5.2 Datenverarbeitung zwischen Personenbezug und Sozialbezug

[Prof. Niko Härting | HÄRTING Rechtsanwälte]

5.2.1 Einleitung

Das Datenschutzrecht steht vor einem Umbruch. Wenn die Pläne der EU-Kommission erfolgreich sein sollten, wird das europäische Datenschutzrecht durch eine Datenschutz-Grundverordnung geregelt werden. Dies bedeutet, dass die Verordnung nicht wie eine Richtlinie von den einzelnen Mitgliedsstaaten umzusetzen ist, sondern direkt geltendes Recht in allen Mitgliedsstaaten wird. Bei den Reformbemühungen ist dabei immer zu bedenken, dass Daten nicht um ihrer selbst willen geschützt werden und bei der Datenverarbeitung Grundrechtsträger (im privaten Bereich) aufeinandertreffen. Der nachstehende Beitrag soll die Datenverarbeitung im Kontext des Personen- und Sozialbezuges erklären und deutlich machen, dass Daten einer Person nicht eigentumsähnlich zugeordnet werden können.

5.2.2 Der Personenbezug von Daten

Nach dem geltenden Datenschutzrecht sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Diesem Begriff fehlt erkennbar die Trennschärfe, er sorgt für ein „Schwarz-Weiß-Prinzip". Je nachdem, ob man von einem „absoluten"[1] oder einem „relativen"[2] Begriffsverständnis ausgeht, gelangt man zu einem sehr weiten oder stark eingeschränkten Anwendungsbereich des Datenschutzrechts. Wie die anhaltende Kontroverse um die Personenbezogenheit von IP-Adressen zeigt, ist dies höchst unbefriedigend.[3]
Vielfach wird in diesem Zusammenhang verfehlt davon ausgegangen, beim Schutzgut des Datenschutzrechts gehe es um den „Schutz von Daten". Es entspricht eben jener Tendenz, Daten um ihrer selbst willen zu schützen, also nach dem „Schwarz-Weiß-Prinzip"[4] zu verfahren. Dabei gerät in Vergessenheit, dass das Allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG), die Privatsphäre, Bezugspunkt des Datenschutzrechts ist.

5.2.3 Der Sozialbezug von Daten

Der Datenschutz läuft Gefahr, zu „l'art pour l'art" zu werden und unreflektiert ein falsches Verständnis von einem eigentumsgleichen Schutz von Daten zu perpetuieren.
Ein weit verbreiteter, sich durch alle politischen Partei und Gesellschaftsschichten durchziehender Fehlglaube ist die Annahme: „Meine Daten gehören mir".[5] Das Bundesverfassungsgericht hat in seiner wegweisenden Volkszählungsentscheidung schon im Jahre 1983 betont, dass es kein Recht des Einzelnen an „seinen Daten" gebe „im Sinne einer absoluten, uneinschränkbaren Herrschaft".[6] Der Einzelne ist eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Informationen, auch soweit sie personenbezogen sind, stellen daher (auch) ein „Abbild sozialer

Realität“ dar, das nicht ausschließlich dem Betroffenen zugeordnet werden kann.[7] Jegliche Anlehnung an eigentumsrechtliche Befugnisse ist dementsprechend verfehlt.
E-Mail-Adressen oder Telefonnummern sind ein gutes Beispiel für die „soziale Realität“, die das Bundesverfassungsgericht meint. Sie dienen der Kommunikation und werden aus diesem Grund ganz selbstverständlich von jedem gespeichert, der mit der betreffenden Person kommunizieren möchte. Wenn es allein der Entscheidung des Adressinhabers überlassen wäre, wer wann und wie lange die e-Mail-Adresse oder Telefonnummer speichern darf, würde dies die soziale Interaktion und Kommunikation erheblich behindern.
Für den Facebook-„Freundefinder“ bedeutet dies, dass es keineswegs selbstverständlich ist, dass die Adressinhaber in ihren Rechten verletzt werden, wenn „ihre“ Adressen zum Abgleich auf die Plattform hochgeladen werden. Gäbe es ein eigentumsähnliches Recht an Postanschriften und Telefonnummern, hätte nie ein Telefonbuch gedruckt werden dürfen.
Daten und Informationen haben (auch) einen sozialen Bezug. Werden Daten monopolisiert und dem ausschließlichen Bestimmungsrecht einer einzelnen Person untergeordnet, droht die jederzeitige „Privatisierung von Informationen“. Daten, die wichtig sind für die soziale Interaktion, die Kommunikation und den gesellschaftlichen Diskurs, könnten durch ein Bestimmungsrecht einzelner Person eigentumsähnlich privatisiert werden. Dies wäre in höchstem Maße gemeinschafts- und gesellschaftsfeindlich.
Ebenso wenig lässt sich von einem „Kontrollrecht“ von vermeintlichen Dateneigentümern ausgehen. Niemand hat ein (quasi-natürliches) Kontrollrecht über Informationen, die die eigene Person betreffen. Würde man in diesem Punkt eine andere Auffassung vertreten, läge in jeglichem zwischenmenschlichen Kontakt ein Eingriff in die Privatsphäre. Was andere über mich wahrnehmen, entzieht sich im zwischenmenschlichen Umgang jeder Kontrolle, zumal die Wahrnehmungen Informationen sind, die sich zwar auf meine Person beziehen, deren Entzug jedoch einen Informationsverlust bedeutet, der sich nicht legitimieren lässt. Ebenso wenig wie es Eigentum an Informationen geben kann, lassen sich Kontrollrechte begründen und abgrenzen, denn:

> „Anders als körperliche Gegenstände können Informationen gleichzeitig den Köpfen von Millionen Menschen gleichzeitig gehören… Die Komplexität personenbezogener Informationen liegt darin, dass sie sowohl Ausdruck des Individuums sind als auch Tatsachen – die historische Aufzeichnung des individuellen Verhaltens.“[8]

5.2.4 Das Spannungsverhältnis von Personen- und Sozialbezug

Jegliches Verbot der Datenverarbeitung und -nutzung bedeutet ein Kommunikationsverbot, das Art. 5 GG sowie Art. 11 EU-GRCh und Art. 8 EMRK auf den Plan ruft.[9] Nicht nur die Konflikte um spickmich.de[10] und die Veröffentlichung der Empfänger von Agrarsubventionen[11] haben hierfür Anschauungsmaterial geliefert. Auch bei den Diskussionen über Anwendungen wie Google Street View[12], Google Analytics, den Facebook-Freundefinder oder den „Gefällt mir“-Button[13] geht es nur vordergründig um Fragen der Auslegung einzelner Normen des Datenschutzrechts. Im Hintergrund steht – neben wirtschaftlichen Interessen – stets der Konflikt zwischen Persönlichkeitsrechten und freier, ungehinderter Kommunikation.
Das Internet ist ein zentraler Bestandteil des öffentlichen Raums, in dem der Austausch von Informationen und die Kommunikation einer offenen Gesellschaft stattfinden.[14] Und

auch für den freien Wirtschaftsverkehr ist das Internet im 21. Jahrhundert unverzichtbar. Einseitigen Tendenzen, den Schutz der Privatsphäre zu überhöhen, muss das Recht entgegenwirken.

Die Verbreitung von personenbezogenen Informationen über das Internet kann Persönlichkeitsrechte erheblich beeinträchtigen. Datensammlungen können dazu führen, dass der Internetnutzer „gläsern" wird und Persönlichkeitsprofile erstellt werden, die die Intimsphäre transparent werden lassen. Die Aufgabe eines modernen Datenschutzrechts muss es daher sein, Persönlichkeitsrechte dadurch zu schützen, dass die Sammlung von Informationen nicht im Geheimen erfolgt und dem Nutzer die Möglichkeit gegeben wird, selbst zu entscheiden, ob und inwieweit er Dienste nutzt, die mit persönlichen Informationen bezahlt werden. Ein modernes Datenschutzrecht schafft Transparenz.[15] Dadurch soll die freie Kommunikation jedoch nicht gehindert werden.

Aus dem Grundrecht auf informationelle Selbstbestimmung folgt die Pflicht des Staates, im privaten Datenverkehr das selbstbestimmte Handeln der Bürger zu schützen. In der privaten Datenverarbeitung liegt jedoch zugleich auch immer eine Grundrechtsausübung, zu deren Schutz der Staat in gleicher Weise verpflichtet ist. So steht die private Erhebung, Verarbeitung und Nutzung von Daten unter dem Schutz der Art. 5, 12, 14 GG/Art. 11, 16, 17 EU-GRCh oder zumindest unter dem Schutz der allgemeinen Handlungsfreiheit (Art. 2 Abs. 1 GG/Art. 6 EU-GRCh). Den Gesetzgeber trifft deswegen die Aufgabe, eine Regelung zu finden, die den verschiedenen Grundrechtsträgern gerecht wird.
Bei Online-Publikationen und der Kommunikation im Netz – insbesondere auch innerhalb sozialer Netzwerke – kommt es zwangsläufig zu Konflikten zwischen Persönlichkeitsrechten und der Meinungs- und Informationsfreiheit.[16] Der Datenschutz hat in diesem Konfliktfeld die Aufgabe, die Persönlichkeitsrechte zu schützen. Ob E-Mail-Adresse, Gerätekennzeichen, Cookie oder IP-Adresse: Es gibt keinen plausiblen Grund, derartige Daten per se unter Schutz zu stellen. Von einem Datum als solchem geht keine Gefahr aus. Wenn die Daten jedoch – allein oder in Verbindung mit anderen Daten bzw. Informationen – Rückschlüsse darauf zulassen, dass ein bestimmter Internetnutzer sich auf Internetseiten mit pikantem Inhalt bewegt hat, ist die Privat- bzw. Intimsphäre des Nutzers berührt. Die Daten erlangen einen Informationswert, der die Persönlichkeitsrechte beeinträchtigen kann.[17]
Das Bundesverfassungsgericht hat zwei Verfassungsbeschwerden gegen Entscheidungen der Zivilgerichte stattgegeben, die den Wert und die Bedeutung freier Kommunikation in eklatanter Weise verkannt hatten. Es ging um Klagen wegen der angeblichen Verletzung von Persönlichkeitsrechten durch Veröffentlichungen. Die Fachgerichte hatten den Klagen jeweils mit der Begründung stattgegeben, dass es an einem hinreichenden „Informationsinteresse" der Öffentlichkeit fehle. Das Bundesverfassungsgericht sah sich daher veranlasst, daran zu erinnern, dass die Informations-, Meinungs- und Kommunikationsfreiheit ihre Rechtfertigung in sich trägt und daher schon die Frage nach einem „Informationsinteresse" zutiefst grundrechtsfeindlich ist. Das Grundrecht aus Art. 5 GG gewährleistet die Selbstbestimmung des einzelnen Grundrechtsträgers über die Entfaltung seiner Persönlichkeit in der Kommunikation mit anderen. Bereits hieraus bezieht das Grundrecht sein Gewicht, das durch ein mögliches öffentliches Informationsinteresse allenfalls weiter erhöht werden kann.[18]

Auch schlechter Journalismus, dilettantische Blogs und reißerische Klatschgeschichten sind durch Art. 5 GG und Art. 11 EU-GRCh sowie Art. 8 EMRK geschützt, ohne dass es auf ein „Informationsinteresse“ ankommt. Hieran zu erinnern, besteht in jüngster Zeit reichlich Anlass, wenn im Zeichen des Datenschutzes Beschränkungen der freien Kommunikation gefordert werden. Auch populäre Forderungen wie die vom Bundesinnenminister wiederholt erhobene Forderung nach einem „Recht auf Vergessen“ oder einem „digitalen Radiergummi“[19] werfen die Frage auf, inwieweit hierdurch in den freien Meinungsaustausch eingegriffen wird und ob sich ein Eingriff durch den Persönlichkeits- und Datenschutz rechtfertigen lässt.

5.2.5 Ausblick

Nie bestand ein so großer gesellschaftlicher Konsens über den hohen Wert des Datenschutzes wie heute. Hinter diesem Konsens verblasst allerdings vielfach das Bewusstsein für den hohen Wert der ungehinderten, freien Kommunikation in einer demokratischen Gesellschaft. Wenn uns in Ägypten die „Facebook-Revolution“ begeistert, müssen wir auch in Europa anerkennen, dass das Internet mehr und mehr zu einer zentralen Lebensader der gesellschaftlichen Kommunikation wird. Beschränkende und regulierende Eingriffe sind nicht schon dadurch legitimiert, dass sie im Zeichen des Datenschutzes stehen. Denn so erfreulich das geschärfte öffentliche Bewusstsein für den Datenschutz ist: Auch die Kommunikationsfreiheit braucht gute Fürsprecher.
Die vernetzte Informationsgesellschaft eröffnet Chancen, die noch vor zwei Jahrzehnten unvorstellbar waren: Das Internet gibt Menschen in aller Welt die Gelegenheit, sich frei und unzensiert zu informieren. Die Ereignisse im arabischen Raum haben deutlich gemacht (und machen es weiterhin), dass es Regierungen nicht mehr möglich ist, ihre Bürger von Informationen abzuschotten. Die Occupy-Bewegung und die Entwicklung der „Piraten“ sind hierzulande Beispiele dafür, dass das Internet die Ausübung von Freiheitsrechten fördern kann und neue Organisationsformen ermöglicht.[20]

Ob und wie Daten vorgehalten und genutzt werden dürfen, muss sich aus einer Abwägung von Persönlichkeitsrechten und den Grundrechten auf freie Kommunikation und freie unternehmerische Betätigung ergeben. Ein generelles Verbot der Datenverarbeitung mit Erlaubnisvorbehalt steht jedoch einer solchen Abwägung entgegen.

1 Vgl. Thilo Weichert IN: Däubler/Klebe/Wedde/Weichert, 3. Aufl. 2010, § 3 Rdnr. 3; Niko Härting (2012): Starke Behörden, schwaches Recht – der neue EU-Datenschutzentwurf. IN: BB 2012. S. 459-466.

2 Vgl. Dammann in Simitis, BDSG, 7. Aufl. 2011, § 3 Rdnr. 21.

3 Vgl. Jens Eckhardt (2011): IP-Adresse als personenbezogenes Datum — neues Öl ins Feuer Personenbezug im Datenschutzrecht — Grenzen der Bestimmbarkeit am Beispiel der IP-Adresse. IN: CR 2011. S. 339 - 344.; Stefan Krüger / Svenja-Ariane Maucher (2011) IN: MMR 2011. S. 433 – 439.; Ulrich Sachs (2010): Datenschutzrechtliche Bestimmbarkeit von IP-Adressen. IN: CR 2010. S. 547 – 552.; Sven Venzke (2011): Die Personenbezogenheit der IP-Adresse – Lange diskutiert und immer noch umstritten? IN: ZD 2011. S. 114-119. Vgl. a. BVerfG v. 24. Januar 2012 – Az. 1 BvR 1299/05.

4 Jochen Schneider/Niko Härting (2011): Warum wir ein neues BDSG brauchen - Kritischer Beitrag zum BDSG und dessen Defiziten in: ZD 2011. S. 63 – 68.

5 Vgl. nur Renate Künast (2008): Meine Daten gehören mir – und der Datenschutz gehört ins Grundgesetz. IN: ZRP 2008. S. 201-205.

6 BVerfGE 65, 1, 41 f. – Volkszählung.

7 BVerfGE 65, 1, 41 f. – Volkszählung.

8 Daniel Solove (2009): Understanding Privacy. Cambridge/London 2009. S. 27.

9 Niko Härting (2011): Kommunikationsfreiheit und Datentransparenz in: AnwBl 2011. S. 246-250.

10 BGH v. 23.6.2009, Az. VI ZR 196/08, NJW 2009, 2888 ff.

11 EuGH v. 9.11.2011, Az. C-92/09; C-93/09, MMR 2011, 122 ff.

12 Nikolaus Forgó/Tina Krügel/Kathrin Müllenbach (2010): Zur Zulässigkeit von Google Street View. IN: CR 2010. S. 616-624.

13 Stefan Ernst (2010): Social Plugins: Der „Like-Button" als datenschutzrechtliches Problem . IN: NJW 2010. S. 2989-2890.

14 Vgl. Niko Härting/Jochen Schneider (2011): Das Dilemma der Netzpolitik. IN: ZRP 2011. S. 233-236.

15 Zum Postulat größerer Transparenz für den Einzelnen s.a. Gesamtkonzept für den Datenschutz der Kommission v. 4.11.2010, Ziff. 2.1.2

16 Vgl. Niko Härting (2011): Kommunikationsfreiheit und Datentransparenz. IN: AnwBl 2011. S. 246-250. Zum hohen Rang der Meinungsäußerungsfreiheit s. a. EMRG, Urteil der Großen Kammer v. 7.2.2012 in der Sache von Hannover gegen Deutschland Nr. 2 (Appl. nos. 40660/08 und 60641/08).

17 Jochen Schneider/Niko Härting (2011): Warum wir ein neues BDSG brauchen. Kritischer Beitrag zum BDSG und dessen Defiziten. IN: ZD 2011. S. 63-68.; Niko Härting/Jochen Schneider (2011): Das Dilemma der Netzpolitik. IN: ZRP 2011. S. 233-236.

18 BVerfG vom 18.2.2010, GRUR 2010, 544, 545 f.; BVerfG vom 9.3.2010, NJW-RR 2010, 1195 ff.

19 Vgl. Hamburger Abendblatt vom 22.6.2010, www.abendblatt.de/politik/deutschland/article1541363/De-Maiziere-fuer-digitalen-Radiergummi-im-Internet.html

20 Niko Härting/Jochen Schneider (2011): Das Dilemma der Netzpolitik. IN: ZRP 2011. S. 233 – 236.; Schneider/Härting, Leitlinien des Datenschutzes, www.schneider-haerting.de/2011/09/leitlinien-des-datenschutzes; Deutscher Anwaltverein, Stellungnahme zu dem Gesamtkonzept des datenschutzes in der Europäischen Union, Stellungnahme 4/2011, www.anwaltverein.de/downloads/Stellungnahmen-11/SN4-2011.pdf; Stellungnahme der DGRI zur DS-GVO vom 21.12.2011, www.dgri.de/index.php/fuseaction/download/lrn_file/stellungnahme-dgri-datenschutzvo.pdf.