Datenschutz beim E-Learning - Zum Verhältnis von Kontrolle und Vertrauen in der Informationsgesellschaft

Jan Hansen[1], Nadine Hatteh[2]

[1]Hessisches Teledia Technologie Kompetenz Center – httc e.V.
Merckstr 25
64283 Darmstadt

[2]Hochschule Darmstadt
Institut für Informationsrecht (i2r)
Haardtring 100
64295 Darmstadt

jan.hansen@httc.de
nadine.hatteh@gmx.de

Abstract: Datenschutzregeln im E-Learning und insbesondere beim Einsatz von Learning Management Systemen an Hochschulen dienen dem Ziel, durch einen Ausgleich zwischen gegensätzlichen Interessen Vertrauen zu schaffen. Der Interessenkonflikt zwischen Daten-Nutzern einerseits und Privatpersonen andererseits wird dargestellt. Lösungen des Interessenkonfliktes durch Datenschutzregeln auf EU - Ebene, auf Bundes- und Landesebene in Deutschland werden diskutiert. Da die Gesetzgebung in sensiblen Bereichen von E-Learning - Veranstaltungen auf pauschale gesetzliche Erlaubnisse zur Datennutzung verzichtet hat, werden abschließend die Anforderungen an eine Einwilligung der Betroffenen erörtert und auf spezifische Umstände beim E-Learning bezogen.

1 Einleitung

Wir leben in der Informationsgesellschaft. Der Umgang mit elektronischen Daten wandelt dabei seinen Charakter. Aus dem ursprünglichen Paradies der kontrollfreien Gegenwelt im Internet wird ein Internet der Überwachung [Ca08]. Die Speicherung von Daten dringt auch ausserhalb der Internets in immer mehr Bereiche des täglichen Lebens ein: RFID-Chips als elektronische Waren-Etiketten, Videoüberwachung, biometrische Erkennungsmethoden, Telekommunikations– und Wohnraumüberwachung werden als bedrohlich empfunden [Bu06]. Andererseits gelten Daten über Personen als profitabler Rohstoff der Informationsgesellschaft [Bö01].

Um so stärker wird das Bedürfnis einzelner Person, die Kontrolle über die sensiblen und wertvollen Daten zu den eigenen Verhältnissen nicht zu verlieren und einen eigenen Einfluss auf die Verwendung der Daten zu behalten. In diesem Spannungsfeld stehen sich auch beim E-Learning an Hochschulen gegensätzliche Interessen gegenüber.

2 Interessenkonflikt

Die Aufgabe des Datenschutzrechtes in der Wissenschaft und im E-Learning an Hochschulen ist es, einen fundamentalen Interessenkonflikt zu lösen: Wissenschaftler und Organisatoren von E-Learning Veranstaltungen wünschen sich die freie Nutzung von Daten, die einzelnen Betroffenen möchten die Nutzung ihrer Daten selber kontrollieren.

2.1 Interesse der einzelnen Betroffenen

Wer mag schon die Vorstellung, dass Daten über die eigenen persönlichen Verhältnisse ohne Kontrolle kursieren? Wenn Betroffene sehen, dass Daten über ihre persönlichen Verhältnisse als Gegenstand wissenschaftlicher Forschung oder als Teilnehmerdaten einer E-Learning Veranstaltung ungehindert zirkulieren, kann dies von den Betroffenen als Bedrohung empfunden werden. Vor derartigen Bedrohungen schützt das „Recht auf Informationelle Selbstbestimmung“. 1983 hat das Bundesverfassungsgericht dieses Recht im sog. Volkszählungsurteil anerkannt [Sh04]. Dem Urteil voraus gegangen war eine bis dahin beispiellose Protestwelle [Ro02] der Bevölkerung gegen das vom Gesetzgeber verabschiedete „Volkszählungsgesetz“, das die Erhebung persönlicher Daten für die Analyse der Gesellschaftsstruktur vorsah. Nach der Einreichung mehrerer Verfassungsbeschwerden gegen das Volkszählungsgesetz entschied das Bundesverfassungsgericht, dass jeder Bürger das Recht hat, selber über die Preisgabe der Verwendung seiner persönlichen Daten zu bestimmen. Gerade unter den Bedingungen der elektronischen Datenverarbeitung gäbe es „keine belanglosen Daten mehr“ [Bv83].

2.2 Interesselage der Wissenschaftler und Betreiber von Learning Management Systemen

Die Interessen der Betroffenen sind jedoch nicht der einzige Aspekt im Kräftespiel der Kontrahenten. Das Grundgesetz gewährt auch die Freiheit der wissenschaftlichen Forschung und Lehre[1], welches den Wissenschaftler oder Lehrenden „beim Auffinden von Informationen, ihrer Deutung und Weitergabe schützt.“ Ohne Informationen können Forschung und Lehre nicht existieren. Für die Betreiber von Learning Management Systemen ist es oft von Vorteil, wenn sie ungehindert alle Daten nutzen können, bei der Verwaltung von Veranstaltungen und beim Usertracking anfallen.

[1] Art. 5 Abs. 3 GG

Wir stehen damit vor der unangenehmen Situation, dass zwei Interessenlagen aufeinander prallen, die beide gute Gründe für sich haben. Eine gerechte Lösung dieses Konfliktes kann nur in einem Kompromiss liegen. Deshalb haben die im Folgenden dargestellten Datenschutz-Regelungen einen Kompromisscharakter.

Dem Verständnis der Datenschutz - Regelungen für die Wissenschaft und das universitäre E-Learning in Deutschland kommen wir näher, wenn wir zunächst in einem ersten Schritt einige Regeln auf der Ebene der Europäischen Union betrachten.

3. Europäische Union

Die EU Richtlinie „95/46/EG des europäischen Parlaments zum Schutz von natürlichen Personen bei der Verarbeitung personenbezogener Daten und zum Schutz des freien Datenverkehrs vom 14. Oktober 1995“ enthält bereits im Namen die doppelte Zielrichtung, zwei entgegen gesetzte Bereiche zu schützen. Sie formuliert grundlegende Strukturen, die im Datenschutz immer wieder anzutreffen sind.

3.1 Grundsätze

Fünf Grundsätze bestimmen die Struktur des Datenschutzrechtes.

1. Der erste Grundsatz des Datenschutzrechts lässt an Deutlichkeit nichts zu wünschen übrig: Alles ist verboten, es sei denn, es ist ausnahmsweise erlaubt [Ro02]. Derartige Konstruktionen heißen in der juristischen Sprache „Verbot mit Erlaubnisvorbehalt und bilden ein wirksames Kontroll-Instrument. „Freiheit“ im Umgang mit personenbezogenen Daten kann für die Betroffenen schwere Folgen haben - sie könnten leicht zu „gläsernen Bürgern“ mutieren [Ro07]. Deshalb ist die Verwendung von personenbezogenen Daten in der Regel verboten. Erlaubt ist sie nur in zwei Fällen: Wer Daten über andere Personen nutzen möchte, braucht entweder eine gesetzliche Erlaubnis oder eine ausdrückliche Einwilligung der betroffenen Person.[2]

2. Der zweite Grundsatz betrifft die Datensparsamkeit. Denn „der beste Datenschutz wird erreicht, wenn gar keine personenbezogenen Daten erhoben, verarbeitet und genutzt werden.“ [RS00] Nur in möglichst kleinem Umfang dürfen personenbezogene Daten genutzt werden, wenn eine Nutzung nicht vermieden werden kann. Nur diejenigen Daten dürfen genutzt werden, die auch tatsächlich gebraucht werden[3]. Diese Begrenzung wird uns im Zusammen mit dem Einsatz von Learning Management Systemen noch beschäftigen.

[2] Art. 7 Ziff. a) der Richtlinie
[3] Art. 6 Abs. 1 Ziff. c) der Richtlinie

3. Außerdem muss die Nutzung der Daten verhältnismäßig[4] sein. Um diesem Grundsatz zu genügen, muss die Nutzung der Daten geeignet, erforderlich und angemessen sein. *Geeignet* sind Daten, wenn sie dazu dienen, einen verfolgten Zweck tatsächlich zu erreichen. Das scheint selbstverständlich zu sein, ist im Alltag aber eine Begrenzung, die bei den verlockenden Möglichkeiten der elektronischen Datenverarbeitung nur zu leicht übergangen wird. *Erforderlich* ist die Datennutzung, wenn es kein anderes Mittel gibt, den Zweck zu erreichen [ET05].Damit ist gemeint, dass die Datennutzung nicht tiefer in den persönlichen Bereich eindringen darf, als es für den geplanten Zweck notwendig ist.

Angemessen ist eine Datenverarbeitung, wenn unter Erwägung aller Vor- und Nachteile ihre Nachteile nicht völlig außer Verhältnis ihren Vorteilen stehen [ET05]. An dieser Stelle kommt die Sinnhaftigkeit der gesamten Datennutzung in den Blick. So wäre es unangemessen, für die Teilnahme an einer Lehrveranstaltung von den Studierenden Persönlichkeitsprofile zu erheben, wobei z. B. Daten zum Freizeitverhalten abgefragt werden, die keinen Bezug zum Prüfungsgegenstand haben.

4. Ein weiterer Grundsatz im Datenschutzrecht betrifft die Zweckbindung[5]. Daten dürfen nur für einen vorher festgelegten Zweck genutzt werden. Erhobene Daten dürfen nicht auf Vorrat gesammelt und dann für jeden Zweck eingesetzt werden, der sich gerade bietet. Werden demnach für die Nutzung einer Lernplattform e-Mail-Adressen der Studierenden gesammelt, so dürfen diese später nicht verwendet werden, um ehemalige Studierende zu einem Alumni-Treffen einzuladen.

5. Der fünfte Grundsatz verpflichtet die Verwender von Daten zur Transparenz: Die betroffenen Personen haben das Recht, umfassend über die Art und den Umfang und die Dauer der Datenverwendung informiert zu werden. Ebenso besteht eine Pflicht der Datenverwender, den Betroffenen diese Informationen zugänglich zu machen.[6]

Allein diese Grundsätze machen deutlich, dass der Datenschutz aus Sicht der einzelnen Betroffenen willkommene Schutzmechanismen und aus Sicht der Datennutzer unangenehme Einschränkungen mit sich bringt. Diese konfliktträchtige Situation macht es sinnvoll, diejenigen Daten näher zu beschreiben, die von den Datenschutzregeln überhaupt erfasst werden. Wenn es gelingt, die eigenen Aktivitäten außerhalb der vom Datenschutz erfassten Informationen zu halten, muss man auf die beschriebenen Konflikte keine Rücksicht nehmen.

[4] Art. 6 Abs. 1 Ziff. c) der Richtlinie
[5] Art. 6 Abs. 1 Ziff. c) der Richtlinie
[6] Art. 10- 12 der Richtlinie

3.2 Personenbezogene Daten

Der Datenschutz erfasst alle personenbezogenen Daten. Daten sind personenbezogen, wenn sie das Identifizieren einer Person möglich machen[7], z. B. der Name, die Adresse, die Telefonnummer, das Geburtsdatum, ein Foto oder auch die e- Mail Adresse. Einzelne, auf den ersten Blick belanglos erscheinende Daten, können in Verbindung mit anderen Daten als Teil einer Hinweiskette einen Personenbezug bekommen. Daten haben also einen dynamischen Charakter. Sie können harmlos sein, aber durch Kombination Eigenschaften erzeugen, die sie zu personenbezogenen Daten machen [PS04].

Vom Datenschutz erfasst sind außerdem alle Arten des Umgangs mit personenbezogenen Daten: Jede Form der Beschaffung und jede Form der Verarbeitung ist erfasst[8] . Damit unterliegt jede Logfunktion in einem LMS ebenso dem Datenschutz wie die Auswertung von Nutzerprofilen. Da auch das Verändern, Übermitteln, Sperren und Löschen oder anderweitige Auswerten vom Datenschutzregeln erfasst wird, gibt es beim Betrieb eines LMS nur zwei Wege, den Datenschutz auf legale Weise zu umgehen.

3.3 Pseudonymisierung und Anonymisierung

Indem Daten anonymisiert oder pseudonymisiert werden, entzieht man sie dem Zugriff der Einschränkungen. Bei der Anonymisierung wird auf alle Daten verzichtet, die einen Bezug zu einzelnen Personen ermöglichen. Bei der Pseudonymisierung wird der Name durch einen offensichtlichen Phantasienamen ersetzt. Alle weiteren Hinweise auf eine individuelle Person werden entfernt. Dadurch wird der Schutz der betroffenen Person gewährleistet und die Daten können in voller Freiheit genutzt und weitergegeben werden.

4. Deutschland

Die Datenschutz-Regelungen in Deutschland orientieren sich an der europäischen Datenschutzrichtlinie, da die Vorgaben der Richtlinie in das nationale Recht der Mitgliedsstaaten umgesetzt werden mussten[9].

In Deutschland wird die Regelungsstruktur dadurch etwas unübersichtlich, dass einschlägige Regelungen auf verschiedenen Ebenen in der Gesetzeshierarchie erlassen wurden. Sowohl auf der Ebene des Bundes als auch auf der Ebene der Länder sind Datenschutzregeln zu finden. Auf der Bundesebene werden wir uns im Bundesdatenschutzgesetz und im Telemediengesetz umschauen. Auf der Landesebene werden Datenschutzgesetze in Schleswig Holstein und Hessen nach Regelungen zum E-Learning an Hochschulen durchsucht.

---

[7] Art. 2a der Richtlinie
[8] Art. 3 I der Richtlinie
[9] Art. 4 Abs. 1 EG Vertrag

4.1 Bundesdatenschutzgesetz (BDSG)

Das Bundesdatenschutzgesetz enthält in § 40 einige Regelungen zum Schutz von personenbezogenen Daten als Gegenstand wissenschaftlicher Forschung. Um diese zentrale Vorschrift besser zu verstehen, ist einkurzer Ausflug in die juristische Methodik hilfreich. Bei der wissenschaftlichen Auswertung personenbezogener Daten kann es zu einer Kollision der Interessen der Forschenden mit den Interessen der Betroffenen kommen (Veröffentlichungsinteresse der Forschenden gegen Geheimhaltungsinteresse der Betroffenen). Die Regelungen in § 40 BDSG sind das Ergebnis einer grundlegenden juristischen Methode der Konfliktlösung – der sog. Interessenabwägung [ET05]. Dabei werden die Standpunkte der Kontrahenten darauf hin untersucht, welche Aspekte jeweils zu ihren Gunsten sprechen. Die Aspekte für die eine oder andere Seite werden dann gegeneinander abgewogen, um herauszufinden, welche Aspekte schwerer wiegen. Dieses Prinzip der Konfliktlösung ist auch im alten Symbol der „Justitia“, der Göttin der Gerechtigkeit zu finden: Die Göttin hält eine Waage in der Hand [Ki84].

Zu Gunsten der einzelnen Betroffenen wirkt es sich aus, wenn die erhobenen Daten sehr exakt sind und ein genaues Bild der Personen zeichnen. Eine Erhebung oder gar Veröffentlichung derartiger Daten wäre ein intensiver Eingriff in die Privatsphäre der Betroffenen. Ebenso würde es eine Hürde darstellen, wenn innerhalb einer Datenkette nur wenige Schritte zur Identifikation einer Person führen. Wenn Daten aus mehreren Lebensbereichen erhoben und verbunden werden, spricht ebenfalls viel dafür, dass die Interessen der Betroffenen bei einer Regelung stark zu berücksichtigen sind [MW02].

Es kann aber auch Aspekte geben, die die Position der Forschenden stärken. Wenn die Erhebung und Verarbeitung der Daten für das Erreichen des Forschungszieles unverzichtbar sind, spricht für eine Verwendung in der Wissenschaft. Ein hohes öffentliches Interesse an den Forschungsergebnissen, z.B. in der Krebsforschung kann die Schwelle zur Rechtmäßigkeit einer Datennutzung senken [MW02]. Deutlich formulierte und kontrollierte Datenschutzregeln innerhalb eines Forschungsinstitutes stärken die Position der Forscher, wenn sie eine wirksame Organisation und Kontrolle der Verantwortlichkeiten im Umgang mit personenbezogenen Daten dokumentieren[10].

Aus diesen Gründen gewährt § 40 BDSG in Bezug auf die Datenverarbeitung für wissenschaftliche Zwecke kein unbegrenztes Recht. Die Datenverarbeitung von personenbezogenen Daten ohne Einwilligung der Betroffenen ist bei Forschungseinrichtungen für den internen Gebrauch erlaubt, wenn die Verarbeitung für ein konkretes, wissenschaftliches Forschungsvorhaben erfolgt.

[10] Anlage zu § 9 BDSG

Personenbezogene Daten dürfen dabei nur soweit verarbeitet werden, wie dies für das konkrete Forschungsvorhaben notwendig ist. Wenn das Vorhaben abgeschlossen ist, müssen die Daten gelöscht werden. Sie können in Ausnahmefällen unter Verschluss gehalten werden, wenn nur auf diese Weise eine Verifikation der Forschung möglich ist [MW02]. In jedem Fall müssen die personenbezogenen Daten jedoch so früh wie möglich anonymisiert oder pseudonymisiert werden[11], um so den Eingriff in die Selbstbestimmungsrechte der Betroffenen so gering als möglich zu halten. Kritisch wird die Sachlage jedoch, wenn die Forschungsergebnisse durch Publikation nach außen gegeben werden sollen. Für die Veröffentlichung personenbezogener Daten muss vorher eine Einwilligung der Betroffenen eingeholt werden[12]. Der Eingriff in die Selbstbestimmungsrechte der Betroffenen ist hier so intensiv, dass die Entscheidung über eine Veröffentlichung den Betroffenen in die Hand gegeben wird.

Einschlägige Regelungen zum E-Learning an Hochschulen sind im Bundesdatenschutzgesetz nicht enthalten.

4.2 Datenschutzgesetze der Bundesländer

Auch in den Datenschutzgesetzen der Bundesländer gibt es Regelungen zur Nutzung von Daten in der Wissenschaft. Die Gesetzgeber auf Landesebene haben aber in vielen Fällen andere Entscheidungen getroffen. So wird z. B. in § 33 des hessischen Datenschutzgesetzes nicht zwischen interner Datennutzung und Veröffentlichung unterschieden. In beiden Fällen muss vorher die Einwilligung der Betroffenen eingeholt werden. Auf eine Einwilligung darf ausnahmsweise nur dann verzichtet werden, wenn ein besonderes Interesse der Allgemeinheit besteht. Eine Verarbeitung pesonenbezogener Daten ist auch dann ohne Einwilligung erlaubt, wenn diese Erhebung vorher von der Hessischen Datenschutzbehörde genehmigt wurde. Die Behörde prüft dabei, ob bei der geplanten Datennutzung die Grundsätze des Datenschutzes in angemessener Weise eingehalten werden. Ohne Einwilligung der Betroffenen sind in Hessen die Wege zur Verwendung personenbezogener Daten in der Wissenschaft sehr schmal.

Das Datenschutzgesetzes Schleswig-Holstein enthält in § 22 eine Entscheidung, die näher am Rahmen des Bundesdatenschutzes liegt. Hier ist die Hierarchie der Maßnahmen deutlich zu erkennen: Wenn möglich, sollen die Daten anonymisiert oder pseudonymisiert werden[13]. Wenn dies nicht möglich ist, dürfen Daten mit Einwilligung der Betroffen oder mit Genehmigung durch die Datenschutzbehörde genutzt werden[14].

[11] § 40 Abs. 2 BDSG
[12] § 40 Abs. 3 Nr. 1 BDSG
[13] § 22 Abs. 1 DSG-SH
[14] § 22 Abs. 3 DSG-SH

Regelungen in den Landesdatenschutzgesetzen können also durchaus voneinander abweichen. Bei Kooperationen zwischen Hochschulen in verschiedenen Bundesländern bergen die unterschiedlichen Datenschutzniveaus verdeckte Fußangeln. Ein Datenaustausch im Gesamtprojekt ist nur dann möglich, wenn sich alle beteiligten Hochschulen an die Regeln des strengsten Datenschutzregimes halten.

Die Suche nach Erlaubnissen wird bei anderen Gesetzen fortgesetzt, die einen engeren Bezug zum E-Learning haben.

5. Learning Management Systeme

Für die Organisation und Durchführung von E-Learning Veranstaltungen werden Learning Management Systeme wie Moodle, ILIAS, Clix oder Black Board eingesetzt. Die Nutzung von Teilnehmerdaten zur Organisation und Verwaltung von Online Veranstaltungen ist durch Erlaubnisse in Landesgesetzen gedeckt[15]. Interessanter aus der Sicht des Datenschutzes ist die Möglichkeit, Daten über das Nutzerverhalten und über die Beiträge der Nutzer zu erheben. Soweit ein LMS als adaptives Lernsystem ausgestaltet ist, können Daten z. B. dazu verwendet werden, die Struktur der angebotenen Lerninhalte und die Gestaltung von Rückmeldungen bei Übungsaufgaben an die Bedürfnisse der Nutzer anzupassen. Ebenso ist es möglich, durch Auswertung von Präferenzen beim Lernverhalten ein Persönlichkeitsprofil eines Lernenden zu erzeugen [Se02]. Im Folgenden werden mehrere Rechtsvorschriften daraufhin untersucht, wie weit sie Erlaubnisse für die Nutzung dieser personenbezogenen Daten im universitären E-Learning enthalten.

5.1 Gesetzliche Erlaubnis

Learning Management Systeme fallen als elektronische Informations- und Kommunikationsdienste unter das Telemediengesetz[16]. Dieses Gesetz erlaubt die Erhebung und zweckgebundene Nutzung von Bestandsdaten[17], also von Daten, die für das Entstehen und für die Abwicklung eines Vertragsverhältnisses zwischen einem Diensteanbieter (Hochschule) und Nutzern (Studierende) ausgetauscht werden müssen. Beim E-Learning an einer Hochschule haben die Studierenden mit der Hochschule zwar nicht einen formalen Ausbildungsvertrag geschlossen. Die Studierenden sind aber als Studentenschaft Teil der inneren Organisation einer Hochschule. Gegenseitige Rechte und Pflichten sind in den Hochschulsatzungen geregelt[18]. Dieses Verhältnis kann wie ein Vertragsverhältnis gesehen werden.

---

[15] z.B. § 6 Landesverordnung zur Nutzung personenbezogener Daten für Verwaltungszwecke der Hochschulen in Schleswig Holstein, § 13 Hessisches Datenschutzgesetz, § 13 Immatrikulationsverordnung Hessen
[16] § 1 TMG
[17] § 14 TMG
[18] z. B. §§ 23 Abs. 1 Nr. 3; § 12 Abs. 1 Hochschulgesetz Schleswig Holstein

Das Telemediengesetz enthält die Erlaubnis[19], sog. Nutzungsdaten zu erheben und zu verwenden. Nutzungsdaten betreffen die Inhalte der genutzten Dienste. Das sind bei einem LMS die Beiträge in Chats, Foren, Workshops, etc. Damit scheint eine weitreichende Erlaubnis gefunden. Leider ist diese Erlaubnis nur dann anwendbar, wenn die Nutzungsdaten erhoben werden, um den Nutzungsumfang entgeltlicher Dienste zu bestimmen, letztlich um eine korrekte Rechnung zu stellen. Die Nutzung eines LMS an einer Hochschule durch Studierende ist aber trotz der Studienbeiträge keine entgeltliche Nutzung, die nach Umfang abgerechnet wird. Die Erlaubnis im Telemediengesetz ist nicht einschlägig.

Sogar eine Erlaubnis zur Erstellung von Nutzerprofilen ist im Telemediengesetz formuliert, wenn die Daten zur bedarfsgerechten Gestaltung von Telediensten verwendet werden[20]. Allerdings dürfen die Daten nur in anonymiserter oder pseudonymisierter Form für die Marktforschung eingesetzt werden. Diese Erlaubnis gilt also auch nicht für die Nutzung von Learning Management Systemen an Hochschulen.

Damit ist unsere Reise durch die gesetzlichen Erlaubnisse beendet[21]. Die Gesetzgeber haben sich auf allen Hierarchie-Ebenen gegen umfassende gesetzliche Erlaubnisse entschieden. Wir stehen vor einer Lücke der gesetzlichen Erlaubnisse. Diese Lücke birgt aber eine Chance, das Vertrauen der Nutzer zu gewinnen. Wenn die Datenverarbeitung an die Einwilligungen der Betroffenen gebunden wird, bekommen die Betroffenen ein Instrument in die Hand, mit dem sie selbst über die Nutzung ihrer Daten entscheiden. Sie erleben sich selbst als bestimmenden Teil der Datennutzung und verwirklichen die informationelle Selbstbestimmung [Rs00]. Um die informationelle Selbstbestimmung zu stärken, regelt § 4 Abs. 1 des Bundesdatenschutzgesetzes, dass die Verarbeitung personenbezogener Daten auch dann erlaubt ist, wenn sich die Datenverwender zwar nicht auf eine gesetzliche Erlaubnis, aber auf eine Einwilligung der Betroffenen stützen können.

5.2 Einwilligung

Die Einwilligung der betroffenen Personen vor der Datenerhebung ist eines der wichtigsten Instrumente im Datenschutz. Deshalb werden die Anforderungen an eine Einwilligung im Gesetz sehr genau beschrieben. Einwilligungen sind nur dann bindend, wenn sie mehrere Voraussetzungen erfüllen[22].

So muss die Einwilligung freiwillig erteilt worden sein. Zwang, Drohung oder Täuschung sind verboten. Betroffene können sich in solchen Fällen auf die Unwirksamkeit der Einwilligung berufen.

---

[19] § 15 Abs. 1 TMG
[20] § 15 Abs. 3 TMG
[21] z. B. gibt es in der einschlägigen Landesverordnung Schleswig Holstein keine Erlaubnis, Daten zur Erstellung von Nutzerprofilen zu erheben oder zu verwenden.
[22] § 4a BDSG

Die Einwilligung muss darüber informieren, was mit den erhobenen Daten geschieht. Umfassend müssen die erhobenen Daten beschrieben werden. Art und Dauer der Verwendung müssen ebenso deutlich gemacht werden wie der Zeitpunkt der Datenlöschung. Von der Einwilligung ist nur das gedeckt, was ausdrücklich beschrieben wurde. Was nicht beschrieben wurde, darf auch nicht geschehen. Formulierung wie „unter anderem werden folgende Daten erhoben …“ sind unbrauchbar, weil ihnen Eindeutigkeit fehlt. Wenn sich im Laufe einer Datennutzung das Ziel der Datenverarbeitung ändert und wenn diese Änderung zu einer neuen Form der Datennutzung führt, müssen ergänzende Einwilligungen eingeholt werden. So wäre es ein Verstoß gegen § 4a BDSG, wenn Teilnehmerdaten einer Online-Lehrveranstaltung für Innenarchitekten ohne Einwilligung an Baumärkte weitergegeben werden.

Außerdem darf die Einholung der Einwilligung nicht an sachfremde Bedingungen geknüpft werden. So ist es beispielsweise rechtswidrig, die Teilnahme an einer Prüfung davon abhängig zu machen, dass die Einwilligung zur Teilnahme an einer Fragebogenaktion des Marktforschungsinstitutes XY erteilt wird.

Die Einwilligung muss auch einen Hinweis darauf enthalten, dass jedem Betroffenen ein folgenloses Widerrufsrecht zusteht. Der Widerruf ist jederzeit möglich. Wenn Betroffene ihre Einwilligung widerrufen, dürfen ihnen hierdurch keine Nachteile gegenüber denjenigen entstehen, die nicht widerrufen haben [ET05]. So könnten Studierende, die in der Lernphase anderen Aktivitäten den Vorzug gegeben haben, auf folgende Idee kommen: Eine vor Beginn einer Online-Veranstaltung erteilte Einwilligung wird widerrufen, denn an der abschließenden Online-Klausur will der Studierende nicht teilnehmen. Die Nicht-Teilnahme an der Klausur dürfe aber keine negativen Folgen haben, weil keine Nachteile gegenüber denjenigen entstehen dürften, die nicht widerrufen haben. Derartige Argumente sind aber ein Missbrauch des Widerrufsrechtes. Der Widerruf wäre unwirksam und der Studierende wäre nicht von der Teilnahmepflicht befreit.

Studierende können ihre Einwilligung auch nicht mit der Begründung zurückziehen, die Teilnahme an der Prüfung wäre nicht freiwillig. Freiwillig war zunächst die Entscheidung, an einer Universität zu studieren, die ihre Studierenden prüft. Freiwillig ist auch die Entscheidung, sich auf einen Studiengang einzulassen, der verbindliche Prüfungsleistungen fordert. Solange diese Grundsatzentscheidung freiwillig getroffen wurde, müssen die Studierenden die Konsequenzen dieser Entscheidung tragen. Ein Widerruf wäre z.B. dann möglich, wenn sich herausstellt, dass der Text der Einwilligung eine wesentliche Lücke enthält und dass während der Veranstaltung Daten erhoben wurden, die weder in einer gesetzlichen Erlaubnis noch in einer Einwilligung beschrieben sind.

Einwilligungen können auch auf elektronischem Weg eingeholt werden. Dies erleichtert die Ausübung des Rechtes auf informationelle Selbstbestimmung in der digitalen Welt.

5.3 Elektronische Einwilligung

Die juristischen Anforderungen an eine elektronische Einwilligung zielen darauf, eine elektronische Entsprechung zur eigenhändigen Unterschrift auf einem Blatt Papier zu erzeugen[23]. So muss die Einwilligung eine eindeutige und bewusste Handlung darstellen. Alle einwilligenden Nutzer sollen durch Anklicken in einem ersten Schritt zu erkennen gibt, dass sie den Inhalt der Einwilligung gelesen und verstanden haben. Dass ein Anklicken diese Bedeutung hat, muss unmissverständlich kommuniziert werden. Durch ein weiteres Anklicken wird in einem zweiten Schritt deutlich gemacht, dass die Nutzer in die beschriebene Verwendung ihrer personenbezogenen Daten einwilligen. Diese Handlungen müssen protokolliert werden und die Protokolle müssen jederzeit abrufbar sein. Die elektronischen Dokumente müssen nach dem aktuellen State of the Art [HS06] dagegen gesichert sein, dass der Inhalt der Einwilligung nachträglich unbemerkt verändert werden kann. Weitere technische Maßnahmen müssen die eindeutige Identifikation einer Person als Urheber der Einwilligung ermöglichen.

Wenn diese Anforderungen erfüllt werden, ist die elektronische Einwilligung ein einfacher und schneller Weg, die informationelle Selbstbestimmung in einer digital geprägten Welt zu sichern. Eine Gesetzgebung, die in sensiblen Bereichen auf die Formulierung von Erlaubnissen verzichtet und die Entscheidung über eine Beteiligung in die Hände der Betroffenen legt, stärkt den Ausgleich gegensätzlicher Interessen und damit das Vertrauen der Beteiligten in die Mechanismen der Informationsgesellschaft.

6. Fazit

Das Gesetz gestattet die Verarbeitung personenbezogener Daten ist nur in zwei Fällen: Die Verarbeitung muss durch eine gesetzliche Erlaubnis oder durch eine Einwilligung gedeckt sein[24]. Diese Aufzählung ist abschließend. Weitere Fälle einer gesetzlich gedeckten Verarbeitung hat der Gesetzgeber nicht definiert.

Existierende gesetzliche Erlaubnisse decken die bei einem adaptiven Lernsystem anfallenden personenbezogenen Daten nur unvollständig. Daher kann nur eine Einwilligung der Studierenden die vollständige Legalität von solchen Verarbeitungen sichern, die über die gesetzlichen Erlaubnisse hinaus gehen.

[23] § 13 Abs. 2 TMG
[24] § 4a BDSG

Literaturverzeichnis

[Bö01] Böhme- Nessler, V.: Cyberlaw- Lehrbuch zum Internet- Recht, Verlag C. H. Beck, München, 2001.

[Bu06] Bull, H.: Zweifelsfragen um die informationelle Selbstbestimmung – Datenschutz als Datenaskese? In: Neue Juristische Wochenschrift 2006, Heft 23, Beck-Verlag, München 2006, S. 1617-1624.

[Bv83] Bundesverfassungsgericht: Volkszählungsurteil. In: Entscheidungen, Band 65, Beck-Verlag München, 1984, S. 1-50.

[Ca08] Capurro, R.: Zwischen Vertrauen und Angst. Über Stimmungen der Informationsgesellschaft. In: (Klumpp, d. et. Al. Hrsg.): Informationelles Vertrauen für die Informationsgesellschaft, Springer-Verlag, Heidelberg 2008, S. 53 – 62.

[ET05] Ehmann, E.; Tinnefeld, M.: Einführung in das Datenschutzrecht, Oldenburg Verlag, München, 1998.

[HS06] Hansen, J.; Selmeczi, K.: Legal Chances and Restrictiona in International Research Projects. In (Dittmann, J. et. al. Hrsg.): New Advances in Multimedia Security, Biometrics, Watermarking and Cultural Aspects, Logos Verlag, Berlin, 2006, S. 135 – 160.

[Ki84] Kissel, O.: Die Justitia- Reflexion über ein Symbol und seine Darstellung in der bildenden Kunst, Verlag C. H. Beck, München, 1984.

[MW02] Metschke, R.; Wellbrock, R.: Datenschutz in Wissenschaft und Forschung. In: Berliner Beauftragter für Datenschutz und Informationsfreiheit (Hrsg.): Materialien zum Datenschutz, Bd. 28, Berlin, 2002, S. 1- 84.

[PS04] Piroth, B.; Schlink, B.: Grundrechte Staatsrecht II, Verlag C. H. Beck, Berlin/ Münster, 2004.

[Ro02] Roßnagel, A.: Handbuch des Datenschutzrecht, Verlag C. H. Beck, Kassel/Saarbrücken 2002.

[Ro07] Roßnagel, A.: Datenschutz in einem informatisierten Alltag, Friedrich Ebert Stiftung, Bonn, 2007.

[RS00] Roßnagel, A.; Scholz, P.: Datenschutz durch Anonymität und Pseudonymität- Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR, München, 2000.

[Sh04] Schwabe, J. (Hrsg.): Entscheidungen des Bundesverfassungsgericht: Studienauswahl (Band 1- 109), Selbstverlag Hamburg, 2004.

[Se02] Seeberg, C.: Life Long Learning, Springer-Verlag, Heidelberg, 2002.