Vorsicht vor Datenspuren! Ein Gespräch zum Selbstdatenschutz

von ***Bettina Pregel*** *am* ***28. Januar 2017***

Beim Selbstdatenschutz geht es um die Frage, wie die Mediennutzer selbst mit ihren Daten im Internet umgehen. Allzuhäufig hinterlassen sie zu viele Datenspuren im Netz, die sie nicht mehr zurücknehmen können – mit teils gravierenden Folgen. Um Mediennutzer zu unterstützen, publiziert die BLM Ratgeber zu diesem Thema. Anlässlich des Europäischen Datenschutztages hat blmplus mit Dr. Kristina Hopf aus dem Referat Jugend- und Nutzerschutz der BLM über die Möglichkeiten des Selbstdatenschutzes gesprochen.

Was bedeutet Selbstdatenschutz?

blmplus: Heute findet der Europäische Datenschutztag zum 11. Mal statt. Wofür steht dieser Tag?

Kristina Hopf: Ziel des Europäischen Datenschutztages ist es, das Bewusstsein der Bevölkerung für den Datenschutz zu fördern. Der Datenschutz ist zwar verfassungsrechtlich gewährleistet, es ist aber auch wichtig, sich selbst vor Datenverlust und -missbrauch zu schützen – Selbstdatenschutz ist hier das Schlagwort. Der Europäische Datenschutztag wird nicht nur in Europa durch Veranstaltungen, Aktionen oder Veröffentlichungen begleitet, sondern auch in den USA und Kanada als „Data Privacy Day“ gefeiert.

Sie haben gerade das Schlagwort „Selbstdatenschutz“ genannt. Was versteht man darunter, und was ist der Unterschied zum Datenschutz?

Beim Datenschutz, der seit dem Volkszählungsurteil 1983 als Verfassungsgut anerkannt ist, geht es um den gesetzlichen Schutz des Einzelnen vor unberechtigter Datenerhebung, -speicherung, -verwendung und -weitergabe. Diesen Rechtsanspruch hat der Einzelne gegenüber dem Staat, Behörden, Firmen und Unternehmen. Der Datenschutzbeauftragte der BLM kümmert sich beispielsweise darum, dass die Landeszentrale und die von ihr zugelassenen Programmanbieter den Datenschutz gegenüber Dritten beachten. Außerdem geht er Beschwerden aus der Bevölkerung nach.

Der Selbstdatenschutz dagegen hat den Mediennutzer im Fokus. Es geht vor allem um die Frage, wie man selbst mit seinen Daten im Internet umgeht. Im Netz geben wir viele Daten von uns preis, teilweise freiwillig und bewusst in sozialen Netzwerken. Teilweise hinterlassen die Nutzer aber auch Datenspuren, die sie meist nicht einmal bemerken und nicht mehr zurücknehmen können. Möglicherweise ziehen diese Spuren aber gravierende Konsequenzen nach sich. Deshalb bedeutet Selbstdatenschutz nicht zuletzt, seine Privatsphäre mittels Datensparsamkeit und Datenkontrolle vor dem eigenen Mitteilungs- und Selbstdarstellungs-Bedürfnis zu schützen.

„Es besteht Handlungsbedarf“

„Ich habe doch nichts zu verbergen, also macht es doch nichts, wenn ich meine Daten zur Verfügung stelle?“ So oder so ähnlich antworten viele Menschen, wenn Sie im Netz ihre Daten preisgeben. Wie denken Sie über diese Haltung?

Diese Haltung überrascht mich immer wieder. Wenn ich jemanden bitten würde, mich einen Blick in Ihre Handtasche, Ihr Tagebuch oder Ihre E-Mails und Fotos auf Ihrem Handy werfen zu lassen, würden die meisten Menschen mit Nein antworten. Kaum ein Mensch erlaubt Unbekannten ohne Grund Einblick in seine privaten Verhältnisse. Ganz anders scheint das bei vielen Menschen zu sein, wenn sie im Internet unterwegs sind. Nach

dem Motto „Ich habe doch nichts zu verbergen“ werden Daten freiwillig öffentlich gemacht. Überwachung und das Ausspähen von Informationen werten viele nur als Kavaliersdelikt. Aber dieses Vorgehen ist nicht harmlos. Der Staat und seine Institutionen sind zwar zum bestmöglichen Schutz der Bürgerinnen und Bürger verpflichtet. Ein Skandal wie die NSA-Abhöraffäre sowie die Datensammlungen großer Konzerne zeigen jedoch: Es besteht – privat wie auf gesellschaftlicher Ebene – Handlungsbedarf.

Können Sie uns Beispiele nennen, warum Selbstdatenschutz wichtig ist?

Immer mehr Arbeitgeber informieren sich über Bewerber für einen freien Arbeitsplatz zunächst im Netz. Wenn man beispielsweise bei Instagram oder Facebook einen schlechten Eindruck hinterlässt, kann dies Auswirkungen auf die Jobchancen oder auch auf ein bereits bestehendes Arbeitsverhältnis haben.

Datenpreisgabe kann auch zu einer Preisdiskriminierung im Internet führen. Teilweise wird von Preiszuschlägen für Nutzer teurer Geräte oder für Bewohner teurer Wohnviertel berichtet. Warum sollte jemand mehr für eine Reise bezahlen müssen, nur weil er von einem kostspieligen Gerät oder aus einer teureren Wohngegend eine Internetseite aufruft

Wenn ich ein neues Gerät kaufe, was sollte ich ganz konkret beachten, um mich vor Datenpreisgabe /-verlust zu schützen?

Bei neuen Geräten sollte man sich immer kurz Zeit nehmen, die Datenschutzeinstellungen zu prüfen. Meist sind die vom Anbieter gewählten Voreinstellungen nicht die datenschutzfreundlichsten, sondern ermöglichen eher eine umfangreiche Datenerhebung. Man sollte bei neuen Geräten oder neuer Technik eine Zugangssperre einrichten. Dies kann durch Eingabe eines PINs, Passwortes oder mittels Fingerabdruckscanner erfolgen. Zum Selbstdatenschutz hat die Landeszentrale die Broschüre „Selbstdatenschutz! – Tipps, Tricks, Klicks“ veröffentlicht.

Tipps für Eltern: Verbote helfen nicht weiter

Welche Tipps haben Sie für Eltern in puncto Selbstdatenschutz bei der Smartphone-Nutzung durch Kinder und Jugendliche?

Statt Verboten rate ich Eltern, mit Ihren Kindern im Gespräch zu bleiben. Je nach Alter sollten Eltern Downloads und Anmeldungen bei Apps nach Möglichkeit gemeinsam mit ihren Kindern vornehmen und zeigen, wie man die Privatsphäre-Einstellungen prüfen kann. Kinder und Jugendliche sollten über die Möglichkeit der anonymen Anmeldung bei einem Internet-Angebot informiert werden. Die frühzeitige Aufklärung junger Menschen ist wichtig. Nachname, Adresse, Geburtsdatum und Telefonnummer haben nichts im Netz zu suchen und sollten nicht an Unbekannte weitergegeben werden. Zur Veröffentlichung von Fotos gibt es zwei klare Regeln: 1. keine intimen und unvorteilhaften Aufnahmen ins Netz stellen oder verschicken und 2. bei Fotos von anderen vor Veröffentlichung oder Versenden diese um Erlaubnis fragen.

Die JIM-Studie 2016 hat gezeigt, dass WhatsApp die meist genutzte App bei Jugendlichen ist. Was sollte bei der Nutzung von Messangern beachtet werden?

Neugierde und Gruppendruck treiben schon Kinder zu WhatsApp, obwohl das Mindestalter nach den Allgemeinen Geschäftsbedingungen 13 Jahre ist. Ein Verbot der Installation auf dem Gerät wäre möglich, ist aber mit einer dauerhaften Kontrolle verbunden und daher kaum durchführbar. Unabhängig von Verboten ist es vor allem wichtig, auf die kritischen Punkte bei der Nutzung von WhatsApp hinzuweisen, wie die Übertragung der Kontaktdaten, die Sichtbarkeit des Online-Status, die Mobbing-Gefahr, die Möglichkeit unangemessener Kettenbriefe, der Erreichbarkeitsdruck, die geforderten Zugriffsberechtigungen. Messenger wie bspw. Threema könnten als Alternative angesprochen und getestet werden. Threema ist ein Schweizer Unternehmen, das sich Datenschutz mittels Verschlüsselung auf die Fahnen geschrieben hat.

Was unternimmt die Landeszentrale, um Eltern und Lehrer hinsichtlich der Möglichkeiten des Selbstdatenschutzes aufzuklären?

Die Landeszentrale übernimmt neben der Schulung von Multiplikatoren auch die Informationsvermittlung gegenüber Pädagogen und Lehrkräften in eigenen Fortbildungsveranstaltungen.

Das Thema Selbstdatenschutz wird auch im Medienführerschein der Stiftung Medienpädagogik Bayern behandelt. Außerdem gibt es verschiedene Veröffentlichungen. Aktuell plant die Landeszentrale eine Publikation zum Thema „Tipps zum sicheren Passwort“.