Maximilian von Grafenstein

Das Zweckbindungsprinzip zwischen Innovationsoffenheit und Rechtssicherheit

Zur mangelnden Differenzierung der Rechtsgüterbetroffenheit in der Datenschutzgrund-VO

Der datenschutzrechtliche Zweckbindungsgrundsatz wurde vor einiger Zeit[1] in den Medien hitzig[2] diskutiert. Anlass gab die Veröffentlichung des aktuellen Ratsentwurfs der Datenschutzgrundverordnung durch European Digital Rights.[3] Unter anderen berichtete der Tagesspiegel, dass durch den aktuellen Entwurf das Zweckbindungsprinzip ausgehebelt werden würde.[4] Der folgende Beitrag möchte mit Blick auf die jeweils verfassungsrechtliche Bedeutung den gesetzgeberischen Spielraum bei der Umsetzung des Zweckbindungsprinzips beleuchten.

1 Einleitung

Die strikte Anwendung des Zweckbindungsprinzips bedeutet, dass personenbezogene Daten nur für die Zwecke verarbeitet werden dürfen, für die sie ursprünglich erhoben wurden.[5] Demgegenüber sieht Artikel 6 Abs. 4 des auf der Plattform von European Digital Rights veröffentlichten VO-Entwurfs im Ergebnis vor, dass Zweckänderungen aus den gleichen gesetzlichen Erlaubnisgründen vorgenommen werden dürfen wie die Datenerhebung selbst. Nur für den Fall, dass die Daten aufgrund des generellen Erlaubnistatbestands in Artikel 6 Abs. 1 lit. f des VO-Entwurfs (wegen „berechtigter Interessen" der verantwortlichen Stelle) erhoben wurden, ist eine Zweckänderung nicht generell erlaubt, sondern nur dann, wenn sie nicht unvereinbar mit den ursprünglichen Zwecken ist.[6] Einige Kritiker sahen in dieser Regelung einen Verstoß gegen das Recht auf informationelle Selbstbestimmung sowie die europäische Grundrechtecharter.[7]

2 Bedeutung des Zweckbindungsprinzips

Die Frage, ob die in dem aktuellen Ratsentwurf vorgesehene Regelung tatsächlich verfassungswidrig ist, ist insbesondere deshalb interessant, weil das Zweckbindungsprinzip einerseits ein intuitiv einleuchtendes Prinzip zum Schutz der durch Datenverarbeitungen Betroffenen darstellt und andererseits in einem Spannungsfeld mit der Offenheit von Innovationsprozessen in Wirtschaft und Gesellschaft steht. Das Prinzip soll einerseits Transparenz, Rechtssicherheit und Vorhersehbarkeit für den Betroffenen ge-

1 Siehe die Zusammenfassung zahlreicher Stellungnahmen auf https://netzpolitik.org/2015/besorgte-reaktionen-auf-leaks-zur-eu-datenschutzreform/, letzter Abruf aller Internetseiten am 6. Oktober 2015.

2 Siehe etwa der Berichterstatter des Europäischen Parlaments Albrecht im Tagesspiegel zum ‚eindeutigen Übertreten der roten Linie' unter http://www.tagesspiegel.de/politik/berlin-will-eu-datenschutz-aushoehlen-banken-sollen-kundendaten-nutzen-duerfen/11458648.html, letzter Abruf am 6. Oktober 2015.

3 Siehe https://edri.org/broken_badly/, letzter Abruf am 6. Oktober 2015.

4 Siehe http://www.tagesspiegel.de/politik/bruessel-regierungen-bohren-loecher-in-datenschutzverordnung/11447506.html.

5 Vgl. v. *Zezschwitz*, Konzept der normativen Zweckbegrenzung, in: Handbuch Datenschutzrecht, München 2003, Rn. 14.

6 Siehe die Gegenüberstellung des aktuellen Ratsentwurfs und des Parlamentsentwurfs unter https://edri.org/files/EP_Council_Comparison.pdf.

7 Siehe etwa Alexander Sanders des Vereins Digitale Gesellschaft e.V. unter https://digitalegesellschaft.de/2015/03/datenschutzverordnung-bundesregierung-opfert/.

Maximilian von Grafenstein LL.M.

leitet am Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG) die Startup Law Clinic des interdisziplinären Forschungsprojekts „Innovation und Entrepreneurship" und schreibt seine Doktorarbeit zu den Wirkungen rechtlicher Regelungsinstrumente auf Innovationsprozesse am Beispiel des datenschutzrechtlichen Zweckbindungsprinzips.
E-Mail: max.grafenstein@hiig.de

währleisten.[8] Andererseits beschränkt es den Handlungsspielraum der datenverarbeitenden Unternehmen, weil es sie grundsätzlich zwingt, zu Beginn eines Verarbeitungsprozesses dessen Ausgang vorherzusagen bzw. sich auf die Verwendungszwecke zu beschränken, die es in diesem Augenblick absehen kann oder die von einem anderen einmal angegeben wurden.[9] Das bedeutet insbesondere für innovative Anwendungen wie aus dem Bereich Big Data eine spürbare Beschränkung, weil hier meistens sehr viele Daten aus unterschiedliche Quellen auf bis dahin noch unbekannte Zusammenhänge untersucht und die Ergebnisse dann für Zwecke unterschiedlicher Geschäfts- und Gesellschaftsbereiche verwendet werden.[10] Ein aktuelles Beispiel sind sog. Social Heat Maps, die Startups mit Daten aus sozialen Medien, von Webseiten und aus weiteren Quellen generieren. Über die Angaben aus Internetauftritten von Cafés, Shops oder Veranstaltungsräumen, aus Nutzerkommentaren in sozialen Medien sowie aus öffentlichen Statistiken können etwa Aussagen darüber getroffen werden, wie belebt ein Stadtviertel oder eine Straßenecke ist, wie viele Leute wann und wo ein Taxi brauchen oder ob die Immobilienpreise steigen.[11] Während Touristen, Taxiunternehmen oder die Immobilienwirtschaft jeweils ein Interesse an solchen Analysen haben, wären diese unter Anwendung einer strikten Zweckbindung unzulässig. Denn weder das soziale Netzwerk noch der Betreiber einer Internetseite konnten voraussehen, dass die Daten einmal für diese Zwecke verwendet würden.

Der Gesetzgeber, der mit der Datenschutzgrund-VO die Datenschutzrichtlinie aus dem Jahr 1995 ablösen möchte, steht nun vor der Herausforderung, diesen Konflikt zwischen Innovationsoffenheit und dem Schutz der Betroffenen zu lösen. Damit stellt sich die Frage, welcher Handlungsspielraum dem Gesetzgeber bei der Umsetzung des Zweckbindungsprinzips zur Verfügung steht. Und noch eine Frage schließt sich an. Denn es ist selbst unklar, was das Zweckbindungsprinzip konkret bedeutet. So wird neben der strikten Zweckbindung auch die Zweckvereinbarkeit als Regelungsmöglichkeit diskutiert.[12] Die Art. 29-Datenschutzgruppe differenziert zum Beispiel in ihrer Stellungnahme zum Zweckbindungsprinzip, dass sich dieses aus zwei unterschiedlichen Anforderungen zusammensetzt: 1.) müssen die Zwecke der Datenerhebung vorweg festgelegt und 2.) dürfen die Daten nicht in einer Weise verarbeitet werden, die unvereinbar mit den ursprünglich festgelegten Zwecken ist. Dabei stellt sie klar, dass die Verarbeitung der Daten zu einem anderen Zweck nicht automatisch ihre Unvereinbarkeit bedeutet. Vielmehr schlägt die Gruppe ein Prüfungsschema vor, nach dem nicht nur der ursprüngliche mit dem neuen Zweck formal verglichen, sondern auch der Kontext der Datenerhebung und die Erwartungen des Betroffenen, die Art der Daten und die Auswirkungen auf ihn sowie die Maßnahmen gegen einen möglichen Datenmissbrauch herangezogen werden sollen.[13] Die Art. 29-Datenschutzgruppe spricht also von Zweckbindung, versteht darunter aber nicht die Identität, sondern nur die Vereinbarkeit der Zwecke.

Selbst im Vergleich zu einer Zweckvereinbarkeit sieht der aktuelle Ratsentwurf in Artikel 6 Abs. 4 allerdings noch einmal eine deutliche Ausweitung der Zweckänderungsmöglichkeiten vor. Eine Antwort auf die Fragen, was das Zweckbindungsprinzip konkret bedeutet, welcher Handlungsspielraum für den Gesetzgeber bei seiner Umsetzung besteht und ob der aktuelle Vorschlag verfassungswidrig ist, sollte mit Blick auf die Schutzgüter, die Reichweite ihres Schutzes und die Regelungsinstrumente erfolgen, die für den Ausgleich der widerstreitenden Interessen der Betroffenen und der datenverarbeitenden Unternehmen auf dem privaten Sektor herangezogen werden.[14] Dafür wird in diesem Beitrag ein Blick auf drei Grundrechtsordnungen geworfen: Die Charta der Grundrechte der Europäischen Union (ECGR), die Europäische Menschenrechtskonvention (EKMR) und das Deutsche Grundgesetz (GG).

3 Gewährleistungsgehalte der datenschutzrelevanten Grundrechte

Die ECGR sieht sowohl ein Recht auf „privacy" in Artikel 7 als auch ein Recht auf „data protection" in Artikel 8 vor. Die Schutzgüter bzw. ihr Zusammenspiel sind durch den EuGH bisher kaum geklärt.[15] Einigkeit herrscht mit Blick auf Artikel 52 Abs. 3 ECGR, dass Artikel 7 ECGR wie der nahezu wortgleiche Artikel 8 EKMR auszulegen ist.[16] Artikel 8 ECGR hingegen basiert nur – zumindest laut den „Explanations of the European Charter of Fundamental Rights" – auf Artikel 8 EKMR. Seine Funktion gegenüber Artikel 7 ECGR wirft noch viele Fragen auf.[17] Auf einen möglichen Lösungsansatz wird am Ende dieses Beitrags eingegangen. Artikel 8 EKMR enthält vier verschiedene Rechte, die sich teilweise überschneiden: Der Schutz des Privat- und des Familienlebens, der Wohnung sowie von Korrespondenzen.[18] Besondere Probleme bei der Schutzbereichsbestimmung bereitet der hier relevante Bereich des Privatlebens. Der EGMR legt das Merkmal

8 Siehe „Opinion 03/2013 on purpose limitation" der Art. 29-Datenschutzgruppe herunterladbar unter http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf, S. 11.

9 Vgl. die Auflistung bei v. *Zezschwitz*, a.a.O., Rn. 3.

10 Siehe etwa die Studie „Innovationspotenzialanalyse für die neuen Technologien für das Verwalten und Analysieren von großen Datenmengen Big Data Management)", S. 9 bis 11, herunterladbar unter http://www.dima.tu-berlin.de/fileadmin/fg131/Publikation/BDM_Studie/StudieBiDaMa-online-v2.pdf.

11 Siehe z. B. *Grözinger* unter http://www.mixxt.de/ressourcen/blog/2015/01/12/die-aussagekraft-von-heat-maps/.

12 Siehe *Eifert*, Zweckvereinbarkeit statt Zweckbindung als Baustein eines modernisierten Datenschutzes, in: Rechtswissenschaft im Wandel, Tübingen 2007.

13 Siehe „Opinion 03/2013 on purpose limitation", a.a.O., Seite 3.

14 Vgl. *Britz*, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Offene Rechtswissenschaft, Tübingen 2010; *Bäcker*, Grundrechtlicher Informationsschutz gegen Private, in: Der Staat – Band 51, 2012, S. 91 ff.

15 Siehe die Rechtsprechung des EuGH einerseits in EuGH, Schecke gg. Land Hessen vom 9. November 2010 (C- 92/09 und C-93/09) cip. 47 and 52, EuGH, Digital Rights gg. Irland vom8. April 2014 (C293/12 and C594/12), cip. 29, und EuGH, Gonzalez gg. Google vom 13. Mai 2014 (C-131/12), cip. 68, 69, and 97, jeweils auf Artikel 7 und 8 ECGR referierend, andererseits in EuGH, Telekom gg. Deutschland vom5. Mai 2011 (C-543/09), cip. 49, 52 and 53, EuGH, SABAM gg. Scarlet vom 24. November 2011 (C-70/10), cip. 50, und EuGH, ASNEF/FECEMD vom 24. November 2011 (C- 360/10), cip. 24 and 48, nur auf Artikel 8 ECGR; *Albers*, Umgang mit personenbezogenen Informationen und Daten, in: Neue Verwaltungsrechtswissenschaft, München 2012, Rn. 43 bis 45; zum Stand im Jahr 2009 *Britz*, EuGRZ 2009, S. 8 bis 9.

16 Statt vieler *Kokott und Sobotta*, International Data Privacy Law, 2013, Vol. 3, No. 4, S. 222 ff, herunterladbar unter http://idpl.oxfordjournals.org/content/3/4/222.full.pdf+html.

17 Vgl. Explanations of the European Charter of Fundamental Rights, 2007/C 303/02, bezüglich Artikel 7 und 8; Albers, a.a.O., Rn. 43 bis 45; *Kranenborg*, Art. 8 Protection of Personal Data, in: The EU Charter of Fundamental_Rights, Oxford and Portland, Oregon 2014, Rn. 8.24; anders u. a. wohl Bernsdorff, Art. 8 Schutz personenbezogener Daten, in: Charta der Grundrechte der Europäischen Union, Baden-Baden 2014., Rn. 13 und 17.

18 *Frowein*, Europäische MenschenRechtsKonvention, Kehl 2009, Rn. 1.

kasuistisch aus.[19] Ein maßgebliches Abgrenzungskriterium ist, ob die fraglichen Lebensbereiche der Öffentlichkeit oder der Privatsphäre zuzurechnen sind. Auf Schwierigkeiten stößt diese Abgrenzung bei sog. Teil-Öffentlichkeiten bzw. bei der Verwendung von allgemein zugänglichen Informationen in neuen bzw. anderen Kontexten.[20] In diesen Fällen stellt der EGMR häufig auf den Schutz des Einzelnen ab, dass mit seinen Daten nur das geschieht, was er vernünftiger Weise erwarten darf („reasonable expectation").[21] Er untersucht eine Verletzung dieser Gewährleistung in der Regel nach dem Kriterienbündel, ob die Daten 1.) unter Verstoß einer besonderen Vertraulichkeitserwartung erlangt wurden (z. B. weil sich der Betroffene zu Hause befunden oder Telekommunikationsmedien benutzt hat), 2.) ein privater oder öffentlicher Anlass vorliegt und 3.) nur eingeschränkt genutzt oder veröffentlicht werden.[22] Ein weiteres wichtiges Kriterium ist, ob der Betroffene überhaupt in der Lage ist oder war, die Erhebung seiner Daten durch entsprechendes Verhalten zu vermeiden (abgelehnt im Fall eines gesetzlichen Durchsuchungsrechts für die Polizei im öffentlichen Raum).[23]

Demgegenüber gewährleistet das deutsche Grundgesetz die „informationelle Selbstbestimmung". Das BVerfG prüft seine Verletzung durch private Akteure im Ergebnis danach, ob der Betroffene eine Wahl- bzw. Kontrollmöglichkeit hatte. Diese Schutzkonzeption rückt die Einwilligung als Instrument der Ausübung der informationellen Selbstbestimmung in ihr Zentrum.[24] Das Gericht prüft im Einzelnen, ob der Betroffene 1.) auf die Leistung, die er im Gegenzug auf die Preisgabe seiner Daten erhält, verzichten könnte (was es bei einer privaten Berufsunfähigkeitszusatzversicherung für Berufstätige verneint hat), ob er 2.) über den Markt auf eine vergleichbare Leistung eines anderen Anbieters ohne erzwungene Datenpreisgabe ausweichen könnte und ob 3.) die Datenpreisgabe – vorausgesetzt dass sie die Persönlichkeitsentfaltung des Betroffenen tiefgreifend berührt – ohne jegliche Kontrollmechanismen erfolgt (wie z. B. eine Möglichkeit, die Datenpreisgabe im Einzelfall überprüfen zu können).[25]

Wird diesen Prüfschemata gefolgt und liegt danach keine Verletzung der Gewährleistungsgehalte vor, insbesondere weil der Betroffene die Datenerhebung vermeiden kann, kommt es auf eine Rechtfertigung durch widerstreitende grundrechtlich geschützte Interessen noch gar nicht an.

19 *Wildhaber*, in: IntKommEMRK, Köln (Loseblattsammlung), Rn. 96 bis 98.

20 *Wildhaber*, a.a.O., Rn. 114 ff. und 323.

21 Ähnlich *Schweizer*, DuD 2009,S. 466 .

22 Siehe etwa EGMR, Case of Perry vs. the United Kingdom vom 17. Juli 2003 (application no. 63737/00), Rn. 40, 41, and 43; EGMR, Case of Peck vs. the United Kingdom vom 28. Januar 2003 (application no. 44647/98), Rn. 61 und 62; EGMR, Case of P.G. and J.H. vs. The United Kingdom vom 25. September 2001 (application no. 44787/98), Rn. 57; jeweils mit weiteren Nachweisen zur vorangegangenen Rechtsprechung.

23 EGMR, Case of Gillan and Quinton vs. the United Kingdom vom 12. Januar 2010 (application no. 4158/05), Rn. 65; EGMR, Case of M.S. vs. Sweden vom 27. August 1997 (74/1996/693/885), Rn. 32.

24 BVerfG, Schweigepflichtentbindung vom 23. Oktober 2006 (1 BvR 2027/02), Rn. 31 bis 34.

25 BVerfG, Schweigepflichtentbindung vom 23. Oktober 2006 (1 BvR 2027/02), Rn. 35 bis 61; die Kriterien aufgreifend *Bäcker*, a.a.O., S. 105 bis 108 mit weiteren Nachweisen zur Kritik.

4 Funktion von Erlaubnis- und Verbotstatbeständen

Weder nach Artikel 8 EKMR bzw. Artikel 7 ECGR noch nach dem deutschen Grundgesetz – insoweit allerdings nur in Bezug auf den privaten Sektor – ist also eine Speicherung und Verarbeitung personenbezogener Daten generell verboten.[26] Eine Art grundsätzliches Verbot mit Erlaubnisvorbehalt ist soweit nicht verfassungsrechtlich zwingend.[27] Eine Verletzung der Gewährleistungsgehalte ergibt sich vielmehr nach dem oben dargestellten Kriterienbündel bzw. Prüfungskatalog. Der Gesetzgeber kann jedoch bestimmte – teils deklaratorische – Erlaubnis- oder Verbotstatbestbestände bestimmen, um für typische Datenverarbeitungskontexte eine höhere Rechtssicherheit zu schaffen. Als typische Erlaubnisnormen bieten sich die speziellen in den Datenschutzrichtlinien oder im BDSG genannten Erlaubnistatbestände an (insofern aber nicht die Generalklausel der „berechtigten Interessen", die als solche keine höhere Rechtssicherheit schafft).[28] Denn der Betroffene kann beispielsweise in der Tat vernünftiger Weise erwarten, dass seine Daten, die im Rahmen der Begründung eines Vertrags erhoben werden, auch für die Durchführung dieses Vertrags verwendet werden (vgl. § 28 Abs. 1 Nr. 1 BDSG sowie Art. 7 lit. b) der Richtlinie 95/46/EC).[29] Verbotsnormen können sich wiederum auf Verwendungskontexte beziehen, die unter keinen Umständen als rechtmäßig denkbar sind. Als Beispiel mag der Fall dienen, dass sich ein Arbeitgeber Daten über eine Bewerberin zu deren Einkaufsverhalten verschaffen möchte, um die Wahrscheinlichkeit einer Schwangerschaft zu berechnen.[30] Die Verwendung der Daten zu diesem Zweck käme einer Umgehung des Rechts der Bewerberin gleich, ihre etwaige Schwangerschaft vor dem Arbeitgeber zu leugnen. Eine solche Datenverwendung, könnte durch einfaches Recht – zumindest klarstellend – ausgeschlossen werden.[31]

5 Zweckangabe als Selbstregulierungsmechanismus

Das Beispiel zeigt, dass der Gesetzgeber nicht alle gegenwärtigen Kontexte und schon gar nicht alle Zukünftigen vorhersehen und über Erlaubnis- oder Verbotstatbestände rechtlich abbilden kann.[32] Neben Auffangklauseln (die für ihre Auslegung die oben genannten Kriterien bereitstellen könnten) liegt es also nahe, Regelungsinstrumente einzusetzen, die nicht auf bestimmte Kontexte setzen, sondern selbst-regulierende Prozesse steuern.[33] Als solche Regelungsinstrumente können das Prinzip der Zweckspezifizierung sowie das darauf aufbauende Prinzip der Zweckbindung verstanden werden.[34] Wird das Prinzip der Zweckspezifizierung als eine Pflicht verstanden, die Zwecke dem Betroffenen gegenüber anzugeben, führt diese im Lichte des Schutzguts der „reasonable expectation" dazu, dass die Erwartung des Betroffenen durch die Zweckangabe selbst gestaltet wird. Solange der Betroffene weiß, zu welchen Zwecken seine Daten verarbeitet werden und er grundsätzlich in der Lage ist, die Datenerhebung durch sein Verhalten zu vermeiden, liegt also keine Verletzung vor (s. o. mit Verweis auf die entsprechenden Entscheidungen).[35] Ähnlich verhält es sich unter Zugrundelegung des Schutzgutes der "informationellen Selbstbestimmung" bezogen auf den privaten Sektor.[36] Auch das Bundesverfassungsgericht prüft, ob der Betroffene die Datenerhebung grundsätzlich vermeiden bzw. beeinflussen konnte. In den meisten Fällen werden die Zwecke der vorgesehenen Datenverarbeitung im Wege der Einwilligung durch den Betroffenen akzeptiert. Nur wenn das Gericht zu dem Ergebnis kommt, dass der Betroffene auf die mit der Datenerhebung verbundene Leistung unbedingt angewiesen war, auf dem Markt auf keine „datenschutzfreundlichere" Alternative zurückgreifen konnte und die Erbringung der Leistung an die Einwilligung gekoppelt ist, verneint es die Wahlmöglichkeit des Betroffenen, weil diese nur scheinbar verwirklicht wurde.[37]

6 Zweckfremde Verarbeitung und Rechtfertigungsspielraum

Auch nach diesem Verständnis kann die Zweckangabe zu einer Einschränkung der Weiterverwendung der Daten führen. Zumindest spricht das Schutzkonzept von Artikel 8 EMRK bzw. Artikel 7 ECGR dafür, dass in dem Augenblick, in dem der Datenverwender dem Betroffenen die zukünftigen Datenverwendungskontexte angegeben hat, der Betroffene erwarten kann, dass seine Daten nur für diese Zwecke und keine anderen verwendet werden. Damit ergeben sich aus dem Gewährleistungsgehalt von Artikel 8 EMRK bzw. Artikel 7 ECGR erste Konturen des Zweckbestimmungs- und Zweckbindungsprinzips. Nach deutscher Konzeption ergibt sich die Zweckbindung aus dem Selbstbestimmungsrecht, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."[38] Dieses würde unterlaufen, wäre die Weiterverwendung nicht an die ursprüngliche Zweckangabe gebunden. Werden die Daten trotzdem zu anderen als den angegebenen Zwecken verwendet, kann dies nun eine Verletzung der jeweiligen Gewährleistungsgehalte darstellen. Diese mag aber durch widerstreitende, verfassungsrechtlich geschützte Interessen gerechtfertigt sein. Für die Güterabwägung könnte man auf Seiten des Betroffenen wieder das zu

26 Zum deutschen Recht *Gusy*, Informationelle Selbstbestimmun und Datenschutz: Fortführung oder Neuanfang?, in: KritV 2000, S. 60; *Buchner*, Informationelle Selbstbestimmung im Privatrecht., Tübingen 2006, S. 79 ff; *Bäcker*, a.a.O., S. 99 bis 101.

27 *Masing*, NJW 2012, S. 2307; a. A. wohl *Karg*, DuD 2013, S. 78.

28 Vgl. *Buchner*, a.a.O., S. 96 ff. und 175; weniger kritisch gegenüber Auffangklauseln *Bäcker*, a.a.O., S. 99 bis 101.

29 Vgl. *Bechler*, Informationseingriffe durch intransparenten Umgang mit personenbezogenen Daten, Halle-Wittenberg 2010.

30 Siehe etwa http://www.welt.de/wirtschaft/webwelt/article114121023/Wie-die-Sammler-von-Big-Data-uns-durchleuchten.html.

31 Vgl. *Buchner*, a.a.O., S. 116.

32 Vgl. etwa *Bäcker*, a.a.O., S. 100; ebenso *Buchner*, a.a.O., S. 97.

33 *Hoffmann-Riem*, Selbstbestimmung in der Informationsgesellschaft, AöR 123 1998, S. 527.

34 Grundlegend *Albers*, a.a.O., Rn. 121 bis 129; *Bäcker*, a.a.O., S. 98.

35 Ähnlich *Bechler*, a.a.O., S. 110 bis 113.

36 Vgl. *Bechler*, a.a.O., S. , 20 und 21 sowie 115 ff. zu der durch das BVerfG konstatierten Gewährleistung, dass „jeder einigermaßen wissen können muss, was sein soziales Umfeld bzw. seine Kommunikationspartner über ihn weiß/wissen"; zum spezifischen Gewährleistungsgehalt der „internen Entfaltungsfreiheit" *Britz*, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, a.a.O., S. 571 bis 573; auf dem Instrument der sog. subjektiven Zweckbindung aufbauend *Forgó/Krügel/Rapp*, Zwecksetzung und informationelle Gewaltenteilung, Baden-Baden 2006, S. 37 bis 39.

37 Siehe BVerfG, Schweigepflichtentbindung vom 23. Oktober 2006 (1 BvR 2027/02), Rn. 33.

38 BVerfG, Volkszählungsurteil (1 BvR 209, 269, 362, 420, 440, 484/83), Rn. 173, und BVerfG, Schweigepflichtentbindung (1 BvR 2027/02), Rn. 31.

Artikel 8 EMRK bzw. Artikel 7 ECGR genannte Kriterienbündel anwenden: Der Eingriff wirkt umso stärker, als die Daten keine öffentliche, sondern eine private Angelegenheit betreffen und je breiter oder vielfältiger die Weiterverwendung angelegt ist. Das Bundesverfassungsgericht stellt zur Bestimmung der Intensität von Eingriffen in das Grundrecht auf informationelle Selbstbestimmung regelmäßig auf die Umstände der Datenerhebung (z. B. heimlich, offen oder im öffentlichen Raum)[39], die Bedeutung der Daten für den Betroffenen (gemessen an der Art der Daten als auch der bezweckten Verwendung)[40] und die konkreten Nachteile ab (sowohl für den Betroffenen als auch für die Gesellschaft als Ganzes)[41]. Eine absolute Grenze zieht es durch ein Umgehungsverbot. Danach darf die Zweckänderung in keinem Fall dazu führen, dass der Verwender der Daten diese nun verarbeiten kann, obwohl er sie ursprünglich beim Betroffenen nicht hätte erheben dürfen (siehe das obige Beispiel der Umgehung des Rechts zur Lüge der Schwangeren).[42] Diese Grundsätze wurden zwar primär für das Verhältnis Bürger-Staat entwickelt, könnten aber für die Bestimmung der Zulässigkeit bzw. Intensität von Eingriffen durch Private grundsätzlich übertragen werden.[43]

Ist die Zweckänderung nicht generell ausgeschlossen, gilt grundsätzlich: Je intensiver der Eingriff desto gewichtiger müssen die gegenläufigen Interessen der privaten Verwender der Daten an einer Zweckänderung sein.[44] Auch hier steht es dem Gesetzgeber frei, Falltypen herauszubilden. So kann er in Fällen, in denen typischerweise die Verarbeiterinteressen das Vertrauen des Betroffenen, dass die Daten ausschließlich für die angegebenen Zwecke verwendet werden, und gegebenenfalls weitere seiner grundrechtlich geschützten Interessen überwiegen, Zweckänderungen über Erlaubnistatbestände zulassen.[45] Umgekehrt kann er – etwa bei Vorliegen einer besonderen, abstrakten Gefahr – auch eine strikte Zweckbindung einführen und so die Möglichkeit ausschließen, dass die Daten in anderen Kontexten verwendet werden; unabhängig davon, ob konkrete Grundrechtsgefahren vorliegen.[46] Eine solche besondere abstrakte Gefahr ist etwa denkbar für besonders sensible Datentypen wie Gesundheitsdaten.[47] Und er kann schließlich Mittelwege einschlagen, indem er Kriterien für die Bestimmung einer Zweckvereinbarkeit im Rahmen einer Einzelfallbetrachtung zur Verfügung stellt.[48] In jedem Fall kommt es auf eine Abwägung der kollidierenden, grundrechtlich geschützten Interessen an.

7 Präzisionsgrad der Zweckangabe

Bevor sich jedoch mit der Frage nach den Regelungsmöglichkeiten für Zweckänderungen befasst wird, ist zu klären, wie präzise die Zwecke angegeben werden müssen. Denn je weiter die ursprüngliche Zweckangabe formuliert ist, desto weniger ist eine Zweckänderung für einen anderen als den ursprünglich vorgesehenen Kontext erforderlich.[49] Tatsächlich wird diese Frage häufig am Beispiel der „Marketingzwecke" oder des „Zwecks zur Weitergabe an Dritte" diskutiert, ohne dass die Diskussion durchweg überzeugende Kriterien für die Bestimmung des Präzisionsgrads der Zweckangabe hervorgebracht hätte.[50] Während das Bundeverfassungsgericht immerhin auf die Überschaubar- und damit Kontrollierbarkeit der Datenverwendung durch den Betroffenen abstellt, gibt der Europäische Gerichtshof keine weiteren Kriterien für die Zweckbestimmung vor.[51] Ein wichtiger Grund dafür kann in der einseitigen Ausrichtung von Datenschutz auf „privacy" oder „informationelle Selbstbestimmung" liegen. Denn solange das Datenschutzrecht nur die Schutzgüter der „reasonable expectation" oder der "informationellen Selbstbestimmung" des Betroffenen schützt, muss es streng genommen ausreichen, die genannten Zwecke in dieser Allgemeinheit anzugeben.[52] Denn dann weiß der Betroffene bzw. hat er darüber selbst bestimmt, dass seine Daten eben für Marketingzwecke verwendet oder an Dritte weitergegeben werden.

Teils zu Recht wird gegen diese allgemeinen Zweckangaben eingewandt, dass der Betroffene so nicht in der Lage ist, die Folgen der Datenverwendung abzuschätzen.[53] Das BVerfG scheint zwar Kriterien für die Zweckangabe bereitzustellen. So verweist es in ständiger Rechtsprechung darauf, dass die Zwecke „bereichsspezifisch und präzise" bestimmt sein müssen.[54] Allerdings ergingen die meisten dieser Urteile in Hinsicht auf Datenverarbeitungen durch den Staat. Dieser ist in der Lage, seine Zwecke über einen Rückgriff auf den in den einfachen Gesetzen meist tatbestandlich ausdifferenzierten Rechtsgüterschutz zu bestimmen.[55] Auch die Nachteile für den Betroffenen lassen sich über die entsprechenden Rechtsfolgen vorhersehen (meistens betreffen diese ohnehin die typischen Zwangs- bzw. Beugungsmittel).[56] Demgegenüber steht datenverarbeitenden Unternehmen auf dem privaten Sektor kein solcher Rückgriff zur Verfügung und die potentiellen Fol-

39 BVerfG, Telekommunikationsüberwachung vom 14. Juli 1999 (1 BvR 2226/94), Rn. 192.

40 BVerfG, Rasterfahndung vom 4. April 2006 (1 BvR 518/02), Rn. 91.

41 BVerfG, Großer Lauschangriff vom 3. März 2004 (1 BvR 2378/98), Rn. 230; BVerfG, Rasterfahndung vom 4. April 2006 (1 BvR 518/02), Rn. 103 und 106.

42 BVerfG, Vorratsdatenspeicherung vom 2. März 2010 (1 BvR 256/08, 1 BvR 263/08 und 1 BvR 586/08), Rn. 236 mit weiteren Nachweisen.

43 Vgl. *Bäcker*, a.a.O., S. 101 bis 104; ähnlich bezüglich der Einwilligung *Masing*, a.a.O., S. 2308.

44 Vgl. zum Interessenausgleich auf dem privaten Sektor *Bäcker*, a.a.O., S. 108 bis 111.

45 Siehe grundsätzlich der aktuelle Artikel 6 Abs. 4 des Ratsentwurfs der Datenschutz-Grund-VO sowie ebenfalls sehr weitgehenden Regelungen zur Zweckänderung in § 28 Abs. 2 und Abs. 5 S. 2 BDSG.

46 Vgl. zur abstrakten Gefahr *Britz*, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, a.a.O., S. 578 f.

47 Vgl. *Mehde*, Datenschutz, in: Handbuch der Europäischen Grundrechte, München 2006, Rn. 24.

48 Siehe der aktuelle Artikel 6 Abs. 3a des Ratsentwurfs der Datenschutz-Grund-VO sowie Artikel 6 Abs. 1 b) der aktuell noch geltenden Datenschutzrichtlinie 95/46/EC.

49 Vgl. *Forgó/Krügel/Rapp*, a.a.O., S. 34; *Mehde*, a.a.O., Rn. 24.

50 Siehe nur die unterkomplexe Begründung des Urteils des LG Berlin, Verbraucherverband gg. Apple vom 30. April 2013 (Geschäftszeichen 15 O 92/12); ebenfalls auf diesen Schwachpunkt des Zweckbestimmungserfordernisses hinweisend *Mehde*, a.a.O., Rn. 24.

51 BVerfG, Schweigepflichtentbindung, a.a.O., Rn. 43; EuGH, Telekom gg. Deutschland, a.a.O., Rn. 66 and 67.

52 Vgl. die wenigen Ansätze, operationalisierbare Maßstäbe für die Bestimmung der Zwecke herzuleiten z. B. *Hoffmann*, Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes, Baden-Baden 1991, oder *Forgó/Krügel/Rapp*, a.a.O.

53 Siehe nur *Simitis*, in: Kommentar zum Bundesdatenschutzgesetz, Baden-Baden 2014, Rn. 77.

54 BVerfG, Volkszählungsurteil vom 15. Dezember 1983 (1 BvR 209, 269, 362, 420, 440, 484/83), Rn. 161.

55 Auch die Literatur orientiert sich letztlich an den Aufgaben bzw. Funktionen der Verwaltung, siehe *Hoffmann*, a.a.O., S. 76 ff., sowie *Forgó/Krügel/Rapp*, a.a.O., S. 35 f. m. w. N.

56 Vgl. *Eifert*, a.a.O.; BVerfG, Kennzeichenerfassung vom 11. März 2008 (1 BVR 2047/05 and 1 BvR 1254/07), Rn. 98 bis 178; BVerfG, Kontostammdaten vom 13. Juni 2007 (1 BvR 1550/03), Rn. 79 bis 124; BVerfG, Telekommunikationsüberwachung vom 14. Juli 1999 (1 BvR 2226/94), Rn. 180 und 181; BVerfG, Großer Lauschangriff vom 3. März 2004 (1 BvR 2378/98), Rn. 307 bis 319; BVerfG, Rasterfahndung vom 4. April 2006 (1 BvR 518/02), Rn. 145 bis 149.

gen sind schwerer vorherzusehen, da der Informationsfluss aufgrund der Vielfältigkeit der Akteure, ihrer Handlungen und Verflechtung in einer freien Marktwirtschaft kaum abschließend beschrieben werden kann.[57]

Um dieser Komplexität mit einem entsprechend differenzierten Maßstab für die Bestimmung der Zwecke zu begegnen, wird in diesem Beitrag die Lösungsmöglichkeit in den Raum gestellt, ob nicht nur die Erwartung bzw. die Selbstbestimmung des Betroffenen, sondern alle verfassungsrechtlich geschützten Risikosphären, sprich Kontexte, herangezogen werden sollten. Damit würde beispielsweise nicht nur die Privatsphäre des Betroffenen, sondern auch seine allgemeine Handlungsfreiheit und, präziser noch, seine speziellen Freiheitsrechte als Maßstab für die Bestimmung der Zwecke relevant. Auch seine Gleichheitsrechte kämen in Betracht.[58] So könnte Preisdiskriminierung über Ausspähen des Surfverhaltens unter Rückgriff auf die Privatautonomie, oder die fehlerhafte Verarbeitung von Informationen durch den Arbeitgeber über die Berufsfreiheit begegnet werden. Der Rückgriff auf den gesamten Grundrechtskatalog legt selbst eine Antwort auf die Frage nahe, auf welche Perspektive für die Zweckbestimmung abzustellen ist: Gibt der Datenverwender nur seine operativen Zwecke des Datenumgangs an, berücksichtigt er nicht die Gefahren für den Betroffenen.[59] Andererseits schätzen die Betroffenen die Gefahren oft unterschiedlich ein, so dass der Verwender sie nur schwer an dessen Stelle vorhersagen kann.[60] Demgegenüber scheint der Rückgriff auf die Gesamtheit des Grundrechtskatalogs eine objektivierte Perspektive auf die Gefahren für den Betroffenen zu erlauben, die der Datenverwender für seine Beurteilung heranziehen kann.

Ein solches Verständnis würde keinen Widerspruch zu den durch den European Court of Justice bzw. das Bundesverfassungsgericht entwickelten Schutzkonzepten, sondern deren Präzisierung darstellen. Eine solche Präzisierung wäre in der Rechtsprechung sogar angelegt.[61] So stellt auch das Bundesverfassungsgericht bei der Feststellung darauf ab, ob überhaupt ein staatlicher Eingriff in den Schutzbereich des Rechts auf informationelle Selbstbestimmung vorliegt, ob nach dem Zweck sowie dem übergreifenden Kontext der Datenverarbeitung eine spezifische Gefahr für die Freiheiten des Betroffenen bzw. seine Interessen zu befürchten ist.[62] Auch bei der Prüfung der Eingriffsintensität zieht es heran, welche Nachteile für den Betroffenen durch die Datenverarbeitung zu erwarten sind (s. o.).

8 Möglicher Lösungsweg – Grundrechte als Maßstab für Zweckbestimmung

Selbst wenn der hier vorgeschlagene Lösungsansatz – insbesondere in Hinsicht auf die weiteren Datenschutzinstrumente, die für den Schutz der verschiedenen grundrechtlichen Gewährleistungsgehalte erforderlich sind – noch nicht im Detail ausgearbeitet ist, spricht zumindest auch die Systematik der ECGR für ein solches Verständnis. Denn hier ist der Datenschutz in Artikel 8 ECGR aus dem Privacy-Schutz in Artikel 7 ECGR ausgelagert bzw. abgekoppelt.[63] Sein Regelungsgehalt ließe sich damit nicht nur auf Artikel 7 ECGR, sondern auch auf die anderen Grundrechte beziehen. Diese Bezugnahme würde zudem verhindern, dass mit fortschreitender Digitalisierung immer mehr Lebensbereiche, die ursprünglich durch die verschiedenen Freiheitsrechte abgebildet wurden, vom grundrechtlichen Datenschutz überlagert werden. Hintergrund ist, dass mit zunehmender Digitalisierung soziale Interaktion immer mehr auf Basis automatischer Datenverarbeitung stattfindet. Ein Datenschutzgrundrecht, dass sich mit einem inhaltlich unabhängigen Gewährleistungsgehalt an die Stelle dieser Freiheitsrechte setzt, würde eine differenzierte Abwägung der widerstreitenden Interessen, insbesondere eine Anknüpfung an die Rechtsprechung verhindern, die den Interessenausgleich der widerstreitenden Grundrechte über Jahrzehnte fortentwickelt hat.[64] Der hier vorgeschlagene Ansatz würde also eine differenzierte Anwendung der datenschutzrechtlichen Schutzinstrumente bzw. Auslegung des einfachen Datenschutzrechts ermöglichen.

In Hinsicht auf die Zweckbindung bleibt festzuhalten, dass Artikel 8 ECGR nach seinem Wortlaut diese nicht verlangt. Vielmehr gibt er nur vor, die Zwecke der Datenverarbeitung zu spezifizieren. Wird der Schutz der „reasonable expectation" aus Artikel 8 EMRK aufgegriffen – auf dem Artikel 8 ECGR immerhin basiert – so ließe sich diese Spezifizierungspflicht als Regulierungsmechanismus für die Gewährleistungsgehalte der anderen Grundrechte verstehen. Die für ihren Schutz erforderlichen Instrumente hängen dann von dieser Zweckbestimmung ab. Dabei kann die Zweckbestimmung zunächst als reiner Anknüpfungspunkt für die Beurteilung der jeweiligen Grundrechtsgefährdung gesehen werden.[65] Wird er darüber hinaus als Pflicht verstanden, die Zwecke dem Betroffenen gegenüber anzugeben, so würde diese Angabe die Erwartung des Betroffenen auf seinen Grundrechtsschutz und damit dessen Umfang ausgestalten. In Bezug auf Artikel 7 ECGR könnte Artikel 8 ECGR so in der Tat als lex specialis angesehen werden, weil die durch Artikel 7 ECGR geschützte Vertraulichkeitserwartung des Betroffenen entfällt, wenn ihm Umstand und Zweck der Datenerhebung vorweg angegeben werden.[66] Die Gewährleistungsgehalte der anderen Grundrechte gäben hingegen vor, wie präzise die Zweckangabe entsprechend ihrer Gefährdung zu erfolgen hat bzw. welche weiteren Schutzinstrumente vorzusehen sind. Mit diesem Regulierungsmechanismus wäre Artikel 8 ECGR als ein eigenständiger, neben Artikel 7 ECGR neu aufgenommener Gewährleistungsgehalt anzusehen.[67]

Für dieses Verständnis von Artikel 8 ECGR mit seiner Pflicht zur Zweckbestimmung bzw. Zweckangabe als Regulierungsmechanismen sprechen zumindest die eben genannten Argumente. Wie weit diese trotz der nur mittelbaren Grundrechtswirkung auch für den privaten Sektor gelten, muss soweit noch offen bleiben.[68] Grundsätzlich muss der Gesetzgeber die Regelungsinstru-

57 Vgl. hierzu *Bäcker*, a.a.O., S. 100.
58 Vgl. *Albers*, a.a.O., Rn. 69 ff; *Britz*, a.a.O., S. 569 bis 574.
59 Vgl. *Mehde*, a.a.O., Rn. 24 a. E.
60 Vgl. *Masing*, a.a.O., S. 2308.
61 *Gusy*, a.a.O., S. 53 ff.
62 BVerfG, Telekommunikationsüberwachung vom 4. April 2006 (1 BvR 518/02), Rn. 69; BVerfG, Kontostammdaten vom 13. Juni 2007 (1 BvR 1550/03), Rn. 67 bis 69.
63 *Marauhn*, Recht auf Achtung des Privat- und Familienlebens, in: Handbuch der Europäischen Grundrechte, München 2006, Rn. 42.
64 *Kronenberg*, a.a.O., Rn. 08.102; a. A. jedoch *Mehde*, a.a.O., Rn. 24.
65 *Albers*, a.a.O., Rn. 123.
66 Vgl. *Bernsdorff*, a.a.O., Rn. 13 und 17, und *Mehde*, a.a.O., Rn. 11 und 13.
67 Vgl. *Mehde*, a.a.O., Rn. 32.
68 Vgl. statt vieler *Szczekalla*, Funktionen der Grundrechte, in: Handbuch der Europäischen Grundrechte, München 2006, Rn. 17.

mente für den privaten Sektor so wählen, dass sie die grundrechtlich geschützten Interessen der durch den Datenumgang Betroffenen mit denen der datenverwendenden Unternehmen in einen Ausgleich bringen.[69] Je nach Gefährdungslage durch den Datenumgang bzw. nach Intensität des Regulierungseingriffs kann sich die Einführung eines präventiven Verbots mit Erlaubnisvorbehalt, die Pflicht zur Zweckbestimmung, Zweckangabe oder sogar zur Zweckbindung als richtig oder unverhältnismäßig erweisen.[70]

9 Klarstellung in der Grund-Verordnung als Auslegungshilfe

In Hinsicht auf die Ausgangsfragen kann das Folgende festgehalten werden: Grundsätzlich steht es dem Gesetzgeber frei, Verwendungskontexte deklaratorisch als erlaubt oder verboten zu benennen, entweder weil sie schon keinen Eingriff bzw., vice versa, einen Eingriff darstellen und unter keinen Umständen gerechtfertigt werden können. Er kann das Erfordernis aus Artikel 8 Abs. 2 ECGR im Sinne einer Pflicht zur Zweckangabe auch auf den privaten Sektor übertragen (wofür seine Strukturierungsfunktion für selbstregulatorische Prozesse spricht). Und er kann im Gegenzug Erlaubnistatbestände für Zweckänderungen schaffen bzw. für Verwendungskontexte, die der Betroffene nicht vermeiden kann – vorausgesetzt dass die Interessen des Verwenders die des Betroffenen typischer Weise überwiegen.[71] Das kann etwa dann der Fall sein, wenn die Datenverarbeitung nicht auf die Individualisierung einer Person abzielt bzw. keine Gefahr für die spätere Verwirklichung ihrer Grundrechte bedeutet. Viele Big Data-Anwendungen könnten so erlaubt sein, selbst wenn die Daten zu anderen Zwecken ursprünglich erhoben wurden und durch den Verwender nicht in (bereits) anonymisierter Form bezogen werden. Das mag zum Beispiel für die eingangs beschriebenen Social Heat Maps gelten.

Was den grundsätzlichen Entwurf der GDPR betrifft, hat sich der Gesetzgeber für den privaten Sektor sowohl für ein präventives Verbot mit Erlaubnisvorbehalt als auch für das Erfordernis der Zweckangabe entschieden. Zweites stellt jedoch weniger einen Selbstregulierungsmechanismus anstelle von Erlaubnistatbeständen, sondern eine neben deren abschließende Auflistung hinzutretende Anforderung für Datenerhebungen dar. In einem zweiten Schritt stellt der eingangs bezeichnete Regelungsentwurf auch für Zweckänderungen Erlaubnistatbestände auf. Die Deckungsgleichheit der Erlaubnistatbestände für Datenerhebungen und Zweckänderungen lässt jedoch daran zweifeln, ob bei der Zweckänderung wirklich eine Abwägung dahingehend stattgefunden hat, dass die Interessen des Datenverarbeiters das Vertrauen des Betroffenen auf die Zweckbindung sowie weitere grundrechtlich geschützte Interessen typischer Weise überwiegen. Denn aufgrund der Deckungsgleichheit scheint es sich sowohl für Datenerhebungen als auch für Zweckänderungen um dieselben Erwägungen zu handeln – was aufgrund der unterschiedlichen Bedeutung für die Grundrechte des Betroffenen überraschend ist.

Vor diesem Hintergrund besteht das Problem des VO-Entwurfs weniger darin, dass er keine strikte Zweckbindung vorsieht, sondern in der fehlenden Differenziertheit ihrer Regelungsinstrumente in Bezug auf die Grundrechtsbetroffenheit.[72] Einerseits unterstellt sie jede Erhebung und Verarbeitung personenbezogener Daten einem Erlaubnisvorbehalt, obwohl viele Datenerhebungen keine konkrete Gefahr auslösen.[73] Andererseits lässt der genannte Entwurf Zweckänderungen zu fast denselben Gründen zu, auch wenn hier der Betroffene die Weiterverarbeitung noch nicht einmal vorhersehen und vermeiden kann (selbst Einwilligungen werden von den Zweckänderungsmöglichkeiten – zumindest nicht ausdrücklich – ausgenommen)[74]. Einerseits verlangt sie, die Zwecke anzugeben, andererseits stellt sie keine Kriterien für die Bestimmung ihres Präzisionsgrads auf. Immerhin verweist Artikel 6 Abs. 3a lit. d) des bezeichneten Entwurfs für Zweckänderungen aufgrund legitimer Interessen auf die „*possible consequences of the intended further processing for data subjects*". Aber auch hier gibt es letztlich keinen Maßstab, um die rechtliche Relevanz der Folgen zu ermitteln. Ungeachtet der Frage, ob das Regelungssystem der GDPR im Ganzen oder die Zweckangabe – geschweige denn eine strikte Zweckbindung – auf dem privaten Sektor sinnvoll ist, möchte dieser Beitrag einen Lösungsvorschlag zumindest für das Problem der Undifferenziertheit machen. Dieser könnte durch eine Klarstellung in Artikel 1 der VO begegnet werden, dass die VO nicht dem Datenschutz an sich, sondern der Verwirklichung aller Grundrechte des durch die Datenverarbeitung Betroffenen dient. Seine Privatheits-, Freiheits- und Gleichheitsrechte könnten damit gleichermaßen für die Bestimmung der Zwecke herangezogen werden. So ließe sich der Vielgestaltigkeit der mit Innovationen verbundenen Gefahren über die Auslegung der teils sehr restriktiven, teils sehr weiten Erlaubnistatbestände differenziert begegnen.

10 Schluss

Angesichts der Geschwindigkeit, mit der sich datenbasierte Technologien, Geschäftsmodelle und Gewohnheiten der Nutzer fortentwickeln, ist es keine leichte Aufgabe, ein Gesetz zu schaffen, das den Ausgleich zwischen Rechtsgüterschutz und Innovationsoffenheit an sich und zudem für einen längeren Zeitraum findet.[75] Die Lösung mag zwischen mehr statischen Erlaubnis- und/oder Verbotsklauseln sowie prozessoffenen Selbstregulierungsmechanismen liegen. In jedem Fall wird die weitere Entwicklung des Rechts auf „privacy" und Datenschutz in den Artikeln 7 und 8 ECGR sowie ihres Zusammenspiels – wie auch des Rechts auf informationelle Selbstbestimmung – mit Spannung zu erwarten sein.

69 Vgl. *Masing*, a.a.O., S. 2301, sowie unter Punkt 6 „Der materielle Aspekt der Entscheidung: Der Grundsätzliche Vorrang des allgemeinen Persönlichkeitsrechts" bei Unterpunkt c) auf http://www.verfassungsblog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh/; a. A. *Karg*, a.a.O., S. 78.

70 Vgl. *Hoffmann-Riem*, a.a.O., S. 527.

71 Dass weder das Erfordernis der Zweckangabe, noch die strikte Zweckbindung für den privaten Sektor zwingen ist, *Masing*, a.a.O., S. 2307.

72 Besonders auf eine differenzierte Anwendung der Regelungsinstrumente „nach Sektoren, Verarbeitungsbereichen, Zwecken und der Sensitivität der Daten" abstellend bereits *Trute*, JZ 1998, Der Schutz personenbezogener Daten in der Informationsgesellschaft, S. 826 und 827.

73 Vgl. kritisch zur Verrechtlichung durch Datenschutzrecht *Hoffmann-Riem*, a.a.O., S. 514 ff.

74 Siehe für den Fall der schuldvertraglichen Einwilligung die gemäß der deutschen §§ 315 ff. BGB eingeschränkten einseitigen Bestimmungsrechte.

75 *Hoffmann-Riem*, a.a.O., S. 537 und 538.