Florian Oppitz

Persönlichkeitsrechte statt Datenschutz

1. Der Datenschutz droht sich zu verselbständigen. Der Bestand an Daten und die Verfügung über Daten, die Quelle von Information und die Verwendung von Informationen werden geschützt ohne Rückbezug auf ihre Funktion oder ihren Nutzen. Daten werden behandelt wie Eigentum, und das ist problematisch.

Eigentum ist nämlich ein Recht des willkürlichen Gebrauchs und des Ausschlusses anderer davon. § 354 ABGB definiert Eigentum als „Befugnis, mit der Substanz und den Nutzungen einer Sache nach Willkür zu schalten, und jeden anderen davon auszuschließen." Eine Eigentümerin kann gemäß § 362 ABGB die „Sache nach Willkür benützen oder unbenützt lassen ... sie vertilgen, ganz oder zum Teile auf andere übertragen, oder unbedingt sich derselben zu begeben, das ist, sie verlassen".

Die Konstruktion des Schutzes von Daten oder Informationen analog zum Schutz der Person oder des Eigentums funktioniert nicht. Eine personenbezogene Information ist etwas anderes als die Person selbst, die Verfügung über eine Ansammlung von Daten etwas anderes als das Eigentum an einer Sache. Schon die Konstruktion des Eigentums als Schutzgut in Augenhöhe mit der Person warf und wirft Fragen der Abwägung auf, die immer wieder zu eigenartigen Ergebnissen führen. Bei Beschädigungen oder Enteignungen gebührt Ersatz, die Ausbeutung meiner Arbeitskraft muss ich hinnehmen.

Informationen sind keine Sachen, keine Gegenstände. Sie sind fast ohne Kosten beliebig oft reproduzierbar, sie lassen sich teilen wie Brot und Fische am See Genezareth. Ich kann sie gleichzeitig hergeben und behalten. Das Urheberrecht behandelt das Recht an Informationen als absolutes Recht, wie das Recht an Sachen. Ich kann jeden so vom Gebrauch meiner Informationen abhalten, als würde ich durch diesen fremden Gebrauch in meinen eigenen Gebrauchsmöglichkeiten eingeschränkt.

2. Es soll hier aber nicht das Urheberrecht im Zeitalter der technischen Reproduzierbarkeit diskutiert werden, sondern eine Klarstellung auf der Ebene der Grundbegriffe erreicht werden. Ist das Recht auf Datenschutz einem absoluten Recht vergleichbar oder existiert es nur in Bezug auf andere Rechtsgüter? Als absolutes Recht schützt es jede Art der personenbezogenen Information, stellt es in die Willkür der bezogenen Person, wie mit „ihren“ Daten umgegangen werden darf. Das ist der Standpunkt des deutschen Grundrechts auf informationelle Selbstbestimmung.

Als funktionsbezogenes Recht schützt das Recht auf Datenschutz dagegen bestimmte Rechtsgüter, typischerweise zusammengefasst als Persönlichkeitsrechte. Zu diesen Rechtsgütern gehören beispielsweise die freie Entfaltung der Persönlichkeit oder der Schutz der Privatsphäre. Das ist der Standpunkt des EGMR oder des österreichischen Datenschutzgesetzes. Im Folgenden möchte ich diese beiden Sichtweisen – die des Grundgesetztes einerseits und andererseits der MRK – näher darstellen. Im Anschluss daran wird die Kritik der Willkür im Datenschutz fortgeführt.

3. Werfen wir zunächst einen Blick auf das Recht auf informationelle Selbstbestimmung. Dieses Recht wurde als Grundrecht durch das deutsche Bundesverfassungsgericht entwickelt. Es gilt als Teil des durch Art 2 Abs 1 iVm Art 1 GG verbürgten allgemeinen Persönlichkeitsrechts. Art 2 Abs 1 GG lautet: „Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt“.

Die „freie Entfaltung der Persönlichkeit“ wird vom BVerfG einerseits als allgemeine Handlungsfreiheit (etwas nach eigenem Willen zu tun oder zu lassen) und eben als allgemeines Persönlichkeitsrecht verstanden. Der allgemeinen Handlungsfreiheit soll nicht näher nachgegangen werden, hier interessiert vor allem das Persönlichkeitsrecht.

Das BVerG definiert das allgemeine Persönlichkeitsrecht als Grundrecht, das „die engere persönliche Interessenssphäre und die die Erhaltung ihrer

Grundbedingungen“ schützt (E 54,148/153; 72,155/170). Innerhalb dieses Bereiches lassen sich wieder einzelne konkrete Garantien unterscheiden (vgl. Epping, Grundrechte^{2}, 250ff; Pieroth/Schlink, Grundrechte. Staatsrecht II^{14}, 85ff; Stern in: Stern (Hg) Das Staatsrecht der Bundesrepublik Deutschland, Band IV/1 Die Einzelnen Grundrechte, §99, S 190ff; Degenhart, Das allgemeine Persönlichkeitsrecht, JuS 1992, 361ff):

- Das Recht der Selbstdarstellung
- Der Schutz der Privatsphäre
- Das Recht auf freie Entfaltung
- Das Recht auf informationelle Selbstbestimmung

Das Recht der Selbstdarstellung umfasst das Recht am eigenen Bild, das Recht am eigenen Wort und den Schutz der persönlichen Ehre. Die Privatsphäre ist insbesondere in Hinblick auf die Intimsphäre (Sexualität) und das Familienleben geschützt. Zum Recht auf freie Entfaltung zählen die Privatautonomie und die Möglichkeit der Resozialisierung.

Mit dem Recht auf informationelle Selbstbestimmung anerkennt das BVerfG seit 1983 ein Recht „selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen“ (E 65, 1/43; 113, 29/46), eine Befugnis „grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden“ (E 65, 1/42). Dieses Recht sei besonders im Zeitalter der Informationstechnologie durch die Möglichkeit der Speicherung und Verknüpfung großer Datenmengen erforderlich: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“ (E 65, 1/43).

Das Recht auf informationelle Selbstbestimmung war beispielsweise berührt in den Fällen einer Rasterfahndung (E 115, 11), einer Erhebung von Telfonverbindungsdaten (E 115, 7), eines Lauschangriffs (E 109, 12), einer Online-Durchsuchung (E 120, 8), einer Section-Control (E 120, 10), einer Vorratsdaten-Speicherung (E 121, 1), einer zwangsweisen DNA-Abnahme (E 103, 2), einer Auskunft über Entmündigungen (E 84, 13) oder einer Volkszählung (E 65, 1).

Das Recht auf informationelle Selbstbestimmung wird als „Auffangrecht“ (Stern, 204; Pieroth/Schlink, 87) gesehen, das eine „Zusammenfassung aller auf Informationen über die Persönlichkeit und insbesondere über die Privatsphäre des Einzelnen bezogenen Aspekte des Persönlichkeitsrechts“ bewirkt (Murswieck, zitiert nach Stern aaO, 204) und „den informationellen Umgang des Staates mit den Bürgern umfassend unter Rechtfertigungszwang“ stellt (Pieroth/Schlink, 87).

4. Die EMRK kennt kein explizites Recht auf Datenschutz. Die meisten Aspekte eines solchen Rechts werden aber durch die Garantie des Schutzes der Privatsphäre in Art 8 MRK erfasst. Dessen Schutzbereich ist allerdings anders ausgestaltet als beim Recht auf informationelle Selbstbestimmung.

Art 8 MRK schützt nicht vor jeder Erhebung oder Verwendung von persönlichen Daten, sondern nur insofern, als dadurch das Privatleben beeinträchtigt werden könnte. Mit Wiederin (Art 8 MRK in: Korinek/Holubek, Österreichisches Bundesverfassungsrecht, Rz 32 ff; sowie § 190 Schutz der Privatsphäre in: Merten/Papier, Handbuch der Grundrechte, Band VII/1 Grundrecht in Österreich, Rz 35 ff) können vier „Pole des Privatlebens“ unterschieden werden:

- Identität,
- Integrität,
- Informationskontrolle,
- Interaktion.

Der Schutz der Identität umfasst den Schutz des eigenen Namens, der eigenen Geschlechtlichkeit und der eigenen Herkunft. Art 8 MRK schützt auch den Ausdruck der eigenen Identität, also die Entfaltung der Persönlichkeit, weshalb die Führung

eines besonderen Lebensstils (der Roma und Sinti etwa), die Gestaltung des eigenen Aussehens oder die Verwendung einer eigenen Sprache erfasst sind.

Als Schutz der Integrität garantiert das Grundrecht die körperliche und seelische Unverletzlichkeit. Der Schutz der Interaktion gewährleistet eine freie Entscheidung über die eigenen sozialen Kontakte seien sie intimer, freundschaftlicher oder geschäftlicher Natur. Geschützt sind die vertrauliche Kommunikation und die Interaktion zur Entfaltung der eigenen Identität, nicht aber schlechthin jede Art der Kommunikation.

Mit „Informationskontrolle“ wird nun der Bereich angesprochen, der am ehesten mit dem Recht auf informationelle Selbstbestimmung vergleichbar ist. Wiederin beschreibt diesen Aspekt als „Recht, alleine gelassen zu werden“ (Art 8 MRK, Rz 35), als Recht ohne fremde Kenntnisnahme zu leben. „Das Recht auf Achtung des Privatlebens sichert dem Bürger daher die Kontrolle über Informationen, die ihn und sein Verhalten betreffen“ (ebd). Entscheidend ist dabei ist nicht die räumliche Abgeschiedenheit, sondern ob in der konkreten Situation mit der Aufmerksamkeit Dritter zu rechnen ist, ob es sich also in der Sichtweise der Betroffenen um vertrauliche Kommunikation oder geheimes Verhalten handelt oder nicht.

Umstritten ist in diesem Zusammenhang die Frage, ob Art 8 vor Beobachtung privaten Verhaltens schützt, oder ob diese Bestimmung auch ein Grundrecht auf freie private Betätigung überhaupt einräumt. Ist es grundsätzlich (nur) verboten, von privatem Verhalten Kenntnis zu nehmen, oder ist es auch untersagt, privates Verhalten zu regulieren? Hier geht die überwiegende Ansicht (vgl VfSlg 12.689/1991) von einem weiten Schutzbereich aus, wird aber von Wiederin kritisiert, der nicht jedes private Verhalten von Art 8 erfasst sehen will, sondern nur solches, das „die eigene Identität und Integrität berührt“ (Art 8 MRK, Rz 36). Beiden Auffassungen gemeinsam ist allerdings die Verbindung des Grundrechtschutzes mit der Sphäre des Privaten. Nicht jede Information über einen Menschen ist geschützt (wie beim Recht auf informationelle Selbstbestimmung), sondern nur eine Information über private oder vertrauliche Angelegenheiten.

Entscheidungen zum Pol „Informationskontrolle“ des Rechts auf Privatleben betrafen etwa eine behördliche Sammlung persönlicher Daten (EGMR, 4.5.2000, *Rotaru*), ein Steuergesetz, das den Finanzämtern Zugang zu Kundinnendaten von Videoverleihen verschaffte (VfSlg 12.689/1991), Personendurchsuchungen (VfSlg 13.708/1994) oder erkennungsdienstliche Behandlungen (EGMR, 18.3.1981, *McVeigh*) samt Speicherung der dadurch gewonnenen Daten (VfGH 16.3.2001, B 1117/99). Auch die in Zusammenhang mit der deutschen Rechtsprechung genannten Fälle sind als Eingriffe in das Recht des Art 8 MRK anzusehen. Kein Eingriff wurde dagegen bei der Verpflichtung, einen Personalausweis bei sich zu haben (EKMR 9.9.1962, *Reyntsens*) oder beim Einsatz eines Lockspitzels zur Überführung eines Rauschgifthändlers (EGMR, 15.6.1992, *Lüdi*) angenommen.

5. Die Reichweite des österreichischen Grundrechts auf Datenschutz (§ 1 DSG) ist für die hier interessierende Frage der Funktionsgebundenheit unklar. Der Wortlaut des § 1 DSG gewährt einen Anspruch auf Geheimhaltung von „personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht“. Ein solches Interesse ist gemäß § 1 Abs 1 2. Satz DSG dann nicht anzunehmen, wenn die Daten allgemein verfügbar oder anonymisiert sind.

Die Frage ist nun, ob der Grundrechtsschutz ein besonderes schutzwürdiges Interesse voraussetzt, oder ob alle personenbezogenen Informationen, die nicht öffentlich sind, vom Grundrecht erfasst sind. Die Rechtssprechung musste diese Frage noch nicht entscheiden, die Forschung ist gespalten. Duschanek (§ 1 DSG in: Korinek/Holubek, Österreichisches Bundesverfassungsrecht, Rz 40 ff) will alle nicht öffentlichen personenbezogenen Daten als schutzwürdig behandeln und verweist diesbezüglich auf die Materialien. Dort heißt es: „Nach Abs 1 gibt es ein Recht auf Datenschutz nur dann, wenn ‚ein schutzwürdiges Geheimhaltungsinteresse (an bestimmten personenbezogenen Daten) besteht’. Dies setzt voraus, dass es überhaupt personenbezogene Daten gibt, die auf eine in ihrer Identität bestimmte (oder zumindest bestimmbare) Person zurückgeführt werden können, und dass diese Daten weiters geheim gehalten werden können, was dann grundsätzlich unmöglich sein wird, wenn sie allgemein zugänglich sind. Freilich bedarf dies der genauen Prüfung im Einzelfall, wobei vor allem auch zu beachten sein wird, ob die allgemeine Zugänglichkeit im Zeitpunkt der beabsichtigten Verwendung tatsächlich noch

besteht. An anderen Daten besteht ein schutzwürdiges Geheimhaltungsinteresse, das jedoch – wie jedes Grundrecht – nicht absolut gilt, sondern durch bestimmte, zulässige Eingriffe beschränkt werden darf“ (RV 1613 BlgNR XX. GP, S 34 f).

Wiederin (Aart 8 MRK, Rz 133ff) verweist dagegen auf den Wortlaut des § 1 DSG, der einen grundrechtlichen Schutz an das Vorliegen grundrechtlicher Interessen knüpft. Dieser Bezug bliebe in der Auslegung Duschaneks „inhaltsleer“, deshalb sei von einem engeren Schutzbereich auszugehen und das Vorliegen eines schutzwürdigen Geheimhaltungsinteressens von Fall zu Fall zu prüfen. Diese Schutzwürdigkeit wird – so wie in der Rechtssprechung zu § 1 DSG 1987 – durch Heranziehung der Wertungen der gesamten Rechtsordnung zu beurteilen sein, wobei dem in § 1 DSG 2000 genannten Schutz des Privat- und Familienlebens besonderes Gewicht zukommt.

6. Das deutsche Recht auf informationelle Selbstbestimmung wurde kürzlich durch den Hamburger Universitätsprofessor Karl-Heinz Ladeur einer grundsätzlichen Kritik unterzogen. Er bezeichnete dieses Grundrecht als „juristische Fehlkonstruktion“ (Ladeur, Das Recht auf informationelle Selbstbestimmung. Eine juristische Fehlkonstruktion?, DÖV 2/2009, 45ff).

Ladeur hält in diesem Aufsatz zunächst fest, dass das Recht auf informationelle Selbstbestimmung in der Interpretation des BVerfG als individuelles Abwehrrecht zu sehen ist, das vor Preisgabe und Verwendung persönlicher Daten bzw. der Offenbarung von persönlichen Lebenssachverhalten schützt. Bei der staatlichen Erhebung und Verwendung von personenbezogenen Informationen liege aber kein klassischer Eingriff in die Freiheit der einzelnen Bürgerinnen vor, sondern die elektronische Datenverarbeitung sei grundsätzlich etwas, was sich in der Sphäre des Staates abspielt. Schon auf dieser konzeptionellen Ebene ist deshalb Vorsicht geboten: Es ist etwas anderes, ob mich der Staat einsperrt, oder ob er mich beobachtet.

In einem nächsten Schritt kritisiert Ladeur die Sichtweise des Rechts auf informationelle Selbstbestimmung, die dieses Recht in Analogie zum Eigentumsschutz und nicht als Persönlichkeitsrecht interpretiert. Information sei nicht

Eigenbesitz des Individuums sondern verweise schon begrifflich auf andere: „Es gibt unendlich viele Informationen, die ein Individuum betreffen, und deshalb von ihm als Gegenstand der informationellen Selbstbestimmung in Anspruch genommen werden könnten, die zugleich so sehr auf andere verweisen, dass ein enges Verständnis diese Grundrechts, da es Informationen als Eigenbesitz des Individuums zurechnen würde, in informationelle Fremdbestimmung umschlagen würde“ (Ladeur, 48). Es wird ein eigentumsartiges Recht an etwas (den Informationen) begründet, da es seinem Wesen nach gar nicht einer Person allein zugeordnet werden kann. „Niemand kann das Recht für sich in Anspruch nehmen, eine Information, die stets eine Relation zu einer Sache oder zu einer andern Person zum Ausdruck bringt, gänzlich seiner Selbstbestimmung zu unterwerfen“ (Ladeur, 49).

Als Folge dieser Fehlkonstruktion sei das Recht auf informationelle Selbstbestimmung „völlig substanzlos“ geworden, es habe „jede Bestimmbarkeit verloren“ (Ladeur, 49). Weil es zu viel erfassen will, verliert es seinen Schutzbereich aus den Augen: „Es erschöpft sich in einem unberechenbaren Recht auf subjektive Willkür. Gegenstand dieser Willkür ist die Inanspruchnahme von *individueller* Selbstbestimmung über die *soziale* Wirkung von Information. ‚Informationelle *Selbst*bestimmung’ wird in einer zirkulären Wendung von jeder ‚Sache’ gelöst und selbst zum Schutzgut stilisiert“ (Ladeur, 49).

Hat aber wirklich jede Information mit Personenbezug einen Eigenwert, der in einer grundrechtlichen Abwägung zu berücksichtigen ist (vgl Ladeur, 51)? Ladeur nennt als Konsequenz dieser Auffassung den Schutz eines Diebes, der mit einem GPS-geschützten Auto davonfährt, vor polizeilicher Ermittlung seines Aufenthaltsortes, und den Schutz einer Person, die unter Verstoß gegen Urheberrecht Daten aus dem Internet herunterlädt, vor Ermittlung ihrer IP-Adresse.

Gegen diese begriffliche Uferlosigkeit schlägt Ladeur eine Interpretation des GG vor, die ohne Recht auf informationelle Selbstbestimmung auskommt. In Bezug auf sensible Daten solle der Datenschutz dem jeweils einschlägigen Grundrecht als „prozedurale Komponente“ (Ladeur, 54) zugeordnet werden. Die Religionsfreiheit könne so vor einer staatlichen Erhebung der Religionszugehörigkeit schützen, die Versammlungsfreiheit vor der Speicherung von Versammlungsdaten oder das Recht

auf Gesundheit vor einer Weitergabe von medizinischen Daten. Diese Lösung scheint eng verwandt zu sein mit der oben geschilderten Interpretation des österreichischen Rechts auf Datenschutz, die jeweils ein „schutzwürdiges Interesse“ daran fordert – solche Interessen sind jedenfalls durch Grundrechtspositionen gegeben.

Einem Großteil dessen, was als Eingriff in das Recht auf informationelle Selbstbestimmung angesehen wird, fehle aber – so Ladeur – in Wirklichkeit die individualrechtliche Komponente. In vielen Fällen staatlicher Datenverarbeitung gäbe es niemanden, der in einer grundrechtlich relevanten Intensität persönlich betroffen ist. In wessen Rechtsposition werde etwa bei einer Rasterfahndung eingegriffen? Es wäre unsinnig anzunehmen, dass Personen, deren Daten im Rahmen einer solchen Fahndung erfasst werden, unter „Generalverdacht“ (53) stünden, vor dem sie zu schützen wären. Wegen dieser fehlenden individuellen Betroffenheit schlägt Ladeur vor, den Datenschutz in diesen Fällen als „Risikorecht“ zu organisieren, wie es aus dem Bereich des Umwelt- oder Technikrechts bekannt sei. Datenschutz sei nach dem Muster der „Risikovorsorge“ zu gestalten, vor staatlicher Datenverarbeitung sei ein „Konzept“ oder eine „Strategie“ zu verlangen, deren Rationalität dann über die Zulässigkeit der Datenerhebung und -verwendung entscheidet. Die Einhaltung dieser Konzepte bzw. Strategien könne von einer unabhängigen Datenschutzbeauftragten überwacht werden.

Grundsätzlich müsse Abschied genommen werden von der einfachen Entgegensetzung gefährlicher Staat – gefährdete Bürgerin. Die Informationstechnologien bieten gerade auch (privaten) kriminellen neue, erweiterte Handlungsmöglichkeiten, vor denen der Staat die Bürgerinnen zu schützen habe - auch durch die Verfügung über personenbezogene Daten.

7. Im Rahmen dieser Arbeit kann der Risikorecht-Ansatz Ladeurs nicht weiter verfolgt werden. Stattdessen wird seine grundsätzliche Kritik am Recht auf informationelle Selbstbestimmung noch einmal aufgegriffen und mit der Rechtslage der MRK und des DSG in Beziehung gesetzt.

Kern der Kritik Ladeurs ist seine Analyse, das BVerfG und die ihm folgende Forschung behandelten das Recht auf informationelle Selbstbestimmung als Eigentumsrecht statt als Persönlichkeitsrecht. Information würde den Menschen zugerechnet wie ein absolutes Recht, nach Willkür die Adressantinnen zu selektieren und andere auszuschließen. Konsequent zu Ende gedacht ist damit jedes „über eine andere reden“ ein Eingriff in ihr Grundrecht, da personenbezogene Informationen, die dieser anderen „gehören“, dabei verwendet werden.

Über die Kritik Ladeurs hinaus kann auch bemerkt werden, das die Eigentums-Struktur von Information, das umfassende Verfügungsrecht über persönliche Daten, als Konsequenz ihrer Transformation in die Warenform angesehen werden kann. Als Ware funktioniert Information nur mit exklusiven Verfügungsrechten, mit Rivalität und Ausschließbarkeit im Konsum. Diese „Eigenschaften“ kommen der Information nicht von Natur aus zu, sie sind soziale Fiktionen.

Für viele Bereiche hat diese Transformation negative externe Effekte. Die Warenform der Information führt zum Marktversagen. Für den demokratischen politischen Prozess ist die offene Debatte ein wesentlicher Erfolgsfaktor. Die Wissenschaft lebt von der Zugänglichkeit und Kritisierbarkeit ihrer Aussagen. Die Kunst stirbt, wenn sie nicht mehr gesehen oder gehört wird. In allen diesen Bereichen führt nur die frei verfügbare Information zu den effizientesten Verfahren und besten Ergebnissen.

Gegen die Sichtweise des Rechts auf informationelle Selbstbestimmung als absolutem Recht sprechen somit nicht nur die damit verbundene konzeptionelle Unschärfe, sondern auch ihre eigene Logik: Der absolute Datenschutz frisst sein Kind, die Zivilgesellschaft.

8. Datenschutz ist somit nicht als Eigentums-, sondern als Persönlichkeitsrecht zu konstruieren, und das bedeutet: Es ist die Frage nach der Funktion des Schutzes zu stellen. Warum sollen bestimmte personenbezogene Informationen vor Zugriff und Verwendung geschützt werden. Es ist im Einzelnen zu begründen, wenn ein Wissen über jemand anderen, wenn eine Information über eine Person der Allgemeinheit (dem Staat, oder anderen Privaten) entzogen werden soll.

Dieses Begründungserfordernis kommt sowohl in der Rechtsprechung des EGMR als auch im § 1 DSG zum Ausdruck als Rückbezug des Grundrechtsschutzes auf „schutzwürdige Interessen“ bzw auf das Privatleben. Nun ist das Problem aber nicht gelöst, in Wirklichkeit beginnt es erst. Die Umstände grundrechtswürdigen Datenschutzes sind noch zu klären, die besonderen Interessen, die in der grundrechtlichen Abwägung eine Rolle spielen sollen, sind noch zu definieren.

Dabei ist das Menschenbild, das einem weiten Verständnis des Datenschutzes zugrunde liegt, doch ein wenig merkwürdig. Die einzelnen Menschen sollen in einen Kokon versponnen werden, der sie von der Welt abschirmt und nur das nach außen treten lässt, was sie freiwillig absondern. Das gute Leben sieht aber anders aus, eine alte und ehrwürdige Tradition der Sozialphilosophie würde es sogar umgekehrt sehen und das Leben in Gemeinschaft, in der Öffentlichkeit als das dem Menschen ganz entsprechende wählen. Unser Wort „Idiot“ stammt von einem griechischen Begriff, der den bezeichnete, der immer zu Hause blieb.

Was wird nun das Private in Zukunft sein? Ist es in Gefahr, von der Informationstechnologie verschlungen zu werden, oder sind wir im Begriff, unsere Ansicht von der Grenze zwischen Privatsphäre und Öffentlichkeit mit Hilfe der Technik zu ändern. Unser Menschenbild steht damit in Frage.

Zunächst muss betont werden, dass diese Flüssigkeit eines sozialen Begriffes nichts Neues ist. Das private Leben hat eine Geschichte. Was vor hundert Jahren als privat galt, ist es heute nicht mehr und umgekehrt. Aber – um die Frage zu wiederholen – wie wird es weitergehen? Vieles spricht dafür, dass sich die Grenze zwischen dem Vertraulichem und dem Allgemeinen verschiebt. Im Magazin der Süddeutschen Zeitung war vor kurzem zu lesen:

„Als das französische Magazin *Le Tigre* vor einigen Monaten ein sogenanntes Google-Porträt veröffentlichte, die detaillierte, unverhüllte Lebensgeschichte eines Menschen, die nur aus dessen Spuren im Internet zusammengesetzt war, reagierte der Porträtierte geschockt. In Zeitungsinterviews bekannte der junge Architekt aus Bordeaux, nach Veröffentlichung des Artikels kaum mehr schlafen zu können, und kündigte einen Prozess gegen das Magazin wegen Verletzung der Privatsphäre an.

Dieses Ansinnen musste der Architekt, ein besonders aktiver Nutzer des Web 2.0 (er hatte über die Jahre allein 17 000 Fotos auf die Datenbank Flickr gestellt), schon bald wieder verwerfen; es war sofort klar, dass es keine juristische Grundlage für seine Klage geben würde. Der Streit um den Artikel wurde in den Medien Anfang des Jahres weltweit gemeldet, erzählte dieses ‚Google-Porträt' doch eine faszinierende Geschichte: Vielleicht zum ersten Mal hatte jemand die Probe aufs Exempel gemacht und die Informationen, die jeder Nutzer freiwillig oder unfreiwillig im Internet hinterlässt, vor allem in den sozialen Netzwerken, zu einer intimen Biografie verdichtet" (Süddeutsche Zeitung, Magazin, Heft 29/2009).

Auf einen anderen Aspekt der neuesten Entwicklungen rund um den Wandel unseres Menschenbildes wies Viktor Mayer-Schönberger hin, der von einem Verlust des Vergessens angesichts der dauernden Verfügbarkeit vergangener Online-Inhalte spricht: „Seit Beginn der Menschheitsgeschichte war es für uns Menschen sehr einfach, Dinge zu vergessen, und relativ schwer, uns an sie zu erinnern – dazu benötigte man Zeit und Geld. Durch die digitalen Technologien hat sich dieses Verhältnis umgekehrt. Heute ist es schwer und zeitaufwendig zu vergessen, und extrem einfach und fast kostenlos, sich zu erinnern. Die Festplatte und Programme wie Outlook erledigen das für uns. Deshalb muss man sich die Frage nach dem Stellenwert des Vergessens stellen. Wie wichtig ist es für unser Leben? Es ist nicht nur für unser Privatleben enorm wichtig. Menschen, die nicht vergessen können, sind sehr krank. Sie können keine Entscheidung mehr treffen, denn es kommen ihnen alle Fehlentscheidungen der Vergangenheit in den Sinn und sie sind dadurch wie gelähmt. Das Vergessen hat also die Funktion, uns handeln zu lassen, indem es vergangene Fehler, aber auch Erfolge verblassen lässt. Auch die Fehltritte anderer verblassen, und man wird mit der Zeit fähig, zu vergeben. Und das erlaubt den Menschen und den menschlichen Gesellschaften, wieder zueinander zu finden und neu anzufangen. So muss man sich die Frage stellen, ob nicht das Vergessen, auch das gesellschaftliche, eine gewisse Funktion erfüllt. (…) Wenn wir Regulierungsmechanismen schaffen, die es den Menschen ermöglichen, selbst zu bestimmen, wie tief und wie lange sie sich im Internet einklinken wollen, dann werden sie die dort gebotene Vielfalt sozusagen ‚maßgeschneidert' nutzen können. Daher bin ich für eine differenzierte Regulierung, die den Einzelnen in die Lage versetzt, selbst Entscheidungen zu treffen"

(in: Wiener Zeitung, Interview, 4.10.2008; zitiert nach dem Online-Archiv der Wiener Zeitung).

Die Menge der synchron und diachron verfügbaren personenbezogenen Daten nimmt also zu und ist einer größeren Zahl von Personen zugänglich als jemals zuvor. Die möglichen Konsequenzen aus dieser Situation, die sich für den Datenschutz ergeben, bewegen sich zwischen zwei gegensätzlichen Polen.

Einerseits, als konservative Option, könnte auf dem traditionellen Ansatz des Datenschutzes behaart werden. Das hätte zur Folge, dass überlegt werden müsste, ob auch für den Bereich privater Preisgabe und Nutzung personenbezogener Daten Schutzpflichten des Staates bestehen. Soll es Regelungen gäben, die den Upload und Download in sozialen Online-Netzwerken beschränken? Soll der Staat die Löschung von privaten Daten gegen den Willen der Betroffenen erzwingen können?

Andererseits, als risikofreudige Option, könnte das Datenschutzrecht die Änderungen des Menschenbildes, die Neudefinition des Privaten nachvollziehen. Das würde eine Verkleinerung des Schutzbereiches nach sich ziehen, eine allgemein freiere Verfügbarkeit personenbezogener Daten. Aber diese Diskussion befindet ich wohl in einem zu frühen Stadium, um bereits konkrete Handlungsempfehlungen ableiten zu können.

Abschließend bleibt festzuhalten: Datenschutz ist kein Selbstzweck. Datenschutz kann dem Schutz von Persönlichkeitsrechten dienen, Datenschutz kann aber auch der Entfaltung der Persönlichkeit im Weg stehen.