ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Sommerakademie 2011

„Optimierte Verantwortungslosigkeit“

Die Verantwortung von IT-Unternehmen für Verbraucherdaten

Referent: Dr. Christian Grugel, BMELV

Die Verantwortung von IT-Unternehmen für Verbraucherdaten

Vortrag anlässlich der Sommerakademie 2011 der Datenschutzakademie im Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein am 29. August 2011 in Kiel

Dr. Christian Grugel

Leiter der Abteilung 2 (Verbraucherpolitik) im Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz

Es gilt das gesprochene Wort!

Sehr geehrte Damen und Herren,

zunächst möchte ich Ihnen danken, dass Sie mir Gelegenheit gegeben haben, mich als der für Verbraucherpolitik zuständige Abteilungsleiter des Ministeriums, das sich intensiv mit Verbraucherschutz, Internet und Datenschutz beschäftigt, zu der Verantwortung von IT-Unternehmen für Verbraucherdaten äußern zu können.

Die Ereignisse der letzten Zeit zeigen, wie sehr das Thema „Datenschutz und Internet“ die Öffentlichkeit in Deutschland bewegt. Es gibt eine Reihe von aktuellen Beispielen für Datenpannen, für die die Unternehmen die Verantwortung trifft: Da ist zum Einen der Diebstahl von mehr als 100 Millionen Daten von Kunden beim Sony Playstation Network und Sony Online Entertainment. Zum Anderen denke ich an die Speicherung von Standortdaten durch das iPhone von Apple. Erst im Mai wurde bekannt, dass Applikationen bei Facebook seit vier Jahren auf die gesamten Profildaten der Nutzer zugreifen konnten. Bei Kamerafahrten für Google Streetview wurden unverschlüsselte Kommunikationsinhalte aus WLAN-Funknetzen erfasst. Es heißt immer wieder, dass es sich um einen „Bug“, einen Fehler, gehandelt habe.

Ob nun Panne oder bewusste Geschäftspolitik: Die Verbraucherinnen und Verbraucher sind verunsichert und beunruhigt – und das zu recht. Hier ist vor allem das Paradebeispiel „Facebook“ zu nennen. So überträgt der „Gefällt mir“-Button Daten von Internetseiten, die den Button eingebunden haben, an Facebook, selbst wenn der Button nicht angeklickt wird. Datenschutz ist vor allem im Zeitalter des Internets eine wichtige Größe, die uns stets vor neue Herausforderungen stellt. Andererseits ist das Internet aus unserem täglichen Leben nicht mehr wegzudenken. Wir informieren uns, erledigen Bankgeschäfte, kaufen ein und kommunizieren. Das erleichtert nicht nur unser tägliches Leben, sondern macht auch Spaß.

Das Internet bringt aber neue Herausforderungen mit sich. Immer mehr Daten können mit wenigen Klicks zusammen geführt werden. Ganze Lebensläufe, häufig auch persönliche Vorlieben, Freunde und vieles mehr sind ohne jede Schwierigkeit zu finden. Das Internet ist eine enorme Wissensdatenbank – das ist von unschätzbarem Wert. Geht es aber um Persönlichkeitsrechte, ist es ein riesiger Unterschied, ob man sich eine Information nur mit Mühe beschaffen kann oder mit wenigen Klicks am Computer. Hier liegt aus meiner Sicht z. B. die Besonderheit von Straßenansichtsdiensten im Internet.

Für den Datenschutz in der digitalen Welt sehe ich drei Akteure in der Pflicht: Die Politik muss den gesetzlichen Rahmen vorgeben. Die Unternehmen haben eine hohe Eigenverantwortung, was die Sicherheit der Daten betrifft, aber auch, was Datensparsamkeit betrifft. Datensparsame Grundeinstellungen sollten der Normalstandard sein. Schließlich kommt es auch auf die Nutzer an: Sie müssen verantwortlich mit den eigenen Daten und den Daten anderer Nutzer umgehen.

In der Verantwortung der Unternehmen liegt es, ihre Angebote nutzerfreundlich, datenschutzfreundlich und transparent zu gestalten, um die Datensicherheit zu gewährleisten. Allein das Eigeninteresse sollte die Unternehmen schon von sich aus dazu bringen, sorgsam mit den ihnen anvertrauten Daten umzugehen. Das scheint aber nicht zu klappen, wie die zahlreichen Sicherheitslücken bei Datenspeicherung und –verwendung sowie die Datendiebstähle zeigen. Hier muss die Wirtschaft in die Pflicht genommen werden. Ich möchte in diesem Zusammenhang auf einige Punkte zu sprechen kommen, die mir im Hinblick auf die Verantwortung der Unternehmen als besonders wichtig erscheinen.

Von erheblicher Bedeutung ist zunächst die Datensicherheit. Der Datendiebstahl bei Sony sowie die Speicherung von Standortdaten durch iPhone und iPad von Apple machen hier dringenden Handlungsbedarf deutlich. Insbesondere der Vorfall bei Sony hat gezeigt, dass die Sicherheit von Daten bei Unternehmen noch nicht überall in dem erforderlichen Maße berücksichtigt und gewährleistet wird. Bei den Sicherheitsvorkehrungen scheint insofern erheblicher Nachholbedarf zu bestehen. Die technische Sicherheit muss gewährleistet sein. Die Datensicherheit ist wesentlich für die Verbraucher. Eine gute Sicherung der Verbraucherdaten durch IT-Unternehmen ist daher zwingend erforderlich.

Dies gilt insbesondere auch für Soziale Netzwerke. Da hier persönlichste Dinge ausgetauscht werden, ist hier auch ein hohes Sicherheitsniveau erforderlich. Solche Daten können nicht nur zu Werbezwecken genutzt werden, sondern auch von Kriminellen missbraucht werden. Angriffsszenarien reichen von der Ausnutzung einer Abwesenheit zum Einbruch über die Versendung besonders vertrauenswürdig erscheinender Mails mit Spionagesoftware, die Passwörter abfischt, bis hin zum Identitätsdiebstahl. Ich erwarte von den Unternehmen, bei der Datensicherheit viel aktiver zu werden. Auch hier, wie auf anderem Gebiet könnte auf eine verstärkte Zusammenarbeit der Unternehmen untereinander gesetzt werden, um hohe Sicherheitsstandards zu erreichen und zu halten.

Erforderlich ist auch mehr Transparenz. Verbraucher müssen wissen, was mit ihren Daten geschieht. Es muss erkennbar sein, bei welchen Diensten die Privatsphäre gut aufgehoben ist und bei welchen weniger gut. Hier müssen die Unternehmen noch Aufklärungsarbeit leisten. Ihre Datenschutzvorschriften müssen verständlich sein und dürfen nicht hinter anderen Inhalten versteckt werden.

Darüber hinaus müssen IT-Unternehmen die Selbstbestimmung der Nutzer wahren. Von besonderer Wichtigkeit ist dabei das Einwilligungserfordernis. Dies gilt für sensible Dienste wie die Markierung von Personen auf Fotos und die Gesichtserkennung. Ein Abgleich von Fotos über Gesichtserkennung darf nur mit ausdrücklicher Einwilligung der betroffenen Person möglich sein.

Daneben müssen auch die Grundsätze „privacy by design“ und „privacy by default“ stärker berücksichtigt werden. Das heißt zum Einen, dass der Datenschutz schon bei der technischen Entwicklung von Produkten und Angeboten berücksichtigt werden muss. Zum Anderen müssen Voreinstellungen datenschutzfreundlich und sicherheitsorientiert sein. Dies gilt neben Sozialen Netzwerken beispielsweise auch für Internet-Browser (z.B. Internet Explorer, Firefox, Opera). Diese sollten datenschutz- und sicherheitsfreundliche Voreinstellungen haben. Auch sollten Computer im Kaufzustand die wichtigsten Sicherheitsvorkehrungen implementiert haben.

Ich möchte auch noch einmal auf die Verantwortung speziell von Anbietern Sozialer Netzwerke zu sprechen kommen. Diese trifft eine besondere Verantwortung, da sie besonders sensible Nutzerdaten verwalten. Es geht hier nicht nur darum, was die Leute selbst öffentlich machen, sondern auch darum, was die Netzwerke mit den Daten tun, ohne dass die Nutzer es wissen. Zwar ist die Kommunikation im Sozialen Netz eine große Bereicherung. Über kein anderes Medium können wir uns so schnell mit vielen Freunden gleichzeitig austauschen wie über Soziale Netzwerke. Dass hier unzählige persönliche Informationen zusammenlaufen, ist aber auch mit besonderen Risiken verbunden. Die in Sozialen Netzwerken eingestellten persönlichen Informationen erfordern auch eine besondere Sensibilität der Anbieter für den Schutz der Privatsphäre. Hierzu gehört, dass – wie bereits erwähnt – die Selbstbestimmung der Nutzer gewahrt wird und diese gefragt werden, bevor ihre Daten zu anderen Zwecken verwendet oder gar an Dritte weiter gegeben werden. Auch die Selbstbestimmung Dritter muss gewahrt werden. Diesbezüglich ist der „Freundefinder“ von Facebook nicht nur in die Kritik geraten, sondern auch Gegenstand einer Klage des vzbv. Auch nach der von Herrn Prof. Caspar, dem Hamburgischen Datenschutzbeauftragten, durchgesetzten Überarbeitung des Freundefinders ist lediglich eine Widerspruchsmöglichkeit gegen die Datennutzung vorgesehen. Erforderlich wäre hier eine ausdrückliche Einwilligung, zumal es sich um die Daten von Dritten handelt, die den Geschäftsbedingungen von Facebook nicht zugestimmt haben. Wie sollten sie auch, sie wissen ja nichts von der Weitergabe ihrer Daten. Soziale Netzwerke müssen vollständige Löschungsmöglichkeiten zur Verfügung stellen. Die VZ-Netzwerke z. B. bieten ihren Nutzern diese Möglichkeit bereits an. Darüber hinaus sollten restriktive Grundeinstellungen gängige Praxis bei Sozialen Netzwerken sein. Das Profil und weitere Inhalte sollten erst nach aktiver Freischaltung für die gewünschte Zielgruppe sichtbar sein.

Ein weiterer Aspekt im Bereich der Verantwortung der Unternehmen ist die zeitnahe und aussagekräftige Erteilung erbetener Auskünfte über die gespeicherten Daten. Als Beispiel möchte ich auf die Erfahrungen eines Bundespolitikers hinweisen, der wissen wollte, wie es mit der Datenvorhaltung in der täglichen Praxis aussieht. Er musste seinen Mobilfunkbetreiber T-Mobile auf die Herausgabe aller über ihn gespeicherten mobilen Vorratsdaten verklagen, um sie überhaupt zu bekommen. Die jetzt veröffentlichten Daten, die über ein halbes Jahr gespeichert waren, sind als Einzeldaten sicher unbedeutend und harmlos, ergeben in der Summe jedoch ein animiertes Bewegungsprofil über das gesamte Leben: Das Profil enthüllt, wann er Bahn fährt, wann er fliegt, in welcher Stadt er sich aufhält, wann er arbeitet und zu welchen Zeiten er vermutlich schläft. Dieses Beispiel zeigt: Im digitalen Zeitalter entstehen permanent Spuren. Wer Zugriff auf sie hat und sie zu deuten weiß, kann fast alles über die betroffene Person herausfinden. Deshalb sollte jedermann jederzeit wissen dürfen, wer welche Informationen über ihn hat. Und er sollte bestimmen dürfen, wer darauf wie zugreifen darf.

Dass Datenschutz- oder Sicherheitsverletzungen unverzüglich abgestellt und Auskunfts- und Löschungsansprüche zügig umgesetzt werden, sollte durch ein effektives Beschwerdemanagement gewährleistet werden. Auch dies liegt in der Verantwortung der IT-Unternehmen. Wenn Verbraucher bei Beschwerden oder Fragen schnell eine Antwort erhalten, nutzt dies der gesamten Branche. Mir ist bewusst, dass dies nicht ohne personellen Aufwand möglich ist. Manche Soziale Netzwerke beschäftigen z.B. eine Reihe von Mitarbeitern, um schnell auf E-Mails reagieren oder auch einen Account, von dem Cyber-Mobbing ausgeht, schnell sperren zu können. Das ist gut so. Bei anderen scheint das E-Mail-Postfach eine Black Box darzustellen. Im Kodex für Geodatendienste ist eine gemeinsame telefonische Beratungsstelle vorgesehen. Dies ist ein gutes Beispiel. Ich hoffe, dass diese bald eingerichtet wird.

Die Politik schafft mit Gesetzen die Rahmenbedingungen. Prinzipiell unterliegen reale Welt und Internetwelt denselben rechtlichen Regelungen. Die Politik muss aber prüfen, bei welchen internetspezifischen

Sachverhalten spezielle Regelungen notwendig sind. Dabei muss auch darauf achtet werden, dass bei diesen Regelungen auch die Rechtsdurchsetzung gesichert ist.

Die Politik kann und muss die Wirtschaft aber auch auf andere Weise mehr in die Verantwortung nehmen. Praktische Verbesserungen können eintreten, wenn aktuelle Datenschutzprobleme in der Öffentlichkeit und gegenüber den Unternehmen thematisiert werden. Von der Politik angestoßene öffentliche Debatten führen auch dazu, dass die Unternehmen ihren Pflichten besser nachkommen. Beispielsweise hat Sony nach der Datenpanne den Dienst abgeschaltet und begonnen, das System grundlegend zu überarbeiten. Auch die öffentliche Debatte über den unzureichenden Schutz der Privatsphäre bei Facebook wurde wesentlich durch die Politik angestoßen. So hat das Unternehmen hat auf die auch vom BMELV geäußerte Kritik reagiert, was die Ankündigung von Veranstaltungen durch Jugendliche betrifft. Damit die private Party im kleinen Kreis nicht durch ein Versehen zur unkontrollierbaren Massenveranstaltung wird, hat Facebook in sein Muster versuchsweise einen ausdrücklichen Warnhinweis für den gewählten Verteilerkreis aufgenommen. Dies ist ein erster Schritt, den wir begrüßen. Noch besser wäre es freilich, wenn die Voreinstellung für die Ankündigung von Veranstaltungen nur für den kleinen Kreis „privat“ ausgestaltet wäre. Die öffentliche Aufmerksamkeit für diese Themen hat konkrete Auswirkungen: Die Nutzer werden sensibler, so dass Facebook manche Senkung der Datenschutzniveaus wieder rückgängig machen musste. Auch für die Durchsetzung des veränderten Umgangs mit den Daten des „Freundefinders“ durch den Hamburger Datenschutzbeauftragten dürfte der öffentliche Rückenwind hilfreich gewesen sein. All das zeigt, dass öffentlicher und politischer Druck – neben effektiven Sanktionsmöglichkeiten der Aufsichtsbehörden, die unerlässlich sind – ebenfalls zum Abstellen von Datenschutzverstößen führen können. Viele Unternehmen haben begonnen, auf Protest zu reagieren. Und: Sie sind angewiesen auf das Vertrauen ihrer Nutzer! Und das ist die Macht der Verbraucher!

Des Weiteren hat die Politik die Möglichkeit, Anstoß zu Selbstverpflichtungen zu geben. Zwar sind Selbstverpflichtungen kein Ersatz für notwendige gesetzliche Regelungen. Sie sind jedoch manchmal geeignet, schneller praktische Veränderungen zu bewirken. Sinnvoll können diese insbesondere in Bereichen sein, bei denen Schwierigkeiten bei der Rechtsdurchsetzung, z.B. im internationalen Kontext, bestehen. Macht ein ausländisches Unternehmen mit, dann gibt es keine langwierigen Auseinandersetzungen um Fragen der Rechtsgeltung. Wesentliche Voraussetzung für funktionierende Selbstregulierungen sind dabei effektive Sanktionsmöglichkeiten. Ein Beispiel dafür ist die Entwicklung der Selbstverpflichtung des BITKOM, der Kodex für Geodatendienste. Das BMELV begrüßt ihn, weil er deutlich macht, dass sich die Anbieter ihrer Verantwortung für den Schutz der Privatsphäre stellen. Die Selbstverpflichtung ist eine Möglichkeit, verloren gegangenes Vertrauen wieder zurück zu gewinnen. Jetzt muss die Selbstverpflichtung mit Leben gefüllt werden. Dabei kommt es auch auf die wirksame Durchsetzung der Verhaltensregeln an.

Neben der Datensicherheit sind Transparenz, Selbstbestimmung und Auskunftsrechte oberstes Gebot. Die Nutzer müssen wissen, was mit ihren Daten passiert. Und sie müssen Einfluss darauf haben können, was mit ihren Daten geschieht und wenn sie eine bestimmte Nutzung ihrer Daten nicht wollen. Die Anbieter tragen eine wesentliche Verantwortung für den Schutz der Privatheit im Internet. Sie sind es, die persönliche Daten erheben, nutzen und weitergeben. Daher müssen sie auch sicher stellen, dass sie dies jeweils im Einklang mit dem geltenden Recht tun, und dass die Daten bei ihnen sicher sind. Nur wenn der Datenschutz und das Recht auf Privatheit auch bei neuen Anwendungen im Netz stärker berücksichtigt wird, werden die Verbraucher Vertrauen in diese Dienste haben. Und Vertrauen ist der Schlüssel auch auf diesem Markt.

Ich danke Ihnen für Ihre Aufmerksamkeit.