Der Schutz des informationellen Selbstbestimmungsrechts im 21. Jahrhundert

Benedikt Buchner

Einleitung

Die folgenden Ausführungen sind ein Versuch, als Jurist Antworten auf die Frage zu geben, ob und wie das Datenschutzrecht den Gefährdungen informationeller Selbstbestimmung, wie sie im Laufe dieser Tagung ausführlich diskutiert werden, wirksam begegnen kann. Es geht um die Frage, wie das Recht sicherstellen kann, dass sich etwa staatlicher Datenhunger und Datenzugriff nicht immer weiter seinen Weg in die Privatsphäre des Einzelnen hinein bahnt, dass Verbraucher nicht für einige wenige Bonuspunkte oder -meilen unbewusst und ungewollt ihre Persönlichkeitsprofile offenbaren, oder dass Sparzwänge und Effizienzinteressen im Gesundheitssektor nicht auf Kosten der Vertraulichkeit der Patientendaten gehen.

Wie schwer es ist, auf all diese und ähnliche datenschutzrechtliche Herausforderungen eine Antwort zu finden, wird gerade auch mit Blick auf die immer noch andauernden Bemühungen um die viel zitierte Modernisierung des deutschen Datenschutzrechts deutlich. Der Anlass für die aktuellen Bemühungen um eine Fortschreibung des deutschen Datenschutzrechts liegt schon weit zurück: Im Jahr 1995 trat die EU-Datenschutzrichtlinie in Kraft, die vom deutschen Gesetzgeber spätestens bis zum Oktober 1998 in nationales Recht umzusetzen war. Der deutsche Gesetzgeber wollte es allerdings nicht bei einer bloßen Umsetzung belassen, sondern den Novellierungsbedarf zum Anlass für eine umfassende Modernisierung des Bundesdatenschutzgesetzes nehmen. So ambitioniert dieses Ansinnen war, so erfolglos war es letztendlich jedoch. Der Gesetzgeber musste erkennen, dass er – zumindest in dem von Europa vorgegebenen zeitlichen Rahmen – eine Umsetzung der europarechtlichen Vorgaben in Form einer zukunftsfähigen und grundlegenden Modernisierung des deutschen Datenschutzrechts nicht bewerkstelligen konnte. Die Folge war ein Kompromiss: Der Gesetzgeber entschied sich dazu, seine europarechtlichen Hausaufgaben einer Umsetzung der Datenschutzrichtlinie sofort zu erledigen, die „richtige" Modernisierung dann aber in Ruhe in einem zweiten Schritt anzugehen.

Dieser zweite Schritt allerdings steht bis heute aus. Trotz der verschiedensten Bemühungen und Anläufe, insbesondere auch der Erstellung eines umfangreichen Modernisierungsgutachtens als Ausgangsbasis für die Neuformulierung des BDSG, haben wir es bis zum heutigen Tage mit einem an sich als Übergangslösung gedachten Bundesdatenschutzgesetz zu tun. Zu schwierig ist es offensichtlich, eine Einigung für eine solch kontroverse Thematik wie die des Datenschutzrechts zu finden, zu hochgesteckt vielleicht auch die Erwartungen an ein neues, „modernes" Datenschutzrecht, zu schwach die Lobby der Datenschützer und zu mächtig die Begehrlichkeiten derjenigen, die nicht weniger, sondern mehr Daten verarbeiten wollen, sei es im Dienste staatlicher Vollzugs- und Sicherheitsinteressen, sei es im Dienste privatwirtschaftlicher Marketing- und Profitinteressen. Umso wichtiger und umso mehr zu begrüßen

Prof. Dr. Benedikt Buchner, Professor des. für Bürgerliches Recht an der Universität Bremen

sind daher Veranstaltungen wie diese Tagung, die das Anliegen des Datenschutzes wieder mehr in das öffentliche Bewusstsein rücken und die Notwendigkeit eines modernen und starken Datenschutzes wieder auf die Tagesordnung bringen.

Lösungsansätze für ein modernes Datenschutzrecht

Wie könnte nun so ein effektives und modernes Datenschutzrecht aussehen, das auf die aktuellen und zukünftigen Gefährdungen informationeller Selbstbestimmung überzeugende Antworten liefert? Jede Stellungnahme hierzu muss zwangsläufig subjektiv ausfallen, betrifft sie doch eine ganze Reihe von Grundüberzeugungen, die jeweils diametral entgegengesetzt ausfallen können:

- Wie definieren wir die Würde und Persönlichkeit des Einzelnen? Orientiert sich diese in erster Linie an der Person desjenigen, der um seiner freien und selbstverantwortlichen Persönlichkeitsentfaltung willen einen Rückzugsraum benötigt, wo er vor der Einsichtnahme Dritter und deren Informationszugriff sicher ist? Oder geht es auch – oder vielleicht sogar in erster Linie – um die Würde und Persönlichkeit desjenigen, der kommunizieren und interagieren will, der sich aus möglichst vielen Quellen unterrichten, das eigene Wissen erweitern und sich so als Persönlichkeit entfalten will?
- Was sehen wir als die größere Bedrohung für Freiheit und Privatautonomie an? Das Droh- und Hemmpotential, das von einem Bewusstsein des Beobachtet- und Registriert-Werdens ausgeht, oder die lähmende Wirkung, die von verordneter Unwissenheit ausgehen kann?
- Was ist für uns die „ursprüngliche Freiheit"? Der Schutz des Einzelnen vor einem Zugriff anderer auf „seine" personenbezogenen Daten, oder umgekehrt die Freiheit anderer zur Information über ihre Mitmenschen? Und was soll entsprechend der Ausgangspunkt einer Informations- und Datenschutzordnung sein: das Verbot der Datenverarbeitung oder deren Freiheit?
- Schließlich auch: Welches Bild haben wir vom Staat, welches Bild von der Privatwirtschaft? Wie groß ist unser Vertrauen in den Staat, wie groß unser Vertrauen in die Privatwirtschaft? Und umgekehrt: Wie groß schätzen wir die Gefahren staatlicher, wie groß die Gefahren privater Datenverarbeitungssysteme für unsere informationelle Selbstbestimmung ein?

Plädoyer für einen zweigeteilten Datenschutz

Um mit letzterer Frage zu beginnen: Welches Bild wir von Staat und Wirtschaft haben, welches Vertrauen oder Misstrauen wir gegenüber staatlichen und privaten Datenverarbeitern hegen, ist ganz maßgeblich für die Entscheidung, ob ein künftiges Datenschutzrecht einheitlich oder zweigeteilt ausgestaltet sein soll, ob also grundsätzlich einheitliche Regeln für die Datenverarbeitung durch staatliche und private Stellen gelten sollen, oder ob für staatliche und private Datenverarbeitung jeweils andere Regelungen gelten sollen.

Bislang haben wir in Deutschland im Grundsatz noch immer einen zweigeteilten Datenschutz, wie er sich insbesondere im Regelungskonzept des Bundesdatenschutzgesetzes widerspiegelt. Wir haben im BDSG einen Abschnitt zwei, der die Zulässigkeit und die Rahmenbedingungen der Datenverarbeitung durch staatliche Stellen regelt, und wir haben einen Abschnitt drei, der die Datenverarbeitung durch private Stellen regelt. Die bisherige Zweigeteiltheit des Datenschutzrechts wird überwiegend mit einer Privilegierung privater Datenverarbeiter gleichgesetzt und entsprechend kritisiert; der Vorwurf lautet, dass die Zweigeteiltheit des Datenschutzrechts letztlich darauf hinauslaufe, das Schutzniveau im Bereich privater Datenverarbeitung abzusenken.

Staatliche Datenverarbeitung stellt aus den verschiedensten Gründen ein besonderes Gefährdungspotenzial für das Recht auf informationelle Selbstbestimmung dar, und dieses besondere Gefährdungspotenzial bedingt auch eine besondere gesetzgeberische Reaktion gerade auf die spezifischen Gefährdungen durch staatliche Datenverarbeiter. Wir brauchen daher auch in Zukunft ein zweigeteiltes Datenschutzrecht. Wir brauchen diese Zweigeteiltheit, weil die Gefährdungen informationeller Selbstbestimmung durch private und staatliche Datenverarbeiter jeweils andere sind und daher auch die datenschutzrechtlichen Antworten jeweils andere sein müssen. Wer demgegenüber einen zweigeteilten Datenschutz mit der Begründung kritisiert, ein solcher werde dem besonderem Gefährdungspotential der privaten Datenverarbeitung nicht gerecht, dem sei entgegengehalten, dass es umgekehrt gerade ein einheitlicher Datenschutzansatz wäre, der das besondere Gefährdungspotenzial *staatlicher* Datenverarbeitung ignorieren würde.

Der Schutz informationeller Selbstbestimmung im Privatrechtsverkehr

Es ist weder überraschend noch unberechtigt, dass unser heutiges Datenschutzrecht einen Ruf als unpraktikabel und uneffektiv hat. Die teils perfektionistische Durchnormierung des Datenschutzrechts hat de facto in vielen Bereichen zu einem gesetzesförmlichen Leerlauf des Datenschutzes geführt. Die gesetzliche Durchdringung und Reglementierung des Datenschutzes führt sogar so weit, dass selbst ein Bundesdatenschutzbeauftragter konstatieren muss, es handele sich hier um ein undurchschaubares Regelwerk. Dementsprechend vernichtend ist die Kritik am gegenwärtigen Datenschutzrecht, wie sie sich allerorten nachlesen lässt. Die Rede ist von einer „überdetaillierten, unübersichtlichen und schwer zu vollziehenden Normenmasse", von einer „Detailversessenheit", von „Unübersichtlichkeit, Unverständlichkeit und Zersplitterung" und von „Normüberflutung und Bürokratisierung".

Die Generalklauseln erweisen sich als das „ideale Mittel", bevorzugte Datenverarbeitungspraktiken auch unter der Geltung des BDSG ohne Abstriche beizubehalten. Im praktischen Ergebnis wird also die scheinbar so strenge Grundregel, dass eine Datenverarbeitung nur zulässig ist, soweit dies gesetzlich erlaubt ist oder der Betroffene eingewilligt hat, durch inhaltslose Generalklauseln und entsprechende Erlaubnistatbestände wieder außer Kraft gesetzt. Im Ausgangspunkt ist zwar auf dem Papier alles verboten, de facto ist aber alles möglich und erlaubt – sei es aus Gründen eines faktischen Vollzugsdefizits, sei es auch ganz „legal" dank allgemeiner dehnbarer Interessenabwägungsklauseln.

Was ist die Konsequenz all dessen? Lassen sich neben all dieser Kritik auch Vorschläge für eine konkrete Lösung finden, und wie könnte eine solche ausschauen? Wenn ein umfassender Regelungsanspruch des Gesetzgebers offensichtlich nicht erfolgreich umzusetzen ist, weder in Form von detaillierten Spezialklauseln noch in Form von allgemeinen Interessenabwägungsklauseln, kann eine Lösung nur dahin gehen, dem Gesetzgeber weniger und dafür den Betroffenen selbst mehr an Entscheidung zu überlassen. Die Grenzziehung zwischen zulässiger und unzulässiger Datenverarbeitung muss so weit wie möglich den Beteiligten selbst überantwortet werden. Wenn eine differenzierende abschließende gesetzliche Festlegung in Form eines detaillierten Katalogs datenschutzrechtlicher Verbots- und Erlaubnistatbestände nicht praktikabel ist und wenn auch der Weg über allgemeine Generalklauseln Vorbehalten begegnet, bleibt als Ausweg nur ein Interessenausgleich im Wege der Privatautonomie. Der Gesetzgeber nimmt also für sich von vornherein nicht in Anspruch, den Interessenkonflikt zwischen Betroffenen und Datenverarbeitern ex ante abschließend für alle Konstellationen sachgerecht regeln zu können. Stattdessen beschränkt er sich auf ein Regelwerk, das auf der Idee der Privatautonomie fußt und Generalklauseln und Detailregelungen nur vorsieht, soweit diese auch praktikabel, verständlich und umsetzbar sind und diese der Datenverarbeitung nicht nur auf dem Papier, sondern auch tatsächlich effektive Grenzen setzen.

Die Aufgabe des Datenschutzrechts muss dahin gehen, Situationen zu fördern, in denen Verbraucher weitestgehend selbst in die Lage versetzt werden, ihre eigenen Interessen zur Geltung zu bringen. Es geht darum, mittels Schaffung entsprechender rechtlicher Rahmenbedingungen einen gerechten Aushandelungsprozess zwischen Wirtschaft und Konsumenten zu gewährleisten. Erst wenn es trotz Schaffung entsprechender rechtlicher Rahmenbedingungen nicht mehr gewährleistet ist, dass der Einzelne selbst seine Rechte und Interessen frei und eigenverantwortlich wahrnimmt, soll der Staat auch inhaltlich gestaltend in private Rechtsverhältnisse eingreifen. Anstatt individuelle Selbstbestimmung durch immer noch spezifischere Tatbestände zulässiger und unzulässiger Datenverarbeitung zu ersetzen, müssen alle gesetzgeberischen Bemühungen zunächst einmal darauf ausgerichtet sein, individuelle

Selbstbestimmung und Eigenverantwortung zu stärken und gesetzgeberische Interventionen auf ein praktikables Maß zu reduzieren. Dies gilt umso mehr, als im bisherigen Datenschutzrecht die Einschränkungen individueller Selbstbestimmung oftmals gerade eine Schwächung informationeller Selbstbestimmung zulasten des einzelnen Betroffenen nach sich ziehen: Die Weite datenschutzrechtlicher Generalklauseln, insbesondere der allgemeinen Interessenabwägungsklauseln, führen in vielen Bereichen dazu, dass eine Verarbeitung personenbezogener Daten de facto am Betroffenen vorbei stattfindet. Dieser kann weder auf die Frage des Ob noch auf die Frage des Wie einer Verarbeitung seiner Daten irgendeinen effektiven Einfluss nehmen.

Schließlich ist staatliche Selbstbeschränkung auch deshalb notwendig, um der Gefahr einer Bevormundung des einzelnen Betroffenen zu begegnen. Datenschutzpräferenzen sind von Person zu Person völlig unterschiedlich ausgeprägt und in dieser Unterschiedlichkeit zunächst einmal auch vom Staat zu respektieren. Als Datenschützer mag man es bedauern, dass Kunden für ein paar Bonuspunkte und Rabattprozente ohne Bedenken bereit sind, dem Handel ihr vollständiges Kauf- und Interessenprofil zu überlassen. Gleichwohl wäre es nicht gerechtfertigt, wenn der staatliche Gesetzgeber ein bestimmtes Wunschbild vom datenschutzbewussten Bürger durch eine paternalistische Datenschutzgesetzgebung forcierte. Solange Kunden auch noch ohne Kundenkarten einkaufen können, oder allgemeiner formuliert: solange der Einzelne noch die Freiheit hat, seine datenschutzrechtlichen Präferenzen auch tatsächlich auszuüben, ist die Art und Weise, wie der Einzelne diese Freiheit ausübt, vom Gesetzgeber grundsätzlich auch so zu respektieren. Es ist grundsätzlich nicht die Aufgabe des Staates, den Bürger im Sinne eines bestimmten idealistischen Leitbildes zu formen. Die Definition des BVerfG für informationelle Selbstbestimmung gilt vielmehr auch heute noch: Informationelle Selbstbestimmung soll dem Einzelnen die Befugnis verleihen, „grundsätzlich *selbst* über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."

Die Gewährleistung tatsächlicher Privatautonomie

Wie kann nun in der Praxis effektiv gewährleistet werden, dass eine privatautonome Einwilligung in die Verarbeitung personenbezogener Daten nicht nur Fiktion, sondern tatsächlich Ausdruck einer informierten und freiwilligen Entscheidung über das Ob und Wie einer Verarbeitung der eigenen Daten ist? Ich möchte hierfür abschließend nur ein paar wenige, aber dafür aus meiner Sicht ganz zentrale Thesen für die künftige datenschutzrechtliche Diskussion aufstellen.

1. Informierte Einwilligung

Eine Einwilligung muss informiert sein, und es ist die Aufgabe derjenigen, die Daten verarbeiten, für diese Informiertheit zu sorgen. Die Forderung nach einer informierten Entscheidung ist zunächst nichts Neues, sie ist eine Selbstverständlichkeit, die auch seit jeher so anerkannt und datenschutzrechtlich vorgegeben ist. Worum es mir hier jedoch geht, ist eine Information, die ihrem Namen gerecht wird. Die bisherige sog. „Information" des Verbrauchers ist oftmals scheinheilig und unehrlich. Verbraucher werden mit detaillierten Einzelinformationen überschüttet, die für ihre Meinungsbildung und für ihren Kenntnisstand ohne jegliche Bedeutung sind, und irgendwo in dieser unüberschaubaren Masse an größtenteils unerheblichen Informationen finden sich einige wenige Informationen versteckt, die an sich von Bedeutung wären, die sich aber in der Masse der Informationen vollständig verlieren.

Der Einzelne muss beim Abschluss eines Mobilfunkvertrags nicht über jede Kleinigkeit der technischen Datenverarbeitungsabläufe informiert werden, insbesondere wenn diese ohnehin gesetzlich erlaubt oder technisch unvermeidbar sind. Informiert werden muss er stattdessen über die Datenverarbeitungsvorgänge, die für sein informationelles Selbstbestimmungsrecht tatsächlich von Relevanz sind und bei denen es gerade auf seine Entscheidung ankommt, inwieweit er eine Datenverarbeitung zulassen möchte oder nicht, also etwa, inwieweit er eine Datenverarbeitung zu Marketingzwecken zulassen möchte oder nicht, inwieweit er mit einer Datenweitergabe an dritte Unternehmen einverstanden ist oder nicht. Interessant ist für den Verbraucher, zu wissen, ob seine Daten über einen längeren Zeitraum hinweg zu sog. Datenprofilen zusammengefügt werden und welche Aussagekraft solche Datenprofile entwickeln können. Interessant wäre auch zu wissen, welchen wirtschaftlichen Wert solche Datensammlungen über ihn möglicherweise haben und ob dieser Wert vielleicht sogar durch das datenverarbeitende Unternehmen im Wege des Adresshandels realisiert wird. All diese Informationen lassen sich ohne weiteres in einer einfachen und allgemein verständlichen Sprache vermitteln und auch durch konkrete Beispiele verdeutlichen. Jedoch wird man sie heute nirgendwo in dieser Form in Datenschutzhinweisen o.ä. finden. Warum nicht? Weil ein solchermaßen informierter Verbraucher „unbequem" wäre, zu viele Fragen oder gar Forderungen stellen würde.

Zu einer echten *Information* gehört auch, dem Betroffenen unmissverständlich bewusst zu machen, dass er eine Einwilligung in die Verarbeitung seiner Daten erteilt. Um dies sicherzustellen, ist jede Einwilligung grundsätzlich in der Form eines echten Opt-In auszugestalten, d.h. dass der Kunde diejenigen Datenverarbeitungsvorgänge, in die er einzuwilligen bereit ist, etwa ankreuzen oder gesondert unterschreiben muss, er seinen Willen also aktiv zum Ausdruck bringen muss. Abzulehnen sind dagegen alle Formen sog. Opt-Out-Lösungen, wie sie heutzutage noch immer vielfach üblich sind, d.h. solcher Lösungen, bei denen es am Verbraucher ist, durch Streichen einer irgendwo, möglicherweise noch versteckt untergebrachten Einwilligungsklausel sein Nicht-Einverständnis zum Ausdruck zu bringen. Zu groß ist bei solchen Opt-Out-Lösungen die Gefahr, dass sich der Einzelne gerade bei umfangreichen und unübersichtlichen Formularverträgen allein infolge bloßer Untätigkeit oder Unwissenheit mit einer Datenverarbeitung einverstanden erklärt, obwohl diese nicht seinem tatsächlichen Willen entspricht.

2. Die Einwilligung als zentraler Erlaubnistatbestand

Eine weitere, ganz zentrale Forderung geht dahin, dass Datenverarbeiter sich grundsätzlich und primär um ein Einverständnis des von der Datenverarbeitung Betroffenen selbst bemühen müssen, anstatt am Betroffenen vorbei die Datenverarbeitung allein auf allgemeine und dehnbare Interessenabwägungsklauseln zu stützen.

Bedeutung hat diese Forderung vor allem für den Bereich der Auskunfteien und des Adresshandels. Die Praxis ist in diesen Bereichen bislang, dass die Datenverarbeitung faktisch am Betroffenen vorbei stattfindet – eben weil es dank allgemeiner Interessenabwägungsklauseln nicht seiner Einwilligung bedarf und daher auch keine Notwendigkeit besteht, den Betroffenen durch nachvollziehbare Informationen und durch eine interessengerechte Datenverarbeitungspraxis im Sinne einer Einwilligung in die Datenverarbeitung zu überzeugen. Stattdessen findet die Datenverarbeitung *am Betroffenen vorbei* statt, was sich in vielerlei Hinsicht in einer Missachtung von grundlegenden Datenschutzrechten des Betroffenen äußert: in einer Missachtung seiner Rechte auf Information und Auskunft, seines Rechts auf richtige Datenverarbeitung, auf die Berichtigung falscher Daten etc.

Die gegenwärtige Datenverarbeitungspraxis von Kreditauskunfteien wie der Schufa liefert hierfür ein ebenso anschauliches wie bedenkliches Beispiel. Die Informationen, die Kreditauskunfteien den Betroffenen über die Art und Weise ihrer Datenverarbeitung liefern, sind ebenso unvollständig wie schwer nachvollziehbar. So weigern sich Kreditauskunfteien bis zum heutigen Tage, Auskunft über die maßgeblichen Kriterien zu erteilen, die für die Bildung des sog. Scorewerts herangezogen werden. Sinn und Zweck dieses Scorewerts ist es, Unternehmen mittels einer einfachen Kennziffer Auskunft über die Kreditwürdigkeit eines potenziellen Vertragspartners zu geben. Je höher die Punktzahl, desto größer die Aussicht auf ein ordnungsgemäßes Zahlungsverhalten des Schuldners. So praktisch und sinnvoll ein solches Bewertungsverfahren auch sein mag, so bedenklich ist es, wenn den Betroffenen standhaft Informationen darüber verweigert werden, anhand welcher Kriterien deren „Score" gebildet wird. Eine Legitimität kann dem Scoring aber erst dann zukommen, wenn die Betroffenen den ihnen zugeordneten Score auch nachvollziehen können. Ansonsten bleibt der Score ein undurchschaubares und willkürlich von Dritten verhängtes Wert- oder Unwerturteil, das den Einzelnen zu einem bloßen Objekt der Datenverarbeitung degradiert.

Ändern wird sich an diesen und anderen Missständen einer Datenverarbeitung erst dann etwas, wenn Datenverarbeiter auf die Einwilligung der Betroffenen selbst angewiesen sind, um deren personenbezogene Daten verarbeiten zu dürfen. Viele der derzeitigen datenschutzrechtlichen Missstände dürften sich dann von selbst erledigen. Der Einzelne wird nur solchen Auskunfteien sein Einverständnis erteilen, die eine transparente, faire und korrekte Verarbeitung seiner Daten gewährleisten können. Es ist an diesen, die Betroffenen dadurch zu überzeugen, dass sie die Strukturen ihrer Datenverarbeitung offen legen und nachvollziehbar erklären, dass sie sich um vollständige Informationen und faire Bewertungsmaßstäbe bemühen und dass sie effektive Verfahren der Fehlerkontrolle und Fehlerbehebung institutionalisieren. Vor allem die Praktiken des Credit Scoring werden sich – zumindest in ihrer jetzigen Form – unter diesen Rahmenbedingungen kaum mehr aufrechterhalten lassen. Wohl niemand wird sich mit einer Kategorisierung seiner Person einverstanden erklären, wenn er noch nicht einmal die zugrunde liegenden Beurteilungsfaktoren und -maßstäbe kennt, wenn er nicht weiß, wer welche Informationen bekommt, und er kaum eine Möglichkeit der Kontrolle und Berichtigung hat.

3. Die Freiwilligkeit der Einwilligung: Ein letztes Wort schließlich zum Aspekt der Freiwilligkeit der Einwilligung.

Man mag den bisherigen Ausführungen entgegenhalten, dass die Idee eines prinzipiellen Entscheidungsvorrechts des Betroffenen dem Grunde nach zwar eine schöne Idee ist, in der Praxis diese Idee aber nur wenig bewirken wird, weil es in vielen Konstellationen, wie etwa auch im Bereich der Kreditauskunfteien, dem Betroffenen ohnehin nicht möglich ist, „frei" über das Ob und Wie einer Einwilligung in die Verarbeitung seiner Daten zu entscheiden. Oder anders formuliert: Die schöne Idee der privatautonomen Einwilligung wird durch die faktische Unfreiwilligkeit der Einwilligung in vielen Fällen von vornherein entwertet.

Richtig ist zunächst einmal, dass eine freiwillige Einwilligung in vielen Fällen tatsächlich nicht erreicht werden kann. Tatsache ist aber auch, dass dieser Mangel an Freiwilligkeit die Idee der Einwilligung nicht grundsätzlich entwertet, und zwar deshalb, weil oftmals die fehlende Freiwilligkeit nicht der eigentlich datenschutzrechtlich problematische Punkt ist. Die Interessen des Datenschutzes sind stets in Einklang mit entgegengesetzten Informationsinteressen

Das Freundeszeichen der Katholischen Akademie in Bayern überreicht Dr. Florian Schuller dem Akademiedirektor des Caritas-Pirckheimer-Hauses in Nürnberg, Prof. Dr. Heimo Ertl, der am 17. März 2007 in den Ruhestand verabschiedet wurde

zu bringen, und es ist oftmals legitim, dass sich Informations- gegenüber Datenschutzinteressen im Ergebnis durchsetzen. Es ist legitim, wenn Vermieter vor Vermietung die Zuverlässigkeit ihrer potenziellen Mieter kennen wollen oder private Krankenversicherungen den Gesundheitszustand potenzieller Versicherungsnehmer. Oder um nochmals das Beispiel der Kreditauskünfte heranzuziehen: Es ist legitim, vom Verbraucher die Offenlegung seiner Kreditwürdigkeit zu verlangen, wenn dieser Vorleistungen egal welcher Art – Kredit, Mobiltelefon, Warenlieferung auf Rechnung etc. – in Anspruch nehmen will. Der faktische Zwang, der damit einhergeht, ist kein datenschutzrechtliches Problem, da bei der Inanspruchnahme von Leistungen niemand ein Recht auf uneingeschränkte Anonymität erwarten kann. Was datenschutzrechtlich nicht in Ordnung ist, sind die oben angesprochenen Defizite: der Umstand, dass die Beurteilungsmechanismen bei Festlegung der Kreditwürdigkeit völlig intransparent sind, dass die Auskünfte sehr fehleranfällig sind und die Kontrollmöglichkeiten unnötig erschwert werden – kurzum: dass der Einzelne so weit wie möglich unwissend und passiv gehalten wird, und zwar aus dem einfachen Grund, dass ein aktiver, informierter und selbstbewusster Verbraucher ungleich mehr Zeit und Geld kosten würde. Eben dies muss aber das Ziel aller künftigen datenschutzrechtlichen Bemühungen sein, und hierfür ist eine erste unabdingbare Voraussetzung, dass der Betroffene zunächst einmal in das Zentrum aller Datenverarbeitungsprozesse rückt, indem es auf seine Einwilligung in die Datenverarbeitung ankommt.

Fazit

1. Wir brauchen ein neues Datenschutzrecht, das wieder einfacher und verständlicher ist und damit auch mehr Chancen auf Akzeptanz und Beachtung hat.

2. Wir brauchen auch in Zukunft ein nach staatlicher und privater Datenverarbeitung zweigeteiltes Datenschutzrecht. Eine solche Forderung zielt nicht darauf ab, die Gefahren privater Datenverarbeitung in Frage zu stellen. Es geht vielmehr umgekehrt darum, dem besonderen Gefährdungspotenzial staatlicher Datenverarbeitung angemessen Rechnung zu tragen.

3. Wir brauchen mehr an Privatautonomie und weniger an staatlicher Regulierung im Bereich der privaten Datenverarbeitung. Im Zentrum eines künftigen Datenschutzrechts muss ein starkes Entscheidungsvorrecht des einzelnen Betroffenen stehen. Es muss primär von dessen Entscheidung abhängen, ob und wenn ja unter welchen Umständen es zu einer Verarbeitung seiner personenbezogenen Daten kommen soll.

4. Wenn sich Datenverarbeiter tatsächlich um ein Einverständnis der Betroffenen bemühen müssen und sich nicht mehr wie bislang auf allgemeine Interessenabwägungsklauseln als Rechtfertigung einer Datenverarbeitung stützen können, und wenn gleichzeitig dafür Sorge getragen wird, dass Datenverarbeiter auch tatsächlich und nicht nur pro forma ihrer Verpflichtung zu einer Information des Betroffenen über das Ob und Wie einer Datenverarbeitung nachkommen, so wären wir schon ein erhebliches Stück weiter auf dem Weg hin zu einem effektiven Schutz informationeller Selbstbestimmung auch unter den Bedingungen moderner Datenverarbeitung. □