Benedikt Buchner

Die Einwilligung im Datenschutzrecht

– vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument

Klassischerweise kommt der Einwilligung die Funktion eines Rechtfertigungsgrunds zu – wer in eine Verletzung seiner Rechtsgüter einwilligt, schließt damit die Rechtswidrigkeit dieser Verletzung aus, egal ob es um Freiheit, körperliche Unversehrtheit oder informationelle Selbstbestimmung geht. Gerade im Fall der informationellen Selbstbestimmung aber kommt der Einwilligung darüber hinaus zunehmend auch eine andere, neue Funktion zu, nämlich die eines Kommerzialisierungsinstruments. Mittels Einwilligung macht sich der Einzelne den wirtschaftlichen Wert seiner personenbezogenen Daten zunutze, er willigt in eine Verarbeitung seiner personenbezogenen Daten ein, um dafür im Gegenzug auch vom Datenverarbeiter eine Leistung (Werbegeschenke, Rabatte, kostenlose Online-Dienste etc.) zu erhalten. Die Einwilligung stellt so betrachtet die Gegenleistung in einem gegenseitigen Vertragsverhältnis dar, es kommt zu einem Tausch „Einwilligung gegen Leistung". Der folgende Beitrag behandelt die rechtlichen Fragestellungen, die mit einer solchen Entwicklung einhergehen.

1 Das Tauschmodell „Einwilligung gegen Leistung"

Beispiele dafür, wie die Einwilligung als Instrument zur Kommerzialisierung der eigenen Daten eingesetzt wird, gibt es viele – vor allem in der Online-Welt. Zahlreiche der sog. „kostenlosen" Angebote in der Online-Welt sind tatsächlich nicht kostenlos, sondern haben sehr wohl ihren Preis, wenn auch nicht in Geld, sondern stattdessen in Form einer Preisgabe persönlicher Informationen: Microsoft beispielsweise bietet sein Betriebssystem auch kostenlos an, wenn man sich im Gegenzug mit einer Online-Protokollierung und Auswertung der eigenen Rechneraktivitäten einverstanden erklärt.[1] Soziale Netzwerke wie studiVZ, Facebook oder MySpace lassen uns „kostenlos" Mitglied in ihren Online-Communities werden, dafür willigen wir im Gegenzug aber darin ein, dass unsere personenbezogenen Daten zu Marketingzwecken verarbeitet werden. Online-Dienste, allen voran Google, bieten ihre gesamte Palette an Dienstleistungen – Email-Account, Suchmaschine, personalisierter Nachrichtendienst – kostenlos an, protokollieren dafür aber das Online-Verhalten ihrer Nutzer und werten dieses aus. Und auch in der Offline-Welt gibt es genügend Beispiele dafür, wie Daten als Tauschgegenstand eingesetzt werden, allen voran das Beispiel der Kundenkarten wie Payback oder Happy Digits, mittels derer wir kostenlos Punkte sammeln und diese in Prämien eintauschen können, dafür im Gegenzug aber darin einwilligen, dass unser Einkaufsverhalten protokolliert und zu Marketingzwecken ausgewertet wird.[2]

Kurzum, das Tauschmodell „Leistung gegen Einwilligung" gewinnt immer mehr an Bedeutung und Verbreitung; die Einwilligung rückt mehr und mehr in das Zentrum vertraglicher Austauschverhältnisse und wird zu einer Hauptleistung im gegenseitigen Vertrag. Diese Entwicklung wiederum wirft für das Datenschutzrecht die Frage auf, ob und wie auf diesen Bedeutungswandel der Einwilligung zu reagieren ist. Zu klären ist insbesondere, welche Rolle die Einwilligung in einem datenschutzrechtlichen Regelungsgefüge überhaupt einnehmen soll, ob und wie das Tauschmodell Leistung gegen Einwilligung mit der Grundidee einer Freiwilligkeit der Einwilligung vereinbar ist und wie sichergestellt werden kann, dass die Einwilligung auch tatsächlich ein Ausdruck echter Selbstbestimmung über die eigenen

Prof. Dr. Benedikt Buchner, LL.M. (UCLA)

Geschäftsführender Direktor des Instituts für Gesundheits- und Medizinrecht (IGMR), Universität Bremen
E-Mail: bbuchner@uni-bremen.de

1 Sog. „Windows Feedback Program"; https://wfp.microsoft.com/Welcome.aspx.

2 Siehe dazu ausführlich auch Wagner (in diesem Heft).

Daten ist. Notwendig ist insbesondere ein datenschutzrechtlicher Ansatz, der real existierende Schutzdefizite nicht willkürlich ausblendet, sondern einer schleichenden Aushöhlung des informationellen Selbstbestimmungsrechts effektiv entgegenwirkt. Zu weit würde es hingegen gehen, dem Datenschutzrecht auch eine erziehende Aufgabe dahingehend zuzusprechen, dass es Verbraucher generell von einer Kommerzialisierung ihrer Daten abhalten soll.

2 Die Rolle der Einwilligung in einem datenschutzrechtlichen Regelungsgefüge

§ 4 Abs. 1 BDSG weist der Einwilligung im Datenschutzrecht eine zentrale Rolle als Erlaubnistatbestand für die Verarbeitung personenbezogener Daten zu. Ausgangspunkt im Datenschutzrecht ist das grundsätzliche Verbot der Verarbeitung personenbezogener Daten. Personenbezogene Daten dürfen nicht verarbeitet werden, es sei denn dies ist ausnahmsweise erlaubt und zwar entweder aufgrund eines gesetzlichen Erlaubnistatbestands oder aufgrund einer Einwilligung des Betroffenen (§ 4 Abs. 1 BDSG). Gerade die Einwilligung erfährt jedoch als Erlaubnistatbestand viel Kritik: Oftmals sei eine solche Einwilligung gerade kein Ausdruck privatautonomer Selbstbestimmung, sondern vielmehr bloße „Fiktion", tatsächlich habe man oftmals gar keine andere Wahl als eine Einwilligung zu erteilen, man sei sich der Erteilung einer Einwilligung überhaupt nicht bewusst oder verstehe gar nicht, in was man überhaupt einwilligt.[3] Kurzum, der Vorwurf lautet, dass die Einwilligung oftmals gerade nichts mit einer gewollten, bewussten und informierten Entscheidung über den Umgang mit den eigenen Daten zu tun hat.

Der Umstand, dass die Einwilligung zunehmend als Instrument genutzt wird, um die eigenen Daten als eine Art von Zahlungsmittel einzusetzen, trägt sein Übriges dazu bei, dass der Einwilligung mit viel Skepsis begegnet wird. Die zunehmende Kommerzialisierung personenbezogener Daten ist für Kritiker ein weiterer Beleg dafür, dass die Einwilligung ein erhebliches Missbrauchspotential in sich trägt, gerade mit Blick auf all diejenigen, die schon für ein paar Rabattpunkte, Bonusmeilen oder sonstige Aufmerksamkeiten bedenkenlos bereit sind, die Vertraulichkeit ihrer Daten aufzugeben und in eine Verarbeitung ihrer personenbezogenen Daten einzuwilligen.[4]

Andererseits ist jedoch auch festzuhalten, dass es – zumindest aus der Perspektive der datenverarbeitenden Unternehmen – de lege lata oftmals überhaupt keine praktikable Alternative zum Erlaubnistatbestand der Einwilligung gibt. Datenverarbeiter sind auf eine verlässliche Legitimationsgrundlage für ihre Datenverarbeitung angewiesen und eine solche verlässliche Legitimationsgrundlage kann oftmals nur die Einwilligung bieten, nicht hingegen die gesetzlichen Erlaubnistatbestände. Nicht nur sind die konkreten Vorgaben gesetzlicher Erlaubnistatbestände oftmals mehr oder weniger unklar, sondern auch ist mitunter noch nicht einmal klar, welches Gesetz überhaupt einschlägig sein soll, in dem Datenverarbeiter dann nach einem gesetzlichen Erlaubnistatbestand für den konkreten Fall suchen könnten.

– Nur ein Beispiel hierfür: Ein Telekommunikationsunternehmen möchte sog. Dienste mit Zusatznutzen[5] anbieten, konkret seine Mobilfunk-Kunden per SMS über Restaurants, Wetter oder Verkehr informieren und zwar jeweils passend zu dem Ort, wo sich diese Kunden gerade aufhalten. Wenn dieses Unternehmen klären möchte, ob die mit einem solchen Informationsdienst einhergehenden Datenverarbeitungsvorgänge datenschutzrechtlich zulässig sind, muss es sich mit einer Vielzahl offener datenschutzrechtlicher Fragestellungen und damit letztlich mit einem ganz erheblichen Maß an Rechtsunsicherheit auseinandersetzen. Unklar ist schon, welches Gesetz überhaupt Anwendung finden soll. Zur Wahl stehen drei Gesetze: Bundesdatenschutzgesetz, Telekommunikationsgesetz und/oder Telemediengesetz. Für die Frage der Anwendbarkeit dieser Gesetze soll es darauf ankommen, welchen Dienst das Unternehmen anbietet – Telemediendienst, Telekommunikationsdienst und/oder sonstiger Dienst. Man wird dann feststellen müssen, dass der konkrete Informationsdienst viel zu komplex ist, als dass er sich einer dieser Kategorien klar zuordnen lassen würde, und wird sodann in einem nächsten Schritt auf das sog. Schichtenmodell ausweichen.[6] Nach diesem Schichtenmodell ist das Informationsangebot des Unternehmens in drei Schichten zu zerlegen: in eine Schicht des physikalischen Netzes (TKG), eine Schicht der Inhaltsdienste (TMG) und eine „oberste Schicht" (das dahinter stehende Vertragsverhältnis, zu dessen Vermittlung der Telemediendienst genutzt wird; BDSG).[7] Entsprechend muss also das Leistungspaket des Telekommunikationsunternehmens „aufgeschnürt" werden und anschließend jedes einzelne Leistungsmerkmal entsprechend eingeordnet werden[8] – all dies allein zu dem Zweck, überhaupt erst einmal feststellen zu können, welches Gesetz zur Anwendung kommen soll. Im Zweifel wird dann das Unternehmen in dem entsprechenden Gesetz ohnehin keinen gesetzlichen Erlaubnistatbestand für eine Datenverarbeitung finden, gerade wenn die Datenverarbeitung zu Marketingzwecken stattfinden soll. Oder aber ein möglicherweise einschlägiger Erlaubnistatbestand ist so vage formuliert, wie etwa im Falle der allgemeinen Interessenabwägungsklauseln, dass auch insoweit ein erhebliches Maß an Rechtsunsicherheit verbleibt.

Im Ergebnis präsentiert sich damit das geltende Datenschutzrecht als ein solch undurchschaubares Durch- und Nebeneinander an Regelungen, dass tatsächlich in vielen Konstellationen der Erlaubnistatbestand der Einwilligung die einzig verlässliche und praktikable Legitimationsgrundlage für eine Datenverarbeitung darstellt. Eben aus diesem Grund ist daher die Einwilligung in einem datenschutzrechtlichen Regelungsgefüge auch unverzichtbar, sie ist als Erlaubnistatbestand für die Datenverarbeitung von zentraler Bedeutung. Daher kann es auch von vornherein nicht darum gehen, die Einwilligung als solche in Frage zu stellen, sondern stattdessen allein darum, wie dieser zentralen Rolle der Einwilligung am besten Rechnung getragen werden kann, wie ins-

3 Siehe insbesondere die grundsätzliche Kritik bei Simitis in ders., BDSG (2006), § 4a Rdn. 3 ff.

4 Simitis a.a.O., Rdn. 5; ders. in Sokol, Neue Instrumente im Datenschutz (1999), S. 14 ff.; Däubler in ders./Klebe/Wedde/Weichert, BDSG (2007), § 4a Rdn. 1; siehe auch Wagner (in diesem Heft).

5 §§ 3 Nr. 5, 98 I TKG.

6 Zum Schichtenmodell als Instrument zur Abgrenzung der Anwendungsbereiche der verschiedenen datenschutzrechtlichen Regelungen siehe Eckhardt in Spindler/Schuster, Recht der elektronischen Medien (2008), § 91 TKG Rdn. 5; Schaar, MMR 2001, 644 (645).

7 Ausführlich Ranke, M-Commerce und seine rechtsadäquate Gestaltung (2004), S. 90 ff.

8 Eckhardt a.a.O.

besondere dafür Sorge getragen werden kann, dass die Einwilligung im Alltag der Datenverarbeitung eben nicht bloß eine Fiktion, sondern auch tatsächlich ein Ausdruck privatautonomer Selbstbestimmung ist.

3 Die Maxime der Freiwilligkeit einer Einwilligung

Eine der zentralen Maximen, die bei jeder Diskussion über das Für und Wider der Einwilligung zuallererst betont wird, ist die der Freiwilligkeit einer Einwilligung. Eine Einwilligung in die Verarbeitung personenbezogener Daten muss gemäß § 4a Abs. 1 S. 1 BDSG stets auf einer „freien Entscheidung des Betroffenen" beruhen. Nochmals konkretisiert wird dieses Freiwilligkeitsprinzip durch das sog. Koppelungsverbot, wie es nunmehr in § 28 Abs. 3b BDSG für die Einwilligung des Betroffenen in eine Datenverarbeitung für Zwecke des Adresshandels oder der Werbung normiert ist.[9] Die datenverarbeitende Stelle darf danach einen Vertragsschluss nicht von solch einer Einwilligung des Betroffenen abhängig machen darf, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Erfasst werden sollen mit diesem Koppelungsverbot die klassischen Konstellationen eines „take it or leave it", also die Konstellationen, in denen man sich mit der Datenverarbeitung zwar nicht einverstanden erklären „muss", in denen man aber, wenn man sich nicht einverstanden erklären sollte, dann eben auch keinen Vertrag bekommt – man also nicht Mitglied eines sozialen Netzwerks werden kann, kein Email-Konto bekommt oder keine Kundenkarte erhält. So betrachtet stellen all die Geschäftsmodelle, die auf der Idee „Leistung gegen Daten" fußen, zunächst einmal einen Verstoß gegen die Freiwilligkeitsmaxime dar und entsprechend geht auch der Vorwurf in der datenschutzrechtlichen Diskussion immer wieder dahin, dass das Freiwilligkeitsgebot insoweit missachtet wird.[10]

Andererseits stellt sich jedoch das Problem fehlender Freiwilligkeit nicht schon allein deshalb, weil die Bereitstellung einer Leistung von einer Einwilligung in die Datenverarbeitung abhängig gemacht wird. Zu einer Zwangssituation kommt es vielmehr erst dann, wenn gar keine Alternative besteht, also auch nicht die Alternative, eine Leistung überhaupt nicht in Anspruch zu nehmen. Solche Konstellationen gibt es durchaus, etwa bei der Wohnungsmiete, bei einer Kontoeröffnung, Versicherung oder beim Telefonanschluss. In solchen Situationen besteht tatsächlich ein Problem der Freiwilligkeit – ein Problem, das der BGH bereits vor mehr als 20 Jahren in seiner Schufa-Entscheidung angesprochen hat. Der BGH hat dort festgehalten, dass dann, wenn Betroffene auf einen Vertragsschluss *angewiesen* sind und dieser Vertragsschluss von einer Einwilligung in die Datenverarbeitung abhängig gemacht wird, tatsächlich keine echte Entscheidungsfreiheit mehr besteht, dass die Einwilligung vielmehr in einem solchen Fall zu einer „reinen Formalität absinkt".[11]

Anders ist es jedoch in den hier angesprochenen Konstellationen, in denen der Betroffene auf einen Vertragsschluss gerade nicht angewiesen ist, er also durchaus eine echte Entscheidungsfreiheit hat, nämlich die Freiheit, die Leistung *als ganze* in Anspruch zu nehmen oder eben nicht. Der Einzelne hat die Freiheit zu entscheiden, ob er beim Einkauf auf die Vertraulichkeit seiner Daten verzichten will oder stattdessen lieber auf die Kundenkarte mit ihren Bonuspunkten und Prämien. Er hat in der Online-Welt die Freiheit zu entscheiden, ob er unter Verzicht auf Vertraulichkeit kostenlose und besonders innovative Dienste in Anspruch nehmen möchte oder ob er stattdessen lieber auf datenschutzfreundlichere Angebote ausweichen möchte, mögen diese unter Umständen auch kostenpflichtig oder weniger innovativ sein. Und auch bei sozialen Netzwerken und Online-Communities wie studiVZ oder Facebook ist eine solche Entscheidungsfreiheit des Einzelnen zu bejahen, zumindest noch zu bejahen. Auch hier hat der Einzelne die Wahl, sich für oder gegen eine Mitgliedschaft in diesen Communities und Netzwerken zu entscheiden. Möglicherweise stellt sich dies in Zukunft irgendwann einmal anders dar, wenn soziale Netzwerke einmal ein unverzichtbarer Bestandteil unseres Soziallebens sein sollten. Solange dies aber noch nicht der Fall ist und man auch noch ohne Mitgliedschaft in einer Online-Community ein normales Sozialleben pflegen kann, stellt sich auch hier kein Freiwilligkeitsproblem, auch dann nicht, wenn eine Mitgliedschaft zwingend an die Erteilung einer Einwilligung geknüpft ist.

Festzuhalten bleibt im Ergebnis, dass in all den hier genannten Konstellationen die Koppelung zwischen Leistungserbringung und datenschutzrechtlicher Einwilligung kein Freiwilligkeitsproblem ist. Die datenschutzrechtliche Maxime der Freiwilligkeit einer Einwilligung darf insoweit nicht überstrapaziert werden. Zum Problem wird eine zwingende Verknüpfung von Leistungserbringung und Einwilligung vielmehr erst dann, wenn der Betroffene auch tatsächlich auf eine bestimmte Leistung angewiesen ist.[12]

4 Die Einwilligung als Ausdruck echter Selbstbestimmung

Das eigentliche Problem in all den angesprochenen Konstellationen ist regelmäßig nicht eines der Freiwilligkeit, sondern eines der *Transparenz*. In vielen Fällen ist die Einwilligung gerade deshalb nicht Ausdruck einer selbstbestimmten Entscheidung über die Datenverarbeitung, weil dem Einzelnen die Erteilung einer Einwilligung überhaupt nicht bewusst gemacht wird. Datenverarbeitende Unternehmen präsentieren ihre Leistung als „kostenlos", obwohl es sich der Sache nach eigentlich um einen gegenseitigen Vertrag in Form eines Tausches „Einwilligung gegen Leistung" handelt. Jedoch versuchen Unternehmen gezielt, diesen Tauschcharakter zu verschleiern, um die Gegenleistung einer Einwilligung möglichst unbemerkt zu bekommen.

9 Siehe § 28 Abs. 3b BDSG: „Die verantwortliche Stelle darf den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen nach Absatz 3 Satz 1 abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Eine unter solchen Umständen erteilte Einwilligung ist unwirksam."

10 Siehe etwa Menzel, DuD 2008, 400 (406); Iraschko-Luscher, DuD 2006, 706 (708); Schapper/Dauer, RDV 1987, 169 (170).

11 BGH, Urt. v. 19.9.1985 – III ZR 213/83 BGHZ 95, 362 (368) – Schufa-Klausel.

12 Ausführlich Buchner, Informationelle Selbstbestimmung im Privatrecht (2006), S. 267 ff.

4.1 Opt-in versus Opt-out

Um dieses Ziel zu erreichen, setzen Datenverarbeiter insbesondere auf eine Form der Vertragsgestaltung: das sog. Opt-out-Modell. Dieses Opt-out-Modell hat für Datenverarbeiter den Vorteil, dass es hier für die Annahme einer Einwilligung gerade keiner aktiven, bewussten Handlung seitens des Betroffenen bedarf. Die Einwilligung im Fall des Opt-out gilt vielmehr bereits von vornherein als erteilt, sie ist bereits entsprechend in einem Klauselwerk vorformuliert und es ist der Betroffene, der, wenn er mit einer Datenverarbeitung nicht einverstanden sein sollte, aktiv werden muss. Es ist der Betroffene, der, etwa durch ein Aus- oder Durchstreichen der Einwilligungsklausel, aktiv sein Nicht-Einverständnis mit der Datenverarbeitung zum Ausdruck zu bringen muss. Bleibt der Einzelne hingegen untätig, egal ob aus Nachlässigkeit, aus Unkenntnis oder vielleicht auch aus falsch verstandener Höflichkeit heraus, wird ihm eine Einwilligung in die Datenverarbeitung einfach so unterstellt.

Das Gegenmodell zu diesem Opt-out ist das Modell des Opt-in. Im Fall des Opt-in ist Nichts-Tun für den einzelnen Betroffenen datenschutzrechtlich „ungefährlich". Nichts-Tun fingiert hier gerade noch keine Einwilligung, vielmehr bedarf es für die Annahme einer Einwilligung der *aktiven, bewussten* Willensbetätigung des Betroffenen, etwa in Form eines Ankreuzens oder einer extra Unterschrift. Datenverarbeiter müssen entsprechend versuchen, den Betroffenen zu einer solchen aktiven Erteilung der Einwilligung zu bewegen, womit dann aber automatisch auch gewährleistet ist, dass sich der Betroffene einer Einwilligung in die Datenverarbeitung bewusst ist. Die Einwilligung wird bei Opt-in also in das Zentrum des Einigungsprozesses gestellt, dem einzelnen Betroffenen wird bewusst gemacht, dass er etwas nicht umsonst bekommt, sondern dass auch er im Gegenzug mit seiner Einwilligung eine Leistung erbringen muss. Das Modell des Opt-in ist damit also ein ganz wesentlicher Schritt hin zu mehr Transparenz, hin zur Schaffung von mehr Bewusstsein auf Seiten des Betroffenen, wenn es um das Tauschmodell Leistung gegen Einwilligung geht.

Umso bedauerlicher ist es daher, dass es der BGH in seiner Payback-Entscheidung vom 16. Juli 2008[13] abgelehnt hat, für eine wirksame Einwilligung in die Datenverarbeitung die Form des Opt-in zu verlangen. Aus Sicht des BGH ist vielmehr eine datenschutzrechtliche Einwilligung auch dann wirksam, wenn sie auf dem Opt-out-Modell beruht. Entscheidend ist aus Sicht des BGH allein, ob das Hervorhebungsgebot des § 4a Abs. 1 S. 4 BDSG gewahrt ist, ob also die Einwilligungsklausel besonders hervorgehoben ist, wenn sie zusammen mit anderen Erklärungen erteilt wird. Im Fall Payback hat der BGH diese Vorgabe als erfüllt angesehen. Aus Sicht des Gerichtshofs war die Einwilligungsklausel im Antragsformular für die Payback-Karte so platziert und drucktechnisch so gestaltet, dass diese Einwilligungsklausel zur Kenntnis genommen werden kann – zumindest vom sog. „mündigen Verbraucher", auf den es laut BGH hier ankommen soll. Ist aber das Hervorhebungsgebot gewahrt, soll nach Überzeugung des BGH auch im Falle des Opt-out grundsätzlich von einem „bewussten und autonomen Willensakt" auf Seiten des Verbrauchers auszugehen sein.

4.2 Das Leitbild (Traumbild) vom mündigen Verbraucher

Gerade das vom BGH hoch gehaltene Leitbild vom mündigen Verbraucher begegnet jedoch Bedenken.[14] Es stellt sich die Frage, ob und inwieweit die These vom mündigen Verbraucher überhaupt die Realität widerspiegelt oder ob hier nicht vielmehr ein unrealistisches Idealbild vom Verbraucher aufrechterhalten wird, das im praktischen Ergebnis zu einem Weniger an Verbraucher- und Datenschutz führt. Konkret für die Frage Opt-in oder Opt-out zeigen Untersuchungen zum Verbraucherverhalten, dass sich die Reaktion von Verbrauchern praktisch nicht ändert, egal ob man diesen ein Opt-in- oder ein Opt-out-Modell präsentiert. Stets legen etwa 20 Prozent der Verbraucher ein aktives Verhalten an den Tag, willigen also im Fall von Opt-in aktiv in eine Datenverarbeitung ein bzw. lehnen im Fall Opt-out eine solche explizit ab.[15] Die große Mehrheit der Verbraucher verhält sich hingegen gänzlich passiv, sei es aus Überforderung, aus Unkenntnis oder auch nur aus Nachlässigkeit – jedenfalls fehlt es bei dieser Mehrheit gerade an dem, was der BGH als „bewussten und autonomen Willensakt" bezeichnet.

Die Frage ist dann aber, ob tatsächlich all diesen passiven Verbrauchern mit dem bloßen Verweis auf ihre Mündigkeit eine Einwilligung in die Datenverarbeitung unterstellt werden soll. Man mag einwenden, dass eine solche Unterstellung auch sonst im Bürgerlichen Recht nichts Ungewöhnliches ist. Grundsätzlich wird im Bürgerlichen Recht dem Erklärenden ein Verhalten selbst dann als Willenserklärung zugerechnet, wenn dieser kein Erklärungsbewusstsein gehabt hat. Allerdings liegt der Grund für eine solche Zurechnung als Willenserklärung in erster Linie im Verkehrsschutz: Der Erklärungsempfänger soll in seinem Vertrauen auf einen bestimmten Erklärungstatbestand geschützt werden.[16] Eben ein solches schutzwürdiges Vertrauen auf Seiten des Erklärungsempfängers fehlt aber in der Konstellation eines Opt-out. Ein Datenverarbeiter, der für seine Vertragsgestaltung gezielt auf das Modell des Opt-out zurückgreift, kann nicht ernsthaft behaupten, dass er im Falle eines Nichtstuns auf Seiten des Betroffenen stets darauf vertraut, dass dieser sich bewusst und gewollt passiv verhalten hat. Im Gegenteil: Der Reiz eines Opt-out-Modells liegt für Datenverarbeiter gerade darin, auch dann zu einer Einwilligung zu kommen, wenn sich der Betroffene dieser nicht bewusst ist. Möchte ein Datenverarbeiter tatsächlich darauf vertrauen, dass er von seinem Gegenüber eine bewusst erteilte Einwilligung bekommen hat, muss er auf die Option des Opt-in-Modells zurückzugreifen. Nur in diesem Fall kommt überhaupt ein schutzwürdiges Vertrauen des Datenverarbeiters auf einen bestimmten Erklärungstatbestand in Betracht.

Schlichtweg inkonsequent wird die Payback-Entscheidung, wenn der BGH im Folgenden für die Einwilligung in SMS- und Email-Werbung plötzlich andere Maßstäbe aufstellt und insoweit das Opt-in-Modell als Voraussetzung für die Wirksamkeit der Einwilligung fordert. Inkonsequent ist diese unterschiedliche Handhabe der Einwilligung vor allem deshalb, weil sich der BGH beide Male, sowohl für die Einwilligung in die Datenverarbeitung als auch für die Einwilligung in Werbung, auf europarechtliche Vorgaben beruft;

13 BGH, Urt. v. 16.7.2008 – VIII ZR 348/06, DuD 2008, 818.

14 Siehe auch Wagner (in diesem Heft).

15 Petri, RDV 2007, 153 (156).

16 Ellenberger in Palandt, BGB (2009), § 130 Rdn. 4; Kramer in MünchKomm BGB (2006), § 119 Rdn. 99.

denn eben diese europarechtlichen Vorgaben sind in beiden Fällen die selben, jeweils ist für die vom BGH explizit betonte „richtlinienkonforme Auslegung" der Einwilligung die Begriffsdefinition der EU-Datenschutzrichtlinie 95/46/EG maßgeblich. Auch für die Einwilligung in SMS- und Email-Werbung wird in der entsprechenden Richtlinie 2002/58/EG explizit auf die Einwilligungsdefinition der Datenschutzrichtlinie verwiesen.[17] Gerade weil sich der BGH so ausdrücklich auf eine „richtlinienkonforme Auslegung" beruft, muss der Gerichtshof sich fragen lassen, wie er hier gleichwohl zu einem grundsätzlich unterschiedlichen Verständnis von Einwilligung kommt – einmal Opt-in, einmal Opt-out – obwohl die einschlägigen Richtlinien ganz klar den Begriff der Einwilligung gleichgeschaltet haben.

Möglicherweise rührt das Bedürfnis, einer Einwilligung in Werbung engere Grenzen zu setzen als einer Einwilligung in Datenverarbeitung daher, dass es zwar durchaus als sehr lästig empfunden wird, unerwünschte SMS und E-Mails zu erhalten, hingegen aber kein entsprechendes Unwohlsein verspürt wird, wenn personenbezogene Daten verarbeitet werden. Unerbetene Werbung hat unmittelbare spürbare Konsequenzen – der unerwünschte Anruf beim Abendessen, das überfüllte Email-Postfach, die unerwünschte SMS auf dem Handy-Display. Anders die unerbetene Datenverarbeitung: Die Verarbeitung personenbezogener Daten hat zunächst einmal keine unmittelbaren, spürbaren Konsequenzen für den einzelnen Betroffenen. Die schrittweise Aushöhlung des Rechts auf informationelle Selbstbestimmung „tut nicht weh", wird regelmäßig gar nicht bemerkt und deshalb fehlt es auch bis zum heutigen Tag noch immer an einem entsprechenden datenschutzrechtlichen Problembewusstsein im Alltag.

Gerade deshalb ist es aber andererseits so wichtig, dass das Datenschutzrecht effektiv ausgestaltet wird, um vor einem schleichenden Verlust an informationeller Selbstbestimmung schützen zu können. Effektiv wiederum kann ein Datenschutzrecht nur dann sein, wenn es auch ein Mindestmaß an Realitätsnähe aufweist. Die Anwendung datenschutzrechtlicher Grundsätze darf sich nicht allein an irgendwelchen realitätsfernen Leitbildern oder Fiktionen orientieren, sondern muss den tatsächlich existierenden Defiziten und Unzulänglichkeiten Rechnung tragen. Dies gilt gerade auch für das Leitbild des mündigen Verbrauchers. Das Datenschutzrecht mag zwar in gewissen Grenzen auch die Funktion wahrnehmen können, Verbraucher zur Mündigkeit zu erziehen, in erster Linie muss es aber Aufgabe des Datenschutzrechts sein, gerade auch den unmündigen Verbraucher effektiv zu schützen.

5 Schutz ja, Bevormundung nein

Keine Aufgabe des Datenschutzrechts ist es demgegenüber, die Entscheidung des Betroffenen als solche zu kontrollieren, indem etwa der Einwilligung des Einzelnen bestimmte Grenzen gesetzt werden oder an die Stelle der Einwilligung gesetzliche Erlaubnistatbestände treten. Dies gilt auch heute noch – trotz aller Datenschutzskandale –, auch wenn durchaus zu Recht darauf verwiesen wird, dass oftmals gerade die Verbraucher selbst an Datenklau und Datenmissbrauch schuld sind, weil sie es sind, die mittels Einwilligung all ihre Daten bereitwillig preisgeben. Gleichwohl, auch wenn dem so ist, muss nichtsdestotrotz auch weiterhin gelten, dass allein der Betroffene selbst entscheiden kann, ob und zu welchen Bedingungen er bereit ist, seine Daten als Kapital einzusetzen. So berechtigt all die Vorbehalte gegenüber einer Kommerzialisierung der eigenen Persönlichkeit auch sein mögen, können diese Vorbehalte es gleichwohl nicht rechtfertigen, dem Einzelnen die Selbstbestimmung über seine Daten zu entziehen. Informationelle Selbstbestimmung bedeutet eben auch Selbstbestimmung dahingehend, wie viel dem Einzelnen seine Privatheit und die Vertraulichkeit seiner Daten wert sind. Entsprechend kann es nicht die Aufgabe des Datenschutzrechts sein, irgendwelche Grenzen für eine „wünschenswerte" oder „verantwortungsvolle" Ausübung des Rechts auf informationelle Selbstbestimmung vorzugeben.

Dem Grunde nach gilt für die Kommerzialisierung personenbezogener Daten dasselbe, was der BGH bereits zur Kommerzialisierung der Persönlichkeitsrechte Prominenter festgehalten hat. Auch bei diesen Persönlichkeitsrechten Prominenter dreht sich die Diskussion immer wieder darum, ob das Recht einer Kommerzialisierung Grenzen setzen muss oder ob es rechtlich hinzunehmen ist, dass Prominente den Werbewert ihrer Persönlichkeit kommerziell nutzen und ihre Individualität zu Markte tragen, um daraus wirtschaftlichen Profit zu schlagen.[18] In seiner Marlene-Dietrich-Entscheidung[19] hat der BGH diese Diskussion im Sinne einer dienenden Funktion des Rechts entschieden. Der BGH hat in dieser Entscheidung klargestellt, dass die Rechtsordnung kein starres System bildet, an dem sich die Wirklichkeit zu orientieren hat, sondern dass dem Recht durchaus auch eine dienende Funktion zukommt, indem das Recht „einen Ordnungsrahmen auch für neue Formen der Vermarktung bieten muss, die im Interesse sowohl des Vermarkters als auch desjenigen liegen, der eine solche Vermarktung seiner Person gestatten möchte."[20]

Gleiches muss dann aber auch für die Kommerzialisierung der Persönlichkeit von solchen Personen gelten, die zwar nicht berühmt sind, die aber zumindest den wirtschaftlichen Wert ihrer personenbezogenen Daten nutzen möchten. Auch insoweit kommt dem Datenschutzrecht eine dienende Funktion zu, muss sich das Datenschutzrecht um solche rechtlichen Rahmenbedingungen bemühen, die sicherstellen, dass der Einzelne auch als Datenhändler in eigener Sache sein Recht auf informationelle Selbstbestimmung effektiv wahrnehmen kann. Der Einwilligung kommt dabei die zentrale Rolle zu, von der rechtlichen Ausgestaltung dieser Einwilligung wird es ganz entscheidend abhängen, ob auch unter den neuen Rahmenbedingungen einer zunehmenden Kommerzialisierung personenbezogener Daten das Recht auf informationelle Selbstbestimmung gleichwohl noch effektiv geschützt und ausgeübt werden kann.

17 Siehe Art. 2 lit f der Richtlinie 2002/58/EG, der für den Begriff der Einwilligung eines Nutzers oder Teilnehmers auf „die Einwilligung der betroffenen Person im Sinne von Richtlinie 95/46/EG" verweist.

18 Peifer, Individualität im Zivilrecht (2001), S. 132 ff.; ders., GRUR 2002, 495 (499); Schack, JZ 2000, 1060.

19 BGH, Urt. v. 1.12.1999 – I ZR 49/97, DuD 2000, 610 – Marlene Dietrich.

20 BGH a.a.O., S. 614.