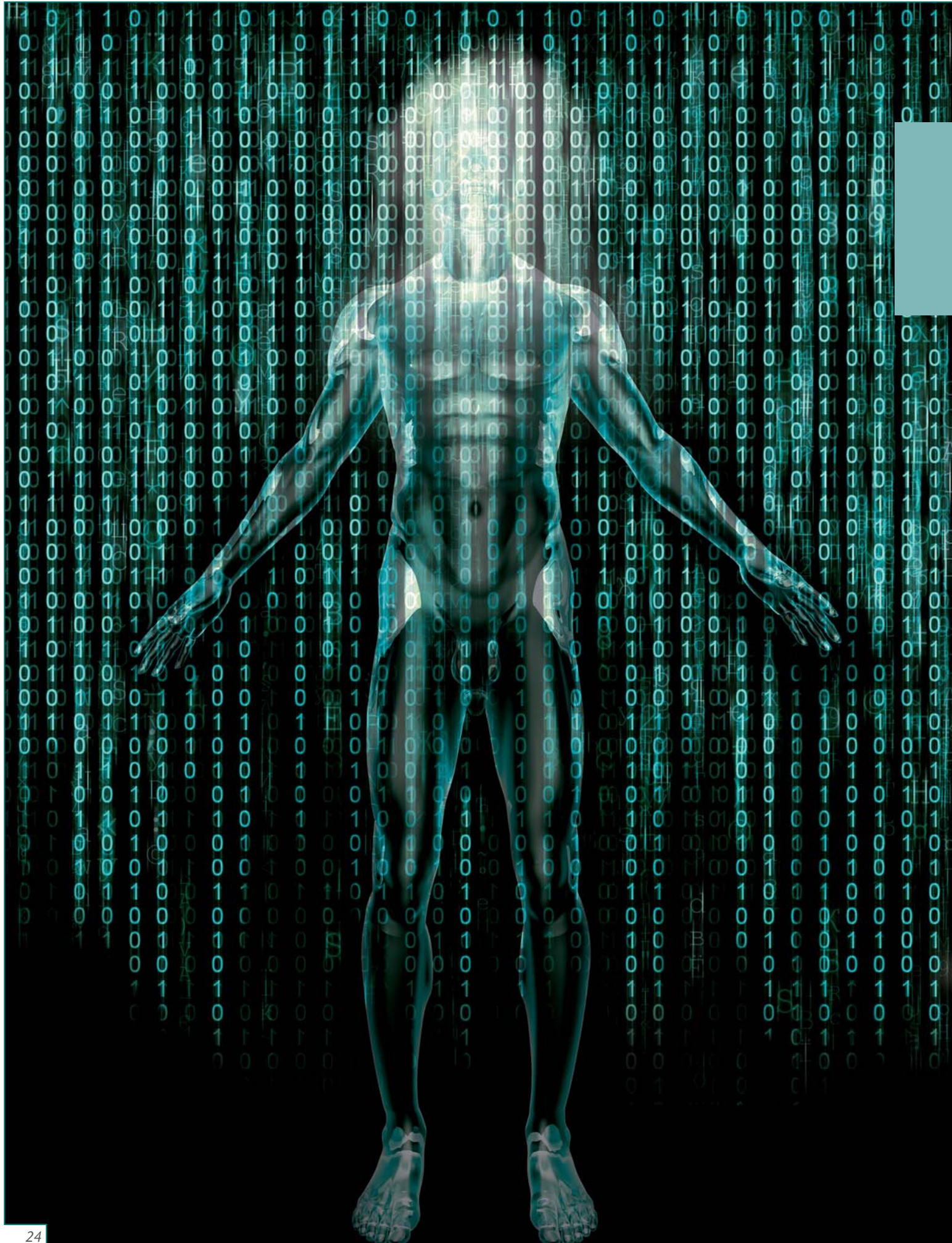




Themen Nr. 18

Der gläserne Mensch – Umgang mit personenbezogenen Daten

Heike Westerwinter



Der gläserne Mensch – Umgang mit personenbezogenen Daten

Heike Westerwinter

Heike Westerwinter ist Diplom-Betriebswirtin und seit 2001 Mitarbeiterin der Gen Re. Zunächst war sie in der Abteilung Integrated Solutions und Consulting für das Haftpflichtunderwriting verantwortlich. Von 2002 bis 2006 leitete Sie in unserem Stützpunkt in Wien den Bereich Casualty Facultative. Seit 2007 ist sie als

Senior Underwriting Specialist in unserer Abteilung Casualty Facultative marktverantwortlich für das fakultative Geschäft der HUK-Sparten in Deutschland und Österreich.

heike.westerwinter@genre.com
Tel. +49 221 9738 833



Datenklau bei der Deutschen Telekom, Ausspionieren der Mitarbeiter bei Lidl, der Regierung zum Kauf angebotene CDs mit Steuersündern, Sicherheitslücken bei sozialen Netzwerken wie Facebook oder SchülerVZ, Vorratsdatenspeicherung, ELENA, Google usw. – all dies sind vertraute Schlagzeilen aus den Medien.

Aber was bedeuten diese Schlagzeilen für Unternehmen oder jeden Einzelnen von uns? Zwingen sie uns zum Umdenken beim Umgang mit unseren persönlichen Daten? Hat der Einzelne überhaupt Einfluss darauf, was mit seinen Daten passiert? Wie kann man sich schützen? Bereits die folgenden Beispiele machen deutlich, dass jedes Unternehmen und jeder Einzelne dem Risiko des Verlusts bzw. der unberechtigten Nutzung seiner personenbezogenen Daten in irgendeiner Form mehr oder weniger regelmäßig bewusst oder unbewusst ausgesetzt ist.

Die unberechtigte Nutzung von personenbezogenen Daten lässt sich grob in drei Gruppen gliedern:

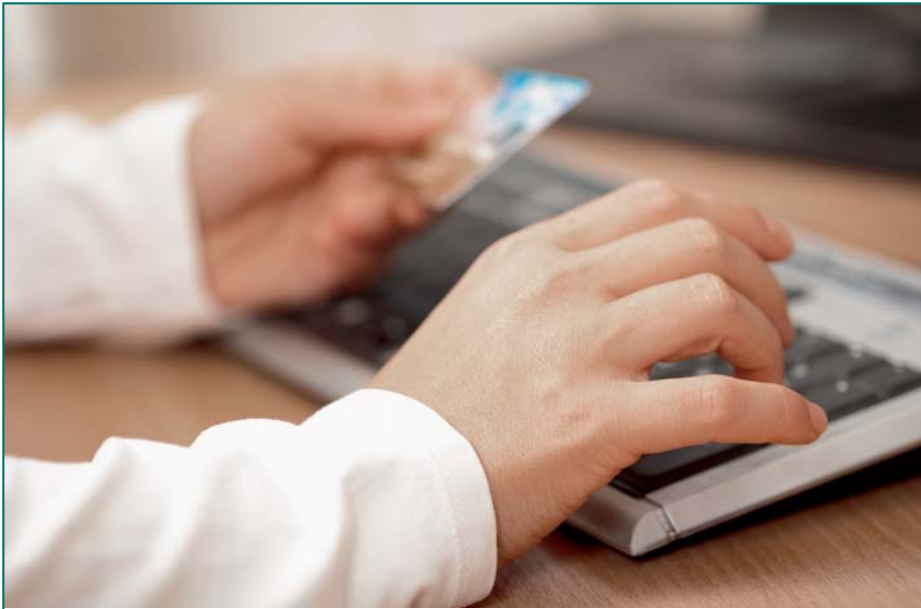
Kriminelle Aneignung personenbezogener Daten durch Dritte

Im August 2008 meldet Spiegel online, dass sich ein Callcenter illegal Kundendaten der Telekom verschafft hat;¹ im Oktober 2008 berichtet Die Zeit über einen weiteren Fall, bei dem die Daten von 17 Mio. Telekom-Kunden entwendet wurden.² Diese Beispiele zeigen, wie schnell jeder Einzelne ohne eigenes Zutun Opfer von Datenmissbrauch werden kann – ein Telefonanschluss reicht.

Gleiches gilt für den Fall, als im Zusammenhang mit Kreditkarten Sicherheitslücken bei einem spanischen Zahlungsdienstleister auftraten und deutschlandweit ca. 300.000 Karten ausgetauscht werden mussten.³

Ein Aufenthalt in Spanien war nicht erforderlich. Ausreichend war die über den Dienstleister abgewickelte Transaktion, unabhängig davon, in welchem Land sie getätigt wurde.

Anders war die Sachlage, als Angestellte eines Discounters mit Kameras überwacht und ihre Telefongespräche belauscht wurden.⁴ Die dabei gewonnenen Erkenntnisse, u. a. über familiäre Probleme, Alkoholsucht, psychische Probleme, wurden genutzt, um unliebsame Mitarbeiter loszuwerden. Unternehmen verstoßen damit eklatant gegen Gesetze. Das heimliche Ausspähen von Beschäftigten ist nur bei begründetem Verdacht einer Straftat, z. B. Diebstahl, zulässig, und auch nur dann, wenn es kein anderes Mittel gibt, den Sachverhalt aufzuklären. Im vorliegenden Fall musste der Discounter ein Bußgeld in Höhe von EUR 1,462 Mio. zahlen.⁵ Obwohl diese Vorgehensweise bisher nur bei einigen



Unternehmen öffentlich geworden ist, bleibt dem einzelnen Arbeitnehmer letztlich nur das Vertrauen in seinen Arbeitgeber, dass dieser nicht zu solch illegalen Mitteln der Mitarbeiterausforschung greift. Die Gewissheit kommt ggf. erst mit der Abmahnung oder Kündigung.

Im „Datenklau“-Fall der Liechtenstein Global Trust (nachfolgend LGT), der den Fall Zumwinkel ausgelöst hat, hatte ein Bankmitarbeiter im Jahr 2002 illegal Daten von Kontoinhabern kopiert und nach seinem Ausscheiden aus der Bank 2006 dem BND zum Kauf angeboten. 2007 verkaufte er diese Daten dann für mehr als EUR 4 Mio. an die deutschen Steuerbehörden.⁶ Hier ist den Betroffenen eine aktive Mitwirkung am entstandenen „Schaden“ durch den Transfer von Geldern an der deutschen Steuer vorbei ins Ausland nicht abzuspüren. Ein gesetzeskonformes Verhalten hätte vor dem Schaden geschützt.

Dieser Fall ist jedoch nicht nur im Hinblick auf den Missbrauch personenbezogener Daten und dessen Folgen interessant. Es stellen sich eine Vielzahl von Fragen, u. a. nach der Rechtmäßigkeit der Weitergabe geheimer Kontodaten durch den Bankmitarbeiter, des entgeltlichen Erwerbs von Bankgeheimnissen durch Steuerbehörden, dem Tätigwerden des BND für die Steuerbehörden sowie der Verwertbarkeit der so erlangten Informationen.

Eine detaillierte Behandlung dieser Fragen würde an dieser Stelle zu weit führen, aber so viel sei gesagt: Die Kopie und Weitergabe der Daten an Dritte erfüllen den Tatbestand der strafbaren Verwertung von Geschäftsgeheimnissen i. S. v. § 17 Abs. 2 Gesetz gegen unlauteren Wettbewerb (UWG). Dieser Verstoß wird nicht durch das Recht zur Strafanzeige legitimiert, insbesondere, wenn hierfür ein hoher Geldbetrag als Gegenleistung gefordert und auch gezahlt wird.

Interessant ist in diesem Zusammenhang auch die von einem Liechtensteiner Gericht stattgegebene Schadenersatzklage eines in Deutschland wegen Steuerhinterziehung verurteilten Bürgers wegen nicht erfolgter Information der vom Datendiebstahl betroffenen Kunden durch die LGT. Dem Kläger sei dadurch das Recht zur Selbstanzeige genommen worden. Die LGT wurde zu einem Schadenersatz von EUR 7,3 Mio. verurteilt. Das Urteil ist jedoch noch nicht rechtskräftig.⁷

Datenverlust oder missbräuchliche Nutzung bei offizieller Weiterleitung bzw. Speicherung personenbezogener Daten

Ein weiterer großer Bereich, in dem Daten missbräuchlich genutzt werden können, ist die offizielle Weiterleitung bzw. Speicherung von personenbezogenen Daten wie beim neuen ELENA- oder im SWIFT-Verfahren.

Elektronisches Entgelt-Nachweisverfahren (ELENA)

ELENA soll ab 2012 das Ausstellen von Papierbescheinigungen der Entgelt-daten durch den Arbeitgeber durch ein elektronisches Verfahren ersetzen. Damit sollen ein wichtiger Beitrag zum Abbau bestehender Bürokratie geleistet und bisherige Verfahrensabläufe beschleunigt werden. Das Projekt ELENA könnte jedoch bald vor dem Aus stehen. Pressemeldungen zufolge will Wirtschaftsminister Brüderle die zentrale Speicherung von Arbeitnehmerdaten wegen der hohen Kosten zumindest zeitweise einstellen. Zuvor hatte auch schon Justizministerin Leutheusser-Schnarrenberger datenschutzrechtliche Bedenken geäußert.⁸ Bürgerrechtler legten sogar in Karlsruhe Verfassungsbeschwerde ein.⁹ Was aber macht ELENA aus Sicht von Datenschützern so bedenklich?

Seit dem 1. Januar 2010 übermitteln Arbeitgeber einen gesetzlich festgelegten Datensatz mit den erforderlichen Gehaltsdetails an die Datenstelle der Deutschen Rentenversicherung Bund. Neben den klassischen „Entgelt-daten“ sind jedoch auch Angaben zu Art und Umfang des Beschäftigungsverhältnisses sowie den Kündigungs-/ Entlassungsgründen zu ergänzen. Die für die Leistungsgewährung benötigten Daten werden bei einer zentralen Stelle geprüft, verschlüsselt und gespeichert. Um die Sicherheit des Verfahrens zu gewährleisten, sind personenbezogene Daten nicht unter einem individuellen Zuordnungsmerkmal wie Name, Steuer- oder Versicherungsnummer gespeichert, sondern unter einer anonymisierten Zertifikats-identitätsnummer. Nur dann, wenn sich der Antragsteller mit seiner qualifizierten elektronischen Signatur mittels einer Signaturkarte (z. B. digitaler Personalausweis, Bank- oder Gesundheitskarte) für das ELENA-Verfahren anmeldet und die Daten freigibt, kann die jeweilige Behörde, z. B. die Bundesagentur für Arbeit, die Entgelt-nachweise abrufen. Der zuständige Sachbearbeiter der Leistungsbehörde muss sich ebenfalls durch ein registriertes Zertifikat ausweisen.

Kritisiert wird, dass in Verbindung mit der o. g. Zertifikatsidentitätsnummer eine umfangreiche Datenbank geschaffen wird, die den Menschen „gläsern“ werden lässt. Außerdem werde der Einzelne durch ELENA seines Rechts auf informationelle Selbstbestimmung¹⁰ beraubt, da er nicht mehr selbst bestimmen kann, ob und welche seiner Daten an staatliche Stellen weitergegeben und dort verwahrt werden.

Im Juli 2009 entschieden die EU-Außenminister, Terrorfahndern den Zugriff auf europäische Kontodaten zu ermöglichen. Die EU-Kommission wurde mit der Aushandlung des sog. SWIFT-Abkommens beauftragt – eine Vereinbarung zwischen den USA und der Europäischen Union über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung für die Zwecke des US-Gesetzes über das Aufspüren der Finanzierung von

Da die kürzlich vom BVerfG gekippte Umsetzung der EG-Richtlinie 2006/24 zur Vorratsdatenspeicherung den zuvor erläuterten Verfahren wieder eine andere Qualität gibt, hier ein kurzer Exkurs:

Vorratsdatenspeicherung

Die Vorratsdatenspeicherung basiert auf der EG-Richtlinie 2006/24,¹⁴ die eine sechsmonatige, vorsorgliche anlasslose Speicherung von Telekommunikationsdaten durch private Diensteanbieter vorsieht. In Deutschland ist sie in § 113 a und b Telekommunikationsgesetz (TKG) verankert. Die Vorschriften wurden durch das Gesetz zur Neuordnung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen eingefügt oder geändert und sind seit dem 1. Januar 2008 in Kraft.

§ 113 a TKG verpflichtet öffentliche Anbieter von Telekommunikations- und Internetzugangsdiensten, Rufnummern der beteiligten Anschlüsse, Zeitpunkt, Dauer, Absender und Empfänger von SMS, MMS sowie E-Mails, Internetprotokoll-Adresse des Internetnutzers und Dauer der Internetnutzung für einen Zeitraum von sechs Monaten zu speichern. § 113 b TKG regelt die Zwecke, zu denen die nach § 113 a TKG gespeicherten Daten verwendet werden dürfen: zur Verfolgung von Straftaten oder Abwehr von erheblichen Gefahren für die öffentliche Sicherheit.

2007 reichte u. a. der Arbeitskreis Vorratsdatenspeicherung Beschwerde beim BVerfG gegen die Umsetzung der o. g. Richtlinie ein.¹⁵ Gegenstand der Beschwerde waren

Nach den Terroranschlägen am 11. September 2001 rückte SWIFT in den Fokus des allgemeinen Interesses.

Es bleibt abzuwarten, ob und ggf. mit welchen Änderungen ELENA umgesetzt wird.

*Society for Worldwide Interbank
Financial Telecommunication – SWIFT*

Nach den Terroranschlägen am 11. September 2001 rückte SWIFT in den Fokus des allgemeinen Interesses, da vertrauliche Daten über Finanztransaktionen an US-Behörden übermittelt wurden. Nach Bekanntwerden dieser Tatsache wurde von Datenschützern diverser europäischer Länder – u. a. Deutschland, Belgien, Schweiz – eine Überprüfung eingeleitet, ob damit das Bankgeheimnis und der Datenschutz verletzt wurden. Als problematisch wird auch angesehen, dass z. B. das BVerfG deutschen Sicherheitsbehörden klare Grenzen bei der sog. verdachtsunabhängigen Jedermannkontrolle setzt, diese aber auf Umwegen über einen belgischen Dienstleister (SWIFT) den US-Behörden ohne jegliche Einschränkung ermöglicht wird. Die belgische Datenschutzkommission beschäftigte sich zwei Jahre mit dem Fall und kam zu dem Schluss, dass sich der Verdacht, SWIFT habe gegen europäisches Recht verstoßen, nicht bestätigt hat.¹¹

Terrorakten auch nach Verlagerung des zentralen Swift-Rechenzentrums aus den USA in die Schweiz. Nachdem im Februar 2010 die Verlängerung des im November 2009 beschlossenen Übergangsabkommens wegen datenschutzrechtlicher Bedenken vom Europäischen Parlament abgelehnt wurde,¹² stimmte es am 8. Juli 2010 dem Swift-Abkommen zu. Es trat am 1. August in Kraft und gilt fünf Jahre. Somit haben US-Fahnder für diesen Zeitraum potenziell Zugriff auf die Bankdaten jedes EU-Bürgers – auch derer, die nicht zu den der Unterstützung von Terrorgruppen Verdächtigen gehören, sondern z. B. lediglich aufgrund einer regionalen Zugehörigkeit ins definierte Datencluster passen.¹³



hauptsächlich die Vorschriften in § 113 a und b TKG, da sich durch sie ermitteln ließ, wer wann mit wem telefoniert und wann er welche Internetseite besucht hat. Wichtig ist in diesem Zusammenhang, dass lediglich die Daten, nicht aber die Inhalte der Gespräche oder Nachrichten gespeichert werden. Am 2. März 2010 entschied das BVerfG,¹⁶ dass § 113 a und b TKG in der Fassung von Art. 2 Nr. 6 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung sowie zur Umsetzung der Richtlinie 2006/24/EG gegen Art. 10 Abs. 1 Grundgesetz (GG) verstoßen und damit nichtig sind. Bereits auf Grundlage dieser Normen gespeicherte Daten sind unverzüglich zu löschen.

Das BVerfG führte jedoch aus, dass eine Vorratsdatenspeicherung nicht grundsätzlich mit Art. 10 Abs. 1 GG unvereinbar sei. Unter der Voraussetzung, dass sie legitimen Zwecken dient und die gesetzliche Ausgestaltung einer solchen umfassenden Datenspeicherung die besondere Bedeutung des mit der Speicherung verbundenden Grundrechtseingriffs im Hinblick auf Datensicherheit, Verwendungsbeschränkung, Transparenz und Rechtsschutz angemessen berücksichtigt, stelle sie keinen Verstoß gegen das GG dar. Als legitimen Zweck konkretisierte das Gericht den begründeten Verdacht einer schweren Straftat oder das Vorliegen tatsächlicher Anhaltspunkte für eine konkrete Gefahr für Leib, Leben oder Freiheit einer Person oder die Sicherheit des Landes. Damit wurde gleichzeitig bestätigt, dass eine verdachtsunabhängige Jedermannkontrolle, wie bereits beim SWIFT-Beispiel erläutert, nicht zulässig ist. Ob und wann ein neues Gesetz kommt, ist noch offen.¹⁷

Die Vorratsdatenspeicherung wäre, sofern sie durch ein entsprechendes Gesetz legitimiert wird, in jedem Fall ein weiterer großer Schritt hin zum gläsernen Menschen, da sich aus den Daten tiefe Einblicke in sein soziales Umfeld und seine individuellen Aktivitäten gewinnen lassen – auch wenn keine Inhalte gespeichert werden. Allein die Kenntnis von Adressat, Uhrzeit und Ort von Telefon-



gesprächen erlaubt bei einer Beobachtung über einen längeren Zeitraum in Kombination mit detaillierten Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen, die ggf. aus anderen Datenquellen erlangt werden, die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile. Ferner würde durch die Vorratsdatenspeicherung das Risiko erheblich steigen, weiteren Ermittlungen ausgesetzt zu werden, ohne selbst Anlass dazu gegeben zu haben. Es reicht aus, zu einem ungünstigen Zeitpunkt in einer bestimmten Funkzelle gewesen oder von einer bestimmten Person kontaktiert worden zu sein.¹⁸

Datenmissbrauch durch fahrlässigen oder unbedachten Umgang mit eigenen personenbezogenen Daten

Tiefe Einblicke in das soziale Umfeld eines Menschen und seine Aktivitäten lassen sich jedoch nicht nur mithilfe einer Vorratsdatenspeicherung gewinnen. Oftmals liefert man selbst das Material, z. B. in sozialen Netzwerken, durch Teilnahme an Rewardsprogrammen, Registrierungen auf diversen Webseiten, Einkäufe im Internet oder „googlen“. Im Gegensatz zu den vorherigen Beispielen kann hier jeder

Einzelne durch den verantwortungsbewussten Umgang mit seinen Daten das Risiko des Missbrauchs reduzieren.

Soziale Netzwerke

Die Teilnahme an sozialen Netzwerken wie Facebook erlangt eine immer größere Bedeutung. Sie haben sich in den letzten Jahren an die Spitze der Onlineangebote katapultiert, nur noch übertrumpft vom allgegenwärtigen Google. Es wird zunehmend schwieriger, sich diesem virtuellen Networking zu entziehen – ohne soziale Netzwerke geht im Internet kaum noch etwas, insbesondere bei den Unter-40-Jährigen. Aber sie schaffen eine Umgebung, in der viele persönliche Informationen öffentlich werden und durch Dritte missbräuchlich genutzt werden können.

Im März 2010 untersuchte die Stiftung Warentest einige der beliebtesten sozialen Netzwerke in Deutschland und stellte dabei deutliche Mängel fest. Kritisiert wurden im Wesentlichen die mangelhafte Sicherung der Nutzerdaten und fehlende Beachtung von Verwertungsrechten.¹⁹

So schränkt z. B. Facebook zwar die Rechte der Nutzer stark ein, genehmigt sich selbst aber weitreichende Rechte,



wird, um Arbeitnehmer zu überwachen.²² So verlor z. B. eine krankgeschriebene Versicherungsangestellte ihre Stelle, weil der Arbeitgeber ihre Aktivität auf Facebook verfolgen konnte, während ihr Betruhe verordnet war.²³

Eins steht auf jeden Fall fest: Ein soziales Netzwerk, das Informationsaustausch und Datenschutz in Einklang bringt, existiert (noch) nicht. Daher muss der Nutzer aktiv werden und die Angabe persönlicher Daten auf das unbedingt Erforderliche beschränken, sich das Einstellen von Fotos sehr genau überlegen und sein Profil nur vertrauten Personen zugänglich machen. Von Datenschützern wird sogar empfohlen, Netzwerke unter Pseudonym zu nutzen und nur Freunden zu verraten, wer sich dahinter verbirgt.



versendet. Daher gilt auch hier, dass lediglich ein sorgsamer Umgang mit der Payback-Karte vor dem „Gläsernwerden“ der eigenen Person schützt.

Google

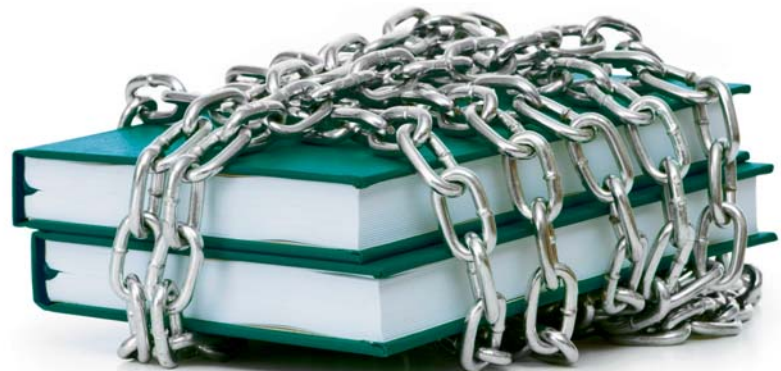
Ein weiteres Beispiel umfassender Datensammlung ist das derzeit allgegenwärtige Google. Kein Tag verging in den letzten Wochen und Monaten, an dem Google nicht zumindest in einem Nebensatz Erwähnung in den Medien fand. Das System Google wird stark von Datenschützern kritisiert. Aber was macht es aus deren Sicht so „bedrohlich“? Wesentlicher Kritikpunkt ist die umfassende Datensammlung: Google identifiziert den einzelnen Benutzer über sog. Cookies und hat somit die Möglichkeit, ohne dessen Wissen ein Benutzerprofil über sein Surfverhalten zu erstellen. Die dadurch gewonnenen Daten werden gespeichert. In seinen Datenschutzbestimmungen rechtfertigt Google die Verwendung dieser Cookies damit, dass sie helfen sollen, die Qualität der angebotenen Serviceleistungen zu

vor allem bei der Weitergabe der Daten an Dritte. Jeder, der Texte und Fotos bei Facebook einstellt, verzichtet durch die Akzeptanz der AGB auf das geistige Eigentum an seinem Werk, indem er Facebook eine nicht exklusive, übertragbare, unterlizensierbare, unentgeltliche, weltweite Lizenz zur kommerziellen Nutzung jeglicher IP-Inhalte (Bilder und Texte) erteilt, ohne zeitliche Begrenzung und sogar auch nach Löschung bzw. Deaktivierung des Nutzerkontos.²⁰ So stellt Facebook z. B. rd. 60 Unternehmen persönliche Daten der Nutzer, wie Alter, Hobbies, Wohnort, politische Überzeugung, Lieblingsbücher und -filme sowie Bildungsstand für personalisierte Werbezwecke zur Verfügung.²¹

Interessant ist auch, dass die CIA Facebook-Profile nutzt, um Personal anzuwerben, oder die iranische Polizei, um bei Verhören den Freundeskreis von Regimegegnern und Demonstranten namentlich zu identifizieren. Arbeitgeber nutzen soziale Netzwerke, um sich ein Bild von Bewerbern zu machen. Unbedacht ins Netz eingestellte Informationen oder Fotos können dazu führen, dass eine Bewerbung erfolglos verläuft. Darüber hinaus vermutet man auch, dass Facebook von Arbeitgebern genutzt

Kundenkarten

Ein gutes Beispiel für ein Datensammlungstool, über das man sich meist keine Gedanken macht, ist das Kundenbindungsprogramm Payback. Es ist bei Verbraucherschutzverbänden umstritten, denn es macht aus dem Benutzer einen gläsernen Kunden. Wird die Payback-Karte an der Kasse vorgelegt, werden Kundennummer, Datum, Filiale, Umsatz und von manchen Partnerunternehmen auch Warengruppencodes an Payback übermittelt. Der jeweils kartenausgebende Partner speichert zusätzlich die gekauften Produkte. Aus den gesammelten Daten lassen sich Rückschlüsse auf den Lebenswandel des Kunden ziehen und der Erfolg von Werbung messen, die Payback gezielt auf Basis der gespeicherten Profile der Nutzer



verbessern. Tatsächlich dienen sie jedoch wirtschaftlichen Interessen, z. B. nutzerspezifischer Werbung.

Die Datenschutzbestimmungen²⁴ von Google lesen sich eindrucksvoll. Jedoch darf man im Hinblick auf diverse Pressemeldungen über Datenpannen der jüngsten Vergangenheit, z. B. bei Google Street View²⁵ oder die Hackerattacke auf Google aus China,²⁶ berechnete Zweifel haben, ob Google den Nutzer nicht doch gläsern werden lässt – in jedem Fall scheint die Privatsphäre wenig geschützt und bietet Hackern ein interessantes Spielfeld.

Neben der Suchfunktion bietet Google diverse andere Dienste wie Google Maps, Google Mail, das soziale Netzwerk Google Buzz oder auch das derzeit häufig in der Presse erwähnte Google Street View an. Auch hier ist die Wahrung der Privatsphäre fraglich. So werden z. B. bei Gmail (Google

Mail) sämtliche E-Mails automatisch durchsucht, um kontextbezogene Werbung einblenden zu können, d. h. Google liest bei jeder E-Mail mit – im Zweifel keine angenehme Vorstellung.

Mögliche Folgen eines Missbrauchs

Telefonmarketing (trotz Verbot), unerwünschte Werbung, Identitätsdiebstahl, unzulässige Kontoabbuchungen, Stalking, Diffamierung, Mobbing, Nachteile bei Bewerbung und Karriere usw. – dies alles kann jedem, der seine persönlichen Daten (gewollt oder ungewollt) preisgibt, passieren. Denn das Internet bietet jedem mit krimineller Energie nahezu unbegrenzte Möglichkeiten, die Daten Dritter missbräuchlich zu nutzen.

Betrachtet man die zuvor genannten Szenarien, wird deutlich, dass die unrechtmäßige Nutzung personenbezogener Daten im Wesentlichen eine Verletzung

von Persönlichkeitsrechten zur Folge hat oder bei den Betroffenen zu Vermögensschäden unterschiedlicher Art führen kann. Darüber hinaus führt eine Datenspeicherung, wie sie z. B. beim ELENA-Verfahren erfolgt, zum Verlust des Rechts auf informationelle Selbstbestimmung,²⁷ d. h. der Einzelne verliert sein Recht, selbst zu bestimmen, welche ihn betreffende Daten an staatliche Stellen gelangen oder dort verwahrt werden dürfen.

Verletzung von Persönlichkeitsrechten

Die Verletzung von Persönlichkeitsrechten ist juristisch gesehen ein komplexes Thema, da in Deutschland das Persönlichkeitsrecht als solches nicht ausdrücklich gesetzlich geregelt ist. Zum einen leitet es sich als Gewohnheitsrecht aus Art. 1 Abs. 1 und Art. 2 Abs. 1 GG her. Zum anderen handelt es sich um ein „sonstiges“ Recht i. S. d. § 823 Abs. 1 BGB. Das allgemeine





Schutz durch das Gesetz

Ist ein Schaden eingetreten, wird jeder Betroffene zunächst sicherlich die Frage nach dem gesetzlichen Schutz stellen. Auf die einschlägigen Gesetze im detail einzugehen, würde den Rahmen dieses Beitrags sprengen. Daher sei hier nur in Kürze Folgendes gesagt:

Zentrales Gesetz ist das Bundesdatenschutzgesetz (BDSG). Es bietet dem Einzelnen Schutz vor Beeinträchtigungen seines Persönlichkeitsrechts durch den Umgang mit personenbezogenen Daten (§1 BDSG). Ferner regelt §4 BDSG die Zulässigkeit von Datenerhebung, -verarbeitung und -nutzung. Weitere wichtige Paragraphen sind die Erlaubnisnormen des §28, die in den §§19, 34 normierten Auskunftsrechte, die Rechte auf Benachrichtigung nach §§19a, 33, die Rechte auf Berichtigung, Löschung und Sperrung in §§20, 35 sowie das Widerspruchsrecht gem. §28 Abs. 4. Darüber hinaus regelt das BDSG in §7 den Schadenersatz, in §43 Bußgelder sowie Strafvorschriften in §44.

Neben dem BDSG gibt es noch eine Vielzahl von Spezialgesetzen, die diesem gem. §1 Abs. 3 Satz 1 BDSG vorgehen. Zu nennen sind insbesondere:

1. Grundgesetz (GG): Erwähnenswert sind in diesem Zusammenhang Art. 1, der die Unantastbarkeit der Würde des Menschen regelt, Art. 2, der das Recht auf freie Persönlichkeitsentfaltung sowie das Recht auf Leben und Unversehrtheit normiert, sowie Art. 10, der das Brief-, Post- und Fernmeldegeheimnis gesetzlich verankert.²⁹
2. Teledienstedatenschutzgesetz (TDDSG): §1 regelt den Schutz von Bestands-, Nutzungs- und Abrechnungsdaten, die im Zusammenhang mit dem Angebot und der Durchführung von Telediensten erhoben, verarbeitet oder genutzt werden, §3 die Grundsätze für den Umgang mit personenbezogenen Daten, §4 die Pflichten des Diensteanbieters, §6 welche Nutzungsdaten erhoben und gespeichert werden dürfen. §9 enthält Bußen bei Verstoß gegen die zuvor genannten Paragraphen.³⁰

Persönlichkeitsrecht soll dem Schutz der Persönlichkeit vor Eingriffen in die Bereiche Individual-, Privat- und Intimsphäre dienen. Die Folgen der unberechtigten Nutzung personenbezogener Daten sind fast immer ein Eingriff in die zuvor genannten Bereiche. Wie schon im Zusammenhang mit der Vorratsdatenspeicherung ausgeführt, ist die Intimsphäre eines Menschen dem staatlichen Zugriff verschlossen und Eingriffe im Bereich der Privatsphäre nur unter strikter Wahrung des Verhältnismäßigkeitsgrundsatzes möglich.

Aus zivilrechtlicher Sicht führt die Verletzung des Persönlichkeitsrechts u. a. zu einem Unterlassungsanspruch gem. §1004 BGB, einem medienrechtlichen Berichtigungsanspruch, beruhend auf analoger Anwendung von §§12, 862, 1004 i. V. m. §249 Satz1 BGB durch die Rechtsprechung, aber auch zu einem Anspruch auf Schadenersatz gem. §823 Abs. 1 BGB und Ersatz des immateriellen Schadens. Voraussetzung für den Ersatz eines immateriellen Schadens ist ein schwerwiegender Eingriff in das Persönlichkeitsrecht. Darüber hinaus ist es erforderlich, dass der Geschädigte durch vorrangige Ansprüche auf Unterlassung bzw. Widerruf keine ausreichende Genugtuung für die erlittenen Beeinträchtigungen erlangen kann.²⁸ Zum immateriellen Schaden hat der BGH in zahlreichen Entscheidungen betont, dass es sich nicht um Schmerzensgeld i. S. v. §847 BGB a. F. handelt, sondern

um einen besonderen Anspruch, der auf dem Schutzauftrag des Grundgesetzes und dem allgemeinen Persönlichkeitsrecht beruht. Es handelt sich um reines Richterrecht. Versuche, den Anspruch auf Ersatz von immateriellen Schäden bei Persönlichkeitsrechtsverletzungen gesetzlich zu regeln, sind bisher gescheitert.

Vermögensschäden

Aus der unberechtigten Nutzung personenbezogener Daten entstehen den betroffenen Unternehmen bzw. Personen in vielen Fällen auch Vermögenseinbußen. So kann der Missbrauch von Konto- und Kreditkartendaten zu unberechtigten Abbuchungen bei den einzelnen Kontoinhabern sowie zu Austauschkosten bei den kartenausgebenden Stellen führen. Auch der sog. Identitätsdiebstahl bietet ein hohes Potenzial für Vermögensschäden. Die Folge können Beratungs-, Gerichtskosten oder sonstige Aufwendungen zur Klärung der Sachlage sein, aber auch Kosten für Mahnungen, nicht bestellte Waren usw. Auf betroffene Unternehmen kommen zudem in der Regel noch erhöhte Aufwendungen für die Wiederherstellung des Imageschadens sowie die Verbesserung der Datensicherheit zu. Ebenso können dem Einzelnen bzw. den Unternehmen auch Steuernachzahlungen und Strafen, so z. B. im LGT-Fall geschehen, drohen.

3. Telekommunikationsgesetz (TKG): Es regelt den Schutz bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten der an der Telekommunikation Beteiligten. In diesem Zusammenhang relevante Paragrafen sind § 87 (zu ergreifende technische Schutzmaßnahmen), § 89 (Datenschutz, insbesondere der Grundsatz der Verhältnismäßigkeit, d. h. Beschränkung der Erhebung, Verarbeitung und Nutzung auf das erforderliche Maß, sowie der Grundsatz der Zweckbindung) sowie § 92 (Datenübermittlung an ausländische nicht öffentliche Stellen).³¹ An dieser Stelle sei ausdrücklich erwähnt, dass § 113a, der die gespeicherten Daten und § 113b, der deren Verwendung regelt, gegen Art. 10 GG verstoßen und gem. Urteil des BVerfG vom 2. März 2010 nichtig sind.

4. Bundesverfassungsschutzgesetz (BVerfSchG):³² § 8 regelt die Befugnisse des Bundesamts für Verfassungsschutz, § 9 die Zulässigkeit der Datenerhebung, d. h. Tatbestände, die die Annahme rechtfertigen, dass die Erhebung zum Schutz gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten erfolgt, §§ 10–19 beziehen sich auf die Speicherung, Veränderung, Nutzung, Berichtigung, Löschung und Sperrung personenbezogener Daten.

5. Sozialgesetzbuch (SGB):³³ Hier sind insbesondere die §§ 94, 95, 96 SGB XI zu nennen, die die Erhebung, Verarbeitung und Nutzung personenbezogener Daten bei Pflegekassen, Verbänden der Pflegekassen, Trägern der Sozialhilfe und des Medizinischen Dienstes regeln.

6. Strafgesetzbuch:³⁴ Es regelt in § 238 den Straftatbestand der Nachstellung. Dieser Straftatbestand ist u. a. erfüllt, wenn jemand „... unter Verwendung von dessen personenbezogenen Daten Bestellungen von Waren oder Dienstleistungen für ihn aufgibt oder Dritte veranlasst, mit diesem Kontakt aufzunehmen ...“

Neben den zuvor erwähnten Gesetzen sind das allgemeine Persönlichkeitsrecht, das sich als Gewohnheitsrecht



aus Art. 1 Abs. 1 GG und Art. 2 Abs. 2 GG herleitet und ein absolutes Recht i. S. d. § 823 Abs. 1 BGB darstellt, das sich ebenfalls aus den zuvor erwähnten Paragrafen des Grundgesetzes herleitende umgangssprachlich als IT-Grundrecht bezeichnete Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie das Recht auf informationelle Selbstbestimmung zu nennen.

Zudem gewinnt auch die Rechtsprechung in diesem Bereich immer mehr an Bedeutung. Das BGH-Urteil zur WLAN-Nutzung vom 12. Mai 2010 mit dem wohlklingenden Namen „Sommer unseres Lebens“ spiegelt eine interessante und spannende Rechtsentwicklung wider: Inwieweit kann ein Internet-Nutzer für die unberechtigte Nutzung von Daten bzw. die Verletzung von Urheberrechten durch einen Dritten haftbar und ggf. schadenersatzpflichtig gemacht werden. Der BGH entschied, dass Inhaber von Funknetzen ihr WLAN mit einem Passwort gegen unberechtigten Zugang absichern müssen.³⁵ Das Urteil stellt den privaten Inhaber zwar von Schadenersatzansprüchen frei, erlaubt aber Abmahnungen und Unterlassungsklagen. Interessant wird sein, welche Auswirkungen sich durch dieses Urteil auf Betreiber öffentlicher Hotspots ergeben.

In den oben genannten Gesetzen geht es im Wesentlichen um die Frage, welche Daten in welcher Form von wem gespeichert und genutzt werden dürfen. Inwieweit sich die Rechtsprechung ggf. in Richtung einer Schadenersatzpflicht von Internet-Nutzern für ein „Fehlverhalten“ Dritter in den nächsten Jahren entwickeln wird, bleibt abzuwarten.

Doch weder Gesetze noch Rechtsprechung können den Missbrauch von personenbezogenen Daten verhindern. Sie bilden lediglich den rechtlichen Rahmen für Schadenersatzforderungen oder strafrechtliche Konsequenzen. Zur Minimierung dieses Risikos bedarf es daher des Risikomanagements.

Gibt es eine Möglichkeit, sich gegen den Missbrauch von Daten oder deren Folgen zu schützen?

Die Antwort lautet: ein „angemessenes“, zwischen Nutzen und Gefahren der virtuellen Welt abwägendes Risikomanagement. Es gibt eine Vielzahl von Möglichkeiten, dem Risiko des Datenmissbrauchs zu begegnen:

Risiken vermeiden

Die einfachste Möglichkeit, dem Risiko des Missbrauchs von persönlichen Daten zu begegnen, ist, dieses Risiko

zu vermeiden. Dies würde aber bedeuten, sich der virtuellen Welt mit all ihren Gefahren, aber auch Annehmlichkeiten in wesentlichen Teilbereichen oder gänzlich zu entziehen. Keine Nutzung einer EC- oder Kreditkarte, kein Online Banking, keine Teilnahme an Bonusprogrammen wie Miles & More oder Payback, kein Internet, kein Telefon – ehrlich gesagt eine undenkbbare Vorstellung und ein eher weltfremdes Lebensmodell für einen modernen Menschen.

Risiken in Kauf nehmen

Eine weitere, wie jedoch bereits am Beispiel „Facebook“ erläutert, letztlich der Sache nicht gerecht werdende Art des Risikomanagements ist die Inkaufnahme des Risikos, dass eigene Daten zweckentfremdet und unberechtigt genutzt werden, getreu dem Motto „Ich habe nichts zu verbergen“. Sicherlich ist dies eine noch von vielen Internetnutzern gelebte Haltung, wahrscheinlich aber eher aus Unkenntnis der möglichen Risiken als aufgrund einer bewussten Entscheidung. In den vergangenen Monaten wurde die Bevölkerung jedoch durch die Medien für Risiken beim Umgang mit Daten (u. a. bei Google) sensibilisiert, daher ist davon auszugehen, dass sich die Einstellung in naher Zukunft ändern wird.

Risiken verringern

Eine den Realitäten einer zunehmend virtuelleren Welt und den damit verbundenen Risiken gerecht werdende Risikomanagementstrategie ist der verantwortliche Umgang des Einzelnen mit eigenen Daten, d. h. das Risiko durch deren restriktive Preisgabe zu verringern.

Des Weiteren sollte man die Interessen der Anbieter, z. B. sozialer Netzwerke wie Facebook, bewusst gegen die eigenen abwägen, insbesondere im Hinblick auf die damit verbundenen Gefahren. Es ist unerlässlich, sich vor der Preisgabe persönlicher Daten über die jeweiligen Allgemeinen Geschäftsbedingungen und Datenschutzbestimmungen zu informieren. Dabei sollte der Benutzer immer kritisch prüfen, welche Rechte er den

Betreibern an den eingestellten Bildern, Texten und Informationen einräumt. Andernfalls könnten längst vergangene Ereignisse auch nach Jahren wieder in Erinnerung gerufen werden und unter Umständen dazu führen, dass man eine Arbeitsstelle nicht bekommt. Auch wenn das Profil längst gelöscht ist, Google, Facebook, X-ing etc. vergessen nie.

Für Unternehmen, die mit personenbezogenen Daten umgehen, heißt es, sich der damit verbundenen Risiken bewusst zu sein und durch entsprechende technische Vorkehrungen für ein hohes Maß an Datensicherheit zu sorgen. Insbesondere ist den herrschenden IT-Strukturen Beachtung zu schenken. Risikomanagement zur Vermeidung von Datenmissbrauch bedeutet für Unternehmen die Implementierung von entsprechenden Kontrollsystemen, eine klare Regelung, wer in welcher Form mit den Daten umgehen darf und Zugriffsrechte hat. So enthalten z. B. Sarbanes-Oxley und Basel II Regelungen zur IT-Compliance. Vorstandmitglieder einer AG haften bei Schäden dieser Art ggf. wegen Organisationsverschuldens gem. § 93 Abs. 2 AktG, Geschäftsführer einer GmbH nach § 43 Abs. 2 GmbHG. In jedem Fall heißt Risiko verringern



für Unternehmen, den Datenschutz ernst nehmen und geeignete Maßnahmen ergreifen.

Risiko übertragen

Eine weitere Form des Risikomanagements kann es sein, die Verarbeitung personenbezogener Daten an Dritte zu übertragen. Dies ist sicherlich nur für Unternehmen relevant und erfordert u. a. eine sorgfältige Auswahl des Drittunternehmens. Bei der Übertragung der Verarbeitung personenbezogener Daten müssen höchste Maßstäbe angelegt werden, da bei einem Verstoß gegen diese Sorgfaltspflichten den Vorstandsmitgliedern einer AG bzw. Geschäftsführern einer GmbH ggf. eine Haftung aus Organisationsverschulden droht.

Versicherungslösungen

Eine weitere Möglichkeit, sich gegen die Folgen von Datenmissbrauch zu schützen, ist eine Versicherung zur Deckung des durch den Missbrauch von personenbezogenen Daten verursachten Schadens.

In diesem Zusammenhang tritt neben die Frage, welche Versicherungskonzepte es am Markt überhaupt gibt, d. h. welche Schäden versicherbar sind, auch die Problematik der rechtlichen Einordnung der entstandenen Schäden.

Eine eindeutige rechtliche Qualifikation als Personen-, Sach- oder Vermögensschaden ist schwierig bzw. umstritten.

So gilt z. B. der Schaden aus einer Persönlichkeitsrechtsverletzung zwar nach h. M. als Vermögensschaden, jedoch gibt es auch Stimmen, die ihn als Personenschaden einstufen, wenn Schmerzensgeldansprüche erhoben werden.³⁶ Im europäischen Ausland gelten Persönlichkeitsrechtsverletzungen überwiegend als Personenschäden.

In diesem Zusammenhang tritt neben die Frage, welche Versicherungskonzepte es gibt, ... auch die Problematik der rechtlichen Einordnung der entstandenen Schäden.

Auch die Frage, ob es sich bei der Beeinträchtigung von Daten um einen Sach- oder Vermögensschaden handelt, ist in der Rechtsprechung nicht



eindeutig geklärt. So setzt nach h. M. ein Sachschaden immer die Beschädigung einer vorher unbeschädigten Sache voraus. Dies ist in jedem Fall bei einer physischen Beeinträchtigung des Datenträgers, die zum Datenverlust führt, zu bejahen. Liegt – wie beim Internet, das nur als Transportmedium dient – keine physische Beeinträchtigung vor, handelt es sich um einen Vermögensschaden. Demzufolge werden die aus dem Missbrauch von personenbezogenen Daten entstehenden Schäden, die rechtlich nicht als Personenschaden einzuordnen sind, in der Regel reine Vermögensschäden oder immaterielle Schäden sein.

Die meisten Versicherungskonzepte bieten keinen oder nur unzureichenden Schutz für einzelne Teilbereiche.

Die überwiegend am Markt vorhandenen IT-Konzepte stellen normalerweise auf die Risiken von Unternehmen aus der IT-Branche ab, nicht aber auf die übrigen Unternehmen bzw. private Schadenverursacher. Wie aber sieht die Versicherbarkeit der Risiken bei diesen Unternehmen aus?

Reine, wenn auch sicherlich am Markt selten vorkommende AHB-Deckungen, bieten keinen Versicherungsschutz für aus dem Missbrauch

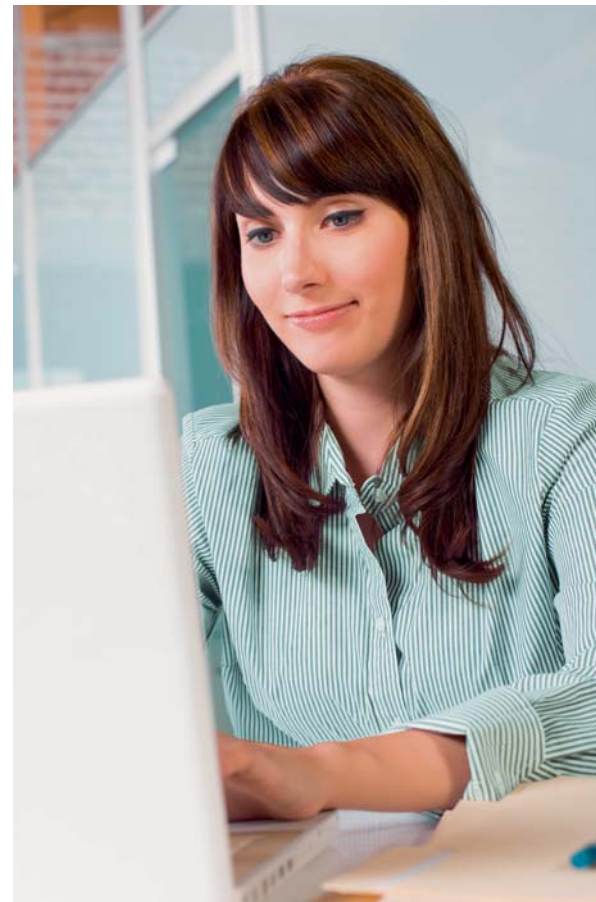
von personenbezogenen Daten resultierende Personen-, Sach- noch Vermögensschäden. Ausgeschlossen sind gem.

§ 7.15 AHB: Haftpflichtansprüche wegen Schäden aus dem Austausch, der Übermittlung und der Bereitstellung elektronischer Daten, soweit es sich handelt um Schäden aus

- (1) Löschung, Unterdrückung, Unbrauchbarmachung oder Veränderung von Daten,
- (2) Nichterfassen oder fehlerhaftem Speichern von Daten,
- (3) Störung des Zugangs zum elektronischen Datenaustausch,
- (4) Übermittlung vertraulicher Daten oder Informationen.

§ 7.16 AHB: Haftpflichtansprüche wegen Schäden aus Persönlichkeits- oder Namensrechtsverletzungen.

Auch viele Konzepte zur Betriebshaftpflichtversicherung werden dem Risiko von Nutzern von IT-Technologien nicht oder nur eingeschränkt gerecht. So bieten die am Markt üblichen Deckungserweiterungen in der Regel nur Versicherungsschutz für Vermögensschäden, indem durch eine Deckungserweiterung abweichend von den



AHB-Ausschlüssen die gesetzliche Haftpflicht für Vermögensschäden aus der Verletzung des BDSG eingeschlossen wird. Schäden als Folge von Persönlichkeitsrechtsverletzungen bleiben ausgeschlossen, da § 7.16 AHB weiterhin zur Anwendung kommt.

Um jedoch den immer häufiger beim Umgang mit personenbezogenen Daten auftretenden Risiken Rechnung zu tragen, wurden vom GDV Zusatzbedingungen zur Betriebshaftpflichtversicherung für die Nutzer von Internet-Technologien entwickelt. Dieses Konzept bietet ihnen Deckung für Schäden aus dem Austausch, der Übermittlung und Bereitstellung elektronischer Daten, soweit diese resultieren aus

- der Veränderung von Daten (inkl. Datenverlust) durch Computerviren und/oder anderen Schadprogrammen oder sonstigen Gründen,
- der Störung des Zugangs zum elektronischen Datenaustausch,
- der Verletzung von Persönlichkeits- sowie Namensrechten,

unabhängig von der rechtlichen Einordnung des Schaden als Personen-, Sach- oder Vermögensschaden. Es wird lediglich auf den Begriff „Schäden“ abgestellt, womit man im Schadenfall die z. T. umstrittene rechtliche Einordnung einzelner Schadenarten umgeht.

Dieses Konzept bietet Unternehmen einen gewissen Schutz, der den jeweiligen besonderen Anforderungen gerecht wird. Wie sieht es aber bei Privatpersonen aus?

Auch die Privathaftpflichtversicherung bietet, ähnlich wie der zuvor dargestellte Zusatzbaustein zur Betriebshaftpflichtversicherung, Deckung für die gesetzliche Haftpflicht des VN für Schäden aus dem Austausch, der Übermittlung und Bereitstellung elektronischer Daten, z. B. im Internet, per E-Mail oder mittels Datenträger, jedoch nur soweit es sich um

- Datenveränderungen durch Computerviren und/oder andere Schadprogramme,



- sonstige Datenveränderungen sowie Nichterfassen/fehlerhaftes Speichern oder
- Störung des Zugangs Dritter zum elektronischen Datenaustausch

handelt. Auch hier spielt die rechtliche Einordnung als Sach- oder Vermögensschaden keine Rolle. Anders als in den Zusatzbedingungen zur Betriebshaftpflichtversicherung gilt in der Privathaftpflichtversicherung § 7.16 AHB unverändert, so dass für Persönlichkeits- und Namensrechtsverletzungen weiterhin kein Versicherungsschutz besteht.

Als Fazit bleibt festzuhalten: Das Risiko des Missbrauchs personenbezogener Daten gänzlich zu vermeiden würde heißen, sich einem modernen, immer mehr vom Internet beeinflussten Leben gänzlich zu entziehen. Ein wachsender, wohlüberlegter Umgang mit den eigenen Daten minimiert das Risiko zumindest in Teilbereichen. Wie gläsern uns die virtuelle Datenwelt letztlich sein lässt, liegt zum großen Teil in der Verantwortung des Einzelnen. Was nicht im Netz ankommt, wird nicht verbreitet, oder: Aus wenigen Puzzleteilen lässt sich noch kein Bild machen.

¹ www.spiegel.de/wirtschaft/0,1518,572855,00.html.

² www.zeit.de/online/2008/41/telekom-datenklau.

³ www.spiegel.de/wirtschaft/unternehmen/0,1518,662075,00.html.

⁴ www.stern.de/wirtschaft/news/unternehmen/ueberwachung-systematische-bespieltzung-im-handel-617392.html.

⁵ www.stern.de/wirtschaft/news/unternehmen/ueberwachung-systematische-bespieltzung-im-handel-638756.html.

⁶ FAZ vom 31. März 2008, Der Fall Liechtenstein.

⁷ Urteil des Fürstlichen Landgerichts Vaduz, Aktenzeichen 06.CG.2009.162,

www.sueddeutsche.de/geld/2.220/urteil-in-liechtenstein-einfach-zu-spaet-gewarnt.

⁸ Spiegel online 5. Juli 2010,

www.spiegel.de/wirtschaft/soziales.

⁹ www.tagesschau.de/inland/elena128.html.

¹⁰ www.datenschutz.de/recht/grundlagen/.

¹¹ www.privacycommission.be/en/press_room/pers_bericht11.html.

¹² www.europarl.europa.eu/news/public/focus_page/008-68312-039-02-07-901-20100128FCS68186-08-02-2010-2010/default_en.htm.

¹³ www.spiegel.de/politik/ausland.

¹⁴ eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:DE:HTML.

¹⁵ www.vorratsdatenspeicherung.de/static/verfassungsbeschwerde_de.html,

www.vorratsdatenspeicherung.de/content/view/78/86/lang/de/.

¹⁶ BVerfG, Urt. v. 2. März 2010 – 1 BvR 256/08 u. a.

¹⁷ BVerfG, NJW 12/2010.

¹⁸ Ebenda.

¹⁹ www.test.de/themen/computer-telefon/test/Soziale-Netzwerke-Datenschutz-oft-mangelhaft-1854798-1855785/.

²⁰ www.facebook.com.

²¹ www.wikipedia.org/wiki/Facebook.

²² Ebenda.

²³ www.20min.ch/news/schweiz/story/20139035.

²⁴ www.google.com/intl/de/privacypolicy.html.

²⁵ www.spiegel.de/netzwelt/netzpolitik/0,1518,694885,00.html.

²⁶ www.spiegel.de/netzwelt/netzpolitik/0,1518,671639,00.html.

²⁷ www.datenschutz.de/recht/grundlagen/

²⁸ BGHZ 35, 363, 369.

²⁹ www.gesetze-im-internet.de/bundesrecht/gg/gesamt.pdf.

³⁰ www.datenschutz-bayern.de/recht/tddsg.html.

³¹ www.gesetze-im-internet.de/tkg_2004/.

³² www.gesetze-im-internet.de/bverfsg/.

³³ www.gesetze-im-internet.de/sgb_11/.

³⁴ www.gesetze-im-internet.de/stgb/gesamt.pdf.

³⁵ BGH, Aktenzeichen 1 ZR 121/08 v. 12. Mai 2010.

³⁶ Vgl. Späte AHB, 1993, § 1 Rn.93.



The people behind the promise.®

Diese Informationen wurden von der Gen Re zusammengestellt und dienen als Hintergrundinformationen für unsere Kunden sowie unsere Fachmitarbeiter. Die Informationen müssen eventuell von Zeit zu Zeit überarbeitet und aktualisiert werden. Sie sind nicht als rechtliche Beratung anzusehen. Bitte sprechen Sie mit Ihrem Rechtsberater, ehe Sie sich auf diese Informationen berufen.

© General Re Corporation und General Reinsurance AG 2010