

Von Orwell bis Facebook – Datensammlungen beim Lernen

Johann Höller

Institut für Datenverarbeitung in den Sozial- und Wirtschaftswissenschaften,
Johannes Kepler Universität Linz, Österreich

Zusammenfassung

Dieser Beitrag beschreibt die Möglichkeiten, digitale Medien für Lehrzwecke unter dem Aspekt „Kontrollsysteme“ einzusetzen. Erfahrungen aus einem Experiment 1984 werden den Möglichkeiten heutiger Anwendungssysteme gegenübergestellt und daraus Schlussfolgerungen für die Nutzung aktueller Tools abgeleitet.

1 Einleitung

„Die Möglichkeiten der modernen Datenverarbeitung sind weithin nur noch für Fachleute durchschaubar und können beim Staatsbürger die Furcht vor einer unkontrollierbaren Persönlichkeitserfassung selbst dann auslösen, wenn der Gesetzgeber lediglich solche Angaben verlangt, die erforderlich und zumutbar sind“ (BVerfG 1983, 6). Die Aussage stammt aus dem legendären „Volkszählungsurteil“ des Bundesverfassungsgerichts in Karlsruhe, mit dem in Deutschland das „informationelle Selbstbestimmungsrecht“ als Grundrecht abgeleitet wurde. 1983 – das war eine Zeit, als das WWW noch nicht einmal erfunden war, E-Mails praktisch nicht für private Zwecke genutzt wurden und viele der heutigen „Neuen Medien“ höchstens Ideen waren, deren Realisierbarkeit noch in weiter Ferne lag.

Computer waren zu dieser Zeit noch weitgehend abgeschottete Inselsysteme; erste Ansätze einer Vernetzung versprach das System „Bildschirmtext“. Es wurden in zwei deutschen Bundesländern eigene BTX-Feldversuchsgesetze erlassen, bei denen mit enormem Aufwand durch wissenschaftliche Begleitforschung die Folgen untersucht werden sollten, die die geplante massenhafte Verbreitung haben werde. Die Prognosen gingen von einer umfassenden Nutzung dieses Dienstes aus – nur die User folgten diesen Prognosen nicht. Dementsprechend gering verbreitet waren auch erste Weiterbildungsangebote, die mit der neuen Technik BTX angeboten wurden (wie etwa an der JKU Lackinger 1984).

Zu einem Überblick über das damalige Verständnis von „Neu“ im Hinblick auf das, was wir heute „Neue Medien“ nennen, siehe Bodenwinkler et al. 1985.

2 Das Orwell-Experiment

Ohne Orwell's Roman „1984“ hätte die Jahreszahl 1984 sicherlich keine so „magische“ Bedeutung erlangt; aber sein 1948 fertiggestelltes (1949 erschienenes) Werk bekam durch die technische Entwicklung auf dem Computersektor in den unmittelbar vorangehenden Jahren eine nicht voraussagbare Aktualität. Auch wenn die damaligen technischen Möglichkeiten noch weit hinter denen zurückblieben, mit denen wir heute konfrontiert sind, war die damalige gesellschaftliche Diskussion sehr geprägt von der Angst vor Überwachung und damit von Datenschutz als rechtlichem Konzept gegen diese drohende Gefahr. Das Volkszählungsurteil passt daher genau in diese Zeit einer gesellschaftskritischen Distanz zu Datensammlung und Überwachung.

Am Institut für Wirtschaftsinformatik und Organisationsforschung wurden damals Studierende in die Softwareentwicklung mittels MAI Business Basic eingeführt: Das dialogorientierte Minicomputersystem zeichnete sich dadurch aus, dass das Betriebssystem und der BASIC-Interpreter praktisch eine Einheit bildeten und so eine sehr einfach zu bedienende Softwareentwicklungsumgebung boten. Da die Syntax bei jeder Zeileneingabe geprüft wurde, erfolgte auch eine unmittelbare Fehlermeldung, wenn etwas falsch war. Diese Systemfunktionalität war der Anknüpfungspunkt für das im Folgenden beschriebene Experiment (siehe dazu auch Mittendorfer 1984).

Vorauszuschicken ist dazu noch, dass auch schon damals die Ressourcen knapp waren und die drei verfügbaren Computerarbeitsplätze daher rund um die Uhr zugänglich gemacht wurden. Um sicherzustellen, dass nur berechnete Studierende (d. h. solche, die in die Lehrveranstaltungen des Instituts aufgenommen waren) das System nutzen konnten, wurde eine Anmeldeprozedur installiert. Damit war die Voraussetzung geschaffen, die Dauer der Tätigkeit sowie die dabei gemachten Fehler den Studierenden zuzuordnen. Es war jedoch nicht Absicht des Projekts, heimlich Daten zu sammeln, sondern ganz im Gegenteil, den Studierenden das Potenzial der Datensammlung bewusst zu machen und den Computer gleichsam als Dialogpartner zu personalisieren.

Fehlermeldungen wurden also nicht einfach als sachliche Information dokumentiert, sondern kommentiert und/oder interpretiert ausgedrückt. Sie wurden auch nicht immer in derselben Art und Weise verwendet, sondern – unter Verwendung von Zufallszahlen – gestreut.

```
Lieber Hans, das war ein Syntaxfehler!  
Dateien haben 6 Zeichen, Keys sind nicht länger als definiert (oder will  
Herr Mittendorfer vielleicht TO releasen?).  
Hans, Du wiederholst Dich! Fehler Nr. 12 hatten wir gerade!  
Herr Mittendorfer, wenn das so weitergeht, beschwere ich mich bei meiner  
Gewerkschaft über Sie! Haben Sie jemals Programmieren gelernt? Wenn ja,  
sagen Sie niemandem wo!
```

Schon diese Art der Kommunikation bewirkte ein starkes Überwachungsgefühl; das wurde komplettiert durch die Tatsache, dass das System ab einem gewissen Fehlerquotienten (Anzahl Fehler je Zeitraum) die weitere Arbeit untersagte und den User „zum Ausruhen“ schickte.

```

1984          BESCHUETZERPROGRAMM          04/01/1984
BIG BROTHER FUER HOELLER HANS              10:13
-----
DU, lieber HANS, arbeitest heute seit 20 Minuten.
In dieser Zeit hast Du insgesamt 14 Fehler 12 gemacht.

Wer soviele Fehler macht, kann entweder nicht programmieren,
oder ist jedenfalls voruebergehend dazu nicht in der Lage.

Aus Ruecksicht auf Deine Gesundheit wirst Du daher heute von der Arbeit
entbunden. Melde Dich bitte sofort ab !!!

Gute Besserung
Dein Grosser Bruder !

>-----

```

Nachdem gerade beim Erlernen einer Programmiersprache Fehler unvermeidlich sind und vieles durch die Methode „Trial and Error“ gelernt wird, war natürlich diese automatisierte Entscheidung eine spürbare Beeinträchtigung – gerade in Zeiten, in denen die verfügbare Zeit ohnehin knapp war. Allerdings war es aus systemtechnischen Gründen nicht möglich, den Benutzer wirklich von der Systemnutzung auszuschließen – als maximale Sanktion war die Blockade des Systems bzw. im Extremfall der Entzug der Benutzerberechtigung für zukünftige Systemanwendungen möglich.

```

1984          BESCHUETZERPROGRAMM          04/01/1984
BIG BROTHER FUER HOELLER HANS              10:17
-----
Und nun lassen Sie mich endlich in Ruhe und melden sich ab mit „/ENDE“
Sie missachten das jetzt zum 3. Mal, warten Sie 30 Sekunden

>-----

```

Die Reaktionen ließen nicht lange auf sich warten: Einige versuchten, das System auf technischer Ebene anzugreifen, die zugrundeliegenden Programme bzw. Dateien zu manipulieren bzw. zu löschen, während andere versuchten, sich dadurch zu behelfen, dass sie die Passwörter mit KollegInnen tauschten (oder sich sonst wie verschafften), um so unter mehreren Identitäten arbeiten zu können. Wieder andere – in deutlicher Minderzahl – versuchten, gemeinsame Protestmaßnahmen zu organisieren.

Es ging bei dem Experiment darum, das Überwachungspotenzial offenbar zu machen; typischerweise passiert Überwachung allerdings „im Geheimen“. Wie auch der aktuelle Fall des Whistleblowers Edward Snowden zeigt, scheut staatliche Überwachung ebenso das Licht der Öffentlichkeit wie entsprechende Datensammlungen von privaten Unternehmen (siehe die umfangreiche Dokumentation bei europe-v-facebook.org).

Existiert haben die Daten, die beim Experiment Orwell verwendet wurden, vorher und nachher in gleicher Weise; den Unterschied machte nur aus, wie sie gespeichert und verarbeitet wurden. Wenn das aber im Geheimen geschieht und die Daten bzw. Entscheidungen daraus den Betroffenen nicht offenkundig gemacht werden, dann ist die Angst vor Überwachung nicht unbegründet.

Selbstverständlich wurden nach Ende des Experiments die Umstände, insb. die Irrelevanz für die Beurteilung, offengelegt sowie die Reaktionen mit den Studierenden diskutiert. Es dauerte aber wesentlich länger, bis das Misstrauen vor möglichen heimlichen Überwachungsmaßnahmen wieder verschwand.

3 Neue Medien heute

Wenn man heute von Neuen Medien spricht, dann meint man damit vor allem die digitalen Medien, die sich durch umfassende Funktionalität, hochgradige Vernetzung und zunehmende Mobilität der verwendeten Endgeräte auszeichnen. Allein schon für den „normalen“ Betrieb fallen also ungeheuerliche Datenmengen an, die für Überwachungs- und Kontrollsysteme genutzt werden können.

Dazu kommt im Kontext von Lernmedien die Tatsache, dass für die Beurteilung die Kontrolle des Lernfortschritts eine Grundvoraussetzung darstellt. Ein bestimmtes Ausmaß an Kontrolle – unterschiedlich je nach Lehrveranstaltungstyp – ist daher systemimmanent.

Es sollte außer Streit stehen, dass trotz dieser Notwendigkeit von Kontrolle nicht jede technisch mögliche Kontrollmaßnahme dadurch gerechtfertigt werden kann, dass sie im Rahmen eines Lehrszenarios durchgeführt wird. Selbstverständlich ist in diesem Zusammenhang primär auf die datenschutzrechtlichen Bestimmungen hinzuweisen – aber auch andere Rechtsvorschriften können Grenzen für den Einsatz von Lernmedien setzen bzw. Anforderungen an deren Verwendung stellen.

3.1 Lernmanagementsysteme

Lernmanagementsysteme, oft auch als Lernplattformen bezeichnet, werden hier als Anwendungsprogramme verstanden, die primär der Bereitstellung und Verwaltung von Lehrinhalten dienen. So bietet etwa die Lernplattform „Moodle“ die Möglichkeit, den Lehrstoff nach Wochen oder Themen in Blöcke zu gliedern, einzelne Blöcke erst unter Bedingungen freizugeben und den einzelnen Blöcken „Arbeitsmaterialien“ bzw. „Aktivitäten“ zuzuordnen.

Arbeitsmaterial können im einfachen Fall Textfelder bzw. Textseiten, Link/URLs oder StreamURLs sein; aber auch größere Objekte wie Dateien, Verzeichnisse und IMS-Content können eingebunden werden. Arbeitsmaterialien sind „passiv“; d. h. sie liefern selbst keine Daten zurück. Das System kann registrieren, wer wann diese Inhalte abgerufen hat – aber Informationen über die Nutzungsdauer bzw. sonstige Details wie etwa die Verweildauer auf einzelnen Seiten eines längeren Dokuments sind nicht verfügbar. Bei kleineren „Portionen“ kann allerdings aus der Sequenz von Aufrufen durchaus auf die Bearbeitungsdauer geschlossen werden.

Aktivitäten sind in Moodle z. B. Foren, Aufgaben und Abstimmungen. Es gibt viele andere Arten von Aufgaben bis hin zur Aktivität „Lernpaket“, wo komplette SCORM-Pakete eingebunden werden können. Aktivitäten sind dazu gedacht, dass Studierende Rückmeldungen an die Plattform – und damit die Lehrenden – liefern. Das kann sich auf organisatorische Fragen ebenso beziehen wie auf Inhalte. Auch hier fallen neben dem gewollten Kern der Rückmeldung begleitend Daten an, die Schlüsse auf das Arbeits- bzw. Lernverhalten denkmöglich erscheinen lassen: Die IP-Adresse und damit ein wahrscheinlicher Standort, Informationen zum verwendeten Endgerät, bei mobilen Geräten möglicherweise auch genauere Informationen über den Standort, Zeitdauer der Lösung der Aufgabe, Informationen über wiederholte Lösungsversuche (wo zulässig) usw.

Es wird wohl kaum jemand daran zweifeln, dass man auch jede aktuelle Lernplattform dazu verwenden könnte, darauf basierend ein Kontrollsystem aufzubauen, das die Mächtigkeit des Orwell-Experiments bei weitem übersteigt. Vielleicht wäre das auch notwendig, denn nach der Erfahrung des Autors dominiert unter der Studierenden-Generation von heute das Gefühl, den Datensammlungen ohnehin nicht entgehen zu können. Sie messen dem Schutz ihrer Daten bzw. der Chance, durch sorgfältigen Umgang mit ihren Daten diese schützen zu können, wenig Erfolgchancen bei.

Diese Haltung ist für die Lehrenden zwar bequem – dennoch insgesamt nicht wünschenswert: „Individuelle Selbstbestimmung setzt aber – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden 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.“ (BVerfG 1983, 46) Auch wenn diese Begründung ungefähr gleich alt ist wie das Orwell-Experiment, hat sie nicht an Aktualität verloren.

Vorbehaltlich besonderer gesetzlicher Vorschriften wird man daher als Richtschnur für die Verwendung von Daten in Lernplattformen festhalten: Daten, mit deren Verwendung die Studierenden rechnen konnten, werden zulässigerweise bei der Beurteilung herangezogen werden können. Besser ist es natürlich, wenn man es dabei nicht bei Vermutungen belässt, sondern den Studierenden klar kommuniziert, welche Informationen für Zwecke der Beurteilung gesammelt und ausgewertet werden. Österreichische Studierende haben ein gesetzliches Recht darauf: § 59 UG regelt die „Lernfreiheit“, die auch das Recht umfasst (Abs. 6), von den Leiterinnen und Leitern der Lehrveranstaltungen vor Beginn jedes Semesters „über die Inhalte, die Methoden, die Beurteilungskriterien und die Beurteilungsmaßstäbe der Lehrveranstaltungsprüfungen“ informiert zu werden.

3.2 Soziale Medien

Unter „Soziale Medien“ sollen im vorliegenden Zusammenhang jene verstanden werden, die das gemeinsame Arbeiten bzw. Lernen mit anderen unterstützen. Typischerweise sind heute

derartige Funktionalitäten auch Bestandteil vom LMS (Lehr 2011, 114). Die Frage, ob solche in LMS integrierte Tools angewendet werden sollen oder eigenständige Spezialanwendungen, ist primär eine Frage des pädagogischen Kontexts (Dalsgaard 2006) und für die hier zu untersuchende Frage von nachrangiger Bedeutung.

Eine wichtige Anwendungskategorie innerhalb der Sozialen Medien stellen Wikis und Blogs dar. Ihnen ist gemeinsam, dass mehrere Personen zusammenarbeiten, um ein Objekt zu schaffen. Während beim Blog eher das Schaffen einer Person im Mittelpunkt steht, die ihre Beiträge der Öffentlichkeit zur Kommentierung bereitstellt, tritt beim Wiki die Person, die Beiträge liefert, eher in den Hintergrund, während das geschaffene Objekt in den Vordergrund rückt. Untiet-Kepp (2012) unterscheidet beim kollaborativen Lernen (nach Roschelle und Teasley 1995, 70) zwei Ebenen der Zusammenarbeit, nämlich die der Kommunikation und der Ko-Konstruktion. „Kollaboration bedeutet somit, dass alle Mitglieder der Lerngruppe an der Bearbeitung der Aufgabe gleichermaßen mitwirken, also eine gemeinsame Lösung ko-konstruieren und während der Erstellung dieser Lösung miteinander kommunizieren. Andere Formen der Zusammenarbeit, vor allem die Kooperation, lässt sich durch diese Betrachtung der zwei Ebenen somit von der Kollaboration abgrenzen, da bei der kooperativen Aufgabebearbeitung die Mitglieder der Lerngruppe die Aufgaben in Teilaufgaben aufteilen. Diese Teilaufgaben werden dann von jeweils einem der Gruppenmitglieder individuell bearbeitet. Die so entstandenen individuellen Teilergebnisse werden im Anschluss an diese individuelle Arbeitsphase zu einem Gesamtergebnis zusammengeführt.“

Gemeinsam ist beiden Arten, dass das geschaffene Objekt ein Werk darstellen kann und dann dem urheberrechtlichen Schutz unterliegt. Der urheberrechtliche Schutz entsteht mit der Schaffung des Werkes – bzw. eines Beitrages dazu. Urheber eines Werkes ist, wer es geschaffen hat (§ 10 öUrhG); bilden die Ergebnisse des Schaffens mehrere Personen eine untrennbare Einheit, dann steht das Urheberrecht allen Miturhebern gemeinschaftlich zu (§ 11 leg. cit). Kollaboratives Arbeiten – typisch für Wikis – führt daher zur Miturheberschaft während die individuelle Bearbeitung von Teilaufgaben den einzelnen Urheber zuordenbar bleibt. Um die Voraussetzungen des Urheberrechts nachvollziehen zu können, müssen daher die einzelnen Aktivitäten bei der Erstellung bzw. Änderung eines Beitrages auf einem Wiki entsprechend aufgezeichnet werden. Allein schon daraus entsteht eine nicht unerhebliche Sammlung von Daten.

Das Urheberrecht erfordert aber nicht, dass der wirkliche Name des Urhebers angeführt wird – aus urheberrechtlicher Sicht ist auch die Verwendung von Pseudonymen („Nicknames“) zulässig. Nicknames haben eine lange Tradition im Internet – und wenn man sich die Begründung des BVerfG zum Volkszählungsurteil in Erinnerung ruft, durchaus auch ihre rechtliche Begründung.

Allerdings kollidiert die Verwendung von Nicknames im Sinne der Anonymität mit dem mit Lehrveranstaltungen verbundenen Erfordernis der Beurteilung der Studierenden. Zumindest gegenüber der Lehrveranstaltungsleitung kann daher die Anonymität bei der Erstellung von Beiträgen nicht bestehen bleiben.

Wenn Kollegen vorsehen, in Lehrveranstaltungen die Veröffentlichung von Beiträgen mit Angabe des Klarnamens zum Bestandteil der Beurteilung zu machen, dann muss das jedenfalls im Grundsatz als problematisch angesehen werden. Es kann sicher Gründe geben, die eine solche Anforderung aufgrund des Studienfortschritts, der Aufgabenstellung der Lehrveranstaltung und ihrer Stellung im Curriculum ausnahmsweise als zulässig erscheinen lassen.

Abgesehen von der rechtlichen Problematik scheint es auch didaktisch wenig sinnvoll, den Studierenden damit zu „drohen“, jeder Fehler wäre lebenslang und unlöslich im Internet nachzulesen. Es mag zwar dann wahrscheinlich Beiträge mit weniger Fehlern geben – aber es wird auch weniger Beiträge geben, vor allem von Studierenden, die noch Unsicherheiten in der Beherrschung des Lernstoffes aufweisen und diese tendenziell von der Mitwirkung unter diesen Umständen abhalten.

Wenn oben ausgeführt wurde, dass die Frage ob in LMS integrierte Tools oder eigenständige Anwendungssysteme verwendet werden, von nachrangiger Bedeutung sei, so kommt dieser Frage unter dem Aspekt der Öffentlichkeit nun doch Bedeutung zu: Wenn solche Tools in einem LMS integriert sind, dann steht der Zugriff idR auch nur angemeldeten Personen offen – und stellt damit dieselbe Situation her, die auch im Hörsaal bzw. Seminarraum herrscht.

Die andere sichere Alternative stellt die Verwendung von öffentlichen Diensten und Verwendung von Pseudonymen dar, deren Anonymität nur gegenüber der Lehrveranstaltungsleitung aufgehoben wird.

Besonders problematisch erweist sich der Einsatz von Tools, die von den Benutzern die Registrierung unter dem tatsächlichen Namen verlangen (vgl. Punkt 4 der Registrierungsbedingungen von Facebook „Facebook-Nutzer geben ihre wahren Namen und Daten an“) und bei denen die ausnahmsweisen Gründe für den Einsatz in der Öffentlichkeit nicht vorliegen: Auch wenn das einfach sein mag und auch die Zielgruppe der Studierenden keine Bedenken hegt, das Werkzeug selbst zu verwenden, sollte man sich den Einsatz solcher Tools gut überlegen. Rechtlich sei angemerkt, dass die Zustimmung aller Betroffenen selbstverständlich den Einsatz unanfechtbar macht – wobei eine solche Zustimmung allerdings jederzeit widerrufen werden kann.

3.3 Elektronische Prüfungen

Eine besondere Form von Aktivitäten sind elektronische Prüfungen, egal ob sie nun auf Multiple-Choice-Tests, offenen Fragen oder sonstigen Frage- oder Aufgabenstellungen beruhen. Wie auch bei Prüfungen ohne Computereinsatz „verschärfte“ Kontrollmaßnahmen gegenüber normalen Lehrveranstaltungsterminen üblich sind, wird dies auch bei elektronisch durchgeführten Prüfungen gerechtfertigt sein.

So wird etwa eine laufende Videoüberwachung von Seminarräumen im Regelfall unzulässig sein – jedenfalls dann, wenn dies den Studierenden nicht offengelegt wird. Wer etwa an einer Lehrveranstaltung teilnimmt, die auch an andere Standorte übertragen wird bzw. bei der andere Studierende via Videokonferenz teilnehmen, wird sich nicht darauf berufen können, von der Bild- und Tonaufzeichnung nicht informiert worden zu sein. Auch ist es in normalen Lehrveranstaltungen unüblich, die Authentizität der Teilnehmer festzustellen.

Im Rahmen von elektronisch abgehaltenen Prüfungen ist es etwa zulässig, zur Feststellung der Authentizität der Personen bzw. der tatsächlichen individuellen Leistungserbringung etwa

- maschinenlesbare Ausweise und deren Daten auszulesen und diesen Echtdaten (z.B. Aufnahme eines aktuellen Bildes) gegenüberzustellen;

- Aufzeichnungen zur Kontrolle der einzelnen Arbeitsschritte (z. B. Screenshots) anzufertigen;
- die Verwendung von nicht zugelassenen Diensten und Funktionen zu verhindern bzw. solche Zugriffsversuche zu protokollieren.

Selbstverständlich gilt auch hier das Gebot, die Studierenden über die getroffenen Überwachungsmaßnahmen zu informieren; die Konsequenz, dadurch die Studierenden an Handlungen zu hindern, die einer Feststellung des tatsächlichen Leistungsvermögens entgegenstehen, ist hier durchaus gewollt und rechtlich anerkannt.

4 Fazit

Computer sind potentiell sehr gute Überwachungs- und Kontrollsysteme – sowohl im nützlichen wie auch im bedrohlichen Sinne. Der Erfolg der Lehre wird gemessen durch Kontrolle, ob bestimmte vorgeschriebene Kompetenzen erreicht wurden. Die Kontrollfunktionen von Computersystemen sammeln eine Unmenge von Daten – oftmals mehr als sinnvoll für den Lehrzweck verarbeitbar sind.

Studierende haben die geringeren technischen Möglichkeiten der Vergangenheit extrem als „Überwachung“ erlebt – Studierende von heute wissen mehr über die Überwachungsmöglichkeiten, scheinen diese aber lethargischer hinzunehmen. Auch wenn also die Gefahr von Beschwerden durch Studierende nicht sehr groß ist, sollten die technischen Möglichkeiten zur Kontrolle nur beschränkt genutzt werden:

- Es nützt in Lernszenarios wenig, alle gemachten Fehler zu dokumentieren; schließlich soll man aus Fehlern lernen und das Ergebnis im Vordergrund stehen.
- Der Zwang zur Nutzung öffentlicher Medien mit Klarnamen ist problematisch und bedarf einer Begründung.
- Man kann auch darauf hoffen, dass Studierende in Zukunft wieder mehr Sensibilität für das Thema Datenschutz mitbringen. Wenn sich Lehrende schon heute darauf einstellen, werden sie auch zukünftig auch keine Probleme haben.

In diesem Sinne gilt die grundsätzliche Empfehlung des Datenschutzes auch hier: Weniger ist Mehr – weniger Kontrolldaten zu sammeln bringt ein Mehr an didaktischem Nutzen und ein Mehr an Datenschutz.

Literaturverzeichnis

- Bodenwinkler, P. (1985). *Neue Technologien für den betrieblichen Einsatz: Anwendungsgebiete und Auswirkungen der Mikroelektronik*, Wien: Orac.
- BVerfG, 1 BvR 209/83 u.a. vom 15.12.1983
- Dalsgaard, C. (2006). *Social software: E-learning beyond learning management systems*, unter: http://www.eurodl.org/materials/contrib/2006/Christian_Dalsgaard.htm (7. 7. 2013)
- Lackinger, H. & Mühlbacher J. (1984). *Lernen mit Bildschirmtext: dezentral und zeitlich ungebunden*, Linz: JKU.

- Lehr, C. (2011). *Web 2.0 in der universitären Lehre*, Boizenburg: Verlag Werner Hülsbusch.
- Mittendorfer, H. (1984). *Experiment Orwell (Arbeiten unter Kontrolle)*, in: Symposium: "Der Computer als Instrument wissenschaftlicher Lehre und Forschung": Salzburg.
- Untiet-Kepp, S.J. (2012). *Adaptives Feedback zur Unterstützung in kollaborativen Lernumgebungen*, Boizenburg: Verlag Werner Hülsbusch.

Kontaktinformationen

Johann Höller, E-Mail: johann.hoeller@jku.at

Johannes Kepler Universität Linz, Institut für Datenverarbeitung in den Sozial – und Wirtschaftswissenschaften

Altenbergerstraße 69, 4040 Linz

Workshop

Zur Forschung im Bereich der Entwicklung interkultureller Benutzungsschnittstellen

Rüdiger Heimgärtner

Thomas Mandl

Christa Womser-Hacker

