Friedrich Naumann STIFTUNG FÜR DIE FREIHEIT

PositionLiberal 100

Das Internet zwischen Datenschutz und Informationsfreiheit

Gérard Bökenkamp

Liberales Institut

JEDER MENSCH BRAUCHT FREIHEIT, UM SEINE ANLAGEN UND FÄHIGKEITEN ENTFALTEN UND VERWIRKLICHEN ZU KÖNNEN. VERFALLEN KULTUR UND WISSENSCHAFTEN, STAGNIERT DIE WIRTSCHAFT. GEISTIGES LEBEN BRAUCHT FREIHEIT GENAUSO, WIE DER KÖRPER DIE LUFT ZUM ATMEN.

Wenn Sie unsere Arbeit unterstützen wollen:
Commerzbank Berlin
BLZ 100 400 00
Spendenkonto: 266 9661 04
Spendenbescheinigungen werden ausgestellt.

Impressum:

Herausgeber
Liberales Institut der
Friedrich-Naumann-Stiftung für die Freiheit
Karl-Marx-Straße 2
14482 Potsdam

Tel.: 03 31.70 19-2 10
Fax: 03 31.70 19-2 16
libinst@freiheit.org
www.freiheit.org

Produktion
COMDOK GmbH
Büro Berlin

1. Auflage 2011

DAS INTERNET ZWISCHEN DATENSCHUTZ UND INFORMATIONSFREIHEIT

Gérard Bökenkamp

Über den Autor:

Gérard Bökenkamp ist Historiker und Referent für Grundsatz und Forschung am Liberalen Institut der Friedrich-Naumann-Stiftung für die Freiheit. Seine Doktorarbeit erschien unter dem Titel „Das Ende des Wirtschaftswunders. Geschichte der Sozial-, Wirtschafts- und Finanzpolitik in der Bundesrepublik 1969-1998." Er war Chefredakteur einer Onlinezeitung und veröffentlichte zahlreiche Beiträge u. a. in der Frankfurter Allgemeinen Zeitung, Deutschlandradio und eigentümlich frei. Er wurde von den Lesern von Freiheit.org zum „Autor der Freiheit 2009" gewählt.

Inhalt

Einführung	5
Datenschutz und Informationsfreiheit	7
Der Staat und die Daten der Bürger: Vorratsdatenspeicherung und Online-Durchsuchung	10
Die Online-Dienstleister und die Daten der Nutzer	13
Die Google Street View-Kontroverse	17
Datenschutz, Internet und Pressefreiheit: Der Fall Wikileaks	20
Schlussfolgerung	21
Literatur	23

Einführung

Datenschutz und Informationsfreiheit gibt es als Gesetzesnormen schon länger als das Internet. Mit der Ausbreitung der Internetnutzung steht die Anwendung und Umsetzung der bestehenden Normen aber vor neuen Herausforderungen. Wie lassen sich die etablierten Kategorien auf das Internet übertragen? Die Informationen im Netz kennen keine territorialen Grenzen, sie kennen keine Begrenzung der Leserschaft, keine praktischen Grenzen der Vervielfältigung, keine materiellen Grenzen der Datenfülle. Alle Empfehlungen bezüglich der gesetzlichen Regelungen des Umgangs mit Daten im Internet stehen deshalb unter einem Vorbehalt – dem der praktischen Umsetzbarkeit. Es gibt keine Garantie dafür, dass das, was als Regelung nachvollziehbar und notwendig erscheint, am Ende mehr sein wird als Papier ohne praktische Relevanz. Untersuchen kann man aber, was man für erstrebenswert erachtet und, auch wenn die Umsetzung im Einzelfall schwierig sein kann, als Richtlinie wünschbar ist.

Datenschutz und Informationsfreiheit können als Prinzipien durchaus in einem Zielkonflikt zueinander stehen. Folgt man dem Gebot der Informationsfreiheit, geht es darum, möglichst allen möglichst viele Informationen zugänglich zu machen. Ohne das Prinzip der Informationsfreiheit würden wir in einer Welt der Unwissenheit leben. Informationsfreiheit ist eine Grundlage für wissenschaftlichen, technischen, politischen, wirtschaftlichen und sozialen Fortschritt. Informationsbeschaffung ist ein Teil der globalen Arbeitsteilung. Bei Naturvölkern ist der Schatz des Wissens, über den jeder Einzelne verfügt, sehr ähnlich dem Wissensschatz seiner Stammesgenossen. Das Prinzip der Arbeitsteilung ermöglichte eine Informationsrevolution. Menschen spezialisieren sich auf unterschiedliche Bereiche der Informationssammlung, -Verarbeitung und -Weitergabe. Ein Zoologe sammelt zum Beispiel Informationen über bestimmte Tierarten und macht diese Informationen durch Fachveröffentlichungen seinen Fachkollegen zugänglich. Seine Fachkollegen fassen diese und andere Informationen in wissenschaftlichen Standardwerken zusammen. Publizisten veröffentlichen die Ergebnisse in populärwissenschaftlichen Sachbüchern. Journalisten schreiben darüber Artikel in Tages- und Wochenzeitungen und produzieren Dokumentationen. So erreicht die Information, die von einem Spezialisten gefunden wurde, schließlich breitere Schichten der Bevölkerung. So wird die Information Allgemeingut und findet Aufnahme in Schulbüchern und in den Standardwerken. Der Stand des allgemeinen Wissens ist umso größer, je schneller und unkomplizierter sich Informationen verbreiten können. Das Internet hat diesen Prozess extrem beschleunigt. Noch nie in der Kommunikationsgeschichte war der Zugriff auf Datenbanken, Meinungen, Stel-

lungnahmen, Filme, Bücher, Bilder usw. so unkompliziert und so preiswert wie heute. Man kann ohne zu übertreiben sagen, das Internet ist das Medium der Informationsfreiheit schlechthin. Die transportierten Datenfluten sind schier unendlich groß und für fast jeden weltweit zugänglich. Das Internet überwindet die Zensur und macht Informationskontrolle zu einem extrem schwierigen Unterfangen, wie erst vor kurzem die Veröffentlichung von Berichten des US-Außenministeriums auf Wikileaks zeigte. Einmal im Netz, sind Informationen kaum wieder einzufangen. Doch Informationen unterliegen auch legalen und legitimen Restriktionen. Nicht alles, was allgemein gewusst werden kann, ist auch für die Öffentlichkeit bestimmt.

Der Datenschutz ist als rechtliches Instrument zur Erhaltung der informationellen Selbstbestimmung geschaffen worden. Datenschützer sehen neben den Chancen des Internet die möglichen Schattenseiten, das Ende der Privatsphäre und eben dieser vom Gesetzgeber geschützten informationellen Selbstbestimmung. Der zentrale Wert, den der Datenschutz verteidigen soll, ein Wert, den gerade Liberale stets hochgehalten haben, ist der Wert der Privatheit. Die Privatheit ist ein unmittelbarer Bestandteil der sozialen Existenz des Menschen. Das hat Wolfgang Sofsky in seinem Buch „Verteidigung des Privaten" unübertroffen auf den Punkt gebracht. Dort schreibt er: „Privatheit ist die Zitadelle der persönlichen Freiheit. Sie bewahrt vor Enteignung und Entmündigung, vor Aufdringlichkeit und Bevormundung, vor Macht und Zwang. Die Festung sichert die Selbständigkeit und Selbstbestimmung. Unerbetene Eingriffe prallen an ihren Bastionen ab. Der Zugang zu persönlichen Daten ist ebenso versperrt wie der Zugriff zu den Räumen der Intimität."[1]

Diese Intimität sehen viele durch die Preisgabe von Daten im Internet in Gefahr und fürchten den gläsernen Menschen. Im Folgenden wird versucht, in Bezug auf das Internet zu beschreiben, wo der Wirkungsbereich des Datenschutzes beginnt und wo er enden sollte. Es soll nach den Prinzipien gesucht werden, nach denen die Speicherung und Weitergabe als legitim zu beurteilen oder zu verwerfen ist. Im ersten Abschnitt werden die Ursprünge und die rechtliche Ausgestaltung des Datenschutzes und der Informationsfreiheit beschrieben. Im zweiten Teil wird anhand des Urteils des Bundesverfassungsgerichts zur Vorratsdatenspeicherung gezeigt, in welchem Maß der Staat die informationelle Selbstbestimmung einschränken darf und in seinem Eifer Daten zu sammeln rechtlich eingeschränkt wird. Im dritten Teil werden die Regeln beschrieben, unter denen private Online-Anbieter mit ihren Kunden agieren und dabei Daten austauschen. Im vierten Teil wird der Sonderfall Google Streetview behan-

1 Wolfgang Sofsky: Verteidigung des Privaten. Eine Streitschrift, München 2007, S. 37.

delt, der im Sommer 2010 zu einer Datenschutz-Kontroverse geführt hat, und anschließend der Fall Wikileaks. Abschließend werden dann die Schlussfolgerungen aus der Behandlung dieser Themen zusammengefasst.

Datenschutz und Informationsfreiheit

Am Beginn der Auseinandersetzung über Privatheit und Datenschutz in den USA stand die Diskussion um eine Nationale Datenbank. Nach dem Vorschlag eines Komitees unter dem Vorsitz von R. Ruggles sollten in dieser alle verfügbaren Daten über die Bürger der USA erfasst werden, um den Statistikern und Budgetplanern einen umfassenden Datenschatz zur Verfügung zu stellen, um ihre Arbeit zu optimieren. Diese Vorschläge entsprachen dem Zeitgeist des Kalten Krieges und der keynesianische Wirtschaftspolitik. Um die ökonomische und soziale Entwicklung „planen" zu können und über alle möglichen Aspekte der nationalen Sicherheit informiert zu sein, schien die Administration einen möglichst umfassenden Datenschatz zu benötigen. Schon damals kristallisierte sich heraus, dass staatliche Planung und der Anspruch auf persönliche Privatheit nur schwer miteinander in Einklang zu bringen sind. Diese Vorschläge standen im scharfen Kontrast zum „Recht, in Ruhe gelassen zu werden" („right to be let alone"), das dem amerikanischen Verständnis von Privatheit entspringt, und wurden in der Presse scharf kritisiert. Es wurde die Befürchtung laut, dass durch die Verknüpfung der Daten Personenprofile und individuelle Dossiers erstellt werden könnten. Die Befürworter der Nationalen Datenbank konnten sich schließlich nicht durchsetzen. Der Forderung nach Schutz der Privatsphäre versuchte der Gesetzgeber im Jahr 1974 mit der Verabschiedung des Privacy Act gerecht zu werden. Dieses untersagte staatlichen Bundesbehörden eine Zweckentfremdung von gespeicherten, personenbezogenen Daten, schrieb Benachrichtigungs-, Auskunfts- und Berichtigungsansprüche des Bürgers gegenüber den Behörden und ein Schadensersatzrecht fest. In den Jahren nach der Erlassung des Privacy Act trat die andere Seite der Medaille stärker in das Zentrum der öffentlichen Diskussion. Nach der Verabschiedung des verbesserten Schutzes der Privatsphäre wurde nun die Forderung nach Information und Transparenz der Regierung lauter. Dieses „Recht auf Information" betrifft die „Aktenöffentlichkeit" und die „Öffentlichkeit der Verwaltung." Dieses war erstmalig bereits 1966 im Freedom of Information Act festgeschrieben worden. Nach der spektakulären Watergate-Affäre wurde dieses noch weiter ausgebaut mit dem Ziel, eine umfassende Öffentlichkeit der Verwaltung zu schaffen. Watergate hatte das Vertrauen in die Regierung massiv erschüttert und das

Verhältnis von Bürgern zu ihrer Administration grundlegend verändert. Das Misstrauen gegen Geheimhaltung und verborgenes Regierungshandeln spielten von jetzt an eine größere Rolle als zu den Hochzeiten der „imperialen Präsidentschaft" (Schlesinger). Neben dem Zugang zu Informationen über Akten und Dokumente traten Computer und Internet stärker in den Fokus der informierten Öffentlichkeit. Im Jahre 1988 wurde der Computer Matching Act und im Jahr 1996 der Electronic Freedom of Information Act erlassen. Durch diese Gesetzgebung wurde der Allgemeinheit ein Online-Zugang zu den Informationen der amerikanischen Bundesbehörden garantiert. Vorbehaltlich begründeter Ausnahmen besitzt jeder Bürger Zugang zu den Akten der Verwaltung. Im Zusammenhang mit der Informationsfreiheit entstand das Konzept eines „free flow of information", eines offenen Marktes von Informationen, der über das Internet allen frei zugänglich sein sollte.[2]

Das Bundesverfassungsgericht hat 1983 im Urteil über die Volkszählung ein Recht auf informationelle Selbstbestimmung aus dem Persönlichkeitsrecht abgeleitet. Das heißt, dass der Einzelne grundsätzlich selbst über die Verwendung seiner persönlichen Daten bestimmen kann. Insoweit steht die informationelle Selbstbestimmung rechtlich im Bezug zur im Grundgesetz verankerten Würde des Menschen. Konkret bedeutet dies unter anderem, dass der Staat keine Datensammlungen ohne zuvor genau festgelegten Zweck erstellen darf und dass dem Staat daraus Informationspflichten über bereits erhobene Daten erwachsen. Der Begriff der personenbezogenen Daten geht von lebenden Personen aus, kann aber im Einzelfall auch Verstorbene betreffen. Es handelt sich dabei um Einzelangaben über persönliche Verhältnisse. Aggregierte Angaben etwa über die politische Einstellung bestimmter Personengruppen in Prozent sind hingegen keine personenbezogenen Daten. Daten gelten nur dann als personenbezogene Daten wenn sie klar einer Person zugeordnet werden können. Aus den Informationen muss sich die eindeutige Identität der Person bestimmen lassen. Beispiele für solche Informationen sind Kennnummern, Sozialversicherungsnummern, markierte Bild- und Tondaten, usw. Die Person muss dabei nicht zwangsläufig bestimmt sein, es genügt, wenn sie bestimmbar ist, etwa wenn durch eine breite und systematische Auswertung von Daten diese zu einer bestimmten Person führen oder wenn durch allgemein zugängliche Quellen wie etwa ein Telefonbuch ein Zusammenhang zwischen einer Information, in diesem Fall einer Telefonnummer, und einer Person hergestellt werden kann. Es kann also von den übrigen einer Behörde zur Verfügung stehenden Informationsquellen abhängen, ob eine bestimmte Information in diesem Kontext

2 M. Tinnefeld, E. Ehmann, R. Gerling: Einführung in das Datenschutzrecht, München 2005, S. 79 ff.

als personenbezogen gelten muss oder nicht. „Die Begriffe der Bestimmbarkeit und des Personenbezugs sind folglich relativ."[3] Bestimmbar ist eine Person dann, „wenn die betreffende Einzelangabe, sei es unter Zuhilfenahme informationstechnischer oder mathematisch-statistischer Analyseprogramme, sei es unter Berücksichtigung des Zusatzwissens der verantwortlichen Stelle, zur Identifikation des Betroffenen führt."[4] Das Recht auf informationelle Selbstbestimmung gilt aber nicht absolut, sondern muss dem Grundsatz der Verhältnismäßigkeit folgen. „Die grundsätzliche Befugnis des Einzelnen, selbst über seine Daten zu bestimmen, kann nicht im Sinne des Rechts einer absoluten, uneingeschränkten Herrschaft Einzelner über die eigenen Daten interpretiert werden. Die autonome und nicht die bedingungslose Person bestimmt das Menschenbild der Verfassung."[5]

Die Tendenz, den Datenschutz exzessiv auszulegen, nährte auf liberaler Seite Befürchtungen, aus dem Abwehrrecht gegenüber dem Staat könnte sich eine Rechtfertigung für Eingriffe in die persönliche Freiheit entwickeln. Christian Hoffmann kritisierte, dass „das derzeitige Datenschutzrecht das Abwehrrecht des Bürgers gegenüber dem Staat kurzerhand auf Privatrechtsebene übertragen hat, dass also auch nicht-öffentliche Stellen dem Datenschutzrecht unterstellt wurden." Dies impliziere fälschlicherweise, dass private Institutionen die Abgabe von Daten erzwingen könnten. Dem liege ein „marxistisches" Verständnis von der „Macht" von Unternehmen zugrunde. Hoffmann betont hingegen, dass der Schutz der eigenen Privatsphäre grundsätzlich in der Eigenverantwortung des Einzelnen liegt. Bei jeder Interaktion müsse das Individuum selbst den möglichen Verlust von Vertraulichkeit in seine Erwägungen mit einbeziehen. Hoffmann verweist darauf, dass die Achtung der Privatsphäre selbst zu einem Wettbewerbsvorteil für private Unternehmen werden könnte und die Möglichkeit besteht, das Verbot der Weitergabe persönlicher Daten in privaten Verträgen fest zu verankern, weshalb nicht zwangsläufig eine staatliche Norm notwendig sei. Der Einzelne dürfe nicht zur Abgabe von Daten und Informationen über sich selbst gezwungen werden. Er könne jedoch im Rahmen von Geschäftsverträgen freiwillig diese Daten weitergeben. Die Preisgabe privater Daten ist die Grundvoraussetzung für die erfolgreiche Abwicklung vieler Geschäftsbeziehungen. „Das Individuum muss also den Nutzen des Vertrages mit dem Verlust der alleinigen Verfügung über die eigenen Daten abwägen."[6]

---

3 Jürgen Kühling, Christian Seidel, Anastasios Sivridis: Datenschutzrecht, Frankfurt a. M. 2008, S. 103.

4 Dies., S. 104.

5 M. Tinnefeld, E. Ehmann, R. Gerling: Datenschutzrecht, S. 147.

6 ef-magazin, November 2005, Nr. 57: Der Irrtum der „Bürgerrechtsliberalen". Warum der gesetzliche Schutz der Daten scheitern muss.

Diese Abwägung kann und darf der Staat dem Einzelnen nicht abnehmen. Die Aufgabe des Staates besteht darin, Vertragsfreiheit und Vertragssicherheit zu garantieren und Transparenz sicherzustellen. Die Weitergabe von Daten ist legitim, wenn der Nutzer dieser Weitergabe zugestimmt hat, sie ist nicht akzeptabel, wenn der Nutzer nach Zurkenntnisnahme der Allgemeinen Nutzungsbedingungen von der Wahrung seiner privaten Daten ausgehen konnte. Wenn Nutzer freiwillig ihre Daten zur Verfügung stellen, dann ist gegen die Verwendung dieser Daten durch den Anbieter nichts einzuwenden. Die Abgabe von Daten ist nicht an sich schlecht, sondern, wie in dieser Abhandlung gezeigt werden wird (Abschnitt 5.), die Grundlage für durchaus innovative Geschäftsmodelle. Problematisch ist lediglich, wenn sich eine Vertragspartei an die entsprechende Vereinbarung nicht hält oder den Vertragspartner in Unkenntnis über die Verwendung der Daten lässt.

Bevor wir zu diesem Themenfeld kommen, betrachten wir zu erst die klassische Form des Datenschutzes als Abwehrrecht gegenüber dem Staat anhand der rechtlichen Auseinandersetzung über die Vorratsdatenspeicherung.

Der Staat und die Daten der Bürger: Vorratsdatenspeicherung und Online-Durchsuchung

Noch 1997 hatte die Bundesregierung die vorsorgliche Speicherung von Daten zum Zweck der Strafverfolgung und der Gefahrenabwehr als mit der Verfassung nicht vereinbar abgelehnt. Nach dem 11. September änderte sich jedoch die politische Großwetterlage. Sowohl das Europäische Parlament als auch der Deutsche Bundestag stimmten einer Richtlinie der EU zur Einführung einer Speicherfrist für Telekommunikations- und Internetdaten zu. Nachdem der Bundestag im Februar 2006 die Richtlinie verabschiedet hatte, suchten die Kritiker der Regelung eine grundsätzliche Klärung beim Bundesverfassungsgericht zu erreichen.[7] Die Beschwerden, über die das BVerfG zu befinden hatte, richteten sich gegen die im Telekommunikationsgesetz festgelegte Verpflichtung, dass die Verkehrsdaten von Telefondiensten, E-Mail-Diensten und Internetdiensten vorsorglich ohne konkreten Anlass gespeichert werden müssen. Die Speicherungspflicht sollte es möglich machen, zu rekonstruieren, wer wie lange mit wem kommuniziert hat. Dies betraf jedoch nicht den Inhalt der Kommunika-

7 Peter Schaar: Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft, München 2007, 117 ff.

tion. Die Speicherungsfrist beträgt sechs Monate. Die Beschwerden richteten sich außerdem gegen den Auskunftsanspruch gegenüber den Anbietern der Dienste zur Ermittlung von IP-Adressen. Dieser Auskunftsanspruch soll es den Behörden ermöglichen, eine bekannte IP-Adresse einem Nutzer oder einer Adresse zuzuordnen. Die Beschwerdeführer sahen durch diese Regelungen das Telekommunikationsgeheimnis und das Recht auf informationelle Selbstbestimmung verletzt.

Das Bundesverfassungsgericht entschied, dass eine Speicherungspflicht selbst im vorgesehenen Umfang nicht von vornherein verfassungswidrig ist, sehr wohl aber die rechtliche Ausgestaltung der Datenspeicherung. Die bisherige Ausgestaltung widerspreche dem Grundsatz der Verhältnismäßigkeit, gewährleiste keine hinreichende Datensicherheit und keine hinreichende Begrenzung des Verwendungszweckes. Das Gericht räumt ein, es handele sich bei der vorgesehenen Vorratsdatenspeicherung um einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt. Auch wenn sich die Speicherung nicht auf die Kommunikationsinhalte erstreckt, lassen sich aus diesen Daten bis in die Intimsphäre hineinreichende Rückschlüsse ziehen." Dies mache die Erstellung von aussagekräftigen Persönlichkeitsprofilen für praktisch jeden Bürger möglich.

Damit eine solche Maßnahme dennoch als verfassungskonform eingestuft werden kann, dürfe die Speicherung der Telekommunikationsdaten nicht direkt durch den Staat, sondern müsse durch die privaten Anbieter der Telekommunikationsdienste erfolgen, sodass die Daten nicht schon bei der Speicherung zusammengeführt werden, sondern verteilt auf einzelne Unternehmen bleiben. Auf diese Weise stehen sie dem Staat nicht unmittelbar in ihrer Gesamtheit zur Verfügung.

Unter diesen Umständen dürfen die Daten zur Strafverfolgung und Gefahrenabwehr verwendet werden, solange der Rückgriff auf die Daten die Ausnahme bleibe. Das Verfassungsgericht erklärt, dass die Einführung der Vorratsdatenspeicherung weiteren Maßnahmen zur Datenerfassung Grenzen setzt: „Durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer." Das Bundesverfassungsgericht macht zur Nutzung der gespeicherten Daten den „durch bestimmte Tatsachen begründeten Verdacht einer auch im Einzelfall schwerwiegenden Straftat" zur Voraussetzung sowie die hinreichend belegte „konkrete Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes", damit die Verhältnismäßigkeit gewahrt bleibt. Nicht zugegriffen

werden soll auf die Verbindungsdaten von Personengruppen, die Verschwiegenheitsverpflichtungen unterliegen.

Der Auswertung der Daten ohne das Wissen der Betroffenen zieht das Bundesverfassungsgericht enge Grenzen. Das Bundesverfassungsgericht legt fest: Eine Verwendung der Daten ohne Wissen des Betroffenen ist verfassungsrechtlich nur dann zulässig, wenn andernfalls der Zweck der Untersuchung, dem der Datenabruf dient, vereitelt wird." Die heimliche Verwendung der Daten dürfe nur vorgenommen werden, wenn sie im Einzelfall erforderlich und richterlich angeordnet ist. Allerdings muss die Benachrichtigung dann wenigstens nachträglich erfolgen. Die Hürden, die das Bundesverfassungsgericht festgelegt hat, sind für Auskünfte über die Identität von bereits bekannten IP-Adressen weit weniger hoch gesetzt. Schon „gewichtige Ordnungswidrigkeiten" genügen als Rechtfertigung. Dabei dürfen die Behörden selbst keine vorsorglich gespeicherten Daten abrufen, sondern erhalten von den Dienstanbietern lediglich personenbezogene Auskünfte über den Inhaber eines bestimmten Anschlusses. Ein begründbarer Anfangsverdacht reicht für die Einholung dieser Information aus. Die Zustimmung eines Richters ist nicht notwendig.[8]

Die Grenzen, die das Bundesverfassungsgericht aufzeigte, machen deutlich, dass es sich bei dem Datenschutz gegenüber dem Staat im Wesentlichen um ein Abwehrrecht handelt. Es geht um Daten, die nicht den Staat selbst als Adressaten hatten, sondern zwischen verschiedenen nicht-staatlichen Akteuren ausgetauscht wurden. Der Staat erscheint hier in der Rolle des ungebetenen Dritten. Die Datenspeicherung ergibt sich in diesem Fall nicht direkt aus der Notwendigkeit der Kommunikation selbst, sondern allein aus den Interessen des Staates, dessen Zielsetzung und Methoden durch die Verfassung Grenzen gezogen werden. Anders verhält es sich mit dem Datenaustausch zwischen zwei Kommunikationspartnern, die aufgrund freiwillig gewählter Vereinbarungen Daten austauschen und verwenden. Diese Fälle behandelt der folgende Abschnitt.

8 Presseerklärung des Bundesverfassungsgerichtes zur Vorratsdatenspeicherung: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.html

Die Online-Dienstleister und die Daten der Nutzer

Einerseits scheinen im Internet viele Dienstleistungen umsonst angeboten zu werden: Wir können kommunizieren, recherchieren, die Welt aus der Ferne und von Nahem betrachten, Bilder und Filme sehen und alles, ohne einen Cent zu bezahlen. Andererseits erscheinen uns die großen Wohltäter – die Anbieter, die das über ihre Portale möglich machen – auch als Datenkraken, die sich illegitimerweise unsere persönlichen Daten aneignen. Datenschützer schlagen Alarm und möchten diesen „Datensumpf" am liebsten trockenlegen. Weil sie eben noch als Wohltäter galten, die ihr Angebot scheinbar umsonst zur Verfügung stellen, scheint die Enttäuschung über ihre „dunkle Seite" besonders groß. Online-Unternehmen sind aber weder Wohltäter, noch bösartige Datenkraken. Sie sind Unternehmen, die für ihre Leistungen eine Bezahlung erwarten, ganz so wie Unternehmen außerhalb des globalen Netzes auch. Beide Eindrücke, der vom Wohltäter und der von der Datenkrake, gehen gleichermaßen an der Sache vorbei und drängen sich auf, weil die Phänomene in der Regel nicht als Einheit betrachtet werden. Bezieht man beides aufeinander, den Umstand, dass diese Unternehmen scheinbar kostenlose Dienstleistungen anbieten und gleichzeitig unbedingt die möglichst vollständige Verwertung unserer Daten wollen, dann löst sich der Widerspruch in Luft auf. Die Online-Dienste sind nicht umsonst, und wir werden auch nicht um unsere Daten betrogen. Daten sind vielmehr eine Währung, mit denen die Online-Dienste bezahlt werden. So wie wir bei unserem Friseur, unserer Tankstelle oder unserem Steuerberater mit Euros bezahlen, so bezahlen wir im Internet mit Daten. Daten stellen im Netz eine Art privater Parallelwährung dar, und wir sind die Emittenten. Die Online-Unternehmen bieten also einen Tausch an, sie stellen ihren Kunden Dienstleistungen und Informationen zum großen Teil unentgeltlich (aber eben nicht kostenlos) oder zu einem ermäßigten (Geld-) Preis zur Verfügung und erhalten ihre „Bezahlung" in Form expliziter oder impliziter Zustimmung zur Verwertung der personenbezogenen Daten. Ein solcher Tausch ist aus liberaler Perspektive unproblematisch – soweit dieses Bezahlsystem transparent gemacht wird und den Regeln der Vertragsfreiheit entspricht. Ein wichtiger Schritt in Richtung Transparenz ist, wenn sich das Bewusstsein dafür durchsetzt, dass es sich um einen Tauschvorgang mit Leistung und Gegenleistung handelt.

Ein Tausch in einem freien Marktsystem muss nicht zwangsläufig in Geld abgewickelt werden, sondern dieser kann auch in der Abtretung von Verfügungsmöglichkeiten bestehen. Ob man eine Dienstleistung mit Papiergeld bezahlt oder mit Gold, Muscheln, Zigaretten, anderen Dienstleistungen, Nutzungsrechten an Grundstücken oder eben mit Daten, das ist für die Beurteilung der Legitimität

des Tauschvorganges als solchen nicht relevant. Entscheidend ist, dass beide Parteien freiwillig und nicht unter Zwang handeln. Solange also niemand mit einer geladenen Pistole hinter dem Nutzer steht und diesen dazu zwingt, eine bestimmte Suchmaschine zu verwenden oder sich in einem sozialen Netzwerk anzumelden, können die privaten Anbieter ihre Nutzungsbedingungen ausgestalten, wie sie es für richtig halten und für ihr Geschäftsmodell als förderlich erachten.

Aus der Perspektive der Geldtheorie ist dieser täglich zigmal durchgeführte Tausch von Daten für Dienstleistungen ein sehr interessanter Vorgang. Ludwig von Mises hat das sogenannte Regressionstheorem aufgestellt. Danach ist Geld aus einem Sachgut mit einem Gebrauchswert entstanden. Daten sind ein Sachgut. Für viele Firmen ist es von großem Vorteil, über Daten von potenziellen Kunden zu verfügen. Der Datenhandel wurde schon betrieben, lange bevor es das Internet gab. Im Internet ist dieses Sachgut entsprechend der Annahmen von Ludwig von Mises zu Geld geworden. Man kann mit Daten Dienstleistungen bezahlen, ganz unabhängig davon, ob in diesem konkreten Fall die Information für den Dienstanbieter selbst einen Mehrwert darstellt oder nicht. Durch den Aufbau eines Datenpools, die Handelbarkeit von Daten und dadurch, dass die Online-Anbieter aus diesem Grund die Daten als Zahlungsmittel akzeptieren oder sogar bevorzugen, werden die Daten zu Geld.

Es handelt sich also um eine evolutionär entstandene Form von Privatwährung. Eine Währung umfasst eine Tauschfunktion und eine Wertaufbewahrungsfunktion. Durch die Hingabe von Daten tauscht der Kunde seine Informationen gegen bestimmte Services, Informations- und Kommunikationsdienstleistungen. Die Informationen werden vom Anbieter gespeichert und können zu einem späteren Zeitpunkt abgerufen werden. Dies bezeichnet eine Wertaufbewahrungsfunktion. Allerdings können Informationen veralten und damit ihren Wert verlieren, so wie auch andere Sachgüter, die im Laufe der Geschichte zum Tausch verwendet wurden, verdarben oder wie auch das Papiergeld, das durch Inflation mit der Zeit an Wert verliert. Daten sind also als Zahlungsmittel geeignet, zur Wertaufbewahrung aber nur begrenzt tauglich. Wer über einen entsprechend großen Datenpool verfügt, kann sich jedoch als ebenso reich ansehen wie derjenige, der Aktien, Anleihen oder Goldmünzen sein eigen nennt.

Marktpreise spiegeln Informationen über die Präferenzen von Millionen von Marktteilnehmern wider. Dies gilt für den Preis, der sich in offiziellem Geld ausdrückt, ebenso wie für den Preis, der sich in der Forderung nach anderen Gütern wie etwa Daten ausdrückt, die diese Tauschfunktion partiell übernehmen. Dass viele Serviceangebote im Internet mit Informationen statt mit Geld

bezahlt werden, spiegelt die Präferenzen von Millionen Kunden wider. Sie bevorzugen für viele Transaktionen, wie zum Beispiel die Nutzung einer Suchmaschine, eine Bezahlung mit ihren Daten gegenüber der Bezahlung mit Geld. Wäre dies nicht so, dann hätten sich am Markt schlicht andere auf direkten Zahlungen beruhende Geschäftsmodelle durchgesetzt. Bezahlt werden müssen die Angebote so oder so auf die eine oder die andere Weise – wenn man sie denn nutzen will.

Gerade weil es sich bei den Internetanbietern um gewinnorientierte Unternehmen handelt, kann man davon ausgehen, dass es ihnen letztlich egal ist, ob sie ihre Gewinne durch ein Online-Bezahlsystem oder durch das Versilbern von Informationen machen. Ein Internet auf der Basis von Geldzahlungen als Alternative zur Datenzahlung wäre unschwer vorstellbar. Die Bezahlsysteme wären noch besser ausgebaut, und für den Zugang zu qualitativ hochwertigen Suchmaschinen oder zu sozialen Netzwerken müsste man wahrscheinlich eine Gebühr in Form von Geld entrichten. Diese Gebühr wäre äquivalent zu dem Tauschwert, den heute die Daten besitzen, die man in diesen Netzwerken hinterlässt und die von den Anbietern verwertet werden können.

Dass sie sich dafür entschieden haben, ihr Geschäftsmodell auf Informationshandel statt auf Gebühren aufzubauen, spricht dafür, dass die Kunden ihre Dienstleistungen lieber mit Informationen als mit dem offiziellen Zahlungsmittel entgelten. Es ist offensichtlich, dass die persönlichen Präferenzen zum Schutz der eigenen Daten beim Durchschnittsbürger geringer ausgeprägt sind als bei den Datenschützern, die damit professionell befasst sind und vor allen anderen daran interessiert sind, das Thema in die Öffentlichkeit zu bringen. Die große Mehrheit tauscht lieber eine Information über das besondere Interesse des Kunden an Bionahrung oder Autozubehör für den gewünschten Service ein, als das entsprechende Angebot äquivalent dazu mit Geld zu bezahlen.

Der Vorwurf gegen das Profitstreben der großen Online-Firmen ist nicht weniger unangebracht als in anderen ökonomischen Zusammenhängen, in denen sich private Unternehmen bewegen, auch. Man kann von dem Anbieter einer Suchmaschine oder eines sozialen Netzwerkes genauso wenig erwarten, dass er seine Dienstleistung ohne Gegenleistung zur Verfügung stellt, wie man vom Besitzer einer Imbissbude erwarten kann, dass er aus lauter Freundlichkeit jeden Tag zum Hotdog-Essen einlädt. Worin diese Gegenleistung besteht, kann der Anbieter selbst festlegen. Am Nutzer liegt es dann zu entscheiden, ob er auf dieses Angebot eingehen will oder nicht. Wenn einem das Geschäftsmodell nicht zusagt, dann muss man sich eben etwas anderes suchen. Denn Leistungen müssen bezahlt werden, in welcher Form auch immer. Die Programmierer,

Webdesigner, Entwickler, Buchhalter und Aktionäre der Online-Unternehmen können (und wollen) ihre Arbeit und ihr investiertes Kapital nicht zum Nulltarif anbieten. Die Internetgiganten und die Legionen anderer Online-Dienste sind keine Wohlfahrtsorganisationen, sondern betriebswirtschaftlich rechnende Unternehmen. Ihre Leistung muss der Kunde in irgendeiner Form bezahlen, sonst werden sie nicht mehr angeboten.

Wer Google, Facebook, Amazon und Co. nutzt, der demonstriert damit, dass diese Dienstleistung einen gewissen Wert für ihn hat, sonst würde er sie nicht in Anspruch nehmen und Zeit in ihre Nutzung investieren. Niemand ist gezwungen, auf die Dienste einer Suchmaschine, eines sozialen Netzwerkes oder einen Bestellservice zurückzugreifen. Wer Informationen braucht, kann auch Zeitung lesen oder in die Bibliothek oder ins Archiv fahren. Wer mit Freunden in Kontakt bleiben will, der kann telefonieren und Briefe schreiben. Wer Bücher oder andere Gegenstände erwerben will, der braucht nur in das nächste Einkaufscenter gehen und kann sich dort nach Belieben eindecken. Das Argument, dass das natürlich viel zeitaufwendiger und arbeitsaufwendiger ist, als kurz einmal online zu gehen, ist kein Argument dagegen.

Würden sich morgen alle Staaten der Welt zusammenschließen und die bisherige Nutzung der Daten durch die Online-Anbieter untersagen, dann hieße das, dass es diese Angebote entweder nicht mehr geben würde oder alles, was bisher durch die Abgabe von Daten bezahlt wurde, in Zukunft mit Geld beglichen werden muss. Was die Unternehmen durch die Verwendung und Weitergabe von Informationen nicht mehr verdienen können, müssten sie auf die Preise umlegen. Hier kommt auch noch der so oft in den Vordergrund gerückte soziale Aspekt zum Tragen. Die Suchmaschinen im Internet kann jeder nutzen, egal ob Bill Gates von seinem Büro aus oder ein indischer Hilfsarbeiter von einem Internetcafé in Kalkutta aus. Ein System, das sich neben der Werbung nur aus Gebühren finanzierte, würde den egalitären Charakter des Internet zurückdrängen. Die so oft geforderte soziale Gleichheit und Teilhabe, die im Internet sehr weitgehend verwirklicht ist, wird gerade durch den Umstand, dass Angebote oft mit Daten statt mit Geldzahlungen beglichen werden, befördert. Denn Daten hat jeder, Geld eben nicht.

Im Grunde ist bei der Produktion von Daten jeder einzelne Marktteilnehmer so etwas wie seine eigene Privatbank, die eine private Daten-Währung emittiert, mit der Internetdienstleistungen bezahlt werden können. Diese private Datenwährung ist eine faszinierende Innovation im dicken Buch der Geldgeschichte. Sie ermöglicht es, dass selbst die Armen der Welt, soweit sie sich Zugang zum Netz verschaffen können, an eine Fülle von Informationen gelangen, die früher

allenfalls Magnaten oder Nachrichtendiensten zugänglich waren. Große Bankhäuser haben im 19. Jahrhundert noch ein teures Informantennetz in Europa und Amerika unterhalten, um an Informationen zu kommen, die heute eben auch dem Hilfsarbeiter in Kalkutta nach zwei Mausklicks zur Verfügung stehen. Diese private Daten-Währung ist durch nichts anderes gedeckt als durch die Erwartung des Anbieters von Online-Diensten, aus diesen Daten Kapital schlagen zu können. Ihre Kaufkraft entsteht durch die Zukunftserwartung der Online-Anbieter, und diese übernehmen auch das Umtauschrisiko der Daten in Geld oder besser gesagt, in die normale Form von Geld.

Dass sich ohne Intervention von außen eine private Daten-Währung herausgebildet hat, die es potenziell fast jedem Erdenbürger mit Netzzugang ermöglicht, weitgehend ohne finanzielle Barrieren auf gigantische Informationsnetze zurückzugreifen und die Dienstleistungen von Weltkonzernen in Anspruch zu nehmen, die diese Informationen und Kommunikationsverbindungen mit großem Aufwand zur Verfügung stellen, ist ein Beweis für die enorme Innovationsfähigkeit sich evolutionär entwickelnder Tauschsysteme. Die Prinzipien, nach denen die Legitimität der Datenverwendung beurteilt werden kann, sind die bekannten Prinzipien der Vertragsfreiheit und der Vertragssicherheit. Dies ist auch schon Grundlage des aktuellen Datenschutzrechtes: „Für die Erfüllung eigener Geschäftszwecke dürfen personenbezogene Daten erhoben, verarbeitet und genutzt werden, soweit sie dazu dienen, den von den Vertragsparteien gemeinsam mit dem Vertrag verfolgten Zweck zu erreichen."[9]

Die Google Street View-Kontroverse

An Googles Projekt „Street View" hat sich eine Datenschutzdebatte entzündet. Diese ist insoweit aufschlussreich, weil sie zeigt, wo die Grenzen der Schutzbestimmungen des Staates liegen. Der Datenschutzbegriff wurde hier aus populistischen Gründen in unzulässiger Weise ausgedehnt. Ziel der Internetfirma ist es, Straßenansichten und öffentliche Plätze im Internet zugänglich zu machen. Die bisherigen Internetkarten werden somit durch eine dreidimensionale Ansicht ergänzt. Dies hat eine zum Teil sehr schrille politische Diskussion ausgelöst. Die Bundesverbraucherschutzministerin Ilse Aigner warf Google „millionenfache Verletzung der Privatsphäre" und sogar Geheimdienstmetho-

9 M. Tinnefeld, E. Ehmann, R. Gerling: Datenschutzrecht, S. 549.

den vor.[10] Damit hat sich die Debatte stark vom sachlichen Kern entfernt. Im Kern geht es nämlich um die Abwägung verschiedener berechtigter Ansprüche und die Bestimmung ihrer Grenzen. Den Prinzipien des klassischen Liberalismus gemäß sollte der Einzelne möglichst uneingeschränkten Anspruch auf die Nutzung seines Grundstückes, Hauses und allem, was sich darauf und darin befindet, besitzen. Daraus ergibt sich für jeden auch das Recht, den Blick auf sein Grundstück durch Zaun, Hecken und Mauern zu verwehren. Er kann aber selbstverständlich nicht verbieten, dass eine Person eine offen dargebotene Hausfassade betrachtet. Auch die Einschränkung, ein öffentliches Panorama zu fotografieren und zu dokumentieren, ist immer ein Eingriff in das Selbstbestimmungs- und Eigentumsrecht des Dokumentierenden, der nur mit einer zwingenden Begründung zu legitimieren ist.

Dies entspricht auch den geltenden Normen des Grundgesetzes. Das Recht auf informationelle Selbstbestimmung findet seine Grenzen beim Recht auf Informationsfreiheit, also dem Recht, sich aus den allgemein zugänglichen Quellen zu informieren. So stellt ein für den schleswig-holsteinischen Landtag von Prof. Johannes Caspar erstelltes Rechtsgutachten zu den datenrechtlichen Implikationen von „Street View" fest: „Dem Ziel des Datenschutzes setzt das Grundgesetz somit immanente Schranken, indem es die Verschaffung solcher Informationen erlaubt, die im öffentlichen Raum grundsätzlich frei zugänglich sind. Dies kann mitunter auch Informationsquellen betreffen, die einen Personenbezug haben und sich auf sachliche Verhältnisse von bestimmten Personen beziehen." Das Gutachten kommt auch zu dem Schluss, die bloße Abbildung von Sachen im Rahmen von Panoramabildern greife nicht in das Recht des Eigentümers zu Besitz und Benutzung seiner Sache ein. Anderenfalls werde dies dazu führen, dass nahezu jede Anfertigung von Aufnahmen unmöglich wäre, da sich stets etwas von fremdem Eigentum auf jedem Bild befindet.

Caspar kommt daher zum Ergebnis, grundrechtlich geschützt sei auch die Sammlung von Straßenansichten zu Dokumentationszwecken, wie sie im Rahmen des Projekts „Street View" durchgeführt wird. Daraus ergebe sich, dass Google grundsätzlich berechtigt sei, Straßenansichten, insbesondere Grundstücke und Gebäude, aufzunehmen und sie für die Allgemeinheit nutzbar im Internet zu präsentieren. Das Gutachten sieht den Datenschutz jedoch dort gefährdet, wo das gesammelte digitale Bildmaterial einen direkten Personenbezug aufweist. Aus diesem Grund fordert das Gutachten eine Anonymisierung

10 http://www.focus.de/digital/internet/google/deutschland-millionenfacher-angriff_aid_477728.html

von zufällig fotografierten Personen, Kfz-Kennzeichen und Hausnummern.[11] Während die ersten zwei Forderungen von Google bereits ganz oder teilweise erfüllt sind, bleibt letzteres juristisch noch umstritten.

Im Gegensatz zum Gutachten für den schleswig-holsteinischen Landtag kommt das Landgericht Köln zu der Einschätzung, dass die Adresse verknüpft mit dem Foto als „individualisierendes Merkmal" nicht ausreicht, um als Eingriff in die Privatsphäre zu gelten. Das Landgericht Köln wies am 13. Januar 2010 die Klage gegen einen Internetanbieter zurück, der Bilder von Häuserfassaden mit Geodaten und der jeweiligen Adresse verknüpft im Internet zugänglich gemacht hatte. Dies tat das Landgericht mit der Begründung, dem Betrachter des Internetangebotes werde letztlich bildlich nicht mehr dargeboten als demjenigen, der selbst durch die Straße geht oder fährt, wobei der normale Passant zusätzlich noch in die Lage versetzt werde, sofort durch Ansicht der Klingelschilder die Namen der Bewohner zu ermitteln. Somit vermittle das Internetangebot weniger Informationen, als selbst der einfache Straßengänger gewinnen könnte.

Damit bezog sich das Landgericht auf ein Urteil des Bundesverfassungsgerichts, das den Schutz der Privatsphäre unter die Voraussetzung stellt, „dass der Betroffene nach den konkreten Gegebenheiten die begründete und für Dritte erkennbare Erwartung hegen darf, dass seine privaten Verhältnisse den Blicken der Öffentlichkeit entzogen bleiben und von ihr nicht zur Kenntnis genommen werden. Die Erwartung einer fehlenden Kenntnisnahme durch die Allgemeinheit liegt allerdings grundsätzlich fern, wenn ein privates Anwesen für jedermann von öffentlich zugänglichen Stellen aus einsehbar ist. Dementsprechend verneinen die Fachgerichte eine Beeinträchtigung des Persönlichkeitsrechts, sofern die Abbildung des Anwesens nur das wiedergibt, was auch für den vor Ort anwesenden Betrachter ohne weiteres zutage liegt."[12] Bei genauerem Hinsehen reduziert sich also die zum gesellschaftlichen Großkonflikt hochstilisierte Debatte über „Street View" auf letzte offene Fragen wie die, ob Hausnummern wie Personen und Kraftfahrzeuge anonymisiert werden sollen und ob die technische Verfremdung von Personen, die Google bereits durchgeführt hat, ausreichend ist, oder ob Frisuren und Haaransätze stärker gepixelt werden sollen. Dass Google einräumte, dass ganze Häuser gepixelt wurden, wenn nur ein Mieter dem widersprach, war Kulanz des Unternehmens und keine aus der Datenschutzgesetzgebung resultierende Notwendigkeit.

11 http://www.landtag.ltsh.de/infothek/wahl16/umdrucke/3900/umdruck-16-3924.pdf
12 http://www.justiz.nrw.de/nrwe/lgs/koeln/lg_koeln/j2010/28_O_578_09urteil20100113.html

Datenschutz, Internet und Pressefreiheit: Der Fall Wikileaks

Die Veröffentlichung von Depeschen der diplomatischen Vertretungen der USA auf der Seite Wikileaks hat große Wellen geschlagen, und über die Legalität und die Legitimität der Veröffentlichungen wurde breit diskutiert. Der Experte für Internetrecht Carsten Ulbricht hat auf den offensichtlichen Umstand hingewiesen, dass wenn man von einem Rechtsbruch durch die Veröffentlichung von Wikileaks ausgeht, dies in derselben Weise auch die Printmedien, die schließlich dieselben Informationen veröffentlichten, wie in diesem Fall den Spiegel oder The Guardian, betreffen würde. Da diese „schlussendlich nichts anderes tun als Wikileaks, nämlich geheime Informationen auswerten und an die Öffentlichkeit geben."[13]

Die Pressefreiheit steht grundsätzlich in einem Spannungsverhältnis zum Geheimhaltungsinteresse des Staates. Geheimnisverrat wird in den meisten Rechtsordnungen mit erheblichen rechtlichen Konsequenzen geahndet. Die Weitergabe diplomatischer Depeschen wäre auch in Deutschland strafbar. Die Weitergabe von Unternehmensgeheimnissen kann sowohl straf- als auch zivilrechtliche Folgen zeitigen. Auch nach deutschem Recht wäre also eine Weitergabe diplomatischer Depeschen an Wikileaks strafbar. Die Veröffentlichung selbst wäre aber vom deutschen Recht durch das Prinzip der Informationsfreiheit gedeckt.

Der gesamte Vorgang von der Beschaffung der Nachrichten bis zur Veröffentlichung ist in Deutschland rechtlich weitgehend vor dem staatlichen Zugriff geschützt. Denn die Informationsfreiheit ist ein selbstständiges Grundrecht neben der Meinungs- und der Medienfreiheit. Geschützt ist das Recht, sich aus „allgemein zugänglichen Quellen ungehindert zu unterrichten." Die Quelle muss so beschaffen sein, dass sie dazu geeignet ist, einem individuell nicht bestimmbaren Personenkreis zugänglich zu sein. Neben Presse, Rundfunk und Film wird auch das Internet von dieser Definition abgedeckt.[14] Der Staat darf den Zugang zu diesen Quellen nicht erschweren. Informationen dürfen jedoch nicht mit der Berufung auf die Informationsfreiheit durch strafbare Handlungen beschafft werden. Hier gibt es aber einen Knackpunkt: Wenn die Information erst einmal an die Öffentlichkeit gelangt ist, so darf die Information weiter-

13 Carsten Ulbricht: Der Fall Wikileaks – Zulässige Inanspruchnahme der Pressefreiheit oder rechtswidriger Geheimnisverrat. http://www.rechtzweinull.de/index.php?/archives/166-Der-Fall-Wikileaks-Zulaessige-Inanspruchnahme-der-Pressefreiheit-oder-rechtswidriger-Geheimnisverrat.html

14 Frank Fechner: Medienrecht, Tübingen 2011, S. 42.

gegeben werden. „Hat ein Behördenmitarbeiter Informationen, die nicht für die Allgemeinheit bestimmt waren, weisungswidrig an den Journalisten einer Zeitung weitergegeben, so ist dieser nicht daran gehindert, die Informationen zu verbreiten."[15] Ulbricht stellt deshalb fest: „Man kann daraus insgesamt ableiten, dass ein strafwürdiges Verhalten nur durch den Amtsträger oder den zur Geheimhaltung Verpflichteten erfolgt, der geheime Informationen preisgibt, nicht aber durch die Medienangehörigen, die die preisgegebenen Informationen – ihrer beruflichen Aufgabenstellung entsprechend – entgegennehmen, selektieren und dann veröffentlichen."

Es ist nicht erkennbar, dass eine Internetplattform prinzipiell anders beurteilt werden sollte als eine Tageszeitung, ein Nachrichtenmagazin oder ein Rundfunksender. Nach Anwendung deutschen Rechts ist das Vorgehen von Wikileaks bei der Veröffentlichung der Depeschen, soweit dieses lediglich Entgegennahme, Auswahl und Veröffentlichung der Informationen umfasst, durch die Pressefreiheit gedeckt, so das Resümee von Carsten Ulbricht.

Nach der in Deutschland vorherrschenden Rechtsauffassung würde also die Veröffentlichung durch Wikileaks unter die Pressefreiheit fallen, weil es keinen grundsätzlichen rechtlichen Unterschied gibt zwischen der Veröffentlichung in einer Zeitung und im Internet.

Schlussfolgerung

Grundsätzlich gilt, dass im Internet erlaubt sein sollte, was auch außerhalb des Internets erlaubt ist, und für ein privates Unternehmen sollten dieselben Spielregeln gelten, die auch für jeden anderen Bürger und den Staat gelten. Jeder Mensch hat das Recht, durch eine Straße zu gehen, öffentliche Plätze zu betreten und sich den Verlauf der Straßen und die Fassaden der Häuser anzusehen. Bislang hat jeder das Recht, öffentliche Plätze und Straßen zu fotografieren und sich die Fotos ins Album zu kleben, was ja Millionen von Touristen jedes Jahr tun. Wenn nun die Touristen ihre Urlaubsfotos ins Internet stellen, was auch immer mehr Bürger tun, dann ist das ebenfalls legal. Dasselbe gilt auch für Google Street View. Eine Lex Google darf es nicht geben. Dies ist eine wichtige Erkenntnis der Kontroverse. Grundsätzlich gilt, dass für die materielle Welt und die virtuelle Welt ein und dasselbe Recht gilt. Dasselbe

15 Frank Fechner: Medienrecht, Tübingen 2011, S. 44.

Presserecht, das die Pressefreiheit für Print-Medien wie den SPIEGEL oder The Guardian definiert, definiert auch die Spielräume und Grenzen einer Online-Publikation wie Wikileaks.

Das Internet ist kein rechtsfreier Raum, aber es gibt auch keinen Grund, ihn aufgrund seiner besonderen Form stärker zu regulieren und zu reglementieren als den öffentlichen Raum. Der zentrale Ansatz zur Beurteilung ist daher die Analogiebildung. Wenn man vor der Frage steht, ob das Vorgehen eines Internetanbieters den Datenschutzbestimmungen entspricht, sollte man nach ähnlichen Beispielen in der „realen" Welt suchen. Wenn das Fotografieren einer Hausfassade und die Veröffentlichung in einer Zeitung kein Problem darstellt, dann gilt das auch für das Internet. Wenn unter bestimmten Bedingungen die Weitergabe von Kundendaten nicht gestattet ist, dann gibt es keinen Grund, warum ein Online-Unternehmen hier eine Ausnahme darstellen sollte.

Wie Christian Hoffmann zu Recht festgestellt hat, ist der Datenschutz gegenüber dem Staat vor allem ein Abwehrrecht. Es muss innerhalb der privaten Sphäre vor allem dem Ermessen jedes Einzelnen überlassen bleiben, welche Verträge er eingeht und zu welchen Bedingungen er bereit ist, seine persönlichen Daten preiszugeben. Die Aufgabe des Datenschutzes gegenüber dem Staat besteht darin, dem gesetzlich erzwungenen Zugriff Grenzen zu setzen, in der Sphäre der Privatwirtschaft darin, Vertragssicherheit zu garantieren. Diese unterschiedliche Stoßrichtung ergibt sich daraus, dass der Staat die Herausgabe von Daten eben erzwingen kann, private Online-Dienstleister jedoch nicht. Sie können, soweit sie nicht konsequent illegal handeln, keine Daten erwerben, die vom Dateninhaber nicht freiwillig veröffentlicht worden sind. Die Verwendung der Daten muss aber entsprechend der Allgemeinen Geschäftsbedingungen, denen der Nutzer zugestimmt hat, erfolgen, sonst handelt es sich um Vertragsbruch. Datenschutz-Bestimmungen, die weit darüber hinausgehen und freien Vertragsparteien die Verwendung privater Daten vorschreiben, würden bald mit dem Grundsatz der Informationsfreiheit kollidieren. Datenschutz ist nicht grenzenlos, sondern muss dem Kriterium der Verhältnismäßigkeit gerecht werden.

Die Sorge vor einer Gesellschaft, in der die Internetnutzer freiwillig ihre Daten etwa in sozialen Netzwerken preisgeben und sich zum „gläsernen" Menschen machen, erregt Unbehagen. Dieses Unbehagen gehört aber nicht in den Bereich des Datenschutzes, sondern in den Bereich der Kulturkritik. Wer freiwillig die Welt an seinem Leben teilnehmen lassen möchte, mag im Einzelfall vielleicht unklug handeln, hat aber ohne Zweifel das Recht, es zu tun.

Literatur

Bundesverfassungsgericht: Presseerklärung zur Vorratsdatenspeicherung: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.html

Johannes Caspar: Gutachten zu Rechtsfragen betreffend den Internet-Dienst Google Street View: http://www.landtag.ltsh.de/infothek/wahl16/umdrucke/3900/umdruck-16-3924.pdf

Frank Fechner: Medienrecht, Tübingen 2011.

Christian Hoffmann: Der Irrtum der „Bürgerrechtsliberalen". Warum der gesetzliche Schutz der Daten scheitern muss, in: ef-magazin, November 2005, Nr. 57.

J. Kühling, C. Seidel, A. Sivridis: Datenschutzrecht, Frankfurt a. M 2008.

Landgericht Köln, 28 O 578/09 http://www.justiz.nrw.de/nrwe/lgs/koeln/lg_koeln/j2010/28_O_578_09urteil20100113.html

Peter Schaar: Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft, München 2007.

Wolfgang Sofsky: Verteidigung des Privaten. Eine Streitschrift, München 2007.

M. Tinnefeld, E. Ehmann, R. Gerling: Einführung in das Datenschutzrecht, München 2005.

Carsten Ulbricht: Der Fall Wikileaks – Zulässige Inanspruchnahme der Pressefreiheit oder rechtswidriger Geheimnisverrat: http://www.rechtzweinull.de/index.php?/archives/166-Der-Fall-Wikileaks-Zulaessige-Inanspruchnahme-der-Pressefreiheit-oder-rechtswidriger-Geheimnisverrat.html

PositionLiberal

Positionspapiere des Liberalen Instituts der Friedrich-Naumann-Stiftung für die Freiheit
Weitere Publikationen unter www.libinst.de

[99] Bodo Herzog
HAUSHALTSLÖCHER UND STEUERENTLASTUNGEN – WAS IST ZU TUN?

[98] Monika Reinsch (2011)
HOCHBEGABUNG IM VORSCHULALTER

[97] Gérard Bökenkamp (2010)
DIREKTE DEMOKRATIE – GESCHICHTE, ENTWICKLUNGEN UND PERSPEKTIVEN FÜR DIE BUNDESREPUBLIK

[96] Marie Popp, René Sternberg (Hrsg.)
LEUCHTTÜRME DER DEUTSCHEN SCHULLANDSCHAFT

[95] Alexander Wimmer (2010)
RISIKEN UND CHANCEN DER DEUTSCHEN KRANKENVERSICHERER IM INTERNATIONALEN VERGLEICH

[94] Kerstin Funk (2010)
KERNPROBLEME DES GESUNDHEITSWESENS IN INDUSTRIELÄNDERN

[91] Harald Bergsdorf (2010)
DIE KULTUR DER FREIHEIT ARGUMENTATIV VERTEIDIGEN LIBERALE GESELLSCHAFT GEGEN RECHTSEXTREMISMUS UND ANDERE FREIHEITSFEINDE

[89] Charles B. Blankart (2009)
AUTONOMIEPRINZIP UND VERWALTUNGSPRINZIP ZWEI ANSÄTZE EINER GEMEINDEORDNUNG

[88] Martin T.W. Rosenfeld (2009)
FINANZIERUNG KOMMUNALER AUFGABEN – ÖKONOMISCHE PRINZIPIEN, MODERNE HERAUSFORDERUNGEN UND INSTITUTIONELLE GESTALTUNGSMÖGLICHKEITEN

[87] Robert Nef (2009)
GEMEINDEAUTONOMIE, DIREKTE DEMOKRATIE UND STEUERWETTBEWERB IN DER SCHWEIZ

[86] Fred E. Foldvary (2009)
DIE PRIVATE BEREITSTELLUNG ÖFFENTLICHER GÜTER VERGANGENHEIT UND ZUKUNFT DES KOMMUNALEN LIBERALISMUS

[85] Immo H. Wernicke (2009)
FINANZKRISE – KRISE DER AMTLICHEN STATISTIK? KRITIK AN STAATLICHER BERICHTERSTATTUNG ZUR LAGE VON WIRTSCHAFT UND FINANZMÄRKTEN IM KRISENJAHR 2008

[83] Jakob von Weizsäcker (2009)
HOHER ZAUN UND ENGE PFORTE? PRIORITÄTEN FÜR DIE EUROPÄISCHE MIGRATIONSPOLITIK

[81] Sibylle Laurischk (2009)
WIE LIBERAL SIND DIE DEUTSCHEN ZUWANDERUNGSREGELUNGEN?

[80] Detmar Doering (2009)
RECHTSSTAAT UND WIRTSCHAFTLICHE FREIHEIT

[79] Tom G. Palmer (2009)
ZWANZIG MYTHEN ÜBER MÄRKTE

[77] Susanne Maria Schmidt/Olaf Steglich (2009)
AUS GEGEBENEM ANLASS – ODER WARUM DIE ORDNUNGSPOLITIK DAS EINZIGE HEILMITTEL FÜR DIE FINANZMÄRKTE IST

[76] Steffen Hentrich (2009)
IN GUTEN HÄNDEN? UMWELTSCHUTZ ALS STAATSAUFGABE

[75] Detlef Parr (2008)
LEISTUNGSSPORT UND BREITENSPORT: GESELLSCHAFTLICHE AUFGABEN?