MODUL 6

Datenschutz im Internet

MODUL 06

| Helmut Eiermann | Barbara Steinhöfel

Der Datenschutz ist ein komplexes Thema und wird in Öffentlichkeit und Politik intensiv diskutiert. Neue Technologien und die Nutzung des Internets machen es fast unvermeidbar, dass jeder von uns Datenspuren hinterlässt. Wann, wo und wie das passiert, welche Folgen das haben kann und wie man sich am besten schützt, wird in diesem Modul erläutert.

1. Die Debatte um den Datenschutz

Nach der Debatte um die Volkszählung im Jahr 1983 führte das Bundesverfassungsgericht im Dezember 1983 auf Grundlage des Allgemeinen Persönlichkeitsrechts das Grundrecht auf informationelle Selbstbestimmung ein. Dieses Recht besagt, dass jeder Bürger das Recht hat, über Preisgabe und Verwendung seiner → personenbezogenen Daten selbst zu bestimmen. Neben diesem allgemeinen Grundsatz im Grundgesetz finden sich wesentliche Datenschutzbestimmungen im Bundesdatenschutzgesetz.

§

Weitere Informationen:

Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz (GG)

Das Thema Datenschutz ist sehr komplex, und die genannten Gesetze beziehen sich nur auf die Bundesrepublik Deutschland. Im Zuge der weltweiten Vernetzung gibt es zwar Tendenzen, die Datenschutzrichtlinien auf europäischer und weltweiter Ebene zu harmonisieren, aber aufgrund unterschiedlicher Wertekanons fällt dies schwer. Und nicht nur auf internationaler Ebene gibt es Schwierigkeiten: Auch hier in Deutschland wird über eine sinnvolle Balance zwischen Datenschutz auf der einen Seite und den Rechten auf Meinungs- und Pressefreiheit auf der anderen Seite heftig diskutiert.

Die Gesetzeslage führt dazu, dass für verschiedene Internetseiten verschiedene Datenschutzrichtlinien gelten. Viele Internetseiten fallen beispielsweise unter US-amerikanisches Recht, weil sie in den USA

bereitgestellt werden. Hat eine Firma jedoch eine deutsche Niederlassung wie beispielsweise Google in Hamburg, sind auch deutsche Datenschutzbestimmungen zu beachten. Stets am deutschen Datenschutzrecht zu messen sind die schriftlich niedergelegten Datenschutzbestimmungen der Anbieter.

Neben diese gesetzliche Komponente tritt eine technische: Die rasante Entwicklung im IT- und Kommunikationssektor bringt immer wieder neue Technologien und Anwendungen hervor. Oft werden hierbei jedoch Daten erhoben, ohne dass der Nutzer Kenntnis davon erlangt. Die Kontrolle über die Weitergabe und Verwendung der eigenen Daten wird damit immer schwieriger.

Weitere Informationen:

Art. 1 Abs. 1 Grundgesetz (GG)

Privatsphäre und Öffentlichkeit

In der Diskussion um den Datenschutz stellt sich meist auch die Frage nach dem Verhältnis von Privatsphäre und Öffentlichkeit. Der Privatraum des Einzelnen ist ein schützenswertes Gut, das ihm durch das Grundgesetz zugesichert ist. Sieht man im Fernsehen oder im Internet jedoch Bilder, die diesen Raum empfindlich stören, beginnt man sich zu fragen, inwieweit Privatsphäre heute noch eine Rolle spielt. Sendungen wie „Big Brother“ oder Pseudo-Doku-Sendungen wie „We are Family“ liefern dem Zuschauer einen tiefen Einblick in die Privatsphäre anderer Menschen, ebenso wie zahlreiche Bilder und Videos, die Internetnutzer ins Netz hochladen. Diese Bilder sollten jedoch dahingehend analysiert werden, inwieweit das Gezeigte der Realität entspricht und authentisch ist, oder inwieweit eine Inszenierung des Alltags vonseiten der Produzenten und „Schauspieler“ stattfindet.

Hinzu kommt, dass zwischen Medien und Wirtschaft ein enges Abhängigkeitsverhältnis besteht. Insbesondere die Medien des privaten Rundfunks leben von ihren Werbeeinnahmen und haben allein deshalb Interesse daran, mit Wirtschaftsunternehmen zusammenzuarbeiten. Die Medien liefern die notwendigen Daten, um die Werbung stärker auf Zielgruppen und die Bedürfnisse Einzelner zu fokussieren, und die Wirtschaft zahlt für diese Informationen.

2. Datensammler

Es mag einem vielleicht seltsam vorkommen, dass es eine andere Person interessieren könnte, welche Bücher oder welche CDs man im Internet kauft. Daten sind jedoch oft die Währung, mit der man im Internet – auch bei kostenfreien Angeboten – „bezahlt". Indem Daten von Nutzern gesammelt und ausgewertet werden, wird beispielsweise individuelle Werbung geschaltet. Es können darüber hinaus Präferenzen bestimmter Zielgruppen erkannt sowie Bewegungsprofile für Internetseiten erstellt werden und vieles mehr. Möchte ein Hersteller ein neues Vitalgetränk auf den Markt bringen, ist es für ihn ein wichtiger Hinweis, dass ähnliche Produkte vor allem von jungen Menschen mit gehobenem Einkommen und starker Gesundheitsorientierung gekauft werden. Auf dieser Grundlage würde der Hersteller sich vielleicht dafür entscheiden, sein Produkt auf sozialen Plattformen zu bewerben, die ein entsprechend kaufkräftiges Zielpublikum haben. Bewegungsprofile geben ihm Auskunft darüber, wie sich Nutzer auf Internetseiten bewegen, was sie zuerst anklicken und wie sie eine Website weiter nutzen. Entsprechend kann er seine Werbung daran anpassen und in die Seite einbetten.

Mit den Daten der Internetnutzer können also Informationen gesammelt werden, die für Wirtschaftstreibende von enormer Bedeutung sind. Ein großes Internetportal wie *facebook.de*, das von mehr als 1,4 Milliarden Menschen weltweit genutzt wird, ist für Werbetreibende entsprechend interessant. Ein Profil auf Facebook hat daher einen durchschnittlichen „Marktwert" von etwa 120 US-Dollar (Stand: Juni 2012).

Neben sozialen Netzwerken sind aber auch Online-Kaufhäuser, E-Mail-Anbieter oder Suchmaschinen an persönlichen Daten interessiert, denn Werbung ist das zentrale Finanzierungs- oder Geschäftsmodell vieler Anbieter. Die Umsätze von Google und Facebook liegen in Milliardenhöhe und gründen zum überwiegenden Teil auf Werbung. Je genauer diese auf die potenziellen Kunden abgestimmt ist, das heißt, je mehr man über sie weiß, desto mehr lässt sich damit verdienen. Untersuchungen zeigen, dass sich mit verhaltensbasierter Werbung mehr als doppelt so viel einnehmen lässt wie mit pauschaler Werbung.

Weitere Informationen:

LINKLISTE „FACEBOOK-MARKTWERT"

Empfehlungen von Freunden und Familie genießen ein sehr großes Vertrauen; sie führen dazu, dass Nutzer ihnen in vielen Fällen folgen. Vor diesem Hintergrund ist es nicht verwunderlich, dass Interessen, Neigungen und Konsumgewohnheiten der Nutzer, ihr soziales Umfeld und deren Aktivitäten im Netz auf das Interesse der Werbewirtschaft stoßen. Laut Branchenangaben entfallen in Deutschland fast neun Prozent der Werbeumsätze auf das Internet; besonders wichtig sind dabei soziale Netzwerke und standortbezogene Dienste.

Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist aber nur dann zulässig, wenn sie durch das Datenschutzrecht oder durch eine andere Rechtsvorschrift erlaubt ist oder eine Einwilligung des Betroffenen vorliegt. Die Einwilligung ist nur wirksam, wenn sie auf einer freien Entscheidung des Nutzers beruht und dieser vorab über den Zweck der Erhebung, Verarbeitung und Nutzung der Daten informiert wurde.

Auch im Hintergrund laufen bei der Internetnutzung Prozesse ab, die datenschutzrechtlich relevant sind. Dazu gehören Updates, bei denen sich beispielsweise Browser und Antivirenprogramm automatisch mit dem Server des Herstellers verbinden und Informationen an diesen übermitteln. Zudem hat jeder Rechner, der sich im Internet befindet, eine IP-Adresse, die eindeutig zugeordnet werden kann. Diese Adresse dient dazu, die Datenpakete, die im Internet verschickt werden, an den richtigen Ort zu senden. Wie eine Telefonnummer besteht sie aus Zahlen und macht jeden Internetnutzer eindeutig identifizierbar.

Falls ein Rechner genutzt wird, auf den weitere Nutzer Zugriff haben, sei es innerhalb der Familie oder durch Fremde in einem Internetcafé, kann auch der Browserverlauf oder die Chronik relevant sein. Das ist eine Liste mit denjenigen Internetseiten, die zuletzt besucht wurden. Man sollte sich der Tatsache bewusst sein, dass weitere Nutzer potenziell Zugriff auf diese Daten haben.

Google

Der Google-Konzern stand wiederholt wegen mangelnden Datenschutzes in der Diskussion. Seine Online-Dienste werden zunehmend ausgeweitet und umfassen neben der marktdominierenden Suchmaschine Google, dem eigenen E-Mail-Programm (Google Mail), einer Videoplattform (Youtube) und sozialen Netzwerken (Google+, Orkut,

Picasa) auch ein mobiles Betriebssystem (Android), Kartendienste, Blogs und viele andere. Bei Google Mail werden zudem sämtliche E-Mails der Nutzer inhaltlich ausgewertet, und auf dieser Grundlage wird individuell abgestimmte Werbung geschaltet. Damit besitzt Google eine Unmenge an Daten, und je mehr Dienste eine Person von Google nutzt, desto genauer kann ein Profil dieser Person erstellt werden.

Darüber hinaus ist Google mit über 95 Prozent Marktanteil allein in Deutschland die bedeutsamste Suchmaschine im Internet und speichert zu jeder Suche neben den Suchbegriffen und dem Zeitpunkt der Suche eine Reihe von Angaben über den Nutzer.

Facebook

Beim Stichwort soziale Netzwerke denken heute alle zunächst an Facebook. Innerhalb einer relativ kurzen Zeit hat sich dieses Netzwerk auch in Deutschland an die Spitze gesetzt. Bei vielen Beobachtern führt dies zu Bedenken: einerseits im Hinblick auf ein zu leichtsinniges und zu offenherziges Kommunikationsverhalten der Nutzer, andererseits aufgrund der maßlosen und intransparenten Speicher- und Verwertungspraxis des Netzwerks. Die Bereitstellung einer Kommunikations- und Distributionsplattform für interessierte Menschen ist deshalb nur die eine Seite von Facebook, seine gigantischen Datenspeicher sind die andere. Der Datenschutz dieses Datengiganten ist aber unzureichend. Die amerikanische Aufsichtsbehörde (Federal Trade Commission – FTC) hat festgestellt, dass Facebook seine Nutzer wiederholt getäuscht und sich nicht an seine eigenen Vorgaben für den Schutz der Privatsphäre seiner Nutzer gehalten hat. Die Prüfungen mehrerer Datenschutzbeauftragten haben diese und weitere Bedenken bestätigt und insbesondere die mangelnde Transparenz bei der Erhebung und Verarbeitung von Nutzerdaten bemängelt. Der Verbraucherzentrale Bundesverband (vzbv) hat Facebook mehrfach wegen Verstößen gegen das Datenschutzrecht in seinen Nutzungsbedingungen abgemahnt. In mehreren Gerichtsverfahren, unter anderem vor dem Europäischen Gerichtshof, wird derzeit die Datenschutzpraxis von Facebook überprüft.

Gegenwärtig bleibt den Nutzern nur die Möglichkeit, ihre Privatsphäre durch restriktive Einstellungen für die Veröffentlichung ihrer personenbezogenen Daten und den Zugriff durch Dritte zu schützen.

Modul 5:
„PRÄSENTATION IM INTERNET“

Weitere Informationen:

LINKLISTE „PRIVATSPHÄRE BEI FACEBOOK“

Interessen des Staates

Nach den Anschlägen vom 11. September 2001 in den USA wurde das Thema Terrorismus weltweit aktuell. Um solchen Anschlägen in Zukunft vorzubeugen, wurden Maßnahmen eingeleitet, die unmittelbar den Datenschutz und die Privatsphäre der einzelnen Bürger betreffen. Im Jahr 2008 wurde hierzu ein Gesetz zur Vorratsdatenspeicherung verabschiedet, das Telekommunikationsanbieter verpflichtete, Verbindungsdaten sechs Monate lang zu speichern. Auch ohne dass ein Verdacht auf eine Straftat vorliegt, sollte danach erfasst werden, wann welcher Telekommunikationsdienst (Telefon, Internet etc.) wie lange genutzt wurde, welche Nummern, E-Mail-Adressen die beteiligten Stellen haben, welche Internetseiten aufgerufen und welche Datenmenge übertragen wurde.

§

Weitere Informationen:

Telekommunikationsgesetz (TKG), Teil 7, Abschnitt 2, § 96

Nachdem dieses Gesetz jedoch durch das Bundesverfassungsgericht für verfassungswidrig erklärt wurde, hat die Bundesregierung im Juni 2015 einen erneuten Gesetzentwurf vorgelegt. Nach diesem sollen Verkehrsdaten, wie zum Beispiel die Rufnummer der beteiligten Anschlüsse, Zeitpunkt und Dauer eines Gesprächs sowie zugewiesene Internetadressen, für die Dauer von zehn Wochen gespeichert werden; für Standortdaten bei Telefondiensten ist eine Frist von vier Wochen vorgesehen. Die Speicherpflicht erstreckt sich nicht auf die Inhalte der Kommunikation, auf Daten der elektronischen Post und aufgerufene Internetseiten. Bei schweren Straftaten dürfen die Strafverfolgungsbehörden die gespeicherten Verkehrsdaten dann unter bestimmten Voraussetzungen abrufen.

Manche Datenschützer befürchten, dass der Staat mit der Begründung der Terrorismusgefahr seine Befugnisse zu sehr ausweitet und damit die Grundrechte der Bürger auf Privatsphäre sowie Meinungs- und Pressefreiheit unangemessen einschränkt. So wurden gegen den Gesetzentwurf von der Konferenz der Datenschutzbeauftragten verfassungsrechtliche Bedenken erhoben, da dieser die Anforderungen, die vom Bundesverfassungsgericht und vom Europäischen Gerichtshof formuliert wurden, nicht ausreichend berücksichtige. Dies gelte insbesondere für den Schutz der Kommunikation von Berufsgeheimnisträgern wie Abgeordneten, Ärzten, Rechtsanwälten oder Journalisten.

Personensuchmaschinen

Personensuchmaschinen wie *yasni.de* machen es möglich, Daten und Informationen, die sich zu einer Person im Internet finden lassen, zu einem Personenprofil zu verknüpfen. Diese Suchmaschinen finden Bilder, Videos, Telefonbucheinträge, Blog- und Forenbeiträge von einer Person ebenso wie Domains, Branchenbucheinträge, E-Mail-Adressen, Dokumente und Nummern von Instant Messengern. Bei der Auswertung von Social-Community-Profilen lassen sich oft auch Familienbeziehungen rekonstruieren sowie Informationen über Lebenslauf, Freundeskreis und Freizeitgestaltung sammeln.

NACH DEM EIGENEN NAMEN SUCHEN

3. Wann und wo werden Daten preisgegeben?

Bei der Bearbeitung eines Profils in einem sozialen Netzwerk wie Facebook oder bei einem Online-Einkauf ist uns meist bewusst, dass wir persönliche Daten preisgeben. Die Daten werden aktiv abgefragt, und ohne beispielsweise unsere richtige Adresse anzugeben, würde bestellte Ware kaum bei uns ankommen. Es gibt aber zahlreiche weitere Gelegenheiten, bei denen Daten von uns gesammelt und verwertet werden, auch ohne dass wir Kenntnis davon erlangen. Anhand eines Tagesablaufes kann man sehen, wo wir überall Daten preisgeben.

Den Daten einen Tag lang auf der Spur

Montagmorgen, 08.30 Uhr

Nach einem ausgiebigen Frühstück haben Sie beschlossen, einige Sachen an Ihrem Rechner zu erledigen. Sie fahren den Rechner hoch und gehen online. Noch bevor Sie überhaupt eine Seite aufgerufen haben, öffnet sich ein Fenster, das Sie daran erinnert, dass Ihr Antivirenprogramm ein Update benötigt. Gleichzeitig verbindet sich das Betriebssystem Ihres Rechners mit dem Server der Herstellerfirma, um ebenfalls Updates vorzunehmen. Zunächst melden Sie sich dann in Ihrem E-Mail-Programm an und entdecken die Nachricht eines Freundes, der von seinem vergangenen Urlaub nach Bolivien berichtet.

EIN DATENTAG:
http://s.rlp.de/Z3m

Neben der eigentlichen E-Mail sehen Sie jetzt verschiedene Werbeangebote für Reisen nach Bolivien. Nachdem Sie die E-Mail gelesen haben, fällt Ihnen ein, dass Sie noch ein Geburtstagsgeschenk für Ihre Tochter benötigen. Sie sind auf der Suche nach einem Buch und gehen auf die Seite des großen Online-Versandhandels amazon.de. Da Sie diese Seite öfter besuchen und dort auch schon bestellt haben, werden Sie mit Ihrem Namen begrüßt. Bereits ein paar Tage zuvor haben Sie sich nach einem Geschenk für Ihre Tochter umgesehen, die sich sehr für Asien interessiert. Sie bekommen daher auf Ihrer individuellen Startseite Angebote rund um das Thema Asien angezeigt. Sie durchstöbern die Angebote und finden ein geeignetes Kochbuch, das Sie aber vorerst nur auf Ihrem Wunschzettel speichern, um sich noch mit dem Rest der Familie abzustimmen.

Da Sie und Ihre Familie sich vor Kurzem einen Hund angeschafft haben, gehen Sie auf die Internetseite Ihrer Heimatstadt und füllen dort das Online-Formular zur Anmeldung der Hundesteuer aus, das Sie dann elektronisch an die Stadt übermitteln. Sie haben sich für eine Quartalszahlung entschieden und überweisen unmittelbar nach Übertragung des Online-Formulars die erste Rate via Onlinebanking. Nachdem Sie sich auf der Seite Ihrer Bank eingeloggt haben, füllen Sie die Überweisung aus und übermitteln sie online mithilfe einer gültigen TAN. Im Anschluss daran lassen Sie Ihre Tätigkeiten im Netz zunächst ruhen und rufen Ihren Sohn via Festnetzanschluss auf der Arbeit an, um ihn nach seiner Meinung zu dem Kochbuch zu fragen.

Montagnachmittag, 17.00 Uhr

Ihre Tochter kommt überraschend zu Besuch und möchte Ihnen etwas Aufregendes im Internet zeigen. Sie hat von dem Dienst Google Street View gehört und beim Ausprobieren entdeckt, dass auch ihr Elternhaus im Internet zu finden ist. Sie sind zunächst begeistert, werden aber nachdenklich, als Ihnen Ihre Tochter von ihren Bedenken im Hinblick auf Datenschutz berichtet.

Als Ihre Enkelin ruft, lassen Sie Ihre Tochter alleine am Rechner zurück. Diese ist auf der Suche nach einer Internetseite, an deren Namen sie sich nicht genau erinnern kann. Allerdings hat sie sie schon einmal an diesem Rechner aufgerufen, deshalb öffnet sie die Chronik beziehungsweise den Browserverlauf, also die Liste mit bereits besuch-

ten Internetseiten. Dabei stolpert Ihre Tochter auch über die Seite, auf der Sie sich zuvor das asiatische Kochbuch angesehen haben. Neugierig, ob Sie inzwischen ebenfalls die asiatische Küche für sich entdeckt haben, öffnet sie die Seite und nimmt sich vor, Sie später darauf anzusprechen.

Montagabend, 22.00 Uhr
Vor dem Zubettgehen wollen Sie prüfen, ob sich in Ihrer Social Community etwas Neues getan hat. Auf der Profilseite Ihres Sohnes entdecken Sie, dass er seinen Beziehungsstatus von „Single" auf „Vergeben" geändert hat und der Gruppe „Grüne in den Stadtrat Koblenz" eingetreten ist. Sie selbst sind in der Gruppe „Adenauer-Gymnasium Bonn – Abitur 1954" und finden dort einen Schulkameraden, der dieser Gruppe neu beigetreten ist und den Sie lange gesucht haben. Nachdem Sie diesem Schulfreund eine Nachricht auf der Pinnwand hinterlassen haben, lesen Sie noch, dass Ihre Enkelin als ihr liebstes Hobby Tae Bo angegeben hat. Da Sie nicht wissen, worum es sich dabei handelt, geben Sie den Begriff bei einer Suchmaschine ein. Nach einigen Klicks wissen Sie, dass es sich um eine Sportart handelt, und gehen beruhigt ins Bett.

Der Spruch „das Internet vergisst nichts" beruht auf verschiedenen Eigenschaften des Internets. Prinzipiell kann jeder Mensch, der online ist, sehen, was andere im Netz veröffentlichen. Das bedeutet Schätzungen zufolge aktuell, dass über drei Milliarden Menschen weltweit potenziell in der Lage sind, diese Daten sehen zu können. Je nach den individuellen Datenschutzeinstellungen betrifft das den Wunschzettel bei *amazon.de*, Blog- und Foreneinträge, Kommentare, Bewertungen oder die Daten in sozialen Netzwerken. Einmal Veröffentlichtes im Nachhinein wieder zu löschen, wäre so, „als würde man eine Tomate durch einen Ventilator werfen und hinterher versuchen, alle Stücke wieder einzusammeln", um es mit den Worten des ehemaligen Bundesdatenschutzbeauftragten Peter Schaar auszudrücken. Sobald Daten, seien es Videos, Fotos oder Blogeinträge, online sind, hat jeder andere Onliner Zugriff darauf und kann sie beliebig kopieren, um sie dann beispielsweise auf einer anderen Plattform zur Verfügung zu stellen. Ein anderer Nutzer kopiert die Daten wiederum von dieser Plattform und so weiter. Auf diese Weise können Daten unglaublich schnell weltweit verbreitet werden.

Weitere Informationen:

LINKLISTE „DIE SCHÖNE NEUE WELT DER ÜBERWACHUNG"

4. Datenspuren im Internet

Jedes Mal, wenn eine Internetseite aufgerufen wird, erzeugt dies eine Datenspur. Ob man in Google, Bing oder Yahoo etwas sucht, sich ein Video ansieht oder einen Blog liest – meist wird dies protokolliert. Zwar ist daraus nicht direkt erkennbar, welche Person dahinter steht, das kann sich jedoch schnell ändern. Im Internet wird eine Reihe von Mechanismen genutzt, um das Surfverhalten der Nutzer zu erfassen. Das löst bei vielen Besorgnis, zumindest aber Unbehagen aus. Der Wunsch nach ➔ Anonymität ist nichts Unanständiges. Wir bleiben im Alltag schließlich oft anonym, zum Beispiel wenn wir an der Kinokasse bar bezahlen, eine Zeitschrift kaufen oder eine DVD. Warum also nicht auch im Internet? Um welche Datenspuren geht es dabei?

IP-Adresse

Die Internetprotokoll-Adresse, kurz IP-Adresse, wird bei jedem Klick mitgeschickt und verrät einiges über den Nutzer. Oft lässt sie sich ziemlich genau dem Wohnort zuordnen oder jedenfalls der Region, aus der man kommt. In Verbindung mit den Angaben, die der Browser mitschickt, ist erkennbar, woher der Nutzer kommt.

TIPP

Haben Sie sich schon einmal gefragt, warum Ihnen in der Regel deutsche Werbung präsentiert wird und keine Anzeigen auf Französisch oder Spanisch? Oder warum bei einer Suchanfrage häufig Unternehmen aus der Region zu finden sind? In der IP-Adresse liegt die Antwort! Auf der Seite utrace.de können Sie Ihre IP-Adresse lokalisieren lassen (➔ Geolokalisierung).

IP-Adressen werden benötigt, um die Datenpakete im Internet zuzustellen, und lassen grundsätzlich Rückschlüsse auf die Person zu. Dies deshalb, weil nicht nur der jeweilige Internet-Anbieter (➔ Provider) in der Lage ist, die IP-Adresse einem Nutzer zuzuordnen, sondern auch jeder Anbieter einer Website, auf der sich der Nutzer registriert, anmeldet oder Name und Adresse hinterlässt.

Cookies

Bestellt man hin und wieder bei einem großen Onlineshop, kann es vorkommen, dass man sofort beim Aufrufen der Seite mit seinem Namen begrüßt wird. Das funktioniert über sogenannte Cookies, kleine Dateien, die auf den PCs abgelegt werden, wenn die Browsereinstellungen dies zulassen. Cookies speichern Informationen im Zusammenhang mit der jeweiligen Internetseite. Dass Cookies auf dem eigenen Rechner vorhanden sind, merkt man beispielsweise daran, dass man beim Ausfüllen von Online-Bestellformularen Daten vorgeschlagen bekommt, die man früher einmal eingegeben hat. Cookies dienen also dazu, Benutzerprofile anzulegen und zu verfolgen, wie sich der Nutzer auf der Internetseite bewegt, wie lange er bleibt und was er sich näher anschaut. Häufig werden Cookies dabei nicht allein von der konkret aufgerufenen Website gesetzt, sondern über dort eingebundene Werbung auch von Werbevermarktern wie z. B. Doubleclick. Beim Besuch einer weiteren Seite, die Werbung des Vermarkters enthält, kann über diese „Drittanbieter-Cookies“ erkannt werden, auf welchen Seiten der Nutzer zuvor war. Wenn man die Cookies zusammennimmt, ergibt sich ein recht gutes Bild über die Interessen des Nutzers.

Weitere Informationen:
LINKLISTE „COOKIES“

Browserchronik

Ähnlich ist es mit der Chronik bzw. der Verlaufsanzeige des Browsers. Wer darauf geachtet hat, dem ist möglicherweise aufgefallen, dass auf Websites benutzte Links die Farbe wechseln können, und dass dies so geblieben ist, wenn die Website nach einiger Zeit erneut besucht wird. Die Information, was der Nutzer sich bei seinem letzten Besuch angesehen hat, wurde offenkundig gespeichert, konkret: in der Browserchronik. Diese Information kann aber von allen Seiten, die besucht werden, ausgewertet werden. Je länger eine Browser-Chronik zurückreicht, desto mehr verrät sie über die Nutzungsgewohnheiten der Surfer. Aus diesem Grund sollte sie hin und wieder gelöscht werden.

Modul 2: „DER BROWSER“

Datenspuren vermeiden

Vieles in Sachen Datenspuren hat man selbst in der Hand, insbesondere das, was man in sozialen Netzwerken und an anderen Stellen über sich preisgibt. Wie man dort sich und andere schützen kann, was

Weitere Informationen:

LINKLISTE „DATENSPUREN IN SOZIALEN NETZWERKEN“

Weitere Informationen:

LINKLISTE „DATENSPUREN VERMEIDEN“

es zu beachten gilt, und an wen man sich wenden kann, wenn man Unterstützung braucht, erfährt man auf den Seiten des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz.

Auch für Cookies und die Chronik des Browsers kann man selbst festlegen, ob man diese will oder nicht oder dass diese Daten von Zeit zu Zeit gelöscht werden. Die meisten Browser bieten einen Privatmodus an, der dafür sorgt, dass solche Datenspuren vermieden werden. Bei anderen Punkten ist die Sache nicht so einfach, weil manches technisch bedingt ist. Aber auch hier lassen sich Datenspuren zumindest reduzieren. So gibt es datenschutzfreundliche Suchmaschinen wie *ixquick.de* oder *startpage.com*, die die IP-Adressen der Nutzer anonymisieren oder gar nicht erst speichern.

5. Digitales Erbe – Zugriff für die Erben?

Immer mehr spielt sich unser Leben auch in der digitalen Welt ab, in sozialen Netzwerken, in E-Mails oder Cloud-Diensten. Dabei werden die digitalen Dienste nicht nur für die Kommunikation, sondern vermehrt auch für die Abwicklung von Einkäufen und sonstigen Geschäften genutzt. Jeder, der längere Zeit das Internet genutzt hat, verfügt über eine hohe Anzahl an Benutzerkonten bei ganz unterschiedlichen Anbietern. Da fällt es schwer, den Überblick zu behalten.

Im Falle des Todes eines Menschen wollen oder müssen sich die Erben mit den digital gespeicherten Daten und Konten des Angehörigen befassen. Diese geben nicht nur Auskunft über Kontakte, sondern zum Beispiel auch über offene Rechnungen oder laufende Verträge. Bei digitalen Geschäften fällt häufig gar kein Schriftverkehr in Papierform mehr an. Erben können deswegen meist nur durch den Zugang zu den digitalen Diensten eines Verstorbenen davon erfahren. Klare gesetzliche Regelungen, nach denen Erben einen Zugriff auf alle vom Verstorbenen angelegten Benutzerkonten erhalten, gibt es derzeit nicht. Mitunter müssen sie selbst mit jedem Anbieter in Kontakt treten und den Erbfall und ihre Berechtigung mühsam nachweisen. Ratsam ist deswegen, sich bereits zu Lebzeiten um den „digitalen Nachlass“ zu kümmern.

Die folgenden Hinweise können den Erben den Zugriff auf das digitale Erbe erleichtern:

- *Fertigen Sie eine Übersicht aller Nutzerkonten mit Benutzernamen und Kennwörtern an.*
- *Speichern Sie die Übersicht am besten auf einem verschlüsselten oder zumindest kennwortgeschützten USB-Stick, den Sie an einem sicheren Ort deponieren, beispielsweise in einem Tresor oder einem Bankschließfach.*
- *Bestimmen Sie eine Person Ihres Vertrauens zu Ihrem digitalen Nachlassverwalter. Stellen Sie für diese Person eine Vollmacht aus, in der Sie festlegen, dass diese Person sich vollumfänglich um Ihren digitalen Nachlass kümmern soll.*
- *Regeln Sie in dieser Vollmacht genau, wie mit Ihrem digitalen Nachlass umgegangen werden soll. Welche Daten sollen gelöscht werden, was soll beispielsweise mit Fotos passieren, wie ist mit Ihrem → Benutzerkonto in einem sozialen Netzwerk umzugehen?*
- *Legen Sie ebenfalls fest, was mit Ihren Endgeräten (Computer, → Smartphone, → Tablet) und den dort gespeicherten Daten passieren soll.*
- *Vergessen Sie nicht, die Vollmacht mit einem Datum zu versehen und zu unterschreiben.*
- *Übergeben Sie Ihrer Vertrauensperson die Vollmacht und informieren Sie Ihre Angehörigen darüber, dass Sie Ihren digitalen Nachlass auf diese Weise geregelt haben.*
- *Teilen Sie Ihrer Vertrauensperson ebenfalls mit, wo sie die Zugangsdaten zu Ihren Kontos findet, also wo Sie zum Beispiel den USB-Stick deponiert haben.*
- *Denken Sie daran, die Auflistung Ihrer → Accounts immer aktuell zu halten. Ergänzen Sie die Auflistung um neue Konten, löschen Sie die Daten in der Liste, wenn Sie sich bei einem Konto abgemeldet haben.*
- *Es gibt auch Firmen, die eine kommerzielle Nachlassverwaltung anbieten. Die Sicherheit solcher Unternehmen lässt sich allerdings nur schwer beurteilen.*

6. Datenmissbrauch

Der sorgfältige Umgang mit den eigenen Daten im Internet ist nicht nur deshalb von Bedeutung, weil anderen Personen ein tiefer Einblick in die eigene Privatsphäre ermöglicht wird, sondern auch weil persönliche Daten in den Fokus krimineller Internetnutzer gelangen können. Anhand von zwei Beispielen soll deutlich gemacht werden, wie Internetdaten für kriminelle Machenschaften missbraucht werden können.

Phishing

Weitere Informationen:
LINKLISTE „PHISHING“

Wie der Klang des Wortes schon andeutet, geht es bei Phishing im weitesten Sinne um das Thema Fischen, genauer gesagt um das Fischen nach Daten mit einem Köder. Als Köder schlüpft eine Person dabei in eine andere Identität, die einer Bank oder eines Onlineshops beispielsweise, mit dem Ziel, an sensible Daten der Nutzer dieser Seiten zu gelangen. Dazu gehören Passwörter, PINs und TANs sowie Kunden- und Kreditkartennummern. Phishing-Attacken können sowohl per E-Mail als auch beim Besuch einer Internetseite erfolgen. Die Betrüger fordern den Nutzer dazu auf, sich auf einer gefälschten Internetseite mit der persönlichen Kundennummer und dem Passwort anzumelden. Durch die Fälschung der Seite können sensible Daten abgegriffen, gesammelt und gespeichert werden. Das Gefährliche daran ist, dass häufig das Design der echten Internetseite oder E-Mails übernommen wird.

Modul 4:
„SICHERES ONLINEBANKING“

Banken machen ihre Onlinebanking-Kunden immer wieder darauf aufmerksam, dass sie niemals per E-Mail die Angabe von Kontonummer, Passwort oder TANs verlangen würden.

Identitätsmissbrauch

Unter Identitätsmissbrauch versteht man die missbräuchliche Verwendung personenbezogener Daten durch Dritte. Name und Geburtsdatum einer Person reichen meist aus, um sich einer anderen Identität zu bemächtigen. Diese Daten finden sich in sozialen Netzwerken in großer Menge, und die Verwendung von Pseudonymen oder die Angabe falscher Daten wird von den Anbietern solcher Seiten häufig untersagt. Ziel des Identitätsmissbrauchs ist meist eine finanzielle Bereicherung, indem im Namen des Betrogenen beispielsweise Geld abgehoben wird oder Einkäufe in Onlineshops getätigt werden. Auch

um Straftaten zu begehen, werden Identitäten anderer Personen missbraucht. Sicherheitslücken sind hier vor allem ungesicherte WLAN-Netzwerke, bei denen Dritte Daten abgreifen können, oder Hackerangriffe, bei denen massenweise Daten von sozialen Plattformen kopiert und gespeichert werden.

Modul 4:
„SICHERES WLAN“

7. Datensparsamkeit

Der radikale Weg, zu verhindern, dass im Internet Daten von uns erhoben werden, wäre die Internetabstinenz. Dies kann und soll aber nicht die Lösung sein. Stattdessen gilt es, sich des bestehenden Risikos bewusst zu sein und stets abzuwägen, in welchem Verhältnis Kosten und Nutzen bei einzelnen Internetanwendungen stehen.

Das Ausfüllen von Online-Formularen
Kauft man online ein, müssen wahre Angaben gemacht werden, damit die Bestellung ankommt. Dennoch können auch hier Daten gespart werden: Oft müssen nicht alle Felder, die in dem Formular angegeben sind, auch wirklich ausgefüllt werden. Notwendige Angaben sind meist mit einem kleinen Stern (*) gekennzeichnet. Dies gilt nicht nur beim Online-Einkauf, sondern auch für die Anmeldung bei einem E-Mail-Anbieter, in einem sozialen Netzwerk oder beim Ausfüllen eines Online-Formulars der Stadtverwaltung.

Lügen ausdrücklich erwünscht!
Bei manchen Angeboten macht es Sinn, ein Pseudonym zu nutzen. In Bezug auf E-Mails bietet es sich an, mehrere Adressen bei verschiedenen Anbietern anzulegen, um diese für unterschiedliche Zwecke zu nutzen. Wenn man sich der Seriosität eines Angebotes nicht sicher ist, kann man eine E-Mail-Adresse angeben, die keine Rückschlüsse auf die eigene Person zulässt (wolkenkratzer123@emailadresse.de).

Für die Registrierung bei sozialen Netzwerken oder E-Mail-Diensten werden in den Allgemeinen Geschäftsbedingungen oft „korrekte Angaben“ verlangt. Umso wichtiger ist, dass man sparsam mit den eigenen Daten umgeht und sich der Tragweite der Angaben bewusst ist. Äußerungen über politische und religiöse Einstellungen, das

Hochladen von Fotos anderer Personen ohne deren Einverständnis oder das Diffamieren anderer Mitglieder sind auf den Seiten von sozialen Netzwerken tabu.

Weitere Informationen:

LINKLISTE „PASSWORTPRÜFER“

Identitätsmanagement

Das Internet und seine Dienste können auch gezielt genutzt werden, um das Online-Profil nach den eigenen Wünschen zu gestalten. Dafür sollte man geschickt entscheiden, wo welche Daten preisgegeben werden. Wenn jemand sich als Experte in Sachen „Geschichte der Stadt Koblenz“ etablieren möchte, bietet es sich an, eine eigene Homepage zu dem Thema einzurichten oder sich mit Blogbeiträgen an bestehenden Internetseiten zu beteiligen. Ebenso kann man eigene Dokumente zum jeweiligen Thema online stellen oder sich in sozialen Netzwerken mit Gleichgesinnten vernetzen.

Weitere Informationen:

LINKLISTE „MUSTERBRIEF ZUR LÖSCHUNG“

Grundsätzliche Tipps zum Umgang mit Daten	
„Informierte Einwilligung“	Prinzipiell kann ein Internetanbieter Ihre Daten auf zulässiger Basis speichern, verwenden und weitergeben, wenn Sie zuvor ausreichend unterrichtet wurden und zugestimmt haben. Diesen Umstand nennt man „informierte Einwilligung“. Lesen Sie sich deshalb die Allgemeinen Geschäftsbedingungen und die Datenschutzerklärung sorgfältig durch, bevor Sie zustimmen!
Seien Sie misstrauisch!	Anonymität im Netz kann eine Chance sein, aber es gibt auch Internetnutzer, die die Möglichkeiten des anonymen Surfens ausnutzen. Seien Sie deswegen vorsichtig und schützen Sie sich vor Datenklau, indem Sie sichere Passwörter nutzen, hohe Sicherheitseinstellungen vornehmen und sich vor allem auf seriösen Seiten bewegen.
Kennen Sie Ihre Rechte!	Jeder Betroffene hat das Recht auf Auskunft, Benachrichtigung, Löschung und Einwilligung, wenn es um die Verwendung seiner persönlichen Daten geht. Außerdem dürfen die Daten grundsätzlich nur für genau den Zweck verwendet werden, für den sie erhoben wurden. Der Nutzer kann einer Verarbeitung oder Nutzung seiner Daten zu Werbezwecken oder im Rahmen der Markt- und Meinungsforschung widersprechen.

8. Das Recht am eigenen Bild

Gerade auf sozialen Plattformen spielt das Einstellen von Fotos eine große Rolle. Stellt man Fotos auf die eigene Homepage oder macht Fotoalben im Netz für einen bestimmten Personenkreis zugänglich, sollte man das sogenannte „Recht am eigenen Bild“ kennen und beachten.

Grundsätzlich gilt, dass Abbildungen, also auch Fotos, nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden dürfen. Abbildungen beziehungsweise Bildnisse im Sinne des Gesetzes sind übrigens nicht nur Fotografien, sondern jede erkennbare Wiedergabe des äußeren Erscheinungsbildes einer Person, also auch in Zeichnungen oder Karikaturen.

Hat man keine Einwilligung des Abgebildeten, so reicht es nicht immer, die Person durch die in Presseveröffentlichungen üblichen Augenbalken unkenntlich zu machen, denn manchmal ist die Person bereits durch den Kontext eindeutig identifizierbar. Die Erkennbarkeit einer Person entfällt auch dann nicht, wenn sie sich altersbedingt verändert hat. Eines Beweises, dass die Person tatsächlich erkannt wird, bedarf es nicht.

Fotografieren erlaubt?

In aller Regel darf man als Privatperson in normalen Situationen immer Fotos machen. Es gibt jedoch ein paar Ausnahmen, die auch durch das Strafgesetzbuch geregelt werden. Das Fotografieren ist nicht erlaubt:

- bei Eingriffen in die Intimsphäre,
- wenn durch die Fotografie die Menschenwürde des Abgelichteten verletzt würde und
- wenn jede denkbare Veröffentlichung oder Verbreitung von vornherein ohne Einwilligung der fotografierten Person unzulässig wäre, wie intime Fotos, Aktfotos etc.

§

Weitere Informationen:

§ 201a Strafgesetzbuch (StGB)

Einwilligung

Wer Fotos veröffentlichen möchte, auf denen Personen zu sehen sind, braucht grundsätzlich deren Einwilligung. Werden Minderjährige abgebildet, so müssen die Erziehungsberechtigten zustimmen. Bei Jugendlichen ist sowohl die Zustimmung der Erziehungsberechtigten als auch die des Minderjährigen erforderlich.

Keine Einwilligung benötigt man nach dem Kunsturhebergesetz, wenn einer der folgenden Punkte zutrifft:

- Es werden Personen der Zeitgeschichte abgelichtet, wie bedeutende Politiker, Sportler, Schauspieler oder Angehörige regierender Königshäuser, oder Menschen, die nur für einen bestimmten Zeitraum im öffentlichen Interesse stehen, beispielsweise Teilnehmer von großen Castingshows. Aber auch hier ist zu beachten, für welchen Zweck die Aufnahme verwendet wird und ob eventuell die Intim- oder Privatsphäre der abgebildeten Person verletzt wird.
- Die abgebildeten Personen sind lediglich „Beiwerk" beispielsweise einer Landschaft oder eines Bauwerkes (Touristen vor dem Mainzer Dom).
- Es werden Versammlungen, Umzüge oder ähnliche Menschenansammlungen (z. B. Demonstrationen) abgelichtet, die in der Öffentlichkeit stattfinden und auf denen Personen erkennbar sind.

Was kann man tun?

Was mit einmal gemachten Fotos passiert, kann der Abgebildete beeinflussen, denn ohne dessen Einwilligung ist es grundsätzlich nicht zulässig, Fotos zu verbreiten. Dies gilt auch für das private Umfeld. Die öffentliche Zurschaustellung, somit auch die Veröffentlichung im Internet, ist ohne Einverständnis also nicht zulässig.

Wird das Recht am eigenen Bild verletzt, kann vom Abgelichteten Strafanzeige erstattet werden. Außerdem hat er Anspruch auf Unterlassung, um die Erstveröffentlichung des Bildes oder eine wiederholte Veröffentlichung zu verhindern, ein Anspruch auf Schadensersatz kann unter Umständen in Betracht kommen.

Wurden die Fotografien unbefugt erstellt, darf man die Herausgabe oder Vernichtung der Negative und aller Abzüge verlangen. Außerdem hat man Anspruch darauf, zu erfahren, inwieweit und wohin die Bilder weitergegeben wurden. Allerdings ist die Verbreitung von Bildern im Internet nur schwer nachzuvollziehen. ||