Ansätze für eine informationelle Gewaltenteilung in Lernplattformen

Reinhard Keil, Felix Winkelnkemper

Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn
{reinhard.keil; felix.winkelnkemper}@uni-paderborn.de

Abstract: Der Alltag von Lehrenden und Lernenden an den Hochschulen ändert sich zunehmend durch netzbasierte Lernplattformen. Werden diese unbedacht und unreflektiert verwendet, bleibt dabei das verbriefte Recht auf informationelle Selbstbestimmung auf der Strecke. Der Datenschutz lässt sich jedoch nicht „einfach so" einführen. Dieser Beitrag stellt mit dem Konzept der informationellen Gewaltenteilung einen Ansatz vor, wie sich Datenschutzinteressen erfassen und in Konsequenzen für die technische und organisatorische Gestaltung von Lernplattformen umsetzen lassen, ohne dass man Experte in juristischen Fragestellungen sein müsste.

1 Einleitung

Die Einführung internetbasierter Systeme an den Hochschulen hat den täglichen Umgang von Studierenden, Lehrenden und Hochschulangestellten nachhaltig verändert. Die Zeiten, in denen Prüfungsanmeldungen auf Zetteln bei den Prüfungsämtern abgegeben wurden, gehen dem Ende entgegen. Auch Briefkästen, in die Studierende einst Lösungen von Heimübungsblättern eingeworfen haben, verwaisen zusehends. Aushänge mit Klausurterminen und Klausurergebnissen sind ebenso verschwunden wie die Seminarlisten zu Semesterbeginn an den Türen der Lehrenden. Doch die internetbasierten Systeme zur Lehr-, Lern- und Prüfungsunterstützung sind nicht nur ein Ersatz für die althergebrachten Arbeitsweisen der Prüfungsorganisation und der Verwaltung von Lehrmaterialien. Web-2.0-Technologien, wie zum Beispiel Wikis und Blogs, sowie moderne Diskursstrukturierungsverfahren (vgl. z. B. [Bl05]) sind in die Systeme integriert und können von den Lehrenden in ihre didaktischen Konzepte eingebunden werden.

Während derart integrierte Systeme allgemein als praktisch angesehen werden und viele Abläufe erleichtert haben, wurde die Betrachtung des Datenschutzes dabei bisher weitgehend vernachlässigt. Das Urheberrecht und die aus ihm entstehenden Probleme standen zunächst im Vordergrund. So widmete sich die im Jahr 2001 im Auftrag des Ministeriums für Schule, Wissenschaft und Forschung des Landes NRW erstellte Publikation „Update – Ratgeber Multimediarecht für die Hochschulpraxis" ausschließ-

lich dem Urheberrecht [Ve01]. Eine Studie aus dem Jahr 2002 mit dem Titel „Anforderungen an eine E-Learning-Plattform. Innovation und Integration“, die im Auftrag desselben Ministeriums erstellt wurde, enthielt zwar bereits einen Abschnitt zum Problemfeld Datenschutz, allerdings finden sich unter der entsprechenden Überschrift nur zwei Sätze: „Bei der Verwendung einer E-Learning-Plattform sind auch Datenschutzprobleme zu berücksichtigen. Personenbezogene Daten, insbesondere natürlich Prüfungsergebnisse, müssen gemäß den geltenden Datenschutzrichtlinien vor unbefugtem Zugriff geschützt werden.“ [Do02] Die weiteren Ausführungen beschäftigen sich mit dem Thema Urheberrecht. Erst 2011 hat der Beauftragte für den Datenschutz des Landes Nordrhein-Westfalen [LDI11] Hinweise gegeben, wie „E-Learning an Hochschulen nach den Grundsätzen des Datenschutzes“ durchgeführt werden soll. Darin werden juristische Anforderungen beschrieben, jedoch wird nicht direkt auf die Ausgestaltung von Lernplattformen eingegangen. Mit den Beiträgen von Eibl [Ei08] sowie Loser und Herrmann [LH09] auf der DeLFI-Jahrestagung gab es erste Hinweise aus der Informatik zu dieser Problematik. Sie untersuchten einige Plattformen in Bezug auf die Einhaltung datenschutzrechtlicher Anforderungen und formulierten erste Gestaltungshinweise. Einen ausführlichen Überblick über die Datenschutzproblematik beim E-Learning gibt die Studie von Roßnagel und Schnabel [RS09]. Sie verdeutlicht insbesondere den Umfang und die Komplexität der Problematik und macht konkrete Vorschläge für Datenschutzordnungen an Hochschulen.

Die allgemeinen Hinweise, Anforderungen und juristischen Erläuterungen zum Datenschutz lassen sich jedoch nur schwer konstruktiv im Alltag bei der Nutzung, der Entwicklung oder der Konfiguration von Lernplattformen umsetzen. Es fehlt an konkreten Handlungsanweisungen, wie ein Lernszenario oder seine technische Umsetzung datenschutzkonform angepasst werden können. Zudem mangelt es häufig an Akzeptanz für die Datenschutzproblematik, sodass die Vorschriften die Arbeit an den Hochschulen eher zu behindern als zu fördern scheinen. Die in diesem Beitrag propagierte informationelle Gewaltenteilung soll die Gewärtigkeit für die Datenschutz-Problematik erhöhen, indem sie die beteiligten Akteure identifiziert und den Fokus auf die kritischen Stellen in ihrer Zusammenarbeit legt, an denen Interessen geschützt werden müssen. Die Grundlage für unsere Überlegungen ist dabei das Recht auf informationelle Selbstbestimmung, das als Grundlage des modernen Datenschutzes gilt und aus dem Volkszählungsurteil des Bundesverfassungsgerichts [Bu83] hervorgeht.

> *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. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.*

Überträgt man diesen Gedankengang auf Lernplattformen, bedeutet dies, dass sich die Nutzer des Systems eventuell anders verhalten, wenn sie nicht absehen können, welche Daten von ihnen erhoben und wie diese Daten dann verwendet werden. Beispiele hierfür folgen in Abschnitt 2. Aus dem Recht auf informationelle Selbstbestimmung leiten sich eine Reihe weiterer grundlegender Anforderungen ab, die sich im Bundesdatenschutzgesetz und den Datenschutzgesetzen der Länder finden.[1] Die Grundlage dieser Gesetze ist das „Verbot mit Erlaubnisvorbehalt", das heißt, dass zunächst einmal die Erhebung und Speicherung von personenbezogenen Daten verboten sind, wenn sie nicht explizit erlaubt sind. Eine solche Erlaubnis kann entweder durch ein Gesetz oder durch eine explizite, freiwillige Zustimmung erfolgen. Die Datenschutzgesetze definieren nicht, welche Nutzung verboten ist, sondern definieren, in welchem Rahmen eine Nutzung erlaubt ist. In diesem Sinne stellen die Gesetze einige grundlegende Anforderungen:

Datensparsamkeit [Bu09, §3a] soll sicherstellen, dass Daten nicht in beliebigem Umfang erhoben und gespeichert werden. So würde beispielsweise das Speichern des Alters der Studierenden in einem Computersystem zur Prüfungsanmeldung gegen die Datensparsamkeit verstoßen, wenn es für die Erledigung der Aufgabe des Prüfungsamts nicht unbedingt erforderlich ist. Dabei ist zu beachten, dass nicht alle gespeicherten Daten eines Datensatzes auch für jeden Nutzer eines Systems angezeigt werden dürfen. So ist es für ein Prüfungsamt zum Beispiel erforderlich zu wissen, wie oft Studierende eine Prüfung abgelegt haben; für die Durchführung der Prüfung selbst ist dies jedoch nicht von Belang.

Aus der Zweckbindung [Bu09, §4] ergibt sich das Verbot, Daten, die für einen bestimmten Zweck erhoben wurden, an anderer Stelle zu verwenden. Sie kommt damit der Befürchtung entgegen, dass Daten ohne weiteres weiterverarbeitet werden können. Werden zum Beispiel für das Versenden aktueller Informationen in einem Kurs E-Mail-Adressen erhoben, dürfen diese nicht in anderen Kursen oder für andere Zwecke genutzt werden.

Probleme mit der Einhaltung der Datenschutzvorschriften beginnen spätestens dann, wenn eine Plattform die Phase der testweisen und eingeschränkten oder freiwilligen Nutzung in einer Hochschule verlässt und in den Massenbetrieb übergeht. So brachte das Datenschutz-Audit [Ho09] für die Lernplattform koaLA[2] (koaktive Lern- und Arbeitsumgebung) an der Universtiät Paderborn einige Probleme zum Vorschein. Da es stets erklärtes Ziel von koaLA war, Studierende untereinander in Kontakt zu bringen und so auch eigenverantwortliches und selbstorganisiertes Arbeiten zu fördern, waren über das System in den von den Studierenden belegten Veranstaltungen Teilnehmerlisten verfügbar. Hier waren alle Teilnehmer des Kurses mit Klarnamen gelistet. Ein Klick auf einen Namen führte zu einem Nutzerprofil, in das der Nutzer neben Namen und Bild auch Interessen, Kontaktadressen etc. eintragen konnte.

[1] Hochschulen in Deutschland sind Einrichtungen der Länder und unterliegen dementsprechend den jeweiligen Landesdatenschutzgesetzen. Diese unterscheiden sich vom Bundesdatenschutzgesetz in den hier angesprochenen Aspekten nicht.
[2] Siehe http://koala.upb.de.

Diese Praxis wurde im Rahmen des Audit-Prozesses (siehe [Ho09]) kritisiert und inzwischen behoben. Im Kern der Kritik stand dabei nicht, dass das System überhaupt eine Liste der Teilnehmer des Kurses bereitstellt. Die Notwendigkeit einer solchen Liste ist für den Veranstalter sicher gegeben und auch durch die Einschreibeordnung der Universität, die die Datenerhebung zur Durchführung von Lehrveranstaltungen und Prüfungen regelt, abgesichert. Dies gilt jedoch nicht für Teilnehmerlisten, die den Studierenden zugänglich gemacht werden. Zwar gibt es Ausnahmefälle, in denen solche Listen aus didaktischen Gründen heraus legitim sind, in der überwiegenden Zahl der Fälle ist dies jedoch nicht der Fall. Loser und Herrmann [LH09] haben beispielsweise festgestellt, dass an zwei von ihnen untersuchten Universitäten in mehr als 90% der durchgeführten Veranstaltungen die Lernplattformen lediglich zur Bereitstellung von Lehr- und Lernmaterialien genutzt werden. Soll es dennoch eine Teilnehmerliste für Studierende geben, so wäre das nur möglich, wenn die einzelnen Studierenden hier explizit zustimmten. Es reicht dabei nicht, die Nutzung der Plattform als solche in einer Datenschutzerklärung als freiwillig zu deklarieren und hierbei zu regeln, dass Teilnehmerlisten in den Veranstaltungen zur Verfügung stehen. Dies wäre nur dann akzeptabel, wenn die Nutzung der Systeme tatsächlich freiwillig wäre. Dies war aber beim an der Universität Paderborn eingesetzten koaLA nicht der Fall. Da das System in einer Vielzahl von Veranstaltungen für die Materialverteilung eingesetzt wird und Materialien auch ausschließlich hierüber verteilt werden, besteht ein faktischer Zwang zur Nutzung des Systems. Nach einer Abwägung des Nutzens der Funktion im Vergleich zum technischen Aufwand einer Umstrukturierung wurden Teilnehmerlisten für die Studierenden zunächst gänzlich entfernt. Lehrenden stehen sie weiterhin zur Verfügung.

Um Datenschutzprobleme wie das vorgenannte lösen zu können, muss eruiert werden, welche Schutzinteressen vorliegen und auf welche Weise diesen Interessen entsprochen werden kann. Hierbei greifen didaktische Fragen, technische Lösungen und organisatorische Maßnahmen ineinander. Die Lehrenden müssen zunächst entscheiden, welche Daten überhaupt notwendig sind. Was nicht notwendig ist, darf gar nicht erst erhoben werden. Die Aufgabe der Techniker ist es dann, klare Schnittstellen zu schaffen, die dafür sorgen, dass alle Beteiligten stets nur auf die für sie relevanten Daten Zugriff haben. Mit organisatorischen Maßnahmen kann dann als letztes dafür gesorgt werden, dass auch an Stellen, an denen eine technische Umsetzung vielleicht unzureichend ist oder nicht beeinflusst werden kann, dennoch ein Schutz der Interessen zu erreichen ist.

2 Informationelle Gewaltenteilung in Lernplattformen

Ein Grundproblem bei der Akzeptanz des Datenschutzes, aber auch bei seinen konkreten Implikationen für die Praxis, ist häufig, dass die unterschiedlichen Schutzinteressen und die daraus resultierenden Folgen nicht erkannt werden. Einen Ansatz hierfür soll das Konzept der informationellen Gewaltenteilung bieten, das sich ebenfalls aus dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 [Bu83] ableitet. Hierbei geht es darum, dass verschiedene Stellen der gleichen Organisation nicht alle Informationen vereinen, sondern innerhalb der Organisation Schranken einziehen, die eine beliebige Kombination der Daten verhindern. Datenschutzprobleme treten dann auf, wenn das Interesse einer Partei, Daten über die andere zu erhalten, dem Schutzinteresse

dieser Partei entgegenstehen. Die Grundannahme bei der informationellen Gewaltenteilung ist hier, dass jede beteiligte Partei nur den Teil der Daten verwaltet, der für sie von Belang ist und ferner nur dann Daten an eine andere Partei überträgt, wenn diese sie für die Durchführung ihrer Aufgaben unbedingt braucht.

Das Prinzip lässt sich gut am Beispiel der Parteien Prüfer und Prüfungsamt verdeutlichen, da in diesem Bereich die Gewaltenteilung bereits durch Vorschriften gesichert ist. Die personenbezogenen Daten, die Lehrende zum Erstellen einer Prüfungsbewertung ansammeln (Übungsabgaben, Prüfungspunkte, Hausarbeiten etc.), bleiben eine definierte Zeit bei ihnen gespeichert und werden dann systematisch gelöscht. Nach der Prüfung wird das Prüfungsergebnis an das Prüfungsamt übergeben, das alle Leistungen sammelt und den Studierenden zu Prüfungen zulässt etc. Die Daten des Prüfungsamts (andere Noten, Nebenfächer etc.) werden wiederum nicht an die Prüfenden herausgegeben, insofern das nicht nötig ist. Der Datenfluss zwischen Prüfer und Prüfungsamt ist also absichtlich minimal gehalten. Der Großteil der bei einer Partei anfallenden Daten wird der jeweils anderen Partie nicht übermittelt.

Für die folgenden Überlegungen werden die Parteien Lehrende, Studierende und externe Dienste betrachtet, da es zwischen ihnen zu Datenschutzproblemen kommt, die im Rahmen der Lernplattformen gelöst werden müssen. Die identifizierten Stellen haben Schutzinteressen, die durch Schranken voneinander abgegrenzt werden. Gleichzeitig gibt es zwischen diesen Parteien häufig noch keine Vorschriften und Regelungen, die die Gewaltenteilung festlegen würden. Auf Grund der Vielzahl denkbarer Szenarien wird dies auch in der Praxis oft gar nicht möglich sein. Aus der Beschreibung der im Folgenden formulierten Schranken kann dann relativ leicht auf infrastrukturelle, technische oder organisatorische Maßnahmen und Ansätze für die konkrete Gestaltung von Lernplattformen geschlossen werden, die den Interessen der jeweiligen Stellen gerecht werden.

2.1 Schranke Lehrende – Studierende

Charakteristisch für eine Kommunikation zwischen Studierenden und Lehrenden ist ein starkes Machtgefälle. Lehrende bewerten die Leistung der Studierenden. Jegliche Äußerung der Studierenden kann dabei potenziell Teil dieser Bewertung werden. Dies impliziert, dass Studierende ein hohes Datenschutzinteresse haben. Informationelle Gewaltenteilung bedeutet hier, dass Daten der Studierenden, die sie den Lehrenden nicht explizit zukommen lassen wollen, diese auch nicht erreichen oder sie zumindest nicht ihnen direkt zuzuordnen sind.

Probleme entstehen zum Beispiel bei Rückkanälen in Lernplattformen. Die meisten Lehrenden würden, das ist hier zumindest zu unterstellen, Äußerungen in Foren nicht nachteilig in die Bewertung der Studierenden einfließen lassen. Wichtig ist jedoch nicht, ob es eine tatsächliche Benachteiligung gibt, sondern ob von Seiten der Studierenden eine solche Benachteiligung vermutet werden kann. Parallel zur Begründung des Bundesverfassungsgerichts gilt hier: „Wer unsicher ist, ob negative oder vorgeblich ‚dumme' Äußerungen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche

Verhaltensweisen aufzufallen.“ [LH09] zitieren einen Studierenden mit der Aussage „Da werden eh nur die schlauen Fragen gestellt. Die dummen werden doch woanders diskutiert.“. Diesem Manko kann in Bezug auf Rückkanäle nur entgangen werden, wenn auch Nachfragen gestellt werden können, ohne dass ein direkter Personenbezug hergestellt werden kann. Lösbar wäre dies beispielsweise durch die Nutzung eines Pseudonyms anstelle der zwanghaften Verwendung des Klarnamens oder gar eine auch für die Lehrenden anonyme Nutzung. Abgesehen von Datenschutzvorschriften entgehen den Lehrenden durch die fehlende Möglichkeit der Pseudonymisierung oder Anonmyisierung auch die eigentlich erwarteten Rückmeldungen.

Ein ähnliches Problem entsteht übrigens beim Einsatz von Wikis in der Hochschullehre. Da es bei einem Wiki üblich ist, dass alle alten Versionen des Textes stets zugreifbar bleiben, liegt für die Studierenden die Befürchtung nahe, dass auch ihre „dummen“, noch unausgegorenen Gedanken aus diversen Zwischenversionen herangezogen und bewertet werden. Die Konsequenz ist wiederum eine Anpassung an diese Situation, nämlich dass Diskussionen, Zwischenversionen etc. außerhalb des Wikis erstellt werden und dann am Ende eine abschließende Version ins Wiki gestellt wird. Ein übliches Wiki scheint also für den Hochschuleinsatz wenig geeignet. Diesem Missstand kann durch eine technische Anpassung begegnet werden: Die ins Unreine geschriebenen Zwischenversionen sind nur für den Studierenden und eventuell seine Lerngruppe interessant und bleiben daher diesen auch vorbehalten. Lehrende erhalten am Ende eine finale Version, die sie bewerten können.

Ein Interesse von Lehrenden ist es, Daten über den Lernerfolg der Teilnehmer einer Veranstaltung zu erhalten. Dem steht das Interesse des Lernenden entgegen, dass aus seinem persönlichen Lernverhalten keine negativen Folgen für ihn entstehen. Lernplattformen wie Moodle bieten Lehrenden die Möglichkeit, die Aktivitäten der Teilnehmer sehr detailliert auswerten zu können. So wird zum Beispiel ersichtlich, wer wann welches Dokument heruntergeladen hat, wer sich wann eingeloggt hat etc. Der Nutzen einer solchen Auswertung ist jedoch fraglich, da die Studierenden, sobald sie Kenntnis über die Auswertung haben, ihr Verhalten ändern, sodass sie den Auswertungskriterien entsprechen. Ein Beispiel hierfür ist den Tutoren aus einer Schule bekannt, in der zwischenzeitlich der Dienst box.net zum Dateiaustausch zwischen Lehrern und Schülern genutzt wurde. box.net ist ein Onlinespeicherdienst, in dem angemeldete Nutzer Zugriff auf einen gemeinsamen Speicherort haben und dort Dateien verwalten oder aber auch direkt ansehen können. Eigentlich zur Gruppenarbeit in Arbeitsteams gedacht, stellt der Dienst Gewärtigkeitsfunktionen bereit. Es ist zum Beispiel ersichtlich, wer ein Dokument zuletzt bearbeitet hat, wer es betrachtet oder heruntergeladen hat. Im Gruppenarbeitskontext sind diese Informationen zumindest teilweise sinnvoll, um den Überblick über den Fortgang des Projekts nicht zu verlieren. Stehen diese Informationen im schulischen Kontext zur Verfügung, verfehlen sie ihren Zweck und sorgen für ein Datenschutzproblem mit geradezu klassischen Folgen. An besagter Schule, an der box.net eingesetzt wurde, um Unterrichtsmaterialien zu verteilen, kommentierten Lehrer, dass einige ihrer Schüler die zur Verfügung gestellten Materialien nicht oder mitten in der Nacht rezipierten. Schüler reagieren darauf mit einem Ausweichverhalten. Die Unterrichtsmaterialien werden pro forma betrachtet, um nicht durch „abweichendes Verhalten“ aufzufallen. Genau so eine Verhaltensänderung

aus Machtlosigkeit über die über das eigene Verhalten erhobenen Daten ist es, die der Datenschutz verhindern soll.

Das Beispiel lässt sich auf eine Vielzahl von Szenarien aus dem Bereich des Learner Tracking übertragen: Angenommen, eine Lernplattform stellte eine Auswertung darüber zur Verfügung, wer wie viel zu einem online verfassten Text beigetragen habe. Sobald Studierenden bewusst wäre, dass ausgewertet wird, wer wie viel zum Inhalt beiträgt, würden die Studierenden sich danach verhalten und dafür sorgen, dass diese Messung ausgeglichen ausgeht. Optimiert wird also nicht die Arbeit der Studierenden, auch nicht die Aufteilung der Arbeit, sondern allenfalls der erhobene Messwert. Der Datenschutz lässt sich hier durch didaktische Überlegungen herstellen: Wenn der Lernerfolg auf diese Art und Weise ohnehin nicht gemessen werden kann, hat die Erhebung von Daten auch keinen Nutzen und kann entfallen. Wenn dennoch Messwerte erhoben werden sollen, sollte dies durch technische Maßnahmen anonymisiert erfolgen. Daraus könnten Lehrende zum Beispiel schließen, dass eines ihrer Angebote nicht wie geplant genutzt wird. Die Information ist für sie von Interesse, verletzt aber gleichzeitig die Interessen der einzelnen Studierenden nicht.

2.2 Schranke Studierende – Studierende

Loser und Hermann [LH09] führen aus, dass zwischen Studierenden kein so großes Machtgefälle herrsche, wie es zwischen Lehrenden und Studierenden der Fall sei. Es sei daher durchaus sinnvoll, dass unter Studierenden Daten verfügbar seien, auf die Lehrende keinen Zugriff haben. Das eben angesprochene abgewandelte Wiki ist ein solches Beispiel, bei dem Studierenden in einem Gruppenarbeitskontext untereinander mehr Daten zur Verfügung stehen, als hinterher den Lehrenden zwecks Bewertung zugänglich gemacht werden. Anzunehmen, alle Studierenden einer Vorlesung stünden auf einer Stufe und hätten keine gegeneinander abzugrenzenden Interessen, geht jedoch zu weit. Informationelle Gewaltenteilung bedeutet also auch, dass die Daten der einzelnen Studierenden bei ihnen selbst verbleiben, von ihnen selbst verwaltet werden und nur dann an andere Studierende weitergegeben werden, wenn dies explizit gewünscht oder unbedingt nötig ist. Es gibt für Studierende beispielsweise gute Gründe, ihre Identitäten in gewissen Zusammenhängen gerade von ihren Kommilitonen fernzuhalten, um zum Beispiel Vorurteilen auf Grund von Geschlecht oder Herkunft zu entgehen.

So stellt auch [Ho09] fest, dass die in nahezu allen E-Learning-Systemen vorhandene Funktion, dass die Teilnehmer eines Kurses eine vollständige Liste der Kursteilnehmer erhalten, nicht zulässig ist. Der oft angebrachte Zweck der Kontaktaufnahme unter den Studierenden, mit denen eine Teilnehmerliste begründet wird, kann nicht einfach erzwungen werden und kann auch nicht pauschal mit didaktischer Notwendigkeit begründet werden. Studierende können durchaus das Interesse haben, an einer Veranstaltung teilzunehmen, ohne dass sie dies durch Erscheinen auf einer Liste kundtun. Soll dennoch eine Liste bereitgestellt werden, kann dies nur für diejenigen geschehen, die mit der Veröffentlichung ihrer Daten einverstanden sind. Eine technische Maßnahme, die Interessen der Studierenden zu schützen, ist also das Verwalten expliziter Zustimmungen dafür, dass ihre jeweiligen Kontaktdaten auf einer kursweiten

Teilnehmerliste erscheinen dürfen. Eine solche Einwilligung darf natürlich nicht erzwungen werden. Nicht korrekt ist es, pauschal bei der Nutzung eines Systems festzulegen, dass die Daten aller Kursteilnehmer stets verfügbar sind.

Das Interesse, die eigenen Daten und Gedanken nicht den Mitstudierenden zu offenbaren, kann in Konflikt stehen zur Planung eines Veranstalters, der im Rahmen seiner Veranstaltung zum Beispiel Foren oder Wikis zur Aufbereitung von Inhalten nutzen will. Um eine solche Veranstaltung durchführen zu können, lässt es sich nicht vermeiden, dass die Studierenden die Beiträge der Kommilitonen und, zwecks Koordination, auch deren Kontaktdaten sehen. Nicht jeder Studierende wird dies aber wollen. Da der Einsatz didaktisch begründet ist und Pseudonyme als technische Maßnahme hier nicht in Frage kommen, bleibt als organisatorische Maßnahme daher nur das Schaffen von Transparenz. Diese bedeutet hier, dass ein Studierender schon vor seiner Entscheidung zur Teilnahme an diesem Kurs darüber informiert wird, dass seine Daten für die Kursteilnehmer öffentlich gemacht werden müssen. Diesem kann er dann zustimmen oder sich gegen eine Teilnahme entscheiden.

Wenn Lernplattformen zur Abgabe von Übungslösungen genutzt werden, müssen Studierende eigene Dokumente ins System hochladen. Die Studierenden haben hier das Schutzinteresse, dass ihre persönlichen Abgaben nicht allen anderen Studierenden zur Verfügung stehen. Diese Anforderung lässt sich technisch durch Rechtevergabe lösen. Die meisten Lernplattformen stellen ferner kursgebundene Kommunikationskanäle z. B. in Form eines Diskussionsforums, in dem inhaltliche Nachfragen gestellt werden können, bereit. Eine Nutzung dieser Rückkanäle wird meist nicht erzwungen. Studierende, die ihre Daten in das Forum eingeben, geben sie für ihren eigenen Zweck, also für genau diese Rückmeldung ein. Studierende haben hier das Interesse, eventuell auch Äußerungen machen zu können oder Dokumente hochzuladen, die nicht direkt ihnen zuzuordnen sind. Um dieser Anforderung gerecht werden zu können, sind zweierlei technische Lösungen denkbar, die unterschiedliche Konsequenzen haben.

Die einfachste Methode ist, dass die Anzeige des Erstellers bei Dokumenten und Beiträgen vom Ersteller unterdrückt werden kann. Hierbei ist klarzustellen, wer die Erzeugerdaten ggf. dennoch sieht. Bei einem Forum zur inhaltlichen Diskussion lässt sich gut begründen, dass Lehrende die Daten des Erstellers sehen, um zum Beispiel direkt mit dem Studierenden per E-Mail in Kontakt zu treten. Bei einem Forum zur Kritik an der Veranstaltung stünde dies den Interessen des Teilnehmers sicher entgegen. Nachteil an dieser Anonymisierung der Beiträge ist, dass auf diese Art und Weise schlecht auf Beiträge Bezug genommen werden kann. Die Verwendung von Pseudonymen würde es einem Teilnehmer ermöglichen, sich ohne Preisgabe seiner Person zu äußern, dennoch aber im Kontext wiedererkennbar zu bleiben. Stehen keine Pseudonyme zur Verfügung und lässt sich die Anzeige eines Erzeugers nicht unterdrücken, bleibt als letzter Ausweg nur noch eine organisatorische Maßnahme. Nutzer werden beim Hochladen von Dokumenten oder Erstellen von Beiträgen darauf hingewiesen, dass diese mit Namen erscheinen. Hinzu kommt das Angebot, Beiträge per E-Mail entgegenzunehmen, die dann über diesen Umweg anonymisiert werden. Letzteres ist natürlich nur dann sinnvoll, wenn es nicht einer der Lehrenden ist, vor dem die Identität verheimlicht werden soll.

Neben Prüfungsorganisation, Materialverteilung und dem Angebot von Rückkanälen ist es das Ziel einiger Lernplattformen, den Studierenden eine flexible Unterstützung anzubieten, ohne dass ein Zusammenhang mit einer Lehrveranstaltung bestehen muss. Das koaLA-System der Universität Paderborn erlaubt beispielsweise das freie Erstellen von Gruppen, das System bid[3], das freie Anlegen von Ordnern und Dateien sowohl mit als auch ohne Unterrichtsbezug. Den Zweck solch freier Strukturen bestimmen die Ersteller und Nutzer selbst. Es ist im Interesse der Studierenden, dass die in diesen Bereichen zwangsläufig angefallenen personenbezogenen Daten in eben diesem Nutzerkreis bleiben, insofern die Nutzer nicht einzelne Elemente explizit veröffentlichen wollen. Erlaubt ein Lernunterstützungssystem das Anlegen privater Gruppen, so müssen die innerhalb dieser Struktur eingestellten Daten, inklusive der Mitgliedschaft in der Gruppe, für den Rest der Nutzer verborgen bleiben.[4] Dieser Anforderung kann technisch nachgekommen werden. Werden auch öffentliche Gruppen angeboten, ist der Nutzer darüber zu informieren, dass er durch das Einstellen von Inhalten in diese Gruppe personenbezogene Daten von sich preisgibt. Es kann nicht unbedingt davon ausgegangen werden, dass die Mitgliedschaft in einer solchen öffentlichen Gruppe automatisch bedeutet, dass jedes Mitglied möchte, dass diese Mitgliedschaft bekannt ist. Man denke nur an eine „Ich werde gemobbt!"-Gruppe. Eine öffentlich einsehbare Teilnehmerliste mit Klarnamen ist hier offenbar nicht sinnvoll. Jedes Mitglied einer Gruppe kann also sein Recht auf informationelle Selbstbestimmung nur dadurch wahren, dass es selbst bestimmen kann, ob es in einer Teilnehmerliste auftaucht, ob es mit Klarnamen, Pseudonym oder gar anonym agieren möchte. Erlaubt eine Lernplattform das eigenverantwortliche Anlegen von eigenen Inhalten in einem Kurs- oder Unterrichtszusammenhang, lässt sich die informationelle Selbstbestimmung nur durch ein flexibles Rechtemanagement wahren, bei dem die Betroffenen selbst bestimmen können, wer auf welches ihrer Dokumente Zugriff hat. Es kann somit auch Inhalte geben, auf die zwar die Mitstudierenden, nicht aber die Lehrenden zugreifen können.

2.3 Schranke Lehrender/Studierende – externe Dienste

Grundlegend für die informationelle Gewaltenteilung ist, dass man überhaupt die Gewalt über die gespeicherten Daten hat. Dies ist nur dann der Fall, wenn die Stellen, an denen die Daten gespeichert werden, vertrauenswürdig sind. Bei allen bisherigen Überlegungen und Szenarien wurde davon ausgegangen, dass die erhobenen personenbezogenen Daten beim E-Learning auf Einrichtungen der jeweiligen Hochschulen selbst gespeichert werden. Stehen an einer Hochschule jedoch keine Lernmanagementdienste zur Verfügung oder bieten diese eine gewünschte Funktion nicht an, wird gerne auf externe Dienste zurückgegriffen. Ein grundsätzliches Problem beim Einsatz externer Dienste ist das mangelnde Wissen über die speichernde Stelle. Während z. B. der Terminkoordinationsdienst Doodle in der Schweiz sitzt, die ein mit der Europäischen Union vergleichbares Datenschutzniveau hat, speichern die Onlinespeicherdienste

[3] Bildung im Dialog (http://www.bid-owl.de/) ist eine Lehr-/Lernplattformen für Schulen in Ostwestfalen-Lippe. Sie wird betrieben von der Bezirksregierung Detmold in Zusammenarbeit mit der Universität Paderborn.

[4] Ausgenommen sind Zugriffe der technischen Betreiber des Forums, die notwendig sind, um die technische Funktionsfähigkeit zu gewährleisten oder aber um ggf. Missbrauch auszuschließen. Auch auf diese Punkte ist in einer Datenschutzerklärung einzugehen.

Dropbox und box.net, mit Hilfe derer Dateien auf mehreren Rechnern und mit einer „Onlinefestplatte“ synchronisiert werden können, ihre Daten außerhalb Europas. Damit ist nicht mehr gesichert, dass die Daten nicht zweckentfremdet werden. Doch selbst wenn man dieses Problem komplett außen vor lässt, ist der Einsatz externer Dienste problematisch, denn häufig bedeutet der Einsatz externer Dienste außerhalb der eigenen Infrastruktur, dass Studierende oder Lehrende gezwungen sind, ihre Daten einem größeren Kreis an Beteiligten zugänglich zu machen, als nötig wäre.

Betrachtet wird im Folgenden die Terminfindung in einer Veranstaltung mittels eines externen Dienstes. Studierende der Veranstaltung haben eventuell kein Interesse daran, dass andere Mitstudierende von der Teilnahme an der Veranstaltung erfahren. Sie wollen eventuell ferner nicht, dass ihre Daten an externe Dienstleister übertragen werden, da sich hier stets das Problem ergibt, dass er nicht absehen kann, was mit den Daten geschieht und welche weiteren Daten eventuell aggregiert werden. Den Autoren ist ein Einsatz an der eigenen Universität bekannt (siehe Abb. 1), bei der die Terminfindung für eine Veranstaltung mit Hilfe des Internetdienstes Doodle durchgeführt wurde. Eine schnelle Suche im Internet nach der Wortkombination „Tutorium Doodle“ brachte eine Vielzahl von Veranstaltungswebsites verschiedenster Einrichtungen hervor, auf denen vergleichbar wie hier geschildert vorgegangen wurde: Jeder Teilnehmer der Veranstaltung wurde gehalten, eine Doodleseite zu besuchen und sich dort mit seinem Klarnamen den für ihn in Frage kommenden Termin einzutragen. Dieser Einsatz ist nach den Grundsätzen der informationellen Gewaltenteilung als sehr kritisch zu bewerten.

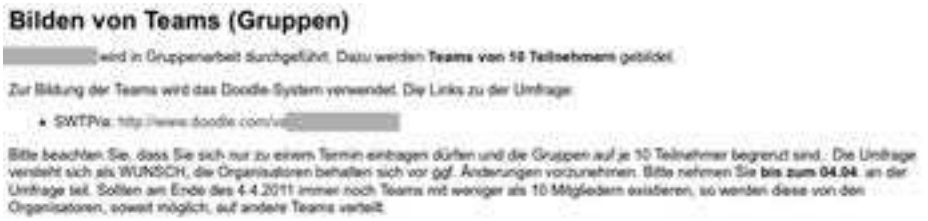

Abbildung 1: Öffentliche Doodle-Terminabstimmung auf einer Veranstaltungswebsite

Da nicht davon ausgegangen werden konnte, dass jeder der Studierenden beim Doodle-Dienst angemeldet ist, wurde eine öffentliche Abstimmung gewählt. Der Zugriff auf die Abstimmung findet dabei über eine kryptische URL statt, die nicht ohne weiteres erraten werden kann. Üblicherweise werden diese URLs per E-Mail weitergegeben. In diesem Fall wurde die Adresse jedoch auf der Website der Veranstaltung veröffentlicht, sodass letztlich jeder, der absichtlich oder zufällig die Veranstaltungswebsite besuchte, Zugriff auf die Terminabstimmung hatte, denn die Eintragungen der an der Abstimmung waren dann sichtbar. Eine solche öffentliche Abstimmung wäre vielleicht noch tragbar gewesen, wenn die einzelnen Studierenden nicht identifizierbar gewesen wären. Doodle erlaubt explizit die Nutzung von Pseudonymen. Die Organisatoren der Veranstaltung verlangten jedoch Klarnamen, um später eine Zuordnung der Teilnehmer zu einzelnen Veranstaltungen vornehmen zu können. Jeder Studierende, und eigentlich sogar jeder, den es interessierte, erhielt also eine vollständige Klarnamenliste der teilnehmenden Studierenden inklusive seiner Terminpräferenzen. Die Anforderungen an den Datenschutz sind ganz offenbar bei dieser Art der Nutzung nicht erfüllt. Der Zwang zu

Klarnamen widerspricht der Datensparsamkeit. Das Eröffnen der kompletten Liste der Teilnehmer für jedermann ist zudem nicht geeignet, sicherzustellen, dass die Daten nur zweckgebunden verwendet werden. Selbst eine Einwilligung der Studierenden würde die Mängel nicht heilen, denn die Teilnahme war ja verpflichtend, eine Freiwilligkeit lag also nicht vor.

Organisatorisch ist kritisch zu hinterfragen, ob die Nutzung eines externen Dienstes wirklich notwendig ist. Wenn dies mit ja zu beantworten ist, muss in jedem Falle Transparenz hergestellt und über die Gefahren dieser Nutzung informiert werden. Augenmerk sollte auch auf die Auswahl der Dienste gelegt werden. Zu Doodle existiert zum Beispiel seit einiger Zeit bereits eine Alternative, die vom DFN-Verein betrieben wird.[5] Die Betreiber sichern hier zu, die Daten nicht weiterzuverwenden. Jede Terminabstimmung muss außerdem mit einem Löschdatum versehen werden, sodass die Teilnehmer der Terminabsprache sicher sein können, dass die Daten nicht über einen unkontrollierbaren Zeitraum gespeichert werden. Überlegt man sich zudem noch eine Möglichkeit, nicht mit Klarnamen auftreten zu müssen, eine Möglichkeit wäre beispielsweise die Nutzung der Matrikelnummer, ist das Datenschutzproblem trotz des Einsatzes eines externen Dienstes stark abgeschwächt worden.

3 Fazit

Die Betrachtung der informationellen Gewaltenteilung in Lernplattformen hat gezeigt, dass zur Gewährleistung des Datenschutzes das jeweilige Lehr-/Lern-Szenario betrachtet werden muss. Es ist zu eruieren, welche Parteien es gibt, welche Schutzinteressen vorliegen und welche Schnittstellen oder Maßnahmen zu ergreifen sind. Diese Betrachtung bezieht sich auf didaktische Fragen (Sind diese Daten notwendig für die Lehre? Worauf kann ich auch verzichten?), technische Lösungen (Welche Daten müssen übertragen werden? Wo werden sie gespeichert? Wann werden sie gelöscht?) sowie organisatorische Maßnahmen (Welche alternativen Möglichkeiten zur Nutzung stehen zur Verfügung? Wird über ein eventuelles Datenschutzrisiko informiert?).

Den Datenschutz von dieser Seite aus zu betrachten dient dreierlei Zielen:

Gewärtigkeit: Allen Beteiligten müssen die Vorteile des Datenschutzes einleuchten, damit sie Beachtung finden und nicht als Hemmschuh empfunden werden. Das Konzept der informationellen Gewaltenteilung kommt dem nach, indem die Interessen der Beteiligten an einer Datenerfassung und die Interessen der Beteiligten am Schutz ihrer Daten in den Vordergrund gestellt werden.

Verständlichkeit: Das Konzept der informationellen Gewaltenteilung ist, so ist unsere Hypothese, leichter zu verstehen als die abstrakten juristischen Anforderungen der Datenschutzgesetze oder eines Datenschutzaudits, da sich diese nach abstrakten juristischen Anforderungen richten. Selbstredend wird aber weder das eine noch das andere durch diese Überlegungen obsolet.

[5] Siehe https://terminplaner.dfn.de.

Flexibilität: Die Überlegungen zur informationellen Gewaltenteilung haben verdeutlicht, dass ein gewisses Schutzinteresse nicht nur auf eine einzige Art bedient werden kann. In einigen Fällen lässt sich durch didaktische Überlegungen bereits die Notwendigkeit zur Datenerhebung minimieren. Ist dies nicht möglich, gibt es häufig verschiedene technische Möglichkeiten, die Interessen der Beteiligten zu schützen. Ist dies nicht der Fall, weil zum Beispiel kein Eingriff in die Technik möglich ist, bleiben organisatorische Maßnahmen, um dem höchstrichterlich verbrieften Recht auf informationelle Selbstbestimmung Nachdruck zu verleihen.

Literaturverzeichnis

[Bu09] Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist

[Bu83] Bundesverfassungsgericht: Volkszählungsurteil, BVerfGE 65, 1, Bundesverfassungsgericht, Karlsruhe, 1983

[Bl05] Blanck, B.: Diskutieren mit der Methode der »erwägungsorientierten Pyramidendiskussion« – ein Beispiel für computerunterstütztes erwägendes Lernen. Zukunftswerkstatt Lehrerbildung; In Neues Lehren und Lernen durch E-Learning. Der didaktische Mehrwert von E-Learning-Konzepten in der Lehrerbildung, Tagungsdokumentation. Münster, 2005, 7. Jg., S. 70-98

[Do02] Doberkat, E. et al.: Anforderungen an eine eLearning-Plattform – Innovation und Integration. Studie im Auftrag des MSWF NRW. Memo Nr. 122, Universität Dortmund; S. 53

[Ei08] Eibl, C. J.: Vertraulichkeit persönlicher Daten in Lern-Management-Systemen. In (Seehusen, S.; Lucke, U.; Fischer, S. Hrsg.): DeLFI 2008 – Die 6. E-Learning Fachtagung Informatik. Bonn; Köllen Druck+Verlag, 2008; S. 317-328

[Ho09] Holl, F.: Datenschutzrechtliche Vorabkontrolle für das System “koala (ko-aktive Lern- und Arbeitsumgebung)” zum Einsatz an der Universität Paderborn, Potsdam, 2009

[LDI11] Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen: E-Learning an Hochschulen nach den Grundsätzen des Datenschutzes, Düsseldorf, 2011

[LH09] Loser, K.; Herrmann, T.: Ansätze zur Entwicklung datenschutz-konformer E-Learning-Plattformen. In (Schwill, A.; Apostolopoulos, N. Hrsg): “Lernen im Digitalen Zeitalter”: DeLFI 2009 – Die 7. E-Learning Fachtagung Informatik. Bonn; Köllen Druck+Verlag, 2009; S. 79-90

[RS09] Roßnagel, A.; Schnabel C.: Datenschutzkonforme Nutzung von E-Learning-Verfahren an hessischen Hochschulen – Abschlussbericht –; Kassel, 2009

[Ve01] Veddern, M.: Update – Ratgeber Multimediarecht für die Hochschulpraxis. Ministerium für Schule, Wissenschaft und Forschung des Landes Nordrhein-Westfalen, 2001