Elisabeth Katzlinger

E-LEARNING

Schutz der Privatsphäre

Sicherheitsaspekte von Learning-Management-Systemen

Lernprozesse in unterschiedlichen institutionellen Zusammenhängen sind zunehmend durch technische Unterstützung geprägt. Es werden sowohl Learning-Management-Systeme wie Moodle oder Blackboard, als auch Social Software wie Weblogs, Wikis, Diskussionsforen oder Chats verstärkt eingesetzt. In diesen Anwendungen werden die Zugangsdaten und die Daten über die einzelnen Aktivitäten aller Beteiligten gespeichert und stehen für Auswertungen zur Verfügung. Dabei kann die Privatsphäre der Beteiligten verletzt werden. Je nach Art der technischen Realisierung und gewählten Konfiguration fallen Nutz- und Interessensprofile an, die personenbezogene Daten enthalten. Mit unterschiedlichen Methoden der Datenauswertung können diese Daten ausgewertet werden und beispielsweise für die Beurteilung der Lernenden oder die Überprüfung der Beteiligung an einer Lehrveranstaltung heran gezogen werden.

Auch an der Johannes Kepler Universität im österreichischen Linz kommen E-Learning-Programme zum Einsatz. Ein wichtiger Aspekt der IT-gestützten Kommunikation ist der Schutz personenbezogener Daten.

Foto: Universität Linz

Um einen reibungslosen Ablauf des Betriebes der Informations- und Kommunikationssysteme zu ermöglichen, werden die Zugangsdaten und Daten über die einzelnen Aktivitäten aller Beteiligten aufgezeichnet, so auch in Lernumgebungen. In „logfiles“ werden alle Aktivitätsdaten festgehalten. Diese Daten dienen zur technischen Überwachung der Systeme. Die Menge der gesammelten Daten und deren Verwendungsmöglichkeiten beinhalten neue, versteckte und offene Risiken für die Privatsphäre der Beteiligten. Die Methoden des „user tracking“ und „user profiling“ sind aus den Bereichen des E-Business wie beispielsweise bei CRM-Systemen (Kundenbeziehungsmanagement) hinlänglich bekannt. Aus der Analyse des Click- und Downloadverhaltens wird ein individuelles Profil erstellt, das für Marketingaktivitäten genutzt werden kann (Pils 2004, S. 336). Bei der Anwendung dieser Methoden auf Lernende ergibt sich eine Reihe von zusätzlichen Problemen. Für den Betrieb eines E-Learning-Systems benötigt man zuverlässige Verfahren zur Authentifizierung, um die Identität der handelnden Personen überprüfen zu können. Insbesondere wenn auch Prüfungsleistungen über dieses System abgenommen werden (Eckert 2003, S. 44). Hier sollen Maßnahmen vorgestellt werden, die dem Schutz der Privatsphäre sowie einem effizienten Identitätsmanagement dienen.

Privatsphäre

Freiheit und Schutz von Information und Kommunikation sind wichtige Dimensionen des Persönlichkeitsschutzes von Menschen, es ist ein auf Verfassungsebene geschütztes Grundrecht. Der Schutz der Privatsphäre umfasst nicht nur das „Recht, in Ruhe gelassen zu werden“, sondern auch das aktive Recht einer Person, darüber zu bestimmen, welche seiner Daten von anderen genutzt werden und in welchem Umfang und unter welchen Bedingungen diese dieses Wissen verwenden dürfen. Entscheidend für Autonomie ist dies deshalb, weil man sich nur dann gegenüber Anderen selbstbestimmt verhalten kann, wenn man weiß, was diese über einen selbst wissen (Kuhlen 1999). Im Zuge der Diskussion der Datenschutzgesetze wurden Mindeststandards

Univ. Ass. Mag. Dr. Elisabeth Katzlinger ist am Institut für Datenverarbeitung in den Sozial- und Wirtschaftswissenschaften (idv) der Johannes Kepler Universität Linz tätig.

bei der Datenerhebung und Datenverarbeitung in Form von „fair information practices“ (www.privacyrights.org) bzw. der „Empfehlung des Rates über Leitlinien für den Schutz des Persönlichkeitsbereiches und den grenzüberschreitenden Verkehr personenbezogener Daten“ (OECD 1980) festgelegt und in acht **Grundprinzipien** formuliert (Langheinrich 2005, S. 334f):

- Beschränkung der Datenbeschaffung („collection limitation“): Daten sollten in rechtmäßiger Weise und wenn immer möglich mit der Einwilligung des Datensubjekts erhoben werden.
- Qualität der Daten („data quality“): Die erhobenen Daten sollten dem Zwecke ihrer Erhebung angemessen, korrekt, vollständig und aktuell sein.
- Zweckbestimmung („purpose specification“): Der Zweck der Datenerhebung sollte vorher festgelegt werden.
- Limitierte Nutzung („use limitation“): Zu einem bestimmten Zweck gesammelte Daten sollten nicht für andere Zwecke genutzt werden.
- Sicherheit der Daten („security“): Die gesammelten Daten sollten adäquat vor Verlust, Diebstahl oder unerlaubten Änderungen geschützt werden.
- Transparenz („openness“): Die Methoden der Datenverarbeitung sollten offen gelegt werden.
- Beteiligung („individual participation“): Dem Einzelnen sollte ein gebührenfreies Recht auf Auskunft sowie die Richtigstellung und Löschung seiner Daten zustehen.
- Verantwortbarkeit („accountability“): Die für die Datenverarbeitung Verantwortlichen sollten für Verstöße zur Rechenschaft gezogen werden können.

Das Konzept der **informationellen Selbstbestimmung** – es gibt dem Einzelnen das Recht, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen – erweitert die „fair information practices“ um einen partizipativen Ansatz. „Die informationelle Selbstbestimmung schützt einmal die selbstbestimmte Entwicklung und Entfaltung des Einzelnen. Diese kann nur in einer für ihn kontrollierbaren Selbstdarstellung und Rückspiegelung durch die Kommunikation mit anderen gelingen“ (Roßnagel 2005, S. 463).

Dem Entwickler und Betreiber von Informationssystemen, hier im speziellen Fall einer Lernumgebung, obliegt die Entscheidung, welche personenbezogenen Daten erfasst und verarbeitet werden. Es stellt sich die Frage, von wem die Daten verarbeitet werden und welche Auswirkungen das auf die Betroffenen hat (Karat 2005, S. 154).

Die **technischen Entwicklungen** bringen neben den erwünschten Wirkungen, wie beispielsweise die Überbrückung von Zeit und Raum, auch eine Reihe von unerwünschten Nebenwirkungen, wie das ungeheure Kontrollpotenzial, das der Informations- und Kommunikationstechnik innewohnt (Peissl 2003, S. 155). Die Gefährdung der Privatsphäre wird sowohl durch die technische Entwicklung der Systeme als auch durch sozioökonomische Veränderungen hervorgerufen. Die technischen Überwachungsmöglichkeiten beinhalten ein Kontrollpotenzial, das oft unbemerkt wirkt (ebda., S. 157).

Stichwörter

Privatsphäre
Datenschutz
Learning-Management-System
Lernplattform
personenbezogene Daten

Gerade im Zusammenhang von **Lernplattformen** wird das Überwachungspotenzial von den Beteiligten, vor allem auf Seiten der Lernenden, kaum registriert. Das Problembewusstsein ist bei den Studierenden wenig ausgeprägt, weil sie einerseits über die Überwachung nicht Bescheid wissen. Auf der anderen Seite stehen die Beteiligten nicht vor der bewussten Entscheidung, welche Daten sie bekannt geben möchten. Allein durch die Benutzung der Lernplattform werden ihre personenbezogenen Daten gespeichert. Die Frage im Sinne der informationellen Selbstbestim-

mung, ob sie ihre personenbezogenen Daten in der Lernplattform preisgeben wollen, stellt sich somit für die Lernenden gar nicht. Wenn sie an einem entsprechenden Kursangebot teilnehmen wollen, müssen sie mit der Lernplattform arbeiten und dort ihre Datenspuren hinterlassen.

summary

Learning processes in different institutions are supported by information and communication technology. Learning Management Systems such as Moddle or Blackboard and social software such as weblogs, wikis, discussion boards or chats are part of the learning environment, too. Via those applications the entry data and data about single activities of members are being archived and are available for analysis. This can bring along possible privacy infringement. According to technical implementation or chosen configuration user-specific profiles are being created, containing personal data. These data can be analyzed applying different methods of filtering and be used for assessing students or checking the attendance in a course.

Identitätsinfrastruktur von Lernplattformen

Die Lehrenden und die Lernenden authentifizieren sich in der Lernplattform. Das Identitätsmanagement befasst sich mit der Verwaltung der Benutzerdaten. Eine Abbildung der gesamten Identität einer realen Person in eine digitale Identität in der digitalen Welt ist nicht möglich. Wichtige Teile einer Identität, wie Name, E-Mail-Adresse, Studienrichtung können in der digitalen Identität abgelegt werden. Es fehlt an einer Anonymität analog zum realen Leben, sich beispielsweise unverbindlich über etwas zu informieren. Auf der anderen Seite besteht ein Mangel an Authentizität bei digitalen Services. Es muss sichergestellt sein, dass sich nicht jemand als jemand anderer ausgibt und dessen Identität für die Nutzung eines Dienstes übernimmt (Hansen 2003, S. 51). Wie wir auch in der realen Welt verschiedene Rollen einnehmen, einmal als Freundin, ein anderes Mal als Arbeitskollegin und unterschiedliche Informationen von uns preisgeben, so können auch verschiedene digitale Identitäten für unterschiedliche Anwendungen angelegt werden.

Die Identität einer Person kann in verschiedene Teilaspekte getrennt werden:

- **Anonymität:** Ein anonymer Benutzer tritt mit keinerlei Identitätsattributen gegenüber einem Dienst auf. Dies ist eine sinnvolle Methode für den Schutz von personenbezogenen Daten, denn es werden keinerlei Daten zur Person erfasst. Auf technischer Ebene bietet das Internet keine absolute Anonymität. Bei jedem Zugriff auf einen entfernten Rechner gibt der Rechner des Benutzers zumindest die IP-Adresse bekannt, damit er auch Daten vom entfernten Rechner erhalten kann. Mit Hilfe der IP-Adresse und des Zeitpunktes der Nutzung dieser Adresse ist es für den Provider einfach, den Rechner dieser Nutzung zu identifizieren. In der Zwischenzeit gibt es eine Reihe von Projekten, die sich damit beschäftigen, das Internet zu anonymisieren bzw. anonymisierende Techniken zu verwenden. Ein Beispiel dafür ist das JAP-System, bei dem die Anfragen eines Benutzers über mehrere unabhängige Knoten geleitet werden und damit die IP-Adresse des Absenders versteckt (Berthold et al. 2004). In Lernplattformen ist der Zugang zu einem beschränkten Teil meist in Form eines „Gast"-Zuganges möglich. Dieser anonymen Identität steht eine sehr eingeschränkte Funktionalität zur Verfügung. Die Teile, die anonym eingesehen werden können, müssen dezidiert freigegeben werden. Der Zugang zu einem bestimmten Kurs ist über einen anonymen Benutzer meist nicht möglich.
- **Pseudoidentität:** Sie ist eine von einer Person selbst gewählte oder von einer anderen Person zugewiesene Repräsentation. Die Person nutzt ein Pseudonym, um sich selbst zu präsentieren. Die Pseudoidentität spiegelt eine Teilidentität wider, die meist ein Interessensgebiet oder ein Wunschbild der Person beinhaltet. Pseudoidentitäten kennt man vor allem aus Chat-Rooms, Online-Spielen, Diskussionsforen usw. Die Identifizierung von Kommunikationsteilnehmern über Pseudonyme ist eine gängige Praxis im Web. Dabei besteht die Möglichkeit, das Pseudonym zu wechseln oder gegenüber verschiedenen Partnern unterschiedliche Pseudonyme zu verwenden (Berthold et al. 2004). Dem Pseudonym werden Ressourcen zur Nutzung zugeordnet, das Pseudonym selbst ist dabei identifizierbarer Schlüssel. In Lernplattformen wird normalerweise nicht mit Pseudonymen gearbeitet. Um eine genaue Zuordnung der Aktivitäten zu ermöglichen, müssen sich die Benutzer beim Einstieg identifizieren.
- **Persönliche Identität:** Sie enthält Attribute einer realen Identität und ist gesetzlich durch das Datenschutzgesetz geschützt. Die Verbindung von Name und E-Mail-Adresse bildet eine

keywords
privacy
learning-management-system
personal data
data privacy

eigenständige digitale Identität. Die Identifizierungsmechanismen in Lernplattformen laufen in der Regel über die Angabe von Benutzernamen und Passwort. Als zusätzliche Attribute werden E-Mail-Adresse und IP-Adresse erfasst. Die Zuordnung zu bestimmten Gruppen (wie beispielsweise Lehrveranstaltungen) wird der Identität zugewiesen und ist im jeweiligen Benutzerprofil ersichtlich. Über Cookies wird die Interaktion zwischen Server und Web-Client teilweise automatisiert. Ein Cookie ist eine kleine Textinformation, die der Browser im Auftrag eines bestimmten Webserver-Hosts speichert und beim nächsten Besuch bei diesem Server wieder zurückliefert (Kerksen 2003, 960). Der Cookie-File speichert Informationen über die Benutzeridentität, letzte Aktivitäten in der Web-Site oder Passwortinformationen. Die Cookie-Technologie birgt eine Reihe von Problemen im Zusammenhang mit der Privatsphäre (Jerman-Blažič 2005).

Identitätsmanagement

Das Identitätsmanagement einer Lernplattform übernimmt die Benutzerverwaltung. Über die Benutzerverwaltung wird auch die Zuteilung der Rollen verwaltet, wie beispielsweise Lehrende, Studierende oder Tutoren. Mit der Zuteilung von Rollen werden auch Rechte und Ressourcen definiert (Abbildung 1).

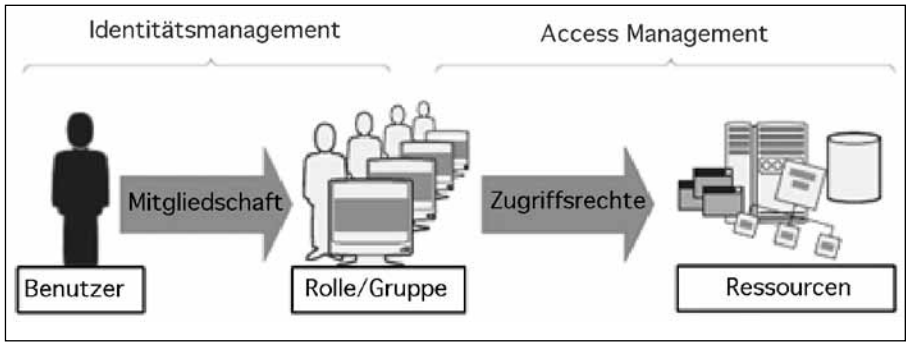

Abb. 1: Identitätsmanagement (Identity- und Accessmanagement 2006).

Die Administration der Lernplattform legt fest, welche Attribute einer Identität verwendet werden. Die Attribute können auch aus anderen Systemen übernommen werden, wie beispielsweise der Studienadministration. Jedem Benutzer steht ein Identitätsmanager zur Verfügung, in dem er selbstständig entscheidet, wann welche Informationen über ihn herausgegeben werden. Der Erstellung dieses Profils kommt besondere Bedeutung zu, weil in der Lernplattform über die digitale Identität kommuniziert wird.

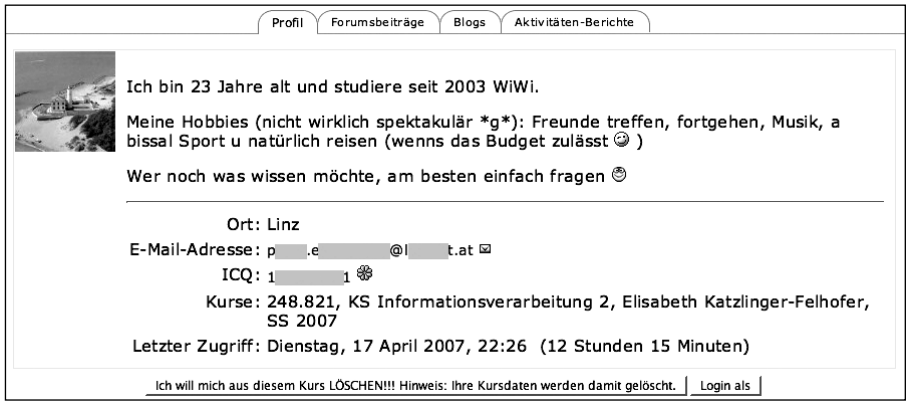

Abb. 2: Benutzerprofil Studierende (aus Moodle).

Abbildung 2 zeigt einen Auszug aus dem Benutzerprofil von Studierenden in der Lernplattform Moodle. Die persönlichen Angaben werden von den Studierenden gemacht, die Informationen über die belegten Kurse und den letzten Zugriff werden vom System ergänzt.

Das Profil kann über den **Identitätsmanager** um benutzerdefinierte Kategorien und Attribute erweitert werden. Das adaptierte Profil steht den potenziellen Kommunikationspartnern innerhalb der Lernplattform zur Verfügung. Es können nicht für verschiedene Gruppen, wie beispielsweise einzelne Lehrveranstaltungen, unterschiedliche **persönliche Profile** erstellt werden. Den Benutzern muss aber klar sein, dass das über den Identitätsmanager geänderte Profil den einzelnen Kommunikationspartnern (wie allen Studierenden aus einer Lehrveranstaltung, Lehrende verschiedener Lehrveranstaltungen) zur Verfügung steht. Lernplattformen zeichnen sich unter anderem auch dadurch aus, dass sie von unterschiedlichen Benutzergruppen verwendet werden. In der Lernplattform meldet sich jeder mit einer Identität (und damit mit einem Benutzerprofil) an. Mit diesem einen Profil wird mit allen anderen kommuniziert.

Jede Person ist meist Mitglied nicht nur in einer sondern in mehreren Gruppen. Innerhalb jeder Gruppe können sich **unterschiedliche Kommunikationsstile** entwickeln, von sehr informell bis sehr formell. Über das Profil können alle Gruppenmitglieder dieselben Informationen über eine Person einsehen. Das bereitet oft Schwierigkeiten, wenn beispielsweise eine Person ihr Profil im Identitätsmanager für eine informelle Gruppe einrichtet, diese Person aber dann Mitglied in anderen (eher formellen) Gruppen wird und das Profil nicht dementsprechend anpasst.

Awareness

Den Mechanismen der gegenseitigen Wahrnehmung (Awareness, Gewärtigkeit) in kooperativen Arbeitsumgebungen kommt eine besondere Bedeutung zu. Ohne detailliert auf das Forschungsfeld der Awareness eingehen zu wollen (Hoffman 2004, 12f), ist als Teil von kooperativen Handlungen die Wahrnehmung der **Handlungen der Kooperationspartner** zu berücksichtigen. Die Formen der Awareness reichen von der Rückmeldung der Anwesenheit der Kooperationspartner bis zur detaillierten Übermittlung bestimmter Handlungen innerhalb des gemeinsamen Handlungsbereiches (Hampel et al. 2004). Das Geschehen sollte kurz- und mittelfristig dokumentiert werden. Awareness-Unterstützung sollte umgebungsspezifisch, antizipierbar konstant und reziprok sein, dadurch lassen sich die Gefahren der Informationsüberlastung und der Verletzung der Privatsphäre minimieren (Pankoke-Babatz et al. 2004, 272).

Für die Unterstützung des Gruppengefüges gibt es mehrere Möglichkeiten, die Kommunikationsbeziehungen zu visualisieren. Die Lernplattform Moodle führt eine Liste aller Personen, die gerade online sind. Die Liste bezieht sich auf alle Personen die diese Lernplattform gerade benutzen und nicht nur auf Personen der eigenen Gruppe oder eines Kurses. Eine andere Visualisierungsmethode stellt die **Beziehungen der Gruppenmitglieder** untereinander grafisch dar. Abbildung 3 zeigt die Beziehungskarte eines Weblogs, der in der Lehre eingesetzt wird. Die Linien visualisieren die Verknüpfungen innerhalb der Blogs, die Helligkeit richtet sich nach der Anzahl der Beziehungen, Blogs mit vielen Verknüpfungen werden heller dargestellt. Die Visualisierung von Beziehungen kann helfen, potenzielle Kommunikationspartner für die direkte Interaktion zu finden. Visualisierungsmethoden helfen, die soziale Gruppen-Awareness zu fördern und zu verdeutlichen. Das kann auch unmittelbare Auswirkungen auf einzelne Personen haben, wenn sich beispielsweise herausstellt, dass eine Person nur wenige Kontakte hat und dieser Umstand dann für alle klar sichtbar wird.

Literatur:

Aimeur, E./Onana, F./Seleman, A., 2006, SPRITS: Secure Pedagogical Resources in Intelligent Tutoring Systems, in: Ikeda, M, Ashley, K., Chan, T.-W. (Eds): IST, Berlin, Heidelberg 2006, p. 237-247.

Berthold, O./Freytag, J. C., Privacy, Datenbank-Spektrum 11(2004), S. 41-44.

Eckert, C., Sicherheit und E-Learning, in: Beitrag zum Workshop „E-Learning: Beherrschbarkeit und Sicherheit", 1. – 2. Juli 2003 an der Technischen Universität Ilmenau, S. 43-50.

Hampel, T./Keil-Slawik, R./Selke, H., Semantische Räume – Von der Navigation zur kooperativen Wissensstrukturierung, in: Keil-Slawik, R., Selke, H., Szwillus, G. (Hrsg.): Mensch & Computer: Allgegenwärtige Interaktion, München 2004, S. 221-230.

Hansen, M., 2003, Nutzeranonymität und Identitätsmanagement – auch für E-Learning?, in: Beitrag zum Workshop „E-Learning: Beherrschbarkeit und Sicherheit", 1. – 2. Juli 2003 an der Technischen Universität Ilmenau, S. 51-62.

Hoffmann, M., Awareness und Adoption kooperativer Wissensmedien im Kontext informeller Zusammenarbeit, Dissertation, Universität Dortmund 2004.

Identity- und Accessmanagement, freie Wissensdatenbank 2006, <http://www.iam-wiki.org>

Jerman-Blaži , B./Klobu ar, T., Privacy Provision in E-Learning Standardized Systems: Status and Improvements, Computer Standards & Interfaces 27 (2005), p. 561-578.

Karat, J./Carat, C. M./Brody, C./Feng, J., Privacy in information technology: designing to enable privacy policy management in organizations. International Journal of Human-Computer Studies 63 (2005), p. 153-174.

Kerksen, S., Kompendium der Informationstechnik, Bonn 2003.

Kuhlen, R., Die Konsequenzen der Informationsassistenten. Was bedeutet informationelle Autonomie oder wie kann Vertrauen auf elektronischen Märkten gesichert werden? Frankfurt/Main 1999.

Langheinrich, M., Die Privatsphäre im Uniquitous Computing – Datenschutzaspekte der RFID-Technologie, in: Fleisch, E., Matern, M. (Hrsg.), Das Internet der Dinge, Berlin 2005, S. 329-362.

Pankoke-Babatz, U./Prinz, W./Schäfer, L., Was gibt's Neues? Asynchrone Gewärtigkeit, in: Keil-Slawik, R/ Selke, H./Szwillus, G. (Hrsg.), Mensch & Computer: Allgegenwärtige Interaktion, München 2004, S. 271-280.

Peissl, W., Privacy in Österreich. Eine Bestandsaufnahme, in: Peissl, W. (Hrsg.): Privacy. Ein Grundrecht mit Ablaufdatum? Wien 2003, S. 155-179.

Pils, M., Electronic Business und Sensible Informations- und Kommunikationssysteme, in: Höller, J./Pils, M./Zlabinger, R. (Hrsg.): Internet und Intranet. Herausforderung E-Business, 3. Aufl., Berlin, Heidelberg 2004, S. 327-359.

Privacy Rights Clearinghouse/UCAN, A Review of the Fair Information Principles: The Foundation of Privacy Public Policy. 13. 11. 2006, <http://www.privacyrights.org/ar/fairinfo.htm>

Reichling, T./Becks, A./Bresser, O./Wulf, V., Kontaktanbahnung in Lernplattformen, in: Keil-Slawik, R./ Selke, H./Szwillus, G. (Hrsg.), Mensch & Computer: Allgegenwärtige Interaktion, München 2004, S. 179-188.

Roßnagel, A., Verantwortung für Datenschutz, in: Informatik Spektrum 1, Dezember 2005, S. 462-473.

Zweig, D./Webster, J., Personality as a moderator of monitoring acceptance, in: Computers in Human Behavior 19 (2005), p. 479-493.

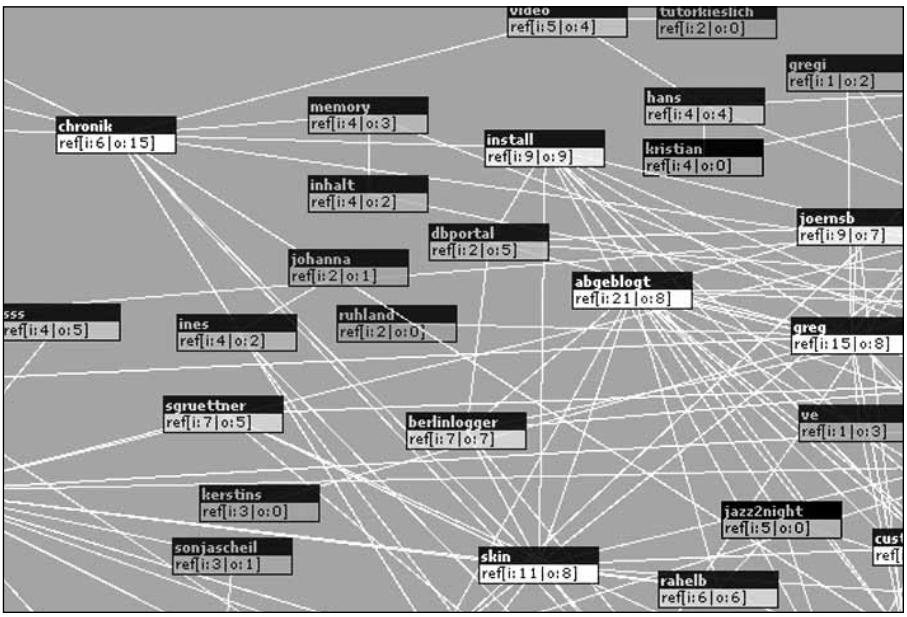

Abb. 3: Beziehungen innerhalb eines Lehre-Weblogs.

Lernplattformen bieten Funktionen, die es erlauben, Lernende im virtuellen Raum zu vernetzen. Ähnliche oder sich ergänzende Fähigkeiten, Interessen und Bedürfnisse können so Bezugspunkte für einen Austausch werden. Dazu müssen personenbezogene Daten der Lernenden erfasst, modelliert und evaluiert werden. Die Profile, die zum Vergleich herangezogen werden, werden auf der einen Seite aus Daten erstellt, die von den Benutzern angegeben werden („profile matching"). Es handelt sich hier um statische Daten, bei denen oft das Problem der mangelnden Aktualität besteht. Auf der anderen Seite werden die aktuellen Benutzerinteressen und Kenntnisse zum Vergleich verwendet. Diese werden als dynamisch betrachtet, da sie aus den Inhalten der Lernplattform abgeleitet werden, die der Benutzer konsumiert („history matching") (Reichling et al. 2004).

Innerhalb einer Lerngruppe bilden sich unterschiedliche Expertisen heraus. Für die Lernenden ist es von Interesse, auf das Expertenwissen anderer zugreifen zu können. Das Problem besteht nun darin, wie die einzelnen Lernenden Informationen über die Expertise der einzelnen Gruppenmitglieder erhalten. Mittels „**collaborative filtering**" wird die Expertise der einzelnen Gruppenmitglieder auf Grund ihres Verhaltens und der Evaluation ihrer Arbeiten durch die anderen Gruppenmitglieder beurteilt (Aimeur et al. 2006, S. 239).

Zweig und Webster führten eine Untersuchung über die Akzeptanz von Monitoring-Systemen zur **Gruppen-Awareness** von geografisch verteilten Arbeitsgruppen durch. Das Monitoring-System stellte den Gruppenmitgliedern die Information bereit, welche Gruppenmitglieder zu einem bestimmten Zeitpunkt interaktionsbereit waren. Bei dieser Untersuchung stellte sich heraus, dass die Akzeptanz von Monitoring-Systemen sehr stark von Persönlichkeitsmerkmalen, wie beispielsweise Extrovertiertheit abhängen. Extrovertierte Personen finden die Monitoring-Systeme fair und hilfreich in ihrer Arbeit, introvertierte Personen sehen darin eine Bedrohung ihrer Privatsphäre (Zweig et al. 2003, S. 490). Kooperative Lernsituationen sind durchaus mit dem Verhalten von Arbeitsgruppen vergleichbar, sodass diese Ergebnisse auch auf Lernsituationen übertragbar sind.

Fazit

Es gilt, für den Datenschutz und die Wahrung der Privatsphäre in Lernplattformen geeignete Rahmenbedingungen zu schaffen. Informations- und Kommunikationssysteme sind gestaltungsbedürftig und gestaltungsfähig. „Gestaltungsentscheidungen sind immer wieder notwendig etwa

bei der Entwicklung technischer Normen, bei der Konzeption der Systeme, bei der Festlegung ihrer Funktionen, bei der Auswahl der Komponenten, bei der Bestimmung von Freiheitsgraden oder bei der Konfigurierung. (...) Bei diesen Gestaltungen entscheiden Informatikerinnen und Informatiker auch immer – bewusst oder unbewusst – über die Chancen und Grenzen informationeller Selbstbestimmung. Datenschutzaspekte sind leicht zu berücksichtigen, wenn dies bei frühen Gestaltungsentscheidungen geschieht, dagegen schwer, wenn dies erst erfolgt, wenn bereits wichtige Strukturentscheidungen getroffen sind, die nachträglich verändert werden müssten“ (Roßnagel 2005, S. 470).

Das Recht auf Privatsphäre steht der Herausforderung einer technischen und gesellschaftlichen Entwicklung gegenüber, die auch vor dem Bildungsbereich nicht Halt macht. Die Menge der Daten und Informationen und deren Verwendungsmöglichkeiten steigen ständig an. Das Spannungsfeld zwischen dem Schutz der persönlichen Freiheit und den Sicherheitsinteressen ist ein zunehmend debattierter Aspekt der **Informationsgesellschaft**. Die Verarbeitung von personenbezogenen Daten wird für die Betroffenen immer intransparenter, wie auch die Befragung der betroffenen Studierenden gezeigt hat. Dadurch wird eine rationale Bewertung des Interessensausgleichs zwischen Privatsphäre und Sicherheit erschwert. Aus der Studierendenbefragung geht hervor, dass den Studierenden nicht bewusst war, dass der Lehrveranstaltungsleiterin die Auswertung der Aktivitätsdaten vorliegen. Es ist somit in dieser Lernplattform den Lernenden nicht transparent, welche Daten in welcher Form den Lehrenden zur Verfügung stehen.

Es sind nicht nur die Lernenden vom Verlust der Datensouveränität betroffen, sondern auch die Lehrenden in gleichem Maße. Den Systemadministratoren stehen die „logfiles“ der Lehrenden für Auswertungen zur Verfügung, die im Zuge der Evaluierung der Lehrenden verwendet werden können.

Es sind nicht nur die Lernenden vom Verlust der Datensouveränität betroffen, sondern auch die Lehrenden in gleichem Maße. Den Systemadministratoren stehen die „logfiles“ der Lehrenden für Auswertungen zur Verfügung, die im Zuge der Evaluierung der Lehrenden verwendet werden können.

Ein Kernbestandteil der informationellen Selbstbestimmung ist die Einwilligung der Betroffenen zur Verarbeitung ihrer personenbezogenen Daten. Mit der Akzeptanz der Nutzungsbestimmungen stimmen die Betroffenen der Verarbeitung zu. Da die Lernplattform ein integraler Bestandteil von Lehrveranstaltungen ist, ist es für die Lernenden nicht möglich, die Zustimmung zur Verarbeitung der personenbezogenen Daten nicht zu geben.

Datenschutz und Schutz der Privatsphäre sind allerdings nicht die einzigen Interessen, die zu berücksichtigen sind. Sie stehen in Konkurrenz mit anderen wichtigen Interessen, wie beispielsweise dem Sicherheitsinteresse oder der **Überprüfbarkeit von Leistungen** der Lernenden. Sie verlangen eine Verarbeitung personenbezogener Daten. Es gilt hier einen Ausgleich der konkurrierenden Interessen zu finden.

Für die Lehrenden stehen Daten zur Verfügung, die vor allem die Überprüfung von formalen Anforderungen erleichtern, wie beispielsweise die Kontrolle des Abgabezeitpunktes von Studierendenarbeiten oder eine geforderte Anzahl von Beiträgen in einem Forum. Die rein quantitative Auswertung der Anzahl von Beiträgen in Lernforen oder Lernchats ist mit Hilfe der Administrationswerkzeuge einfach möglich, für die **Leistungsbeurteilung** aber nicht unbedingt sinnvoll. Die Erfahrungen mit diesen Werkzeugen haben gezeigt, dass die Studierenden sehr rasch ihr Verhalten an rein quantitative Auswertungsmethoden anpassen und dann vor allem Quantität produzieren.

Neuere Entwicklungen zum Schutz der Privatsphäre in Informations- und Kommunikationssystemen setzen vermehrt auf den Systemdatenschutz. Die technischen Systeme sollen so gestaltet werden, dass der Personenbezug der Daten auf das notwendigste beschränkt wird. Damit wird der Interessensausgleich zwischen Informationszugang und Datenschutz bei der Technikgestaltung zu einer ständigen Herausforderung.

Kontakt:

Univ. Ass. Mag. Dr. Elisabeth Katzlinger
Institut für Datenverarbeitung in den Sozial- und Wirtschaftswissenschaften (idv)
Johann Kepler Universität Linz
Altenberger Str. 69
4040 Linz
ÖSTERREICH
Tel.: +43 732 2468-9348
Fax: +43 732 2468-8660
E-Mail: elisabeth.katzlinger@jku.at