Martina Schlögel

Das Bundesverfassungsgericht, die informationelle Selbstbestimmung und das Web 2.0

Von der Schwierigkeit in den Weiten des Internets einen sicheren (Daten-) Hafen zu finden

1. Das Bundesverfassungsgericht und die informationelle Selbstbestimmung

In seiner 60-jährigen Bestehensgeschichte sah sich das Bundesverfassungsgericht zwei Mal dazu veranlasst, im Rahmen eines zur Entscheidung vorgelegten Sachverhalts durch Auslegung und Interpretation der Verfassung ein neues Grundrecht zu statuieren. Sowohl das Recht auf informationelle Selbstbestimmung aus der Anfangszeit der elektronischen Datenverarbeitung im Jahre 1983 als auch das Recht auf den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme aus dem Jahre 2008 betreffen den Schutz persönlicher Daten vor staatlichem Zugriff. Doch auch in den Entscheidungen zur Rasterfahndung[1] und zur Vorratsdatenspeicherung[2] setzten sich die Richter mit den Gefahren der automatisierten Verarbeitung und Verknüpfung personenbezogener Daten auseinander.

1.1 Das Volkszählungsurteil des Bundesverfassungsgerichts und der Beschluss zur Rasterfahndung

Das Recht auf informationelle Selbstbestimmung, das im Rahmen richterlicher Rechtsfortbildung geschaffen wurde, ist als eigenständiges Grundrecht zu werten[3].

Der Anlass für die Entscheidung zum Volkszählungsgesetz im Jahre 1983 erscheint aus heutiger Sicht eher harmlos. Es sollten – wie die eigentliche Bezeichnung des Gesetzes beschreibt – zum Zwecke einer an den wirtschaftlichen, ökologischen und sozialen Zusammenhängen ausgerichteten Politik das Volk, die Berufs-, Wohnungs- und Arbeitsstätten gezählt werden (vgl. Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (VZG) vom 25.03.1982, BGBl. I, S. 369). Doch bei vielen Bürgern regte sich die Furcht, einer anonymen staatlichen Bürokratie hilflos ausgeliefert zu sein, gepaart mit dem Unbehagen vor der zunehmenden Komplexität technischer Möglichkeiten

1 Beschluss des Bundesverfassungsgerichts vom 04.04.2006, BVerfGE 115, 320.
2 Urteil des Bundesverfassungsgerichts vom 02. März 2010, BVerfGE 125, 260.
3 Vgl. Andreas Fisahn, / Martin Kutscha, *Verfassungsrecht konkret*, Berlin 2008, S. 31.

gerade auf dem Gebiet der Informationsverarbeitung[4], weshalb die Vorstellung eines »gläsernen Bürgers« zur Schreckensvision avancierte.

Als Reaktion auf diese neue Freiheitsbedrohung konstituierte das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung, dessen Schutzbereich alle personenbezogenen Daten und alle Daten, die dazu geeignet sind, einen Bezug zu einer bestimmten Person herzustellen[5], umfasst. Dieses neue Grundrecht leiteten die Karlsruher Richter aus den Art. 2 I i.V.m. 1 I GG – dem allgemeinen Persönlichkeitsrecht – ab. Schon vor dem Urteil zum VZG war in der Rechtswissenschaft anerkannt, dass dieses die aus dem Recht der Selbstbestimmung resultierende Befugnis des Einzelnen umfasst, selbst über den Zeitpunkt und den Umfang der Offenbarung persönlicher Lebensverhältnisse zu entscheiden[6]. Mit der Fortentwicklung des allgemeinen Persönlichkeitsrechts reagierte der erste Senat auf die mit dem Terminus »automatische Datenverarbeitung« beschriebene Entwicklung der Technik im Informationssektor. Aus heutiger Sicht muten die Überlegungen der Richter – ohne diese überhöhen zu wollen – in Teilen geradezu prophetisch an:

> *»Individuelle Selbstbestimmung setzt aber – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, dass dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen über mögliche Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. […] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seine Bürger begründeten demokratischen Gemeinwesens ist.«*[7]

Träger des 1983 statuierten Grundrechts kann nach h.M. wegen des Bezugs der Art. 2 I i.V.m. Art. 1 I GG auf den einzelnen Menschen nur eine natürliche Person sein, nicht

4 Vgl. Wolf-Rüdiger Schenke, »Verfassungskonformität der Volkszählung« in: *Neue Juristische Wochenschrift* Nr. 44 (2007), S. 2777.

5 Vgl. Andreas Fisahn / Martin Kutscha, *Verfassungsrecht konkret*, aaO. (FN 3), S. 33. Laut der Autoren fallen auch Daten, die auf den ersten Blick belanglos erscheinen mögen, unter den Schutzbereich, so etwa Adressen, Telefonnummern oder Bilddaten, wobei nicht nur elektronisch, sondern auch herkömmlich gespeicherte Daten umfasst sind.

6 Vgl. Friedrich Schoch, »Das Recht auf informationelle Selbstbestimmung« in: *Jura* Nr. 5 (2008), S. 353.

7 BVerfGE 65, 1, 43.

aber eine juristische Person[8]. Nicht vom Schutzbereich des Rechts auf informationelle Selbstbestimmung umfasst ist die freiwillige Preisgabe personenbezogener Daten des Einzelnen, da in diesem Fall eine von staatlicher Seite grundsätzlich zu respektierende Einwilligung des betroffenen Bürgers vorliegt.

Die Entscheidung zur Rasterfahndung kann unter dem Aspekt des Datenschutzes als inhaltliches Bindeglied zwischen dem Volkszählungsurteil und der Entscheidung zur Onlinedurchsuchung gesehen werden. Beide Entscheidungen befassen sich mit den Gefahren der Erhebung, Speicherung und Kombination von Daten. Die von den technischen Möglichkeiten des Internets ausgehenden spezifischen Gefahren standen jedoch erst bei den beiden im Folgenden (siehe unter I 2.) erläuterten Entscheidungen im Mittelpunkt.

Bei der Rasterfahndung handelt es sich um eine polizeiliche Fahndungsmethode, die auf die elektronische Datenverarbeitung zurückgreift. Die Polizeibehörden lassen sich hierbei von anderen öffentlichen oder privaten Stellen personenbezogene Daten übermitteln, um einen automatisierten Abgleich der Daten miteinander vorzunehmen. Durch diesen Abgleich soll diejenige Schnittmenge von Personen ermittelt werden, auf die bestimmte, vorab festgelegte und für eine betriebene Ermittlung als bedeutsam angesehene Merkmale zutreffen[9]. In ihrer Entscheidung betonten die Richter das besondere Gewicht der durch die Rasterfahndung erfolgenden Grundrechtseingriffe. Dieses ergäbe sich aus der Reichweite der Befugnis, der Möglichkeit der Verknüpfung von Daten aus öffentlichen und privaten Beständen und besonders aus der Tatsache, dass die von der Befugnis erfassten Daten nach Art und Umfang nicht eingegrenzt seien. Umsichtig führten die Richter aus, dass in Hinblick auf die Eingriffsintensität der Rasterfahndung nach dem 11. September 2001 auch berücksichtigt werden müsse, dass sie sich gegen Ausländer bestimmter Herkunft und muslimischen Glaubens richte. Mit einer derartigen Maßnahme sei stets das Risiko verbunden, Vorurteile zu reproduzieren und diese Bevölkerungsgruppen in der Öffentlichkeit zu stigmatisieren[10]. Zudem führten die Richter als Gefahren derartiger Datensammlungen an, dass das Risiko der Betroffenen, zum Gegenstand staatlicher Ermittlungsmaßnahmen zu werden, weit über das Risiko, einem ungerechtfertigten Verdacht ausgesetzt zu werden, hinausgehe, und dass von der Heimlichkeit der Maßnahme ein erheblicher Einschüchterungseffekt ausgehe. Auch bei der – im Folgenden dargestellten – Entscheidung zur Online-Durchsuchung stand die Gefährlichkeit staatlicher Datensammlungen im Mittelpunkt. Durch den geplanten Einsatz des viel zitierten »Bundestrojaners« kam dem Vorhaben der Sicherheitsbehörden aber sowohl in technischer Hinsicht als auch die Eingriffstiefe und –intensität betreffend eine neue Qualität zu.

8 Vgl. Friedrich Schoch, Das Recht auf informationelle Selbstbestimmung, aaO. (FN 6), S. 356.
9 Vgl. BVerfE 115, 320, 321.
10 Vgl. BVerfGE 115, 320, 351.

1.2 Das Recht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und das Urteil zur Vorratsdatenspeicherung

Mit der erheblich gewachsenen Bedeutung des Internets für die Persönlichkeitsentfaltung korrespondiert notwendig auch die Zunahme der Gefährdungspotentiale. Neben vielen anderen, vor allem von Privaten ausgehenden Gefährdungen, ermöglicht das Internet auch den staatlichen Zugriff auf die vom Bürger genutzten technischen Ressourcen, die seine mit der Internet-Nutzung verbundenen, aber auch alle sonst dort abgelegten Daten erfassen[11]. Der Begriff Online-Durchsuchung ist in gewisser Weise irreführend, denn es handelt sich um keine Maßnahme der Durchsuchung im Sinne der §§ 102ff. StPO, sondern um die Anwendung speziell zur Ausforschung von Daten entwickelter Softwareprogramme (»Trojanische Pferde«), die von Polizei oder Nachrichtendiensten über das Internet in einen bestimmten Computer eingeschleust werden können[12]. Diese »Spionageprogramme« agieren ohne Wissen des Computernutzers und dienen der Ausspähung der auf der Festplatte gespeicherten Daten und anderer Anwendungen wie etwa der Internet-Nutzung oder dem Versenden von E-Mails[13].

Die Entscheidung des Bundesverfassungsgerichts war in zweifacher Hinsicht bemerkenswert. Zum einen haben die Beschwerdeführer die Nichtigkeit einer Schlüsselnorm des reformierten Verfassungsschutzgesetzes des Landes Nordrhein-Westfalen erreicht, und zum anderen haben sie mit ihren Verfassungsbeschwerden das Gericht dazu bewogen, ein neues Grundrecht zu schaffen – zum zweiten Mal in der Geschichte des Gerichts überhaupt –, das Recht auf die »Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme«. Das Gericht hat der Online-Durchsuchung einen »breit wirksamen Riegel«[14] vorgeschoben, der kaum noch Raum für die Infiltration von Computern lässt. Denn das so genannte Computerschutzrecht darf nach dem zweiten Leitsatz des Urteils nur eingeschränkt werden, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Zu diesen Rechtsgütern gehören nach der Rechtsprechung des Gerichts Leib, Leben oder Freiheit von Personen sowie der Bestand des Staates und die Grundlagen menschlicher Existenz[15].

Im Einzelnen erklärte das Bundesverfassungsgericht den § 5 II Nr. 11 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen für mit den Art. 2 I GG i.V.m. Art. 1 I GG, Art. 10 I GG und Art. 19 I 2 GG für unvereinbar und nichtig. Die Richter führten hierzu aus, die Vorschrift wahre insbesondere nicht das Gebot der Verhältnismäßigkeit, denn ein derart schwerer Grundrechtseingriff wie die heimliche Infiltration

11 Vgl. Martin Eifert, »Informationelle Selbstbestimmung im Internet. Das Bundesverfassungsgericht und die Online-Durchsuchungen« in: *Neue Zeitschrift für Verwaltungsrecht* Nr. 5 (2008), S. 521.

12 Vgl. Martin Kutscha, »Verdeckte „Online-Durchsuchung" und Unverletzlichkeit der Wohnung« in: *Neue Juristische Wochenschrift* (2007), S. 1169.

13 Vgl. Martin Kutscha, »Verdeckte „Online-Durchsuchung" und Unverletzlichkeit der Wohnung«, aaO. (FN 12), S. 1169.

14 Vgl. Axel Tschentscher, »Das Grundrecht auf Computerschutz« in: *Aktuelle Juristische Praxis* Nr. 4 (2008), S. 385.

15 Vgl. Axel Tschentscher, Das Grundrecht auf Computerschutz, aaO. (FN 14), S. 385.

eines informationstechnischen Systems setzte grundsätzlich zumindest die Normierung einer qualifizierten materiellen Eingriffsschwelle voraus. Zudem verfüge die Vorschrift nicht über hinreichende Vorkehrungen, um Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung zu vermeiden.

Das neue Grundrecht leitete das Gericht – wie schon im Volkszählungsurteil – aus dem allgemeinen Persönlichkeitsrecht nach Art. 2 I GG i.V.m. Art. 1 I GG ab. Der erste Senat entschied, dass die Anordnung der heimlichen Infiltration grundsätzlich unter den Vorbehalt einer richterlichen Anordnung zu stellen sei, und dass ein Gesetz, das zu einem derartigen Eingriff ermächtigt, Vorkehrungen zum Schutz des Kernbereichs privater Lebensführung enthalten müsse. Es wurde aber auch klar abgegrenzt, dass die bloße Teilnahme des Staates an öffentlichen Kommunikationsvorgängen und das Wahrnehmen öffentlich zugänglicher Kommunikationsinhalte noch keinen Grundrechtseingriff darstellen.

Wohl wachgerüttelt und ermutigt durch die Entscheidung zur Online-Durchsuchung formierte sich ab dem Jahr 2008 in der Bevölkerung – erstmals wieder seit den Protesten gegen das Volkszählungsgesetz in den 1980er Jahren – breiter Widerstand gegen eine flächendeckende, verdachtsunabhängige staatlich angeordnete Datenspeicherung. Bei der Entscheidung zur Vorratsdatenspeicherung reichten – einmalig in der Geschichte des Bundesverfassungsgerichts – 34.000 Bürgerinnen und Bürger eine Verfassungsbeschwerde in Form einer Sammelklage gegen das am 1.1.2008 in Kraft getretene »Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG« ein. In Frage standen die Erhebung, Speicherung und Verwendung von Telekommunikationsdaten in Rahmen sicherheitsbehördlicher Ermittlungen. Unter Telekommunikations-Verkehrsdaten versteht man die Daten, die bei der Erbringung eines Telekommunikationsdienstes – wie etwa Festnetzanschlüsse, Mobiltelefone, Internetzugangsdienste und E-Mail-Postfächer – erhoben, verarbeitet oder genutzt werden[16]. Da die elektronische Kommunikation mittlerweile zu einem festen Bestandteil des Lebensalltags fast aller Bevölkerungsgruppen geworden ist und dabei eine Vielzahl von Datenspuren erzeugt wird (wie etwa Rufnummern, Rufum- und -weiterleitungen, Namen, Anschriften, Benutzerkennungen, Internetprotokolladressen, Kalenderdaten, Uhrzeit und Dauer der Kommunikation sowie Daten zum Standort der Nutzer) handelte es sich bei der Vorratsdatenspeicherung um eine Maßnahme von bislang nicht da gewesener Streubreite[17].

Dass der erste Senat vor seiner Entscheidung in der Sache dem Antrag der Kläger auf den Erlass einer einstweiligen Anordnung am 11.03.2008 teilweise stattgab, zeigte bereits, dass die Richter den aufgeworfenen Fragen zum Datenschutz eine große Bedeutung beimaßen. In ihrem Urteil machten die Richter dem Gesetzgeber im Rahmen ihrer Ausführungen zur Frage der Verhältnismäßigkeit der gesetzlichen Ausgestaltung der Vor-

16 Vgl. § 3 Nr. 30 Telekommunikationsgesetz (TKG).

17 Vgl. Martina Schlögel, »Die Karlsruher Entscheidung zur Vorratsdatenspeicherung: Lässt das Bundesverfassungsgericht die Bürger im Regen stehen?« in: Gesellschaft – Wirtschaft – Politik Nr. 2 (2010), S. 168.

ratsdatenspeicherung konkrete Vorgaben hinsichtlich künftiger Regelungen. Hierbei wurde detailliert auf die Anforderungen an exekutives Handeln bei der Datensicherheit, bei der unmittelbaren Datenverwendung, sowie für die Transparenz der Datenübermittlung, und auf die Anforderungen an den Rechtsschutz und bei Sanktionen im Falle von Rechtsverletzungen eingegangen[18].

Zusammenfassend lässt sich festhalten, dass das Bundesverfassungsgericht in den vergangenen Jahren im Weg der richterlichen Rechtsauslegung und Rechtsfortbildung für die Bürger einen klar definierten Bereich geschaffen hat, in dem sie Schutz vor staatlichem Zugriff auf ihre Daten genießen.

2. Das Web 2.0 als neue Dimension des Internets und die damit verbundenen Gefahren für den Datenschutz

2.1 Kennzeichen und Nutzung des Web 2.0

In seinen Anfängen war das Internet ein Medium, das seinen Nutzern allein den Konsum von Informationen ermöglichte[19]. Das bedeutete, dass viele Nutzer Inhalte rezipierten, die von wenigen Anbietern bereitgestellt worden waren. In den vergangenen Jahren avancierte das Internet zum multifunktionalen Leitmedium, in dem grundsätzlich die Möglichkeiten aller bisherigen Medien inkludiert sind[20]: Tageszeitungen stellen Teile ihrer Inhalte auf ihre Internetseiten, bzw. beschäftigen eigene Online-Redaktionen, man kann über das Internet Bücher lesen, telefonieren und fernsehen, um nur einige der Möglichkeiten exemplarisch zu nennen.

Die Weiterentwicklung zum Web 2.0 ist ein Phänomen des 21. Jahrhunderts und ging mit der Entstehung von (Kommunikations-) Plattformen im Internet einher, die den Nutzern die Möglichkeit bieten, Inhalte im Netz mitzugestalten. Ein besondere Erfolgsgeschichte sind die »Sozialen Netzwerke«, bei denen eine Gemeinschaft von Menschen oder Gruppierungen durch eine interaktive Webanwendung miteinander verbunden ist[21]. Hierunter fallen etwa Facebook, StudiVZ, Xing oder Twitter, aber auch andere auf Kommunikation und Interaktion ausgelegte Websites wie zum Beispiel Wikipedia und zudem die unzähligen Blogs, die von Privaten oder Firmen ins Netz gestellt werden.

Die Nutzer Sozialer Netzwerke erstellen – nicht zwingend unter ihrem tatsächlichen Namen – ein Profil, in das sie, anhängig von ihrer Intention und den aus dem Zweck des Netzwerks resultierenden Möglichkeiten zur Eingabe, persönliche Daten eintragen und

18 Vgl. Martina Schlögel, Die Karlsruher Entscheidung zur Vorratsdatenspeicherung: Lässt das Bundesverfassungsgericht die Bürger im Regen stehen?, aaO. (FN 17), S. 168.

19 Vgl. Volker Erd, »Datenschutzrechtliche Probleme sozialer Netzwerke« in: *Neue Zeitschrift für Verwaltungsrecht* Nr. 1 (2011), S. 19.

20 Vgl. Phillippe Gröschel, »Bedrohen soziale Netzwerke den Datenschutz? Wie neue Angebote im Internet einen Wandel in der Gesellschaft auslösen« in: *Das Anwaltsblatt* Nr. 4 (2011), S. 276.

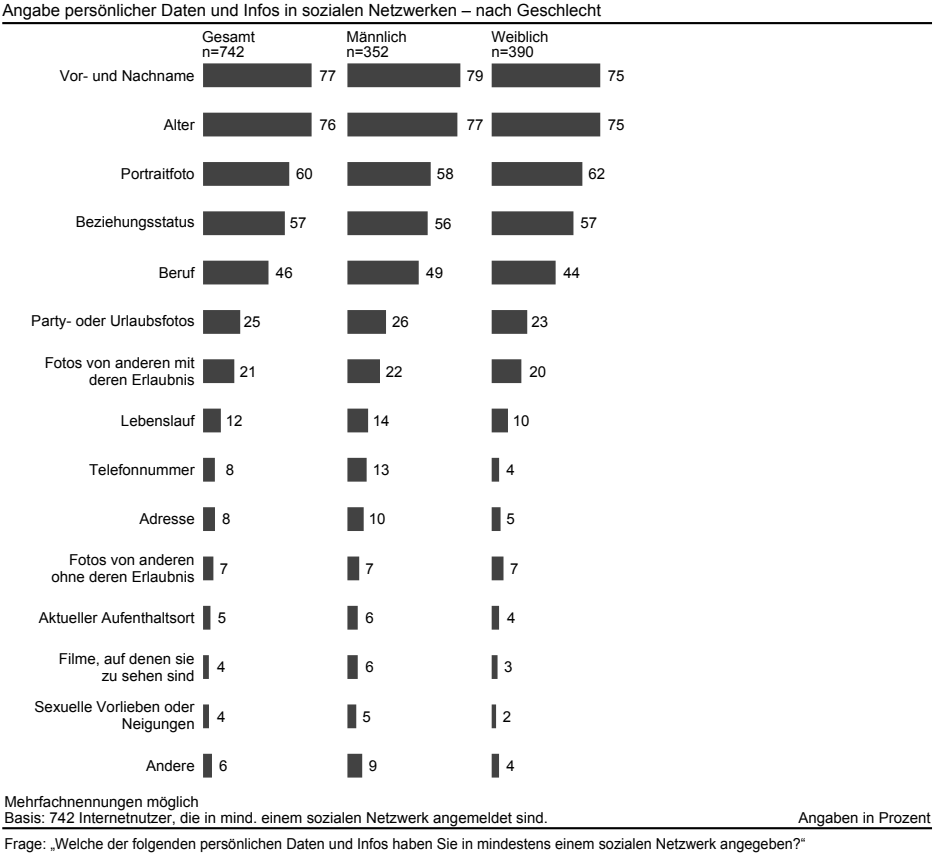
21 Vgl. Indra Spieker, »Kommunikation als Herausforderung« in: *Das Anwaltsblatt* Nr. 4 (2011), S. 256.

gegebenenfalls auch eigene Fotos hochladen, weshalb diese Netzwerke auch als »Netzgemeinschaft mit User Generated Content« bezeichnet werden[22]. Im Jahr 2011 verfügten 74,7 % aller Deutschen über einen Internetzugang[23]. Von diesen Internetnutzern waren im Jahr 2011 76% in mindestens einem Sozialen Netzwerk angemeldet und 74% aller Nutzer gaben an, in diesen Netzwerken aktiv zu sein, wobei es hier deutliche altersabhängige Unterschiede in der Verteilung gibt[24]. Von den 14- bis 29-jährigen Internetnutzern sind mit 94% beinahe alle in einem Sozialen Netzwerk aktiv, und auch die Gruppe der 30- bis 49- jährigen ist mit 76% aktiven Nutzern noch recht stark vertreten[25]. Das am häufigsten – nämlich von 42 % aller Nutzer – frequentierte Netzwerk ist Facebook, mit deutlichem Abstand gefolgt von »wer-kennt-wen« (18 Prozent), »StayFriends« (17 Prozent) und »meinVZ« (10 Prozent)[26].

Überraschend ist die Offenheit, mit der die Nutzer Sozialer Netzwerke persönliche Daten und Informationen preisgeben. So geben etwa 77% aller Nutzer ihren Vor- und Nachnamen an, 76% nennen ihr Alter, 60% laden auf ihrem Profil ein eigenes Portraitfoto und 25% eigene Party- oder Urlaubsfotos hoch, und immerhin 4% äußern sich zu ihren sexuellen Vorlieben oder Neigungen (vgl. unten stehende Abbildung)[27].

22 Vgl. Niko Härting / Daniel Schätzle, Rechtsverletzungen in »Social Networks« in: *Der IT-Rechts-Berater* (2010), S. 39.
23 Vgl. Initiative D21, »(N)Onliner Atlas 2011«, http://mcaf.ee/c2beh (Stand 12/2011).
24 Vgl. Bitkom, »Soziale Netwerke. Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet«, http://mcaf.ee/uh57 w (Stand 12/2011).
25 Vgl. Bitkom, Soziale Netwerke. Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet, aaO. (FN 24).
26 Vgl. Bitkom, Soziale Netwerke. Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet, aaO. (FN 24).
27 Vgl. aaO. (FN 24).

Abbildung: Angabe persönlicher Daten und Informationen in sozialen Netzwerken



Quelle: Bitkom, »Soziale Netwerke. Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet«, aaO. (FN 24).

Die Unterscheidung zwischen realer und virtueller Welt wird gerade für intensive Internetnutzer zunehmend obsolet, denn so wie Telefon und Fernsehen Teile unserer realen Welt sind, so ist in weiten Teilen der Lebens- und Arbeitswelt die Nutzung des Internets untrennbar mit dem Alltag verbunden. Das führt dazu, dass negative Verhaltensweisen, die ein Teil unserer gesellschaftlichen Realität sind, auch in Sozialen Netzwerken zu finden sind[28], so etwa das Mobbing, das mittlerweile unter dem Begriff des »Cyber-Mobbing« im Zusammenhang mit den Selbsttötungen von Teenagern traurige Bekanntheit erlangt hat[29]. Die von Wolfgang Hoffmann-Riem als »Zukunftseuphoriker« be-

28 Vgl. Phillippe Gröschel, Bedrohen soziale Netzwerke den Datenschutz, aaO. (FN 20), S. 276.
29 Vgl. Frank Patalong, »Tod eines Teenagers« in: *Spiegel Online* (18.11.2007), http://mcaf.ee/6321t (Stand 12/2011).

zeichneten Befürworter neuer technischer Entwicklungen preisen das Web 2.0 als Segen für die Demokratie, da es eine neue Qualität öffentlicher Kommunikation und neue Möglichkeiten der Verbindung von herrschaftsfreier horizontaler Kommunikation und politischer Teilhabe ermöglicht, welche der demokratischen Regierungsform neue zivilgesellschaftliche Legitimation verschaffen werde[30].

2.2 Welche Akteure können die informationelle Selbstbestimmung im Web 2.0 bedrohen?

Generell sind drei Gruppen von Akteuren denkbar, die das Recht auf informationelle Selbstbestimmung von Internetnutzern verletzen können: staatliche Organe (z.B. die Sicherheitsbehörden des Bundes und der Länder), große Konzerne, die Dienste oder Plattformen anbieten (z.B. Google oder Facebook) oder Einzelpersonen (z.B. Hacker oder Kriminelle, die versuchen – etwa mittels schädlicher Software (so genannter »Malware«) – Daten wie Konto- oder Kreditkartennummern abzugreifen).

Aus dem Blickwinkel der informationellen Selbstbestimmung zeigt sich ein grundlegender Wechsel der Gefahrenquelle. Die oben vorgestellten Entscheidungen der Karlsruher Richter betreffen alle den Schutz des Bürgers vor staatlichem Handeln, das bis zur jeweiligen Entscheidung des Bundesverfassungsgerichts seine Legitimation in technikverliebtem (sicherheits-) gesetzgeberischem Übereifer fand. Als in den ersten zehn Jahren nach den terroristischen Anschlägen des 11. September 2001 im Rahmen der Terrorismusbekämpfungs- und Präventionsmaßnahmen das Misstrauen des Staates ins Unermessliche wuchs, und der Staat aus bürgerrechtlicher Perspektive gleichsam als »Big Brother« zu agieren schien, war es am Bundesverfassungsgericht, den Grundrechten zu ihrer angemessenen Geltung zu verhelfen, und sicherheitsbehördliche Befugnisse entsprechend einzuhegen.

Betrachtet man das Web 2.0 – und hier insbesondere die stark frequentierten Sozialen Netzwerke –, so scheint die von ihnen ausgehende Gefahr für die Daten ihrer Nutzer momentan ungleich größer zu sein, denn die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Private steht entsprechenden staatlichen Aktivitäten in nichts mehr nach[31]. Die dort zur Anwendung kommenden Datenschutzbestimmungen jedoch sind überaus uneinheitlich und stehen häufig nicht im Einklang mit dem deutschen Datenschutzrecht.

Deshalb wird im Folgenden der Fokus auf der Bedrohung der informationellen Selbstbestimmung durch das Web 2.0 – und hier insbesondere auf der Frage des Datenschutzes bei den Branchengiganten der Social Networks – liegen.

30 Vgl. Wolfgang Hoffmann-Riem, »Mediendemokratie als rechtliche Herausforderung « in *Der Staat* Nr. 42 (2003), S. 193.

31 Vgl. Friedrich Schoch, Das Recht auf informationelle Selbstbestimmung, aaO. (FN 6), S. 353.

2.3 Arten der Bedrohung der informationellen Selbstbestimmung

Rechtsverletzungen finden in der virtuellen Welt ebenso statt wie in der realen; gerade die vermeintliche Anonymität im Internet kann zur Verletzung von Urheberrechten und zur Missachtung von Persönlichkeits- oder Namensrechten verleiten[32]. Doch auch wenn eine steigende Zahl von Nutzern ihre Lebensumstände in Sozialen Netzwerken präsentiert, darf das nicht zu einer Auflösung des Persönlichkeitsrechts führen[33]. Ebenso wie im realen Leben sind auch bei der Nutzung des Internets »Kern und Regelungszweck des Persönlichkeitsrechts […], den Einzelnen vor der Gefährdung seiner immateriellen Integrität und Selbstbestimmung zu schützen und ihm einen autonomen Bereich eigener Lebensgestaltung zu bewahren, indem er seine Individualität unter Ausschluss anderer entwickeln und wahrnehmen kann«[34].

Soziale Netzwerke bieten ihren Nutzern unentgeltlichen Zugang zum Netzwerk und zu der zum Zwecke der Nutzung bereitgestellten Plattform. Bereits aufgrund der Tatsache, dass Unternehmen wie Google oder Facebook global agierende Konzerne sind, sollte den Nutzern bewusst sein, dass das Kapital dieser Unternehmen in den Daten ihrer Mitglieder liegt. Zwar haben diese Unternehmen selbst regelmäßig kein eigenes Interesse an der Nutzung der Daten, wohl aber an deren Weitergabe an Dritte zu deren direkter oder indirekter Nutzung (in Form von Werbung im Sozialen Netzwerk)[35]. Soziale Netzwerke gewinnen dadurch an Wert, dass sie eine große Zahl oder eine besondere Gruppe von Mitgliedern erreichen, so dass die so generierten Datensammlungen für verschiedenste Branchen von großem Interesse sind. Generell lässt sich sagen: Je differenzierter das Niveau der gewonnenen personenbezogenen Daten ist, umso effektiver kann Werbung eingesetzt werden, umso aussagekräftiger sind Datenkombinationen und umso wertvoller werden die Daten aus den Nutzerprofilen[36].

Nun ist nicht generell jede Verwendung von Nutzerdaten durch die Betreiber Sozialer Netzwerke widerrechtlich und ein illegitimer Eingriff in das Recht auf informationelle Selbstbestimmung. In Deutschland richtet sich die Rechtmäßigkeit der Erhebung und Verwendung von Daten zu Marketingzwecken nach den §§ 11 ff Telemediengesetz (TMG), hinter denen die Vorschriften des Bundesdatenschutzgesetzes (BDSG) als allgemeine Regelungen zurücktreten[37]. Unter rechtlichen Aspekten lassen sich die Angaben, die Nutzer in Sozialen Netzwerken machen, in die folgenden Gruppen einordnen: Anmeldedaten, Nutzungsdaten, Profildaten und Nutzungsprofile.

32 Vgl. Niko Härting,/ Daniel Schätzle, Rechtsverletzungen in »Social Networks«, aaO. (FN 22), S. 39.
33 Vgl. Frank A. Koch, »Grundlagen des Persönlichkeitsrechts und allgemeine Gefährdungen im Internet« in: *Der IT-Rechts-Berater* (2011), S. 128.
34 Vgl. Frank A. Koch, Grundlagen des Persönlichkeitsrechts und allgemeine Gefährdungen im Internet, aaO. (FN 33), S. 129.
35 Vgl. Indra Spiecker, Kommunikation als Herausforderung, aaO. (FN 21), S. 256.
36 Vgl. Volker Erd, Datenschutzrechtliche Probleme sozialer Netzwerke, aaO. (FN 19), S. 19.
37 Vgl. Niko Härting, / Daniel Schätzle, Rechtsverletzungen in Social Networks, aaO. (FN 22), S. 40.

Unter Anmeldedaten werden die Daten verstanden, die für die Anmeldung in einem Netzwerk eingegeben werden. Diese stellen nach § 14 I TMG Bestandsdaten dar und dürfen erhoben werden, soweit sie für die Begründung, die inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer für die Nutzung von Telemedien erforderlich sind. Bei den Nutzungsdaten handelt es sich nach § 15 I Nr. 1-3 TMG um die personenbezogenen Daten eines Nutzers, die erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Hierunter fallen Merkmale zur Identifikation des Nutzers (§ 15 I Nr. 1 TMG), Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung (§ 15 I Nr. 2 TMG) und Angaben über die vom Nutzer in Anspruch genommenen Telemedien (§ 15 I Nr. 3 TMG). Denkbar sind hier darüber hinaus die Anzahl von Downloads oder auch Benutzername und Passwort[38].

Da die Profildaten von den Nutzern freiwillig zur Verfügung gestellt werden, können diese nicht an den Anforderungen des TMG gemessen werden; vielmehr ist hier das BDSG einschlägig. Nach § 28 III BDSG ist »die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung […] zulässig, soweit der Betroffene eingewilligt hat (…)«. Wenn der Betroffene i.S.d. § 28 IV BDSG widerspricht, muss eine Nutzung von Profildaten zu Werbezwecken unterbleiben. Sofern das Surfverhalten eines Internetnutzers erfasst wird, handelt es sich um Nutzungsprofile i.S.d. § 15 III TMG. Deren Erstellung ist zulässig, wenn sie zu Zwecken der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien unter der Verwendung von Pseudonymen erstellt werden und dem Nutzer eine Widerspruchsmöglichkeit gegeben wird, auf welche er gem. § 15 III 2 TMG hinzuweisen ist, und das Verbot der Zusammenführung mit Daten über den Träger des Pseudonyms nach § 15 III 3 TMG gewahrt wird. Die Einhaltung dieser Regelung erscheint durchaus problematisch, da die Mehrheit der Nutzer von Diensten wie Facebook, Xing oder StudiVZ ihr Profil unter ihrem bürgerlichen Namen anlegen[39].

Neben diesen legalen Möglichkeiten der Datennutzung durch die Betreiber gibt es jedoch auch neue technische Verfahren, die sich in rechtlichen Grauzonen bewegen, weil die Nutzer von Netzwerken in diesen Fällen unzureichend oder gar nicht über die Verwendung ihrer Daten informiert werden. Zudem gibt es Verfahren, die zumindest deutschem Datenschutzrecht zuwider laufen, da die Nutzer oder auch Dritte häufig nichts von der Verwendung und Verknüpfung ihrer Daten wissen und darüber hinaus keine Einspruchsmöglichkeit eingeräumt bekommen. Im Folgenden sollen zwei neuere und häufig eingesetzte technische Verfahren zur Persönlichkeitserfassung kurz vorgestellt werden: Die »Gesichtserkennung« und das »Geotagging«[40].

38 Vgl. Niko Härting, / Daniel Schätzle, Rechtsverletzungen in Social Networks, aaO. (FN 22), S. 40.

39 Vgl. Niko Härting, / Daniel Schätzle, Rechtsverletzungen in Social Networks, aaO. (FN 22), S. 40.

40 Die folgenden Ausführungen beziehen sich – soweit nicht anders gekennzeichnet – auf den Beitrag von Frank A. Koch, »Schutz der Persönlichkeitsrechte im Internet: spezifische Gefährdungen« in: *Der IT-Rechts-Berater* (2011), S. 158ff.

Bei der Gesichtserkennung kommt frei zugängliche Software zum Einsatz, die Personen allein anhand ihrer Gesichter oder biometrischen Daten identifizieren kann. Derartige Software ist mittlerweile auch als App für Smartphones erhältlich, so dass mit der Handykamera aufgenommene Bilder anderer Personen in Echtzeit mit der Bildersammlung in Facebook abgeglichen werden können. Facebook-Nutzer haben die Möglichkeit, in den Datenschutzeinstellungen ihres Profils anzugeben, dass sie nicht automatisch identifiziert werden möchten. Ungleich problematischer ist die Situation jedoch für diejenigen, die keine registrierten Nutzer von Facebook sind und vielleicht noch nicht einmal wissen, dass sie fotografiert werden. Das Geotagging baut auf der Gesichtserkennung auf und erreicht eine noch größere Eingriffstiefe in das allgemeine Persönlichkeitsrecht: Werden – z.B. über die Ortungsdaten des Handys – auch Zeit und Ort von Photographien gespeichert, so lassen sich – auch aus den im Sozialen Netzwerk von Nutzern hochgeladenen Bildern – Bewegungsprofile der fotografierten Personen erstellen.

Zudem erfassen viele Anbieter von Diensten das Nutzungsverhalten ihrer Kunden im Internet (zumeist ohne deren Wissen) zu Marketingzwecken, was als »Tracking« bezeichnet wird und aggregieren diese Daten zu umfassenden Verhaltens- und Bewegungsprofilen (»Data Mining«)[41]. Beim »Data Mining« geht es nicht nur um Daten, die die Person selbst betreffen, sondern auch um deren Relation zu anderen Personen, wobei zur Analyse der Datenmengen automatische und semiautomatische Werkzeuge zur Aufdeckung von Verhaltensmustern zum Einsatz kommen, und die so gewonnenen Informationen ebenso gesondert abgespeichert werden können wie Nutzerprofile selbst[42]. Diese Vorgehensweisen können einen schweren Eingriff in die Persönlichkeitsrechte des betroffenen Nutzers darstellen. Ähnliche Profile können entstehen, wenn Nutzer eines Sozialen Netzwerks auf den Seiten anderer Anbieter so genannte »Social Plugins« anklicken (z.B. der »Like Button« von Facebook) und so dem ihnen verbundenen Personenkreis im Netzwerk eine Empfehlung zusenden. Insbesondere bei Facebook werden die Daten der Mitglieder schon beim bloßen Aufrufen der fremden Website übertragen, ohne dass der »Like Button« gesondert angeklickt werden muss. Neben Rechtsverletzungen, die Anbieter Sozialer Netzwerke bzw. die Käufer der von denen angebotenen Daten begehen, sind des Weiteren »Rechtsverletzungen 2.0« durch andere Nutzer denkbar, wie etwa Urheberrechtsverletzungen[43], »ID-Klau«, rechtsverletzende Postings oder das Veröffentlichen so genannter »Partybilder«.

2.4 Das Niveau des Datenschutzes in Sozialen Netzwerken

Die Mehrheit der Nutzer Sozialer Netzwerke läuft Gefahr, die von einer Datensammlung und Datenrekombination ausgehenden Gefahren zu verkennen oder zu unterschät-

41 Vgl. Frank A. Koch, Schutz der Persönlichkeitsrechte im Internet: spezifische Gefährdungen, aaO. (FN 40), S. 158ff.

42 Vgl. Vgl. Indra Spiecker, »Kommunikation als Herausforderung« in: *Das Anwaltsblatt* Nr. 4 (2011), S. 258.

43 Siehe hierzu den Beitrag von Johannes Fritz im vorliegenden Band.

zen[44]. Die Orte, von denen aus Eingriffe in die informationelle Selbstbestimmung erfolgen können, lassen sich unter rechtlichen Gesichtspunkten folgendermaßen unterteilen: Deutschland, das europäische Ausland (EU und der Europäische Wirtschaftsraum (EWR)) und das außereuropäische Ausland. Die Datenschutzbestimmungen der Anbieter Sozialer Netzwerke unterscheiden sich sehr voneinander, abhängig davon, in welchem Land das Unternehmen gegründet worden ist und in welchen Ländern es hauptsächlich agiert. Von größtem Interesse für die Nutzer ist die Frage, welches Datenschutzniveau vom jeweils genutzten Anbieter gewahrt wird.

In der deutschen Rechtswissenschaft wird von einer weiten Anwendbarkeit des BDSG ausgegangen, da das BDSG auf dem Territorialprinzip beruht und ihm jede verantwortliche Stelle unterliegt, die personenbezogene Daten in Deutschland erhebt, verarbeitet oder nutzt[45]. In § 1 V BDSG wird – in Umsetzung der EG-Datenschutzrichtlinie (RL 95/46/ EG vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DS-RL)) – normiert, wann bei grenzüberschreitenden Sachverhalten innerhalb der EU oder des EWR das BDSG zur Anwendung gelangt. Darüber hinaus bestimmt § 1 V 2 BDSG, dass das BDSG Anwendung findet, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedsstaat der EU oder in einem anderen Vertragsstaat des Abkommens über den EWR belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt.

Für den grenzüberschreitenden Datenverkehr innerhalb von EU und EWR stellt Art. 4 Abs. 1 lit. a) DS-RL auf den Ort der Niederlassung des Verantwortlichen ab, und hebt damit das Territorialprinzip zugunsten des Niederlassungsprinzips auf. Von dieser Regelung sollen insbesondere Unternehmen profitieren, die sich noch nicht oder kaum im innereuropäischen Ausland engagiert und dort keine Niederlassung errichtet haben. Das Ziel sind die Förderung des grenzüberschreitenden Handels und des Binnenmarkts, da gemäß der Richtlinie Unternehmen zunächst auf der Grundlage des Datenschutzrechts ihres Heimatlandes agieren können[46].

Der Düsseldorfer Kreis, der Zusammenschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich[47], forderte in seinem Beschluss vom 08.12.2011: »Auch Betreiber, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, müssen sich deutschem Datenschutzrecht unterwerfen, wenn sie ihre Datenerhebung durch einen Rückgriff auf Rechner von Nutzern in Deutschland verwirklichen (§ 1 V 2 BDSG). Daher ist auch ein Inlandsvertreter als Ansprechperson für die Datenaufsicht zu bestellen (§ 1 V 3 BDSG). Eine Anwendung des BDSG kann nicht dadurch

44 Vgl. Indra Spieker, Kommunikation als Herausforderung, aaO. (FN 21), S. 257.

45 Vgl. Florian Jotzo, »Gilt deutsches Datenschutzrecht auch für Google, Facebook und Co. bei grenzüberschreitendem Datenverkehr?« in: *Multimedia und Recht* (2009), S. 233.

46 Vgl. Florian Jotzo, Gilt deutsches Datenschutzrecht auch für Google, Facebook und Co. bei grenzüberschreitendem Datenverkehr?, aaO. (FN 45), S. 235.

47 Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen (privaten) Bereich haben sich nach dem Ort ihres ersten Zusammentreffens im Jahr 1977 als »Düsseldorfer Kreis « benannt. http://mcaf.ee/3eswx (Stand 12/2011).

umgangen werden, dass eine rechtlich selbständige Niederlassung in einem anderen Staat des EWR gegründet wird.«[48]

Der Düsseldorfer Kreis fordert in seiner Erklärung zum Datenschutz in Sozialen Netzwerken unter anderem, dass:

1. Informationen darüber, welche Daten erhoben werden, und für welche Zwecke diese verarbeitet werden, leicht zugänglich und verständlich sein müssen.
2. Sämtliche Voreinstellungen auf dem Einwilligungsprinzip beruhen müssen, wenn nicht die Mitgliedschaft zwingend die Angabe solcher Daten voraussetzt. Insbesondere ist es nicht rechtmäßig zunächst mit der Datenverarbeitung zu beginnen und nur eine Widerspruchsmöglichkeit vorzusehen.
3. Ohne ausdrückliche und bestätigte Einwilligung des Abgebildeten es unzulässig ist, anhand von Fotos biometrische Gesichtserkennungsmerkmale zu erheben, zu speichern oder zu verwenden. Es ist zudem unzulässig Social-Plugins (z.B. den Like-Button von Facebook) auf Websites einzubinden, wenn dadurch eine Datenübertragung an den Anbieter des Sozialen Netzwerkes erfolgt und die Nutzer nicht bereits vorher bezüglich der Datenübertragung informiert wurden und ihnen eine Möglichkeit zur Unterbindung der Datenübertragung eingeräumt wurde. Nur wenn die Nutzer verlässliche Informationen über die übermittelten Daten und deren Zweck erhalten, können sie rechtswirksam ihre Einwilligung erklären. In der Regel werden Anbieter deutscher Websites nicht über die nötigen Kenntnisse bezüglich der Datenverarbeitungsvorgänge verfügen, um die Nutzer entsprechend zu informieren. Daher begehen die Anbieter der Websites selbst Rechtsverstöße, wenn sie Social-Plugins einbinden, die sie in Bezug auf die Datenverarbeitung nicht überblicken können.[49]

Die genannten Forderungen zeigen, dass aus deutscher Perspektive erheblicher Regelungs- und Handlungsbedarf besteht. Der Branchenriese Facebook stellt sich all dieser rechtlichen Vorgaben zum Trotz auf den Standpunkt, dass – da die Server für Facebook Europa in Irland stehen – soweit Facebook in Europa agiert, lediglich irisches Datenschutzrecht zur Anwendung kommen könne[50].

Volker Erb differenziert in seiner exemplarischen Untersuchung zur Anerkennung des Datenschutzrechts durch Soziale Netzwerke zwischen zwei Typen von Netzwerken: Solche, die wie Amazon, Ebay, StudiVZ, SchülerVZ und Xing das deutsche Datenschutzrecht exakt oder weitestgehend genau akzeptieren, und solchen, die das kaum bis überhaupt nicht tun: »Die Datenschutzignoranten heißen Google, die Tochter YouTube sowie die Unternehmen Facebook und Twitter.«[51]

48 Vgl. Blog zu Datenschutz und Datensicherheit der Kinast & Partner Rechtsanwälte, »Datenschutzticker.de«. http://mcaf.ee/z35wq (Stand 12/2011).

49 Obige Ausführungen sind dem Beschluss des Düsseldorfer Kreises zum Datenschutz in Sozialen Netzwerken vom 08.12.2011 entnommen, der unter folgendem Link im Original abrufbar ist: http://mcaf.ee/3eswx (Stand 12/2011).

50 Vgl. Blog zu Datenschutz und Datensicherheit der Kinast & Partner Rechtsanwälte, »Datenschutzticker.de«, aaO. (FN 48).

51 Volker Erb, Datenschutzrechtliche Probleme sozialer Netzwerke, aaO. (FN 19), S. 21.

Der jüngst erschienene Bericht des irischen Data Protection Commissioner Billy Hawkes[52], der über einen Zeitraum von drei Monaten die technischen Abläufe bei Facebook überprüft hat und insbesondere der Frage nachgegangen ist, ob das Netzwerk gegen die EU-Datenschutzrichtlinie und die irischen Datenschutzgesetze verstößt, gelangt zu einem salomonischen Urteil: Facebook würde zwar nicht unbedingt gegen geltendes Recht verstoßen, müsse aber an einigen Punkten deutlich nachbessern, wozu sich das Unternehmen jedoch bereits bereit erklärt habe[53]. Die Nachbesserungsliste des obersten irischen Datenschützers ist nahezu identisch mit den oben genannten Forderungen des Düsseldorfer Kreises. Deren Umsetzung wird im Juli 2012 vom Data Protection Commissioner überprüft werden. Bei Facebook wurde der Bericht begrüßt und eine Kooperation mit der zuständigen irischen Stelle zugesagt, wobei die Triebfeder des Handelns nicht in einer unlängst erwachten Sensibilität für datenschützerische Belange, sondern im für 2012 geplanten Börsengang des Unternehmens zu liegen scheint.

3. Die Grenzen des deutschen Gesetzgebers und des Bundesverfassungsgerichts

Obige Ausführungen machen eines deutlich: Im Bereich des Web 2.0 und in rechtlichen Fragen Sozialer Netzwerke stößt der deutsche Gesetzgeber recht rasch an die Grenzen seiner Regelungsbefugnis. In diesem Sinne äußerte sich auch der ehemalige Richter am Bundesverfassungsgericht und Berichterstatter im Medienrecht Wolfgang Hoffmann-Riem in einem Interview mit der Frankfurter Allgemeinen Zeitung: »Die Globalisierung der Kommunikation erhöht Risiken und erschwert Rechtsschutz, ja macht ihn vielfach unmöglich.«[54]

Der amtierende Präsident des Bundesverfassungsgerichts, Andreas Voßkuhle, warnte unlängst in einem Interview vor der Nutzung des Sozialen Netzwerks Facebook und bezeichnete das Surfen auf dessen Seiten als »risikogeneigte Tätigkeit«[55]. Voßkuhle beklagte, dass zwischen der Macht des Unternehmens Facebook, dessen Server außerhalb von Deutschland stehen, und der auf 16 Bundesländer zersplitterten Kontrolle der Datenschützer die »Gefahr einer Schieflage« bestünde und deutete an, dass das Bundesverfassungsgericht gezwungen sein könnte, zu prüfen, ob sich das Facebook-Angebot mit dem Recht auf informationelle Selbstbestimmung verträgt[56]. Mit dieser Äußerung bekräftigt er die Ansicht derer, die aus dem Recht auf informationelle Selbstbestimmung – in Anlehnung an die Lüth-Entscheidung[57] des Bundesverfassungsgerichts – neben der

52 Presseerklärung vom 21.12.2011, http://mcaf.ee/j1hag (Stand 12/2011).
53 Vgl. Kilian Haller,/ Johannes Kuhn, »Irlands Datenschützer zwingen Facebook zu Zugeständnissen« in *Sueddeutsche.de* (21.12.2011), http://mcaf.ee/vspq9 (Stand 12/2011).
54 Reinhard Müller im Gespräch mit Wolfgang Hoffmann-Riem, »Der Staat muss Risiken eines Missbrauchs durch Infiltrierung vorbeigen« in: *Frankfurter Allgemeine* (09.10.2011), http://mcaf.ee/5m6ao (Stand 12/2011).
55 Focus Online, »Voßkuhle warnt vor der Sammelwut von Facebook« (06.11.2011), http://mcaf.ee/evo8 m (Stand 12/2011).
56 Focus Online, Voßkuhle warnt vor der Sammelwut von Facebook, aaO. (FN 55).
57 BVerfGE 7, 198.

Grundrechtsgewährleistung auch eine Schutzpflicht des Staates für die informationelle Selbstbestimmung des Einzelnen gegenüber mächtigen Privaten ableitet[58].

Vor dem Hintergrund des häufigen Vorwurfs des Gesetzgebers an die Richter des Bundesverfassungsgerichts, sie würden – statt sich in richterlicher Selbstbeschränkung zu üben – mit ihrer Rechtsprechung die Rolle des Ersatzgesetzgebers an sich reißen, erstaunt folgende Aussage des letzten Bundesministers des Inneren, Thomas de Maiziére:

»Bei der Analyse des gesetzgeberischen Handlungsbedarfs ist auch zu beachten, dass die Gerichte durch die Auslegung und Fortbildung der bereits in Kraft befindlichen Regelungen schneller und flexibler auf neue Entwicklungen des Internets reagieren können als der Gesetzgeber. Dieser tut in vielen Fällen daher gut daran, sich in Zurückhaltung zu üben.«[59]

Offensichtlich spricht vieles für ein »starkes Mandat« der Karlsruher Richter, über Fragen des Datenschutzes in Sozialen Netzwerken zu entscheiden, sollte eine entsprechende und zulässige Klage das Bundesverfassungsgericht in den nächsten Jahre erreichen. In diesem Fall müsste sich der erste Senat mit zahlreichen offenen Fragen befassen: Wie soll damit umgegangen werden, dass der Bürger selbst seine Daten preisgibt und sich dadurch gefährdet? Wie stellt sich die rechtliche Einschätzung dar, wenn sich der Einzelne seiner Privatsphäre – wenn auch nur für einen beschränkten Teilnehmerkreis – entäußert, er dabei aber auch auf Fotos oder in Berichten die Privatsphäre Dritter preisgibt[60]?

Allen offenen Fragen zum Trotz mehren sich die Stimmen derer, die vor einer »Verrechtlichungsfalle[61]«, vor »chilling effects[62]« in Form einer überobligatorischen Selbstzensur und vor staatlicher Bevormundung[63] der Nutzer warnen.

Weltweit existieren heute in 75% aller Staaten keine spezifischen Regelungen zum Datenschutz, und bei den bestehenden Datenschutzgesetzen gibt es enorm große inhaltliche Unterschiede[64].

Der deutsche verfassungsändernde Gesetzgeber hat zum Thema Internet bislang geschwiegen, vielleicht aufgrund der Erkenntnis, dass die Informations- und Kommunikationsmöglichkeiten des Internets global sind, Staat, Recht und Verfassung demgegen-

58 Vgl. Martin Kutscha, »Grundrechtlicher Persönlichkeitsschutz bei der Nutzung des Internet. Zwischen individueller Selbstbestimmung und staatlicher Verantwortung« in: *Datenschutz und Datensicherheit* Nr. 7 (2011), S. 463 mit weiteren Nachweisen.

59 Thomas de Maiziére, »Das Internet als politische und gesellschaftliche Herausforderung« in: *Die Politische Meinung* Nr. 492 (2010), S. 6.

60 Vgl. Jochen Schneider, »Rechtsfragen von Social Networks. Einführung zur Beitragsreihe« in: *Der IT-Rechts-Berater* (2011), S. 10.

61 Vgl. Elke Gurlit, »Verfassungsrechtliche Fragen des Datenschutzes« in: *Neue Juristische Wochenschrift* (2010), S. 1141.

62 Stefan Alich,/ Georg Nolte, »Zur datenschutzrechtlichen Verantwortlichkeit (außereuropäischer) Hostprovider für Drittinhalte « in: *Computer und Recht* (2011), S. 741.

63 Thomas de Maiziére, Das Internet als politische und gesellschaftliche Herausforderung, aaO. (FN 59), S. 5.

64 Vgl. Ursula Widmer, »Die globale Informationsgesellschaft: Ist der Datenschutz noch zu retten?« in: *Das Anwaltsblatt* Nr. 4 (2011), S. 278.

über hingegen territorial begrenzt und damit regional[65]. Unter wirtschaftlichen Aspekten wird vor der Errichtung einer »Datenschutz-Festung Europa[66]« gewarnt, um nicht den essentiellen Informationsfluss zwischen den Kontinenten aufgrund für andere Länder unerfüllbarer datenschutzrechtlicher Vorgaben zum Erlahmen zu bringen. Die EU ist hier schon aktiv geworden und hat z.B. mit den Vereinigten Staaten von Amerika das »Safe Harbor« Abkommen geschlossen, das gewährleistet, dass personenbezogene Daten legal in die USA übermittelt werden können. Den »Ausgangspunkt für diese Vereinbarung bilden die Vorschriften der Art. 25 und 26 der Europäischen Datenschutzrichtlinie, nach denen ein Datentransfer in Drittstaaten verboten ist, die über kein dem EU-Recht vergleichbares Datenschutzniveau verfügen. Dies trifft auf die USA zu, da es dort keine umfassenden gesetzlichen Regelungen zum Datenschutz gibt, die dem europäischen Standard entsprechen.[67]«

In der aktuellen Debatte stehen sich zwei Lager gegenüber: Während die Befürworter einer regulatorischen Intervention auf eine gesetzgeberische Regulierung Sozialer Netzwerke hoffen, bauen die Befürworter staatlicher Zurückhaltung auf eine transparente Information der Nutzer[68] und auf »Binding Corporate Rules«[69], also verbindlichen Unternehmensregelungen zwischen Unternehmensgruppen.

Der deutsche Idee der Gründung einer »Stiftung Datenschutz«, die Produkte und Dienstleistungen auf ihre Datenschutzfreundlichkeit prüfen, Bildung im Bereich des Datenschutzes stärken, den Selbstdatenschutz durch Aufklärung verbessern und ein Datenschutzaudit entwickeln soll[70], verharrt bislang im Entwicklungsstadium.

Bei allen in der Diskussion befindlichen Lösungsansätzen gilt es eine zentrale Frage zu entscheiden und dabei eine grundsätzliche Wertung zu treffen: Ist die informationelle Selbstbestimmung in den Augen der Gesellschaft noch zeitgemäß und erstrebenswert, so dass eine Diskussion über »digitale Menschenrechte«[71] angestoßen werden sollte, oder will die Gesellschaft den Schritt in ein »Post Privacy Zeitalter« vollziehen?

65 Christoph Gusy,/ Christoph Worms, »Grundgesetz und Internet« in: *Aus Politik und Zeitgeschichte* Nr. 18-19 (2009), S. 26.

66 Vgl. Vgl. Ursula Widmer, Die globale Informationsgesellschaft: Ist der Datenschutz noch zu retten?, aaO. (FN 64), S. 280.

67 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, »Safe Harbor« in: *Internetpräsenz des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit*, http://mcaf.ee/83ntr (Stand 12/2011).

68 Vgl. Niko Härting, »Datenschutz zwischen Transparenz und Einwilligung. Datenschutzbestimmungen bei Facebook, Apple und Google « in: *Computer und Recht* (2011), S. 169.

69 Vgl. Sabine Grapentin, »Datenschutz und Globalisierung – Binding Corporate Rules als Lösung? « in: Computer und Recht « (2009), 693.

70 Vgl. Presseerklärung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit Nr. 6/2011 (08.02.2011), http://mcaf.ee/06z74 (Stand 12/2011).

71 Thilo Weichert, »Datenschutz und Meinungsfreiheit: Regulierung im BDSG. Grundrecht aus Art. 5 GG durch eine Anpassung des Bundesdatenschutzgesetzes verwirklichen« in: *Das Anwaltsblatt* Nr. 4 (2011), S. 255.

Zusammenfassung

In seiner 60-jährigen Bestehensgeschichte sah sich das Bundesverfassungsgericht zwei Mal dazu veranlasst, durch Auslegung und Interpretation der Verfassung ein neues Grundrecht zu statuieren. Sowohl das Recht auf informationelle Selbstbestimmung aus der Anfangszeit der elektronischen Datenverarbeitung im Jahre 1983 als auch das Recht auf den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme aus dem Jahre 2008 betreffen den Schutz persönlicher Daten vor staatlichem Zugriff.

Im Hinblick auf das Internet – und hier insbesondere das Web 2.0 – gibt es zwei Dilemmata: Zum einen gibt es für den Gesetzgeber kaum eine Möglichkeit, Internetnutzer davon abzuhalten, intime Details im Netz preiszugeben, ohne sich dem Vorwurf auszusetzen, paternalistisch zu sein und die Meinungsäußerungsfreiheit der Bürger zu beschneiden. Das andere Dilemma liegt in der Diskrepanz zwischen den globalen Informations- und Kommunikationsmöglichkeiten des Internets und der territorialen Begrenztheit von Staat, Recht und Verfassung.

Summary

In its 60-year existence the German Federal Constitutional Court has deemed it necessary on two occasions to set down a new fundamental right by interpreting the constitution. Both the right to informational self-determination and the right to the guarantee of the confidentiality and integrity of information technology systems concern the protection of personal data from governmental intervention.

With regard to the Web 2.0 there are two dilemmas: The first of these deals with the fact that it is extremely difficult for the legislator to prevent people from divulging personal details without restricting an individual's freedom of expression. The second is that the Internet operates on a global level whereas states, constitutions and law are territorially restricted.

Martina Schlögel, The FCC, informational self-determination and the Web 2.0. The Difficulty of Finding a Safe (Data) Harbour in the Wide Expanses of the Internet