Welche Informationen über die Universität gehören in das Internet? Standpunkte des Behördlichen Datenschutzbeauftragten

Allgemeines

Universität ist die Gemeinschaft der Studierenden und Lehrenden. Bereits an dieser Stelle ist zwingend ein Informationsaustausch notwendig. Aber die Universität als Zentrum von Lehre und Forschung kann sich nicht nur intern austauschen, sondern muß auch am Informationsaustausch außerhalb der Universität teilnehmen. Gerade die rasante Entwicklung der elektronischen Datenverarbeitung führte in den letzten Jahren dazu, daß die (Wissenschafts-)welt ein „global village" geworden ist[1] und auch die Humboldt-Universität zu Berlin an den Gesprächen auf dem Marktplatz dieses Dorfes teilnehmen muß.

Allerdings hat gerade dieser Tage der Berliner Landesdatenschutzbeauftragte sehr anschaulich vor der leichtfertigen Preisgabe eigener Daten gewarnt und darauf hingewiesen, daß internationale Adressenhändler mit der ihnen eigenen Methodik auf den deutschen Markt drängen. Niemand, der solche Warnung in den Wind schlägt, sollte sich über die übervollen Briefkästen mit Werbung für Plastikschrott aus allen Teilen der Welt wundern.

Ferner kann die Universität nicht machtherrlich über die Daten Ihrer Mitglieder verfügen und für die Mitglieder Entscheidungen treffen, da die Universität den Humboldtschen Idealen einer demokratischen, korporativ verfaßten und selbstverwalteten Universtät verpflichtet ist.

Diese Probleme, der notwendige internationale Informationsaustausch, der Datenschutz der einzelnen Mitglieder und die Gefahr des Mißbrauches der Daten, gilt es zu lösen. Hierbei werden die Techniker und Datenschützer oftmals der Entwicklung hinterherrennen. Durch die ständige Kooperation und wechselseitige Akzeptanz zwischen Datenschutz und Rechenzentrum an der Humboldt-Universität zu Berlin konnten eine Reihe von Lösungen erarbeitet werden, wie sie in den Artikeln dieses Heftes dargestellt sind. Hinsichtlich der Rechtsgrundlagen können wir uns hierbei fast ausschließlich auf bestehende Gesetze, insbesondere das Bundesdatenschutzgesetz und das Berliner Datenschutzgesetz beziehen. Durch die Interpretation dieser Normen und unter Beachtung der Rechtsgedanken, die das Bundesverfassungsgericht in seiner grundlegenden Entscheidung zum Volkzählungsgesetz[2] dargestellt und somit normiert hat, lassen sich fast alle Einzelfälle lösen. Voraussetzung ist allerdings, daß keine der Parteien, die am Lösungsprozeß beteiligt sind, auf ihren Auffassungen beharrt, sondern auch neue Wege geht. Nicht der Weg, der vor zwanzig Jahren an einer anderen Universität beschritten wurde, soll wiederholt werden, sondern die Erfahrungen dieser Wege anderer Einrichtungen mit ihren Höhen und Tiefen sollen in eine neue Lösung einfließen. Das Rechenzentrum der Humboldt-Universität zu Berlin ist hierbei besonders innovativ, und auch ich bemühe mich um Flexibilität.

Freiwilligkeit

Selbstverständlich steht es jedem Bürger frei, seine eigenen Daten im Wege der Freiwilligkeit beliebig weit zu streuen. Sollten Studenten, Wissenschaftler und sonstige Mitarbeiter das Bedürfnis haben, sich in ihren Homepages „outen" zu müssen, steht dem nichts im Wege. Die Verfassung, aufgrund der das informationelle Selbstbestimmungsrecht gewährt wird, gewährt uneingeschränkt Privatautonomie, daß heißt auch die Freiheit, sich scheinbar unvernünftig zu entscheiden. Lediglich bei verfassungswidrigen Aussagen (politisch extremistischen Aussagen, pornographischen Inhalten, die Straftatbestände darstellen u.ä.) muß die Universität als Anbieter einschreiten, um Schaden, sowohl ideeller als auch materieller Art abzuwenden.

Wissenschaftsprivileg

Wissenschaftliche Fachinformationsdienste sind, auch aufgrund des Verfassungsranges, den die Wissenschafts- und Forschungsfreiheit genießt, datenschutzrechtlich privilegiert (§ 10 Abs. 5 Bundesdatenschutzgesetz BDSG). Das heißt, daß wissenschaftliche Informationen, soweit sie keine schützenswerten personenbezogenen Daten enthalten, in einem automatisierten Abrufverfahren vorrätig gehalten werden. Allerdings muß auch hier beachtet werden, daß geeignete technische und organisatorische Maßnahmen zur Sicherung des Verfahrens und seiner Vorgaben festgelegt und eingehalten werden. Vor einigen Jahren führte das Fehlen solcher technischen und organisatorischen Maßnahmen zu einem Datenleck an der Universität von Berkley, Kalifornien[3]. Der Mitarbeiter des Rechenzentrums der HU, Herr Geschonneck, hat allerdings in seinem Beitrag in diesem Heft aufgezeigt, daß wir uns um entsprechende Maßnahmen bemühen.

Diese beiden Felder reichen aber nicht aus, um den Informationsaustausch in befriedigendem Maße zu erfüllen. Vielmehr benötigen diejenigen, die an einem Informationsaustausch interessiert sind, Ansprechpartner. Diese können sich freiwillig als solche anbieten.

In bestimmten Fällen ist es aber auch notwendig, daß die Universität nicht nur als anonyme Behörde auftritt, vielleicht noch mit einer oder zwei natürlichen Personen als Galionsfiguren. Vielmehr kann z.B. ein Vorle-

[1] wie uns die Werbung jeden Tag erzählt!
[2] BVerfGE 65, S. 1 ff.
[3] s. Clifford Stoll, Kuckucksei

sungsverzeichnis nicht sinnvoll sein, wenn nicht die Lehrenden darin genannt werden.

Bei bestimmten studentischen Projekten ist die Nennung der Beteiligten förderlich, um mehr Mitstreiter zu erreichen.

Studienbewerber und akademisch Interessierte wollen Informationen der Zentralen Universitätsverwaltung. Hierbei soll die Begegnung mit der Universität kein „Blind date“ werden, sondern man will von Anfang an mit der zuständigen Stelle in Verbindung treten.

Einwilligung und universitätsinterne Lösungen

Nicht immer werden diese Fälle des Informationsaustausches mit dem Mittel der Einwilligung möglich sein. Oftmals liegt keine Einwilligung zum Zeitpunkt der Datenabfrage vor. Dadurch konnten die Daten nicht rechtzeitig vorrätig gehalten werden. Sobald die Voraussetzungen erfüllt sind, ist die Information schon veraltet. Die Daten können universitätsintern bei einer extensiven Auslegung des § 15 BDSG vorrätig gehalten werden. Dies setzt voraus, daß

a) der Anlaß und Zweck des Abrufverfahrens zulässig sind,
b) die Datenempfänger bestimmbar sind,
c) die Art der Daten, die abgerufen werden können, bestimmbar und begrenzt ist und
d) die technischen und organisatorischen Maßnahmen zur Sicherung des Verfahrens und seiner Vorgaben (Auflagen) vorliegen (z.B. Firewall-Konzept).[4]

Aber aus diesem Vorrat dürfte nicht ohne weiteres ins Internet übermittelt werden.

Personenbezogene Daten im Internet und die rechtliche Lösung

Um auch nach außen hin Daten vorrätig halten zu können, müssen die Datensätze minimiert werden. Ferner sind die entsprechenden technischen Voraussetzungen zu schaffen, um einen Datenfischzug zu verhindern oder zu erschweren.

Die technischen Voraussetzungen entwickeln die Techniker, wobei der Datenschutz sicherlich kritische Anmerkungen und Bedenken beisteuert. Die Minimierung der angebotenen Datensätze ist nur im Konsens aller Mitgliedergruppen der Hochschule möglich. Nur dann kann auch ohne Einwilligung und Aufklärung über jeden Einzelfall, in dem Daten übermittelt werden könnten, aufgrund des sogenannten „überwiegenden Allgemeininteresses“ [5] ein Datenvorrat zum Informationsaustausch und zur Darstellung der Universität im Internet vorrätig gehalten werden.

Ohne einer solchen Vereinbarung vorzugreifen, die in einer Satzung des Akademischen Senats ihren Abschluß finden müßte, bin ich der Auffassung, daß im wissenschaftlichen Bereich die Namen und Dienstadressen der Hochschullehrer und wissenschaftlichen Mitarbeiter verwendet werden dürfen. Bei studentischen Mitarbeitern und Sekretariatskräften ist die Einwilligung erforderlich. Im Bereich der Verwaltung sind nur die personenbezogenen Daten der Mitarbeiter bis hinab zur Referatsleiterebene aufzuführen, die in außenwirksamen Bereichen arbeiten. Bezüglich der Veröffentlichung der Daten der anderen Mitarbeiter ist deren Einwilligung erforderlich.

Einen Mißbrauch können wir nicht mit absoluter Sicherheit ausschließen. Demnach müssen Hochschullehrer und leitende Mitarbeiter der Universität weiterhin damit leben, daß Anlageberater und Versicherungsvertreter sie nun vielleicht auch per E-Mail „konsultieren“. Aber wenigstens den nicht so im Rampenlicht der Öffentlichkeit stehenden Mitarbeitern müssen wir die „Dienstsphäre“ schützen.

André Kuhring,
Behördlicher Datenschutzbeauftragter
E-Mail: andre=kuhring@uv.hu-berlin.de

[4] zu den einzelnen Feldern und ihrer Definition vergleiche Stange, Datenschutz Recht und Praxis, Rdn. 134 ff.

[5] vgl. zu diesem Begriff Däubler, Gläserne Belegschaft, S. 77 ff. unter ausdrücklicher Bezugnahme auf die Bundesverfassungsrechtsprechung