieft werden. Sie seien im Folgenden lediglich stichwortartig erwähnt.

6.1 Durchsetzung des Urheberrechts in sozialen Medien

Die teilweise als prekär wahrgenommene Durchsetzung des Urheberrechts und der verwandten Schutzrechte im Online-Zeitalter betrifft auch Social Media-Plattformen. Massnahmen gegen Urheberrechtsverletzungen im Internet (z.B. durch den Austausch nicht lizenzierter Musik-, Film- und Textdateien mittels Filesharing und Streaming) werden gegenwärtig im Rahmen der vom EJPD eingesetzten Arbeitsgruppe AGUR12 diskutiert. Im Rahmen bisheriger Sitzungen waren sich die Mitglieder einig, dass auf eigenen oder fremden Urheberrechtsverletzungen basierende Geschäftsmodelle wirksam bekämpft werden müssen. Dabei sollen die Betreiber von Infrastrukturen (Provider), deren sich solche Geschäftsmodelle bedienen, im Rahmen des Zumutbaren, technisch Möglichen und rechtlich Erlaubten Hilfestellung leisten.[277]

Darüber hinaus hat das SECO seit 2012 einen Runden Tisch installiert, der im Rahmen der geltenden Gesetzgebung prüfen soll, wie Urheberrechtsverletzungen im Internet datenschutzkonform ermittelt und strafrechtlich verfolgt werden können.

6.2 Wettbewerbsrechtliche Probleme sozialer Medien

Einzelne Aspekte der dominanten Position bestimmter Social Media-Plattformen und ihrer Auswirkungen auf die Interessen der Kundschaft werden im Bericht erörtert (Lock-In-Effekte, Recht auf Zugang zu [marktmächtigen] Social Media-Plattformen).

Darüber hinaus ist einem Missbrauch marktbeherrschender Stellung in anderen Branchen auch bei sozialen Medien durch die üblichen Instrumente des allgemeinen Wettbewerbsrechts (v.a. im Kartellgesetz) zu begegnen.

[277] Einzelheiten finden sich unter https://www.ige.ch/urheberrecht/agur12.html .

6.3 Social Media-Angebote von Rundfunkveranstaltern

Wie andere Medienunternehmen sind auch die Veranstalter von Radio und Fernsehprogrammen zunehmend in sozialen Medien präsent. Grundsätzlich setzt ihnen das Recht diesbezüglich keine besonderen Schranken. So wurde bislang im Rahmen des RTVG bewusst auf eine entsprechende Regulierung verzichtet.

Eine Ausnahme gilt allerdings für die SRG. Ihr aus den Empfangsgebühren finanzierter Auftritt in den sozialen Medien gehört zum übrigen publizistischen Angebot (üpA), dessen Umfang gemäss Art. 25 Abs. 3 Bst. a RTVG in der Konzession zu regeln ist. Nach dem Vorschlag des Bundesrates sollen die Verantwortlichkeiten für problematische Äusserungen detaillierter geregelt und die Aufsichtskompetenzen geklärt werden. So soll auf gesetzlicher Ebene festgehalten werden, dass die von der SRG-Redaktion gestalteten Beiträge – nicht aber die nutzergenerierten Beiträge (user generated content) – bestimmte Mindestanforderungen zu beachten haben (Achtung der Menschenwürde, der Grundrechte, Verbot der Gewaltdarstellung, Jugendschutz; bei bestimmten Angeboten auch das Sachgerechtigkeitsgebot und das Vielfaltsgebot). Diese Mindestanforderungen sollen auch für Einträge der Redaktion in einem Blog oder einem Forum gelten.[278]

6.4 Kommunikation unter Kriminellen in geschlossenen Netzwerken

Der Fokus des vorliegenden Berichts liegt auf sozialen Netzwerken, welche sich durch ihre Durchlässigkeit und Öffentlichkeit auszeichnen, und den daraus resultierenden Problemen. Spezifische Probleme stellen sich bei der heimlichen Kommunikation zwecks Begehung von Straftaten wie etwa dem Austausch von Pornografie in P2P-Netzwerken.[279]

Ihnen wird nach geltendem Recht zum Teil mit Massnahmen verdeckter Ermittlung begegnet. So werden Mitarbeitende der nationalen Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) gestützt auf die Schwyzer Polizeiverordnung als verdeckte Vorermittler gegen pädokriminelle Täter in Chats, Online-Plattformen oder privaten P2P-Tauschbörsen tätig.[280] Zudem betreibt KOBIK ein Monitoring von P2P-Netzwerken zur Erkennung pädosexueller Straftaten.[281]

6.5 IT-Spionage (Monitoring durch ausländische Geheimdienste oder Private)

Die Überwachung von Online-Kommunikation durch Geheimdienste ist im Zusammenhang mit den 2013 bekannt gewordenen Enthüllungen von Edward Snowden (ehemaliger Mitarbeiter des US-Auslandsgeheimdienstes National Security Agency NSA) verstärkt ins öffentliche Bewusstsein geraten.[282] Über Schnittstellen ist es der NSA möglich, auch die Inhalte von Social-Media-Plattformen zu überwachen, zu sammeln und aufzubewahren.

Das Phänomen der IT-Spionage – sei es durch ausländische Geheimdienste oder durch Private - ist nicht primär ein Problem sozialer Plattformen, sondern betrifft noch stärker die ausschliesslich private Online-Kommunikation. Der Bundesrat hat in der Antwort auf die Ip. 13.3558 Eichenberger „Cyberspionage. Einschätzung und Strategie“[283] vom 20.06.2013 auf die „Strategie zum Schutz der Schweiz vor Cyber-Risiken (Nationale Cyber-Strategie NCS) vom 27. Juni 2012 und den dazu gehörenden Umsetzungsplan verwiesen. Der am 15. Mai 2013 verabschiedete Umsetzungsplan NCS[284] betrifft die in der

---

[278] Botschaft zur Änderung des Bundesgesetzes über Radio und Fernsehen (RTVG) vom 29. Mai 2013, BBl 2013 5017.

[279] Durch aktives Monitoring konnte KOBIK 2012 insgesamt 417 am Austausch von Kinderpornografie Beteiligte identifizieren; vgl. Jahresbericht KOBIK 2012, S. 1.

[280] Jahresbericht KOBIK 2012, S. 13.

[281] Vgl. dazu etwa Lentjes Meili Christiane, Präventiv oder Repressiv? Das Verwirrspiel um verdeckte polizeiliche Operationen, in Festschrift Donatsch, Zürich 2012, S. 437ff.

[282] Die USA haben seit mindestens 2007 in grossem Umfang die Telekommunikation und insbesondere das Internet global und verdachtsunabhängig überwacht und die so gewonnenen Daten auf Vorrat gespeichert.

[283] http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133558.

[284] http://www.isb.admin.ch/themen/01709/01711/index.html?lang=de

Strategie vorgesehenen 16 Massnahmen. Mit der Strategie verfolgt der Bundesrat die Ziele, Bedrohungen im Cyberbereich frühzeitig zu erkennen, die Widerstandsfähigkeit von kritischen Infrastrukturen zu erhöhen, die Cyberrisiken zu reduzieren und Vorfälle zu bekämpfen.

In der Antwort auf die Ip. 13.3033 Schwaab „Wie können Personendaten von Schweizer Bürgerinnen und Bürgern in den Händen amerikanischer Unternehmen geschützt werden?“[285] vom 06.03.2013 nahm der Bundesrat Stellung zu verschiedenen Fragen der schweizerischen Rechtslage und Praxis im Bezug auf das Herausverlangen von Personendaten von Bürgerinnen und Bürgern von Drittstaaten aus der Datenwolke (cloud) durch die US-Behörden. Dabei hebt der Bundesrat neben der nötigen Eigenverantwortung jedes Einzelnen bei der Handhabung der eigenen Daten das Sensibilisierungsprogramm „Jugend und Medien“ des Bundes[286] sowie die Beratungsfunktion des EDÖB hervor . Neben Ausführungen zum Vertragsrecht und der möglichen Anwendbarkeit des IPRG[287] und des LugÜ[288] verweist der Bundesrat auf die laufenden Arbeiten zur Revision des DSG[289], wo u.a. geprüft werden soll, ob das geltende Recht in diesem Bereich ausreicht oder nicht.

7 Handlungsempfehlungen

Im Folgenden werden Empfehlungen vorgestellt, wie den in Kap. 4 und 5 identifizierten Problemen begegnet werden sollte. Wie ausgeführt, ist das materielle Schweizer Recht dabei häufig ausreichend und lassen sich viele Probleme in der Praxis nicht allein – und vielleicht nicht einmal primär – mit juristischen Instrumenten lösen. Daher werden neben rechtlichen Aspekten auch Fragen der Information und Bewusstseinsbildung sowie weitere Aspekte angesprochen.

7.1 Notwendigkeit der Schaffung neuer rechtlicher Vorschriften

7.1.1 Ausgangslage: Gefahr einer Überregulierung

Wie oben dargestellt ist in verschiedener Hinsicht denkbar – wenn auch nicht gewiss –, dass der Wortlaut der geltenden Rechtsvorschriften und ihre (gerichtliche) Anwendung im einzelnen Streitfall keine befriedigenden Antworten auf die durch soziale Medien aufgeworfenen Fragen erlaubt. Es ist nicht ausgeschlossen, dass punktueller Regelungsbedarf besteht. Grundsätzlich ist allerdings vor gesetzgeberischem Aktivismus und einer Überregulierung zu warnen. Wie in anderen einem raschen Wandel unterworfenen Bereichen droht vorschnelles Eingreifen (gewissermassen ein Erlass von Vorschriften auf Vorrat) unbeabsichtigte Wirkungen zu entfalten.

Sorgfältig zu prüfen ist jeweils auch, ob bestehende Mechanismen der Selbstregulierung (z.B. der oben unter Ziff. 5.4.1 erwähnte Code of conduct der dem Verband simsa angeschlossenen Hosting-Provider in der Schweiz, aber auch die Nutzungsbedingungen einzelner ausländischer Plattformen wie Facebook oder Twitter) nicht ausreichen.

7.1.2 Internationale Aspekte beschränken einzelstaatlichen Regelungsspielraum

Für eine Zurückhaltung des schweizerischen Gesetzgebers sprechen auch die ausgeprägten grenzüberschreitenden Zusammenhänge. Vielen Problemen lässt sich durch isolierte Vorschriften eines einzelnen Staates gar nicht sinnvoll begegnen. Wie erwähnt haben viele der auch in der Schweiz stark genutzten Plattformen ihren Sitz im Ausland.

Statt aufwändiger und nur beschränkt wirksamer einzelstaatlicher Regelungsaktivität bedarf es verstärkter internationaler Anstrengungen: Der Europarat weist zu Recht darauf hin, dass in einem Rechtssystem getroffene Regulierungsmassnahmen den Zugang und die Benutzung des Internets in

---

[285] http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133033.

[286] http://www.bsv.admin.ch/themen/kinder_jugend_alter/00071/03045/

[287] Bundesgesetz vom 18. Dezember 1987 über das Internationale Privatrecht (IPRG), SR 291.

[288] SR 0.275.12.

[289] SR 235.1.

anderen Rechtssystemen sowie die fortbestehende Funktionsfähigkeit der Internetinfrastruktur erheblich beeinträchtigen können[290]. Folglich bedarf der grenzüberschreitende Informationsaustausch im Internet der Auseinandersetzung auf multilateraler Ebene. Dies umfasst insbesondere Sachverhalte, die verschiedene Rechtssysteme betreffen, was immer häufiger vorkommt im Zuge der Entwicklung grenzüberschreitender Plattformen, wie etwa sozialer Netzwerke, oder mit dem Aufkommen von cloud computing[291].

7.1.3 Kohärenz der gesamten Rechtsordnung ist zu beachten

Wird für gewisse Einzelbereiche auf nationaler Ebene dennoch ein Regelungsbedarf erkannt, so ist stets die Kohärenz der gesamten Rechtsordnung im Auge zu behalten. Viele problematische Aspekte im Zusammenhang mit Social Media sind auch in anderen Lebensbereichen anzutreffen: Das Recht auf Vergessenwerden und die mangelnde Herrschaft über die eigenen Daten ist auch bei anderen Formen der Online-Kommunikation und generell im Alltagsleben ein Thema[292], der Persönlichkeitsschutz wird auch durch Äusserungen in herkömmlichen Massenmedien (Presse und Rundfunk) bedroht, der Jugendschutz wird auch durch Computergames gefährdet, Pornografie beschränkt sich nicht aufs Internet usw.

Für sehr viele Fragen besteht deshalb bereits eine gesetzliche Regelung in allgemeinen, nicht auf Social Media zugeschnittenen Gesetzen wie dem Strafgesetzbuch, dem Zivilgesetzbuch oder dem Datenschutzgesetz. Isolierte und allein auf das Phänomen sozialer Netzwerke zugeschnittene Gesetzesvorschriften bergen die Gefahr einer Zersplitterung und laufen tendenziell der Kohärenz der Rechtsordnung entgegen. Grundsätzlich empfiehlt es sich daher, eine allfällige Weiterentwicklung im Rahmen bestehender Regelwerke anzustreben und sich stets zu fragen, ob sich eine bestimmte problematische Entwicklung ausschliesslich im Bereich sozialer Netzwerke abspielt oder ob sie nicht auch auf andere Lebensbereiche übertragbar ist.

7.2 Prüfung eines Spezialgesetzes für soziale Netzwerke

7.2.1 Ausgangslage

Im Postulat „11.3912 – Rechtliche Basis für Social Media“ wurde die Frage aufgeworfen, ob der Entwicklung wie im Bereich von Radio und Fernsehen mit einer spezialgesetzlichen Regelung hinsichtlich sozialer Netzwerke begegnet werden sollte.

7.2.2 Regelungszuständigkeit des Bundes

Dabei ist zunächst zu prüfen, ob der Bund überhaupt für die Schaffung von Vorschriften über den Inhalt von Social Media zuständig ist. Für die öffentliche Kommunikation auf Social Media-Plattformen kann sich der Bund auf Art. 93 Abs. 1 BV stützen. Diese Verfassungsbestimmung bezeichnet die Gesetzgebung über die öffentliche fernmeldetechnische Verbreitung von Darbietungen und Informationen als Sache des Bundes. Diesen Plattformen kann der Bund inhaltliche Vorschriften machen. Leistungsaufträge fliessen zwar für sie – anders als für Radio und Fernsehen – nicht unmittelbar aus der Verfassung (Art. 93 Abs. 2 BV). Dem Bund steht es aber frei, den anderen Formen öffentliche fernmeldetechnische Verbreitung von Darbietungen und Informationen auf dem Wege der Gesetzgebung inhaltliche Vorgaben zu machen.[293] Gestützt darauf kann der Bund seine grundrechtliche Pflicht zum Schutz eines freien, pluralistischen Austauschs von Informationen und Gedanken wahrnehmen.

---

[290] Siehe etwa die Erklärung über die Grundsätze der Internet Governance sowie die Empfehlung CM/Rec(2011)8 über den Schutz und die Förderung der Universalität, Integrität und Offenheit des Internets.

[291] Für die Weiterverfolgung dieser Fragestellungen empfiehlt die vom Europarat eingesetzte Ad Hoc Advisory Group on Cross-Border Internet den vom Europarat in derartigen Fragen befürworteten Ansatz der „multi-stakeholder participation“.

[292] Vgl. etwa Flückiger Alexandre, L’autodétermination en matière de données personnelles :un droit (plus si) fondamental à l’ère digitale ou un nouveau droit de propriété ?, in: AJP/PJA 2013, S. 837ff.

[293] AB 1983 N 1353 (Votum Nationalrat Schüle).

Für nicht an die Öffentlichkeit gerichtete Inhalte, die über soziale Netzwerke ausgetauscht werden, kann sich der Bund zwar nicht auf Art. 93 BV stützen. Regelungskompetenzen lassen sich aber aus verschiedenen Verfassungsbestimmungen ableiten. So bezeichnet Art. 92 Abs. 1 BV das Fernmeldewesen als Sache des Bundes. Gestützt darauf wurden im FMG nicht nur Regeln über die fernmeldetechnische Übertragen erlassen, sondern beispielsweise auch über Spamming oder Mehrwertdienste.[294] Darüber hinaus kann sich der Bundesgesetzgeber für zivilrechtliche Vorschriften auf Art. 122 und für strafrechtliche auf Art. 123 BV stützen. In diesem Rahmen wäre er auch zuständig, bei Bedarf allfällige Sonderregeln für soziale Medien zu schaffen.

7.2.3 Notwendigkeit einer spezialgesetzlichen Regulierung?

Eine dem Rundfunk ähnliche Spezialregulierung für öffentliche Äusserungen in Social Media rechtfertigt sich bloss, wenn sie zur Erhaltung oder Förderung einer freien öffentlichen Kommunikation notwendig ist. Dies ist beim vielfältigen Angebot verschiedener Social Media-Plattformen schon im Ansatz weniger wahrscheinlich als im Bereich von Radio und Fernsehen, der herkömmlicherweise her von einer Knappheit des Angebots geprägt war (Frequenzknappheit). Auch dort ist die Notwendigkeit von Leistungsaufträgen unter Vielkanalbedingungen weniger ausgeprägt als bei Monopolverhältnissen oder zumindest bei einem den Markt klar dominierenden (öffentlichen) Programmveranstalter.

Eine Regelung erscheint erst dann erforderlich, wenn ohne entsprechende Aktivität eine freie Kommunikation nicht gewährleistet ist, wie sie für die Entfaltung der Einzelnen und aus demokratischer Sicht erforderlich ist. Dies kann beispielsweise dann der Fall sein, wenn die für gesellschaftliche und demokratische Prozesse unabdingbare Vielfalt in den Medien nicht mehr zum Ausdruck kommt, etwa weil Minderheiten nicht über reale Chancen verfügen, sich wirkungsvoll Gehör zu verschaffen.

Zwar ist auch im Bereich der sozialen Netzwerke nicht ausgeschlossen, dass einige wenige Plattformen eine überragende Bedeutung erlangen, welche durch das freie Spiel der Marktkräfte nicht ausreichend reguliert wird. Die für gesellschaftliche und demokratische Prozesse unabdingbare Vielfalt der Meinungen würde diesfalls für ein staatliches Eingreifen sprechen. Dies wäre etwa der Fall, wenn bestimmte Bevölkerungsgruppen keine echte Chancen hätten, an der Kommunikation über massgebende Social Media-Plattformen teilzunehmen. Dafür gibt es gegenwärtig keine Anhaltspunkte. Vielmehr ist davon auszugehen, dass sich gegenwärtig auch Minderheiten auf den Plattformen wirkungsvoll Gehör verschaffen können. Abgesehen davon ist die Mehrheit der praktisch bedeutenden Anbieter im Ausland ansässig und würden Leistungsaufträge des schweizerischen Gesetzgebers deshalb weitgehend ins Leere laufen. Eine Notwendigkeit für eine spezialgesetzliche Regulierung in einem eigenen Social Media-Gesetz ist aus heutiger Sicht nicht zu erkennen.

7.2.4 Notwendigkeit einer Anpassung bisheriger Gesetzesnormen?

Wie dargelegt sollte eine allfällige Reaktion auf die durch soziale Netzwerke geschaffenen neuen Problemlagen nicht durch ein Spezialgesetz oder isolierte Einzelregelungen für Social Media erfolgen, sondern durch die Anpassung bestehender, oft allgemein formulierter Rechtsvorschriften. Sollten sich diese punktuell als unzureichend erweisen, so ist eine Ergänzung bestehender Gesetzestexte zu prüfen.

7.2.4.1 Vertiefte Prüfung datenschutzrechtlicher Fragen

Im 4. Kapitel wurden zahlreiche datenschutzrechtliche Probleme im Zusammenhang mit Social Media identifiziert. Das gilt etwa für Fragen des Rechts auf Vergessenwerden und allgemein für die mangelnde Kontrolle der Nutzenden über ihre Daten.

Das geltende schweizerische Datenschutzgesetz ist als Rahmengesetz sehr allgemein formuliert. Bei umsichtiger Anwendung erlaubt das DSG den zuständigen Behörden und Gerichten tendenziell, auch den neuen datenschutzrechtlichen Problemen Rechnung zu tragen. Ob dies ausnahmslos gilt oder ob

---

[294] Botschaft zur Änderung des Fernmeldegesetzes (FMG) vom 12. November 2003, BBl 2003 7966, 8003.

nicht gewisser gesetzlicher Anpassungsbedarf besteht, bedarf - auch im Hinblick auf im Entstehen begriffene Revisionen der Datenschutzregeln in der EU und im Europarat - näherer Prüfung. Entsprechende Prüfungsarbeiten werden gegenwärtig unter Federführung des EJPD vorgenommen. Eine breit zusammengesetzte Begleitgruppe Datenschutzgesetz (DSG) ist daran, das gesamte Datenschutzgesetz und dessen Durchsetzungsmassnahmen zu analysieren. Dazu gehören auch die durch neue Phänomene wie die Social Media aufgeworfenen Aspekte.

Das EJPD hat den Auftrag, dem Bundesrat bis spätestens Ende 2014 Vorschläge zum weiteren Vorgehen zu unterbreiten.

7.2.4.2 Prüfung, ob die Zuordnung der Verantwortlichkeit zu regeln ist

Wie oben (Ziff. 5.3) dargelegt, ist angesichts der aktuellen Entwicklungen und der Signale der Justiz auf dem Gebiet des Zivilrechts angezeigt, dass der Bundesrat den gesetzgeberischen Handlungsbedarf für eine Regelung der Verantwortlichkeit von Internet-Dienstleistern (neben den Access- und Hosting-Providern auch der Plattformbetreiber) erneut prüft. Diese Prüfung ist anspruchsvoll, zumal sich in der Zwischenzeit auch im Ausland eine differenzierte Rechtsprechung entwickelt hat, die sorgfältig zu analysieren ist. Entsprechende Arbeiten sind noch im Jahr 2013 unter Federführung des EJPD in Angriff zu nehmen.

Im Rahmen dieser Arbeiten ist auch eine Prüfung weiterer Problembereiche nicht ausgeschlossen. So könnte sich die Frage stellen, ob die gegenwärtigen Regeln für die Löschung von bzw. der Sperre des Zugangs zu illegalen Inhalten anzupassen sind.

7.2.4.3 Fernmelderecht und Social-Media-Plattformen

Die rechtliche Einordnung der von Social-Media-Plattformen teilweise auch angebotenen verschiedenen Übertragungsdienste ist schwierig. Das geltende Fernmelderecht, das in einer Zeit geschaffen wurde, in der es noch keine von der darunterliegenden Transportinfrastruktur losgelösten Dienste gab, hält dafür keine passenden Antworten bereit. Heute sind andere Geschäftsmodelle verbreitet (z.B. Finanzierung über Werbung), es gelten andere technische Bedingungen und es gibt viel mehr verschiedene Transportdienste, welche mit geringem Aufwand weltweit angeboten werden können. Welche Regeln des Fernmelderechts für solche Dienste gelten sollten, muss nicht nur für Social Media, sondern für alle Dienste geprüft werden, die (oft kostenlos) z.B. über Internet erbracht werden, ohne dass der eigene Internet-Service-Provider dazu um Erlaubnis gefragt werden muss (sog. „Over-the-top“-Dienste). Diese Fragen werden in der Vernehmlassungsvorlage zur Revision des Fernmeldegesetzes, deren Erarbeitung der Bundesrat noch in der laufenden Legislaturperiode in Auftrag zu geben beabsichtigt, vertieft angegangen werden.

7.2.4.4 Beobachtung, ob Datenmitnahme geregelt werden muss

Es ist sinnvoll, die Entwicklung der sozialen Medien daraufhin zu verfolgen, ob sie ihre Kundschaft halten wollen, indem sie die Mitnahme eigener Daten zu Konkurrenzunternehmen verhindern (vgl. dazu oben 4.3.7). Der Bund sollte diesen Markt beobachten und im Bedarfsfall ein Recht zur Datenmitnahme einführen. Allenfalls könnte es sich auch als sinnvoll erweisen, die Schnittstellen zwischen verschiedenen Social-Media-Plattformen zu regulieren und z.B. den grössten Plattformen vorzuschreiben, dass ihre Nutzenden auch mit denen anderer Plattformen Daten wie private Nachrichten austauschen können müssen. Möglicherweise werden in den kommenden Jahren auch Erfahrungswerte aus dem Ausland über solche Rechte vorliegen. Diese könnten zur Beurteilung des Regelungsbedarfs ebenfalls beigezogen werden.

7.3 Information und Sensibilisierung

Sowohl auf internationaler wie auf nationaler Ebene wird davon ausgegangen, dass Chancen und Risiken sozialer Netzwerke nicht allein durch rechtliche Regeln (und deren Durchsetzung) beeinflusst werden. Optimale Ergebnisse lassen sich nur durch Rückgriff auf ausserjuristische Instrumente wie die Förderung des Bewusstseins der beteiligten Kreise erzielen.

7.3.1 Recht auf Vergessenwerden

Die European Network and Information Security Agency (ENISA) hat darauf hingewiesen, dass heute bestehende technische Lösungen keinen ausreichenden Schutz für publizierte Daten vor einem nicht autorisierten Duplizieren durch Dritte und eine allfällige Wiederveröffentlichung nach deren „offizieller" Löschung bieten[295]. Zugleich wurde festgestellt, dass rein technische Lösungen für die Durchsetzung des Rechts auf Vergessenwerden in einem offenen System wie dem Internet nicht ausreichend seien. Vielmehr sei ein interdisziplinärer Ansatz nötig, der das Recht auf Vergessenwerden technisch wie rechtlich definiere[296].

Das Vergessenwerden auf Social-Media-Plattformen kann jedoch in vielen Fällen bereits durch vorausschauendes Handeln erleichtert werden. Wie z.B. der EDÖB empfiehlt, ist es sinnvoll sich vor der Veröffentlichung immer zu fragen, ob man in einem Bewerbungsgespräch mit den entsprechenden Daten konfrontiert werden möchte – und zwar auch noch in zehn Jahren[297]. Auch sollten keine Personendaten von Dritten veröffentlicht werden. Diese Prinzipien sind zwar allgemein bekannt, sollten aber immer wieder ins Bewusstsein gerufen und mit anschaulichen Beispielen belegt werden. Dies könnte z.B. im Rahmen des nationalen Programms „Jugend und Medien" geschehen.

7.3.2 Ehr- und Persönlichkeitsverletzungen, Cyberbullying und Cyberstalking

Kommt es in sozialen Netzwerken zu falschen Tatsachenbehauptungen, ehrenrührigen Werturteilen oder rechtswidrigen Entblössungen, sind strafrechtliche, zivilrechtliche und wirtschaftliche Aspekte im Schweizer Recht geregelt (s. vorne Ziff. 4.4.1.3). Wie Privatpersonen bei Verletzung ihrer Persönlichkeitsrechte konkret vorgehen können, wurde unter Ziff. 5.5.2 beschrieben. Problematisch bleibt die Tatsache, dass verletzende Inhalte unüberschaubar schnell und weitläufig verbreitet werden können.

Was Cybermobbing und Cyberstalking anbelangt, hat der Bundesrat wiederholt festgehalten, dass zum heutigen Zeitpunkt keine Anhaltspunkte vorliegen, wonach das bestehende strafrechtliche Instrumentarium nicht ausreichen würde (s. vorne Ziff. 4.4.2.3).

Aus der Tatsache, dass die materielle Rechtslage bei Persönlichkeitsverletzungen, bei Cybermobbing und Cyberstalking klar ist, kann jedoch nicht gefolgert werden, dass dies den Nutzenden von Social-Media-Plattformen auch bekannt ist. Eine einfach verständliche Aufbereitung der Rechtslage könnte hier sinnvoll sein, ergänzt durch allfällige Handlungsempfehlungen. Für das schulische Umfeld bestehen bereits Gefässe wie die educa guides[298] oder die Plattform „Jugend und Medien"[299], die in diese Richtung ausgebaut werden könnten. Für andere Zielgruppen und Lebenszusammenhänge wäre zu prüfen, welche Gefässe und Angebote sich für diese Aufgabe eignen und wie diese umgesetzt werden kann.

7.3.3 Kinder und Jugendliche

Wie oben (Ziff. 4.6.1.3) erwähnt, wird der Bundesrat im Rahmen der Revision des Datenschutzgesetzes Massnahmen zu einem verbesserten Datenschutz von Minderjährigen prüfen.[300] Mit rechtlichen Instrumenten alleine lässt sich ein wirksamer Jugendmedienschutz allerdings nicht realisieren. Von zentraler Bedeutung ist die Förderung der Medienkompetenz von Kindern und Jugendlichen sowie von Erziehungs- und Betreuungspersonen über die Chancen und Gefahren von digitalen Medien. Hier

---

[295] European Network and Information Security Agency (ENISA), The right to be forgotten – between expectations and practice, Heraklion 2011; http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten?searchterm=the+right+to+be+forgotten .

[296] ENISA, The right to be forgotten, S. 11 ff.

[297] http://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00693/index.html?lang=de#sprungmarke10_9.

[298] http://guides.educa.ch/de/recht.

[299] http://www.jugendundmedien.ch/home.html.

[300] Bericht zur Evaluation des Bundesgesetzes über den Datenschutz vom 9.12.2011, Ziff. 5.2.2 (BBl 2012 350).

knüpft das „Nationale Programm Jugend und Medien“ an[301], welches der Bundesrat mit Beschluss vom 11. Juni 2010 für die Jahre 2011-2015 lanciert hat. Das Programm will dazu beitragen, dass Eltern, Lehr- und Betreuungspersonen über die notwendigen Medienkompetenzen verfügen, damit sie eine aktive Begleitrolle der Medienaktivitäten von Kindern und Jugendlichen wahrnehmen. So wurde mit www.jugendundmedien.ch ein Referenzportal für den Jugendmedienschutz in der Schweiz aufgebaut. Das Portal beinhaltet eine systemtische Übersicht der in der Schweiz bestehenden Information- und Schulungsangebote sowie von kantonalen Strategien und Massnahmen im Bereich Jugendmedienschutz. Die im Rahmen des Programms veröffentlichte Broschüre „Medienkompetenz – Tipps zum sicheren Umgang mit digitalen Medien“ gibt Eltern, Kindern und Lehrpersonen praktische Ratschläge[302]. Sie widmet sich Themen wie Cybermobbing, Chats, Computerspielen, Pornografie und sozialen Netzwerke und äussert sich u.a. auch explizit zu der Frage, ob Lehrer und Eltern mit Jugendlichen in sozialen Netzwerken befreundet sein sollten. Das Programm fördert überdies die Zusammenarbeit der verschiedenen Stellen und Anspruchsgruppen im Jugendmedienschutz und unterstützt Fachpersonen bei Sensibilisierungsaktivitäten. Gefördert werden auch die Qualitätssicherung von bestehenden Angeboten sowie innovative Methoden zur Vermittlung von Medienkompetenz (Peer Education, Zugangsstrategien zu allen Bevölkerungsgruppen).

Da für das Schulwesen die Kantone zuständig sind, sind deren Aktivitäten für die Förderung der IKT-Kompetenzen von Bedeutung. Die EDK verfügt über eine Strategie zur Einbettung der IKT in den Schulen[303]. Überdies erliess sie Empfehlungen für die Ausbildung von Lehrpersonen im Bereich der Informations- und Kommunikationstechnologien[304] und das Profil für die Zusatzausbildungen für Ausbildende im Bereich Medienpädagogik[305]. Unter dem Bildungsserver „educa.ch“ finden Lehrpersonen Unterrichtsmaterialien und weiterführende Informationen zur Thematik, wie die Informationsbroschüre der Schweizerischen Kriminalprävention SKP „Safersurfing - Sicherheit in sozialen Netzwerken“[306], welche über Cybermobbing, sexuelle Übergriffe und den sinnvollen Umgang mit persönlichen Daten in sozialen Netzwerken informiert. Im Januar 2013 veröffentlichte die SKP auch die Informationsbroschüre „My little Safebook“ für einen sicheren Umgang mit sozialen Medien für Eltern und für Jugendliche[307].

Neben den oben genannten Fördermassnahmen hat der Bundesrat das Bundesamt für Sozialversicherungen (BSV) beauftragt, im Rahmen des nationalen Programms Jugend und Medien Empfehlungen zur zukünftigen Ausgestaltung des Jugendmedienschutzes in der Schweiz auszuarbeiten.

Das BSV hat zur Erfüllung dieser Aufgabe eine begleitende Expertengruppe bestehend aus Vertreter/innen des Bundes, der Kantone und der Wirtschaft eingesetzt und vier wissenschaftliche Mandate zur Erarbeitung fundierter Grundlagen vergeben:

Mandat 1 untersucht die Entwicklungs- und Nutzungstrends im Bereich der digitalen Medien und damit verbundene Herausforderungen für den Jugendmedienschutz (Herbst 2012 - Sommer 2013)

Mandat 2 nimmt eine Erhebung und Überprüfung der Regulierungsaktivitäten der Kantone vor (Frühling 2013 - Sommer 2014).

---

[301] http://www.jugendundmedien.ch/de.html.

[302] http://www.jugendundmedien.ch/fileadmin/user_upload/Chancen_und_Gefahren/Broschuere_FAQ_Medienkompetenz_dt.pdf .

[303] Strategie der EDK im Bereich Informations- und Kommunikationstechnologien und Medien vom 01.03.2007 (http://edudoc.ch/record/30020/files/ICT_d.pdf?version=1). Siehe auch die Erklärung zu den Informations- und Kommunikationstechnologien im Bildungswesen vom 08.06.2000 (http://www.edudoc.ch/static/web/arbeiten/erkl_ikt_d.pdf).

[304] Empfehlungen für die Grundausbildung und Weiterbildung der Lehrpersonen an der Volksschule und der Sekundarstufe II im Bereich der Informations- und Kommunikationstechnologien vom 25.04.2004; siehe: http://www.edudoc.ch/static/web/aktuell/medienmitt/empf_ict_lb_d.pdf.

[305] http://edudoc.ch/record/38148/files/Profil_ICT_d.pdf.

[306] http://guides.educa.ch/sites/default/files/sicherheit_netzwerke_d.pdf.

[307] http://news.skppsc.ch/de/2013/01/24/neue-broschure-my-little-safebook-fur-einen-sicheren-umgang-mit-den-sozialen-medien/.

Mandat 3 evaluiert die Umsetzung und Wirkung der Selbstregulierungsmassnahmen der Branchen in der Schweiz (Film, Computerspiele, Telekommunikation und Internet) (Frühling 2013 - Sommer 2014).

Mandat 4 analysiert medienspezifische und medienübergreifende Regulierungsmodelle verschiedener Länder, identifiziert „Good Practice"-Beispiele und formuliert Empfehlungen für die Schweiz (Frühling 2013 - Sommer 2014).

Bis 2015 soll festgestellt werden, welcher Regulierungsbedarf auf Bundesebene besteht und ob allenfalls die Schaffung verfassungsrechtlicher Grundlagen notwendig ist.

7.3.4 Ausbau Medienkompetenz der Bevölkerung

Wie oben ausgeführt, wird im schulischen Umfeld, für Kinder und Jugendliche sowie für deren Betreuungspersonen bereits heute einiges getan, um deren Medienkompetenz zu verbessern. Da Social Media ein sehr junges und damit dynamisches Phänomen sind, müssen die einschlägigen Webseiten, Publikationen u.a. laufend auf ihre Aktualität hin überprüft und gegebenenfalls überarbeitet werden.

Ausserdem ist zu prüfen, inwiefern auch in anderen Zielgruppen der Ausbau der Medienkompetenz insbesondere auf den Umgang mit Social Media hin ein Thema ist.[308] Zudem bietet es sich an, Social Media selbst für alle Zielgruppen vermehrt zur Vermittlung von Informationen und für die Sensibilisierung zu ausgewählten Fragen einzusetzen.

[308] So wendet sich z.B. die Comic-Broschüre „Geschichten aus dem Internet, die man selber nicht erleben möchte" an ein breites Zielpublikum, s. http://www.geschichtenausdeminternet.ch/.

8 Beantwortung der Fragen aus dem Postulat

Die im Postulat aufgeworfenen Fragen lassen sich nach oben stehenden Ausführungen wie folgt beantworten:

- Wie ist die aktuelle Rechtslage in der Schweiz und international in Bezug auf Social Media?

Die aktuelle Rechtslage ist sowohl in der Schweiz als auch im Ausland dadurch geprägt, dass soweit ersichtlich bislang kaum Regelungen geschaffen wurden, welche sich spezifisch und ausschliesslich auf das neue Phänomen der Social Media beziehen. Vielmehr werden die bestehenden Rechtsnormen bislang auch auf die Kommunikation in sozialen Netzwerken angewendet.

- Wie beurteilt der Bundesrat die Schaffung eines eigenen Social-Media-Gesetzes, das den Besonderheiten dieser neuen Kommunikationsformen Rechnung trägt?

Für ein eigenes Social Media-Gesetz nach dem Vorbild der bisherigen spezialgesetzlichen Regulierung von Radio und Fernsehen besteht aus heutiger Sicht kein Bedarf.

- Wo bestehen Lücken im Gesetz und wie können sie geschlossen werden?

Aufgrund bisheriger Erfahrungen springen im geltenden schweizerischen Recht keine grösseren Regelungslücken ins Auge. Die meist allgemein gehaltenen Regelungen in bestehenden Gesetzen (z.B. DSG, StGB, ZGB, UWG) erlauben bei umsichtiger Anwendung eine angemessene Antwort auf die meisten Probleme, welche soziale Plattformen für einzelne Betroffenen und die Allgemeinheit schaffen oder schaffen könnten. Ob sich diese Vorschriften in der Praxis bewähren werden, ist allerdings ungewiss. In einzelnen Bereichen scheinen punktuelle Verbesserungen möglich. Aus diesem Grunde sind in verschiedener Hinsicht (z.B. in Sachen Datenschutz und Jugendschutz) Abklärungen notwendig oder bereits im Gange. Es ist im Auge zu behalten, dass sich die entsprechenden Abklärungen nicht auf Social Media beschränken, sondern eine Vielzahl weiterer Fragen tangieren.

9 Weiteres Vorgehen

Wie in Kapitel 7 dargestellt, sind derzeit verschiedene substanzielle Aktivitäten in der Bundesverwaltung im Gange, welche auch Fragen einer allfälligen gesetzlichen Regelung von Social Media betreffen.

- **Datenschutzrechtliche Fragen** werden derzeit im Rahmen der laufenden Revisionsarbeiten zum DSG erörtert (Federführung EJPD). Die durch soziale Plattformen aufgeworfenen Fragen betreffen nur einen von zahlreichen in diesem Rahmen zu prüfenden Themenbereichen. Die Ergebnisse sind insbesondere für rechtliche Fragen rund um die mangelnde Kontrolle der Nutzenden über ihre Daten in sozialen Netzwerken (und gewisse Verbesserungen etwa durch datenschutzfreundliche Voreinstellungen) und das Recht auf Vergessenwerden von zentraler Bedeutung. Das EJPD hat den Auftrag, dem Bundesrat bis Ende 2014 Vorschläge zum weiteren Vorgehen zu unterbreiten.

- **Fragen des Jugendmedienschutzes** werden gegenwärtig bis 2015 im Rahmen des vom Bundesamt für Sozialversicherung betreuten Projekts „Jugend und Medien“ analysiert. Dabei wird geklärt, ob auf Bundesebene ein Regulierungsbedarf besteht und gegebenenfalls neue rechtliche Grundlagen zum Schutz von Kindern und Jugendlichen nötig sind. Zudem werden Empfehlungen zur zukünftigen Ausgestaltung des Jugendmedienschutzes in der Schweiz erarbeitet.

Darüber hinaus ist es angezeigt, weitere Aktivitäten vorzunehmen:

- Zu prüfen ist, ob im **Zivilrecht** gesetzgeberischer Handlungsbedarf besteht, um die Zuordnung der Verantwortlichkeit von Plattformbetreibern sowie technischen Dienstleistern (Access- und Hostingprovider) zu regeln. Diese Abklärungen beschränken sich nicht auf das Phänomen der sozialen Netzwerke, sondern betreffen ganz allgemein die rechtliche Verantwortlichkeit von Online-Dienstleistern (Providern). Das EJPD wird sich dieser Frage annehmen und dem Bundesrat bei Bejahung eines Gesetzesänderungsbedarfs eine Vernehmlassungsvorlage unterbreiten.

- Ebenfalls zu prüfen ist, welche **Regeln des Fernmelderechts** künftig für Social-Media-Plattformen gelten sollen. Sie sind bisher den Vorschriften des Fernmeldegesetzes (z.B. Meldepflicht, transparente Preisgestaltung, Bekämpfung von Spam) nur ausnahmsweise unterworfen. Diese Aspekte wird das UVEK im Rahmen der Vernehmlassungsvorlage zur Revision des FMG klären. Gemäss der aktuellen Planung wird die FMG-Revision vom Bundesrat in der laufenden Legislaturperiode in Auftrag gegeben.

- Im Hinblick auf eine allfällige Regulierung wird das UVEK sich auch dem Problem von Social-Media-Plattformen widmen, welche ihre Kundschaft halten wollen, indem sie die Mitnahme eigener Daten zu Konkurrenzunternehmen verhindern. Möglicherweise erweist es sich in Zukunft als nötig, ein **Recht auf Datenmitnahme** einzuführen oder die Schnittstellen zwischen Social-Media-Plattformen zu regulieren. Zu beobachten ist auch eine allfällige Regulierungstätigkeit im Ausland.

Die verschiedenen Aktivitäten und Abklärungen betreffen wie erwähnt nicht ausschliesslich Social Media, sondern sind im Zusammenhang der gesamten Rechtsordnung zu sehen. Wichtig ist allerdings, dass sich die verschiedenen Aspekte auch hinsichtlich von Social Media zu einem inhaltlich kohärenten Gesamtbild zusammenfügen. Aus diesem Grund ist es von wesentlicher Bedeutung, dass der Informationsfluss zwischen den beteiligten Amtsstellen gewährleistet ist.

Angesichts der zahlreichen bekannten – aber auch allfälliger weiterer – Regulierungsaktivitäten mit einem mehr oder weniger grossen Bezug zu Social Media ist die Gefahr nicht von der Hand zu weisen, dass der Blick für die Gesamtproblematik verloren geht. Mittelfristig erscheint es daher sinnvoll, zu gegebener Zeit eine erneute Standortbestimmung aus der Optik der sozialen Medien vorzunehmen. In diese Analyse wird auch die rasche Entwicklung auf internationaler Ebene sowie die sich abzeichnende Rechtsprechung zu vielen Streitfragen einfliessen. Daraus dürften sich Hinweise auf die Stärken und Schwächen der bisherigen Regulierung ableiten lassen.

Gesamthaft erscheint es aus heutiger Sicht angezeigt, bis Ende 2016, wenn die genannten Arbeiten abgeschlossen sind bzw. ihre Stossrichtung deutlicher erkennbar ist, im Sinne einer Zwischenbilanz eine erneute Standortbestimmung zur rechtlichen Basis für Social Media vorzunehmen.

10 Verzeichnisse

10.1 Verzeichnis der Abkürzungen

ABl.	Amtsblatt der Europäischen Union
AGUR12	Arbeitsgruppe zur Optimierung der kollektiven Verwertung von Urheberrechten und verwandten Schutzrechten
AWV	Arzeimittel-Werbeverordnung
BAG	Bundesamt für Gesundheit
BAKOM	Bundesamt für Kommunikation
BBl	Bundesblatt
BehiG	Behindertengleichstellungsgesetz
BehiV	Behindertengleichstellungsverordnung
BGBl	Bundesgesetzblatt (öffentliches Verkündungsblatt der Bundesrepublik Deutschland)
Blog	Weblog, auf einer Website geführtes Tagebuch oder Journal
BV	Bundesverfassung
DSG	Datenschutzgesetz
EDK	Schweizerische Konferenz der kantonalen Erziehungsdirektoren
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
EU	Europäische Union
EuGH	Europäischer Gerichtshof (oberstes rechtsprechendes Organ der Europäischen Union)
EWSA	Europäischer Wirtschafts- und Sozialausschuss
ENISA	European Network and Information Security Agency (Europäische Agentur für Netz- und Informationssicherheit)
FMG	Fernmeldegesetz
Fn.	Fussnote
FTC	Federal Trade Commission (Bundeswettbewerbs- und Verbraucherschutzbehörde USA)
HMG	Heilmittelgesetz
H.R.	House of Representatives (Repräsentantenhaus des U.S.-Kongresses)
Hrsg.	Herausgeber
IKT	Informations- und Kommunikationstechnologien
insb.	insbesondere
i.V.m.	in Verbindung mit
IPRG	Bundesgesetz über das internationale Privatrecht
JStG	Jugendstrafgesetz
JStPO	Jugendstrafprozessordnung
Kap.	Kapitel
KG	Kartellgesetz
KJFG	Kinder- und Jugendförderungsgesetz
KJFV	Kinder- und Jugendförderungsverordnung
KOBIK	nationale Koordinationsstelle zur Bekämpfung der Internetkriminalität
LGV	Lebensmittel- und Gebrauchsgegenständeverordnung
LugÜ	Lugano-Übereinkommen
MStG	Militärstrafgesetz
NR	Nationalrätin

OR	Obligationenrecht
P2P	Peer to Peer
RSS	Really Simple Syndication, Format für die strukturierte Veröffentlichung von Änderungen auf Websites
RTVG	Bundesgesetz über Radio und Fernsehen
RTVV	Radio- und Fernsehverordnung
SECO	Staatsekretariat für Wirtschaft
Simsa	Swiss Internet Industry Association (Branchenverband der Schweizer Internet-Wirtschaft)
SKP	Schweizerische Kriminalprävention
Slg	Sammlung der Rechtsprechung des Europäischen Gerichtshofs (EuGH)
s.o.	siehe oben
SR	Systematische Sammlung des Bundesrechts der Schweiz
SRG	Schweizerische Radio- und Fernsehgesellschaft
StGB	Strafgesetzbuch
TABV	Tabakverordnung
URG	Urheberrechtsgesetz
U.S.C.	United States Code (Sammlung und Kodifikation des Bundesrechts der USA)
UWG	Bundesgesetz gegen den unlauteren Wettbewerb
vgl.	vergleiche
WBF	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung
WLAN	Wireless Local Area Network
z.B.	zum Beispiel
ZGB	Zivilgesetzbuch
Ziff.	Ziffer

10.2 Literaturverzeichnis

Aguiton C./Cardon D., The Strength of Weak Cooperation: an Attempt to Understand the Meaning of Web 2.0, Communication & Strategies, no.65, 1st quarter 2007 (**zit. Aguiton C./Cardon D.**).

Bächli Marc, Das Recht am eigenen Bild. Die Verwendung von Personenbildern in den Medien, in der Kunst, der Wissenschaft und in der Werbung aus der Sicht der abgebildeten Person, Basel 2002 (**zit. Bächli Marc, Das Recht am eigenen Bild, Basel 2002**).

Baeriswyl Bruno, Kleingedrucktes unter der Lupe - Die Allgemeinen Geschäftsbedingungen (AGB) von Sozialen Netzwerken versprechen keinen Datenschutz, in: digma 2010 S. 56.

Bianchi della Porta Manuel/Robert Vincent, Responsabilité pénale de l'éditeur de médias en ligne participatifs, in: Medialex 2009, S. 19ff.

Boyd D.M./Ellison N.B., Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), article 11, 2007 (**zit. Boyd D.M./Ellison N.B.**)

Egli Urs, Soziale Netzwerke und Arbeitsverhältnis, in: Jusletter 17.01.2011.

Elixmann Robert, Datenschutz und Suchmaschinen. Neue Impulse für den Datenschutz im Internet, Berlin 2012.

Engel C./Knieps G., Vorschriften des Telekommunikationsgesetzes über den Zugang zu wesentlichen Leistungen: Eine juristisch-ökonomische Untersuchung, Baden-Baden 1998. (**zit. Engel C./Kniwps G.**)

Epiney Astrid/Fasnacht Tobias (Hrsg.), Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes, Zürich 2012.

European Network and Information Security Agency (ENISA), The right to be forgotten – between expectations and practice, Heraklion 2011.

Epiney Astrid/Probst Thomas/Gammenthaler Nina (Hrsg.), Datenverknüpfung. Problematik und rechtlicher Rahmen, Zürich 2011.

Hilty Lorenz/Oertel Britta/Wölk Michaela/Pärli Kurt, Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern, Zürich 2012 (**zit. Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zürich 2012**).

Jöhri Yvonne, Werbung im Internet: rechtsvergleichende, lauterkeitsrechtliche Beurteilung von Werbeformen, Zürich 2000 (**zit. Jöhri Yvonne, Werbung im Internet, Zürich 2000**).

Keller Claudia, AGB von Social-Media-Plattformen, in: Medialex 2012 S. 188ff.

Latzer M./Just N./Metreveli S./Saurwein F. (2012). Internet-Anwendungen und deren Nutzung in der Schweiz. Themenbericht aus dem World Internet Project – Switzerland 2011. Universität Zürich, Zürich.

Mayer-Schönberger Viktor, Delete: Die Tugend des Vergessens in digitalen Zeiten, Berlin 2010.

Meyer Julia, Identität und virtuelle Identität natürlicher Personen im Internet, Baden-Baden 2011.

Neuberger, Christoph, „Soziale Netzwerke im Internet. Kommunikationswissenschaftliche Einordnung und Forschungsüberblick“. In: Neuberger, Christoph; Gehrau, Volker (Hrsg): StudiVZ. Diffusion, Nutzung und Wirkung eines sozialen Netzwerks im Internet. Wiesbaden 2011, S. 33 - 96.

Schmidt, Jan, „Was ist neu am Social Web? Soziologische und kommunikationswissenschaftliche Grundlagen“. In: Zerfass, Ansgar; Welker, Martin; Schmidt, Jan (Hrsg): Kommunikation, Partizipation und Wirkungen im Social Web. Bd. 1. Köln 2008, S. 18 - 40.

Schweizer Alex, Data Mining – ein rechtliches Minenfeld. Rechtliche Aspekte von Methoden des Customer Relationship Management (CRM) wie Data Mining, in: digma 2001 S. 108.

Schweizer Michael, Das Recht am Wort nach Art. 28 ZGB, in: Medialex 2011 S. 197ff.

Schweizer Michael, Recht am Wort: Schutz des eigenen Wortes im System von Art. 28 ZGB, Bern 2012 (**zit. Schweizer Michael, Recht am Wort, Bern 2012**).

Streiff Ullin/von Kaenel Adrian/Roger Rudolph, Arbeitsvertrag Praxiskommentar, 7. Aufl., Zürich 2012.

Studer Melanie/Schweizer Matthias/Brucker-Kley Elke, Sterben und Erben in der digitalen Welt, in: Jusletter 17.12.2012

Von Rimscha M. Björn, Geschäftsmodelle für Social Media . In: Petra Grimm und Oliver Zöllner (Hrsg.): Schöne neue Kommunikationswelt oder Ende der Privatheit? Die Veröffentlichung des Privaten in Social Media und populären Medienformaten. Stuttgart 2012, S. 297–311.

Weber Rolf, E-Commerce und Recht. Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, 2. Aufl., Zürich 2010.

Weber Rolf/Volz Stephanie, Online Marketing und Wettbewerbsrecht, Zürich 2011.

10.3 Gesetzesverzeichnis

Bundesgesetz vom 15. Dezember 2000 über Arzneimittel und Medizinprodukte (HMG), SR 812.21.

Bundesgesetz vom 13. Dezember 2002 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.

Bundesgesetz vom 30. März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (OR), SR 220.

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

Bundesgesetz vom 21. Juni 1932 über die gebrannten Wasser (Alkoholgesetz, AlkG), SR 680.

Bundesgesetz vom 18. Dezember 1987 über das Internationale Privatrecht (IPRG), SR 291.

Bundesgesetz vom 20.Juni 2003 über das Jugendstrafrecht (JStG), SR 311.1.

Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen vom 6.Oktober 1995 (KG), SR 251.

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

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

Bundesgesetz vom 9. Oktober 1992 über das Urheberrecht und verwandte Schutzrechte (URG), SR 231.1.

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

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

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

Militärstrafgesetz vom 13. Juni 1927 (MStG), SR 321.0.

Schweizerische Jugendstrafprozessordnung vom 20.März 2009 (JStPO), SR 312.1.

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

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

Übereinkommen vom 23. November 2001 über die Cyberkriminalität, SR 0.311.43.

Übereinkommen vom 30. Oktober 2007 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (LugÜ), SR 0.275.12.

Übereinkommen vom 20. November 1989 über die Rechte des Kindes, SR 0.107.

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

Übereinkommen Nr. 182 vom 17. Juni 1999 über das Verbot und unverzügliche Massnahmen zur Beseitigung der schlimmsten Formen der Kinderarbeit, SR 0.822.728.2.

Verordnung des EDI vom 23. November 2005 über alkoholische Getränke, SR 817.022.110.

Verordnung 5 vom 28. September 2007 zum Arbeitsgesetz (Jugendarbeitsschutzverordnung, ArGV 5), SR 822.115.

Verordnung vom 17.Oktober 2001 über die Arzneimittelwerbung (AWV), SR 812.212.5.

Verordnung des WBF vom 4. Dezember 2007 über gefährliche Arbeiten für Jugendliche, SR 822.115.2.

Verordnung vom 19. November 2003 über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen (BehiV), SR 151.31.

Verordnung vom 17.Oktober 2012 über die Förderung der ausserschulischen Arbeit mit Kindern und Jugendlichen (KJFV), SR 446.11.

Lebensmittel- und Gebrauchsgegenständeverordnung vom 23. November 2005 (LGV), SR 817.02.

Radio- und Fernsehverordnung vom 9. März 2007 (RTVV), SR 784.401.

Verordnung vom 11. Juni 2010 über Massnahmen zum Schutz von Kindern und Jugendlichen sowie zur Stärkung der Kinderrechte, SR 311.039.1.

Verordnung vom 27. Oktober 2004 über Tabakerzeugnisse und Raucherwaren mit Tabakersatzstoffen (TabV), SR 817.06.

10.4 Verzeichnis abgekürzter internationaler Materialien

10.4.1 Europarat

Abridged Report of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) - 29th Plenary Meeting vom 10. Dezember 2012, T-PD (2012) RAP 29 Abr_en (**zit. Abridged Report of the Consultative Committee of Convention 108, T-PD (2012) RAP 29 Abr_en**).

Ad Hoc Advisory Group on Cross-Border Internet, 4th meeting, executive summary vom 13. & 14.10.2011 (**zit. Ad Hoc Advisory Group on Cross-Border Internet**).

Empfehlung Rec(2004)16 des Ministerkomitees des Europarats vom 15.12.2004 über das Recht auf Gegendarstellung in der neuen Medienumgebung (**zit. Empfehlung Rec(2004)16 über das Recht auf Gegendarstellung in der neuen Medienumgebung**).

Empfehlung Rec(2006)12 des Ministerkomitees des Europarats vom 27.09.2006 über die Befähigung von Kindern zum Umgang mit den neuen Informations- und Kommunikationstechnologien (**zit. Empfehlung Rec(2006)12 über die Befähigung von Kindern zum Umgang mit den neuen Informations- und Kommunikationstechnologien**).

Empfehlung CM/Rec(2007)2 des Ministerkomitees des Europarats vom 31.01.2007 betreffend Medienpluralismus und Vielfalt der Medieninhalte (**zit. Empfehlung CM/Rec(2007)2 betreffend Medienpluralismus und Vielfalt der Medieninhalte**).

Empfehlung CM/Rec(2008)6 des Ministerkomitees des Europarats vom 26.03.2008 über Massnahmen zur Wahrung der Meinungs- und Informationsfreiheit im Hinblick auf Internetfilter (**zit. Empfehlung CM/Rec(2008)6 zur Wahrung der Meinungs- und Informationsfreiheit im Hinblick auf Internetfilter**).

Empfehlung CM/Rec(2009)5 des Ministerkomitees des Europarats vom 08.07.2009 zum Schutz der Kinder gegen schädliche Inhalte und Verhaltensweisen und zur Förderung ihrer aktiven Beteiligung am neuen Informations- und Kommunikationsumfeld (**zit. Empfehlung CM/Rec(2009)5 zum Schutz der Kinder gegen schädliche Inhalte und Verhaltensweisen und zur Förderung ihrer aktiven Beteiligung am neuen Informations- und Kommunikationsumfeld**).

Empfehlung CM/Rec(2010)13 des Ministerkomitees des Europarats vom 23.11.2010 über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling (**zit. Empfehlung CM/Rec(2010)13 über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling**).

Empfehlung CM/Rec(2011)7 des Ministerkomitees des Europarats vom 21.09.2011 zu einem neuen Medienbegriff (**zit. Empfehlung CM/Rec(2011)7 zu einem neuen Medienbegriff**).

Empfehlung CM/Rec(2011)8 des Ministerkomitees des Europarats vom 21.09.2011 über den Schutz und die Förderung der Universalität, Integrität und Offenheit des Internets (**zit. Empfehlung CM/Rec(2011)8 über den Schutz und die Förderung der Universalität, Integrität und Offenheit des Internets**).

Empfehlung CM/Rec(2012)3 des Ministerkomitees des Europarats vom 04.04.2012 zum Schutz der Menschenrechte mit Bezug auf Suchmaschinen (**zit. Empfehlung CM/Rec(2012)3 zum Schutz der Menschenrechte mit Bezug auf Suchmaschinen**).

Empfehlung CM/Rec(2012)4 des Ministerkomitees des Europarats vom 04.04.2012 über den Menschenrechtsschutz in sozialen Netzwerken (**zit. Empfehlung CM/Rec(2012)4 über den Menschenrechtsschutz in sozialen Netzwerken**).

Erklärung des Ministerkomitees des Europarats vom 07.12.2011 über die Achtung der Meinungs-, Versammlungs- und Vereinigungsfreiheit im Zusammenhang mit privat betriebenen Internetplattformen und Online-Diensteanbietern (**zit. Erklärung über die Achtung der Meinungs-, Versammlungs- und Vereinigungsfreiheit im Zusammenhang mit privat betriebenen Internetplattformen und Online-Diensteanbietern**).

Erklärung des Ministerkomitees des Europarats vom 21.09.2011 über die Grundsätze der Internet Governance (**zit. Erklärung über die Grundsätze der Internet Governance**).

Erklärung des Ministerkomitees des Europarats vom 20.02.2008 zum Schutz der Würde, Sicherheit und Privatsphäre von Kindern im Internet (**zit. Erklärung des Europarats zum Schutz der Würde, Sicherheit und Privatsphäre von Kindern im Internet**).

Modernisation of Convention 108: New Proposals of The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) vom 27.04.2012, T-PD-BUR(2012)01Rev2_en (**zit. Modernisation of Convention 108, T-PD-BUR(2012)01Rev2_en**).

10.4.2 Europäische Union

Stellungnahme der Artikel-29-Datenschutzgruppe 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten vom 22.03.2012 (00727/12/DE WP 192), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-2 (**zit. Art. 29-DSG Stellungnahme 00727/12/DE WP 192**).

Bericht der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 13.09.2011 über die Anwendung der Empfehlung des Rates vom 24.09.1998 zum Jugendschutz und zum Schutz der Menschenwürde und der Empfehlung des Europäischen Parlaments und des Rates vom 20.12.2006 über den Schutz Minderjähriger und den Schutz der Menschenwürde und über das Recht auf Gegendarstellung im Zusammenhang mit der Wettbewerbsfähigkeit des europäischen Industriezweigs der audiovisuellen Dienst und Online-Informationsdienste – Schutz der Kinder in der digitalen Welt –, KOM(2011) 556 endgültig (**zit. Bericht der Kommission, KOM(2011) 556 endgültig**).

Beschluss Nr. 1351/2008/EG des Europäischen Parlaments und des Rates vom 16.12.2008 über ein mehrjähriges Gemeinschaftsprogramm zum Schutz der Kinder bei der Nutzung des Internets und anderer Kommunikationstechnologien, ABl. L 348 vom 24.12.2008 S. 118 (**zit. Beschluss Nr. 1351/2008/EG über ein mehrjähriges Gemeinschaftsprogramm zum Schutz der Kinder bei der Nutzung des Internets und anderer Kommunikationstechnologien**).

Empfehlung des Europäischen Parlaments vom 26.03.2009 an den Rat zur Stärkung der Sicherheit und der Grundfreiheiten im Internet (2008/2160(INI)), ABl. C 117 E vom 06.05.2010 S. 206 (**zit. Empfehlung EU-Parlament zur Stärkung Sicherheit und Grundfreiheiten im Internet, (2008/2160(INI))**).

Empfehlung 2006/952/EG des Europäischen Parlaments und des Rates vom 20.12.2006 über den Schutz Minderjähriger und den Schutz der Menschenwürde und über das Recht auf Gegendarstellung im Zusammenhang mit der Wettbewerbsfähigkeit des europäischen Industriezweiges der audiovisuellen Dienste und Online-Informationsdienste, ABl. L 378 vom 27.12.2006 S. 72 (**zit. Empfehlung über den Schutz Minderjähriger und den Schutz der Menschenwürde und über das Recht auf Gegendarstellung im Zusammenhang mit der Wettbewerbsfähigkeit des europäischen Industriezweiges der audiovisuellen Dienste und Online-Informationsdienste, 2006/952/EG**).

Entschliessung des Europäischen Parlaments vom 15.12.2010 zum Einfluss der Werbung auf das Verbraucherverhalten (2010/2052(INI)), ABl. C 169 E vom 15.06.2012 S. 58-65 (**zit. Entschliessung zum Einfluss der Werbung auf das Verbraucherverhalten (2010/2052(INI))**).

Gemeinsame Mittelung an das Europäische Parlament und den Rat „Menschenrechte und Demokratie im Mittelpunkt des Auswärtigen Handelns der EU – Ein wirksamerer Ansatz“ vom 12.12.2011, KOM(2011) 866 endgültig (**zit. Gemeinsame Mitteilung Menschenrechte und Demokratie im Mittelpunkt auswärtigen Handelns, KOM(2011) 866 endgültig**).

Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Bericht über die digitale Wettbewerbsfähigkeit Europas: Hauptergebnisse der i2010-Strategie 2005-2009“ vom 04.08.2009, KOM(2009) 390 endgültig (**zit. Mitteilung „Bericht über die digitale Wettbewerbsfähigkeit Europas Hauptergebnisse der i2010-Strategie 2005-2009“, KOM(2009) 390 endgültig**).

Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Europäische Strategie für ein besseres Internet für Kinder“ vom 02.05.2012, KOM(2012) 196 endgültig (**zit. Mitteilung der Kommission „Europäische Strategie für ein besseres Internet für Kinder“, KOM(2012) 196 endgültig**).

Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Zwischenbewertung des Mehrjahresprogramms der Union zum Schutz der Kinder bei der Nutzung des Internets und anderen Kommunikationstechnologien“ vom 03.02.2012, KOM(2012) 33 endgültig (**zit. Mitteilung der Kommission „Zwischenbewertung des Mehrjahresprogramms der Union zum Schutz der Kinder bei der Nutzung des Internets und anderen Kommunikationstechnologien“, KOM(2012) 33 endgültig**).

Mitteilung der Kommission an den Rat und das Europäische Parlament „Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität“ vom 28.03.2012, KOM(2012) 140 endgültig (**zit. Mitteilung „Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität“, KOM(2012) 140 endgültig**).

Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25.10.2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates, ABl. L 304 vom 22.11.2011 S. 64-88 (**zit. Richtlinie 2011/83/EU über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG und der Richtlinie 1999/44/EG sowie zur Aufhebung der Richtlinie 85/577/EWG und der Richtlinie 97/7/EG**).

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995 S. 31-50 (**zit. Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr**).

Schlussfolgerung des Rates vom 11.05.2012 zur Förderung des Kreativitäts- und Innovationspotenzials junger Menschen, ABl. C 169 vom 15.06.2012 S. 1-4 (**zit. Schlussfolgerung zur Förderung des Kreativitäts- und Innovationspotenzials junger Menschen, 2012/C 169/01**).

Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zum Thema „Das Internet der Dinge“ vom 18.09.2008, ABl. C 077 vom 31.03.2009 S. 60-63 (**zit. Stellungnahme „Das Internet der Dinge“ 2009/C 77/15**).

Stellungnahme des Ausschusses der Regionen zum Thema „Eine digitale Agenda für Europa“, ABl. C 015 vom 18.01.2011 S. 34-40 (**zit. Stellungnahme „Eine digitale Agenda für Europa“, 2011/C 15/07**).

Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zum Thema „Verantwortlicher Umgang mit sozialen Netzwerken und Verhinderung der durch soziale Netzwerke verursachten Probleme“ vom 19.09.2012, ABl. C 351 vom 15.11.2012 S. 31-35 (**zit. Stellungnahme „Verantwortlicher Umgang mit sozialen Netzwerken und Verhinderung der durch soziale Netzwerke verursachten Probleme“, 2012/C 351/07**).

Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 25.01.2012, KOM(2012) 11 endgültig (**zit. Vorschlag EU Datenschutz-Grundverordnung, KOM(2012) 11 endgültig**).

10.4.3 Deutschland

Antwort der Bundesregierung auf die kleine Anfrage „Rechtsextremismus im Internet“ vom 07.06.2010, Drucksache 17/1930 (**zit. Antwort Bundesregierung auf Anfrage „Rechtsextremismus im Internet“, 17/1930**).

Gesetzesentwurf des Bundesrates zur Änderung des Telemediengesetzes vom 03.08. 2011, Drucksache 17/6765 (**zit. Gesetzesentwurf Änderung Telemediengesetz, 17/6765**).

Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes vom 15.12.2010, Drucksache 17/4230 (**zit. Gesetzesentwurf Beschäftigtendatenschutz, 17/4230**).

10.5 Studien & Berichte

Bernet ZHAW Studie Social Media Schweiz 2012.

eHealth Suisse Bericht Öffentliches Gesundheitsportal.

ENISA Threat Landscape Report vom 28.09.2012.

EU Kids Online Final Report, September 2011.

Jahresberichte 2011 und 2012 Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK).

Optimus Studie „Sexuelle Übergriffe an Kindern und Jugendlichen in der Schweiz“, Februar 2012.

Stiftung Warentest „Datenschutz bei Onlinenetzwerken“, 2010.

Studie des Bundesamtes für Statistik „Internet in den Schweizer Haushalten. Ergebnisse der Erhebung Omnibus IKT 2010“.

Unveröffentlichte Zahlen aus der netTEEN-Studie (Perren S. & Sticca F., 2012. Jacobs Center for Productive Youth Development, Universität Zürich).

Wikimedia Stiftung: Geschäftsbericht 2010/2011.