

**PASCHEN**

---

Rechtsanwälte

Berlin Bonn Frankfurt Leipzig München

**Rechtliche Aspekte der IT-Sicherheit im  
mittelständischen Unternehmen**

**Vortrag zur IBM-Veranstaltung**

**IT-Sicherheit im mittelständischen Unternehmen**

## **1. Teil**

# **Arbeitsrechtliche Aspekte der Datensicherheit und der Datenschutz bei Computernutzung im Betrieb**

von Rechtsanwalt Michael Schmidt, Berlin

## **2. Teil**

# **Datenschutz im Internet**

von Rechtsanwalt Michael Clobes, Frankfurt a.M.

Vervielfältigung und Wiedergabe – auch auszugsweise- nur mit Zustimmung der Verfasser gestattet.

Wir weisen ferner darauf hin, dass wir den Vortrag nach bestem Wissen erstellt haben, aber für die inhaltliche Richtigkeit keine Gewähr übernehmen können.

Die Vortragsform wurde beibehalten.

# 1. Teil

## Arbeitsrechtliche Aspekte der Datensicherheit und der Datenschutz bei Computernutzung im Betrieb

Die Frage der IT-Sicherheit in mittelständischen Betrieben ist natürlich mit der Frage verknüpft, welche Pflichten hierbei die betreffenden Mitarbeiter bzw. alle Mitarbeiter des Unternehmens zu erfüllen haben. Auf der anderen Seite stellt sich natürlich auch die Frage, welche Verpflichtungen den Arbeitgeber namentlich im Zusammenhang mit dem Datenschutz gegenüber den Mitarbeitern treffen.

### **1.1. Arbeitsvertragliche Zulässigkeit**

Zunächst soll hier nochmals ganz kurz dargestellt werden, unter welchen Voraussetzungen überhaupt die Einführung von Internet und Intranet im Betrieb möglich ist und was hierbei zu beachten ist.

Hier gilt im Grundsatz, dass der Arbeitgeber bei der Organisation des Arbeitsprozesses frei ist. Er kann kraft seines Weisungsrechtes den Inhalt und die Modalitäten der Arbeit bestimmen, ist deswegen auch grundsätzlich frei in der Befugnis, die Arbeit an neuen Geräten oder Geräten mit erweiterter Funktion anzuordnen. Dies bedeutet, dass der Arbeitgeber auf Grund seines Direktionsrechtes sowohl die Nutzung des Intranets wie auch die Nutzung des Internets in betrieblicher Hinsicht anordnen kann. Eine gewisse Einschränkung kann sich hier lediglich hinsichtlich solcher Arbeitnehmer ergeben, denen auf Grund ihrer persönlichen Fähigkeiten die Arbeit am vernetzten PC unmöglich ist. Hier ist ggf. an eine unternehmensinterne Versetzung oder – schlimmstenfalls - an eine (Änderungs-)Kündigung zu denken.

Weiter ist zu berücksichtigen, dass bei der Einführung des Internetzugangs der Gleichbehandlungsgrundsatz zu beachten ist. Dies bedeutet, dass der Arbeitgeber nicht ohne sachlichen Grund einen Arbeitnehmer schlechter als andere behandeln darf. Wird daher bestimmten Arbeitnehmern die Möglichkeit des Internetzugangs eingeräumt, muss dies – wenn keine sachlichen Gründe entgegenstehen, auch anderen vergleichbaren Arbeitnehmern

gewährt werden. Zulässig wäre jedoch beispielsweise, dass lediglich in der Einkaufsabteilung ein Internetzugang eingeräumt wird, hingegen in der Buchhaltung, die lediglich mit unternehmensinternen Vorgängen betreut ist, nicht.

## **1.2. Beteiligungsrechte des Betriebsrates**

Sofern das Unternehmen über einen Betriebsrat verfügt, ist auch zu berücksichtigen, dass dieser an der Einführung des Internets/Intranets zu beteiligen ist. Dies ergibt sich aus § 90 BetrVerfG. Hier erstreckt sich diese Beteiligung des Betriebsrates darauf, dass dieser Vorschläge unterbreiten und Bedenken mitteilen kann. Wichtig ist, dass die Nichtbeteiligung des Betriebsrates als Ordnungswidrigkeit mit einem Bußgeld geahndet werden kann.

Ein über das bloße Beratungsrecht hinausgehendes Mitbestimmungsrecht des Betriebsrates sieht der neue § 97 Abs. 2 BetrVerfG vor:

Voraussetzung für das Eingreifen des § 97 Abs. 2 BetrVerfG ist, dass der Arbeitgeber Maßnahmen geplant oder durchgeführt hat, die die Tätigkeit der betroffenen Arbeitnehmer ändern und dadurch die beruflichen Kenntnisse und Fähigkeiten der Arbeitnehmer zur Erfüllung ihrer Aufgaben nicht mehr ausreichen. In diesem Fall kann der Betriebsrat bei der Einführung von Maßnahmen der betrieblichen Berufsausbildung mitbestimmen. Wann diese Schwelle erreicht ist, muss durch die Rechtsprechung noch geklärt werden, m.E. dürfte jedoch die alleinige Einrichtung eines Mailprogramms nicht ausreichen. Etwas anderes könnte beispielsweise gelten, wenn mit diesem Programm oder generell mit der betrieblichen Vernetzung völlig neu Arbeitsabläufe und Methoden verbunden sind. Nur der Vollständigkeit halber sei an dieser Stelle auch noch die Bildschirmarbeitsverordnung erwähnt, die für Bildschirmarbeitsplätze bestimmte Mindestanforderungen (niedrige Strahlung, regelmäßige Pausen, Augenuntersuchungen, Reflexions- und blendungsfreier Bildschirm) vorschreibt.

Auch hier besteht wieder ein Mitbestimmungsrecht des Betriebsrates.

Festzuhalten bleibt somit, dass die Einführung von Internet/Intranet im Betrieb kraft des Direktionsrechtes des Arbeitgebers im wesentlichen problemlos möglich ist. Bei Vorhandensein eines Betriebsrates ist dieser jedoch zu beteiligen. Die Beteiligung des

Betriebsrates kann je nach Umfang der Maßnahme über ein bloßes Beratungsrecht hin zu einem Mitbestimmungsrecht gehen.

## **2. Regelung für die Internetnutzung**

Sind nun die vorstehenden Hürden genommen und im Betrieb ist ein Intranet mit der Möglichkeit des Internetzugangs für einige oder alle Arbeitnehmer etabliert, stellt sich die Frage nach der Notwendigkeit einer Regelung für diese Internetnutzung. Viele Unternehmen räumen den Mitarbeitern die Möglichkeit zur privaten Internetnutzung ein, ohne Einzelheiten näher festzulegen. Davon ist dringend abzuraten. Sind keine Regelungen vorhanden, geht dies in aller Regel zu Lasten des Arbeitgebers.

### **2.1. Abgrenzung von privater zu betrieblicher Nutzung**

Bevor wir uns der Frage zuwenden, wann von einer erlaubten Internetnutzung zu privaten Zwecken auszugehen ist, muss zunächst abgegrenzt werden, wann eine private oder dienstliche Nutzung vorliegt. Dies mag auf den ersten Blick ganz eindeutig auf der Hand liegen, es gibt jedoch – wie immer, wenn Juristen beteiligt sind – auch Streitfälle.

Eine dienstliche Nutzung liegt dann vor, wenn ein Bezug zu den Aufgaben des Arbeitnehmers gegeben ist und die Aufgabenerfüllung durch die Internetnutzung gefördert werden soll. Hierbei kommt es noch nicht einmal darauf an, ob die Vorgehensweise im Einzelfall zweckmäßig ist, es reicht allein die Absicht aus, die Arbeit voranzubringen.

Das Arbeitsgericht Wesel hat sogar entschieden, dass in der ersten Phase des Umgangs mit dem Internet das Erlernen auch dann dienstlichen Charakter haben könne, wenn es um Surfen in Bereichen mit privaten Themen gehe. Man muss also als Arbeitnehmer nur geschickt argumentieren und die Auffassung vertreten, man habe sein Internet-know-how verbessern wollen.

Neben der dienstlichen Nutzung gibt es die Privatnutzung aus dienstlichem Anlass. Hier lässt sich auf die von der Rechtsprechung bereits entschiedenen Fälle aus der Telefonnutzung zurückgreifen. Eine Privatnutzung aus dienstlichem Anlass wird beispielsweise dann bejaht, wenn wegen einer länger sich hinziehenden Sitzung private Termine abgesagt werden

müssen. Liegt keine der vorbenannten Konstellationen vor, spricht man von einer rein privaten Nutzung. Ob die Privatnutzung gestattet wird, obliegt dem Arbeitgeber grundsätzlich nach eigenem Ermessen. Er entscheidet frei darüber, in welchem Umfang er seinen Mitarbeitern oder anderen Personen Nutzungsmöglichkeiten einräumen will. Das Arbeitsverhältnis gibt im normalen Fall nicht das Recht, Installationen des Arbeitgebers für eigene Zwecke zu verwenden. Ein Anspruch auf Nutzung der Kommunikationsmittel des Arbeitgebers besteht nur in ganz wenigen Ausnahmefällen, nämlich dann, wenn keine Verschiebung auf die Freizeit bzw. ein anderes Medium möglich ist.

Aus vorstehendem lässt sich also ableiten, dass die private Nutzung von e-mail und Internet im Regelfall der Zustimmung des Arbeitgebers bedarf. Diese kann ausdrücklich entweder durch arbeitsvertragliche Gestattung oder eine Betriebsvereinbarung oder aber durch eine Erklärung des Arbeitgebers, die im Betrieb bekannt gemacht wird, erfolgen.

Schwieriger sind die Fälle zu beurteilen, in denen lediglich eine konkludente, d.h. stillschweigende, Einwilligung vorliegt. Diese wird auf jeden Fall dann anzunehmen sein, wenn die Privatnutzung gegenüber dem einzelnen Arbeitnehmer abgerechnet wird oder wenn die vom Arbeitgeber zur Verfügung gestellte Liste mit Lesezeichen auch private Links enthält. Hierbei wird allerdings zu berücksichtigen sein, dass beispielsweise der Microsoft Explorer bereits einige Links in der Vorinstallation enthält, so dass man hier sicherlich nicht davon ausgehen können wird, dass der Arbeitgeber sich durch die Verwendung des Microsoft Internetexplorers damit auch einverstanden erklärt habe, dass seine Arbeitnehmer privat surfen.

## **2.2. Zeitliche und inhaltliche Beschränkungen**

Teilweise wird die Auffassung vertreten, wenn bereits privates Telefonieren gestattet sei, dass auch in vergleichbarem Umfang private e-mail und privates Internetsurfen möglich sei. Dies soll insbesondere dann gelten, wenn bei einer Flatrate für den Arbeitgeber ohnehin keine zusätzlichen Kosten entstehen. Ich halte dies insoweit für zweifelhaft, weil auch dann, wenn die private Internetnutzung keine zusätzlichen Providerkosten verursacht, diese zumindest dann – wenn sie während der Arbeitszeit geschieht -, durchaus mit erheblichen Kosten für den Arbeitgeber verbunden sind. Es gibt immer wieder Untersuchungen, die von Milliardenbeträgen ausgehen, die der Privatwirtschaft auf Grund von Arbeitszeitverlusten

durch privates Surfen entstehen. Zulässig ist es sicherlich, das Internetsurfen sowohl zeitlich (beispielsweise außerhalb der Arbeitszeiten), dem Umfang nach und auch inhaltlich (beispielsweise keine Erotikseiten) zu beschränken.

### **2.3. Erteilung und Widerruf der Erlaubnis**

In all den Fällen, in denen der Arbeitgeber das Internetsurfen bisher uneingeschränkt erlaubt hat und dieses nun entweder einschränken oder gänzlich verbieten möchte, stellt sich die Frage, ob dies ohne weiteres zulässig ist. Hier kommt es – wie fast immer – darauf an, unter welchen Voraussetzungen die private Nutzung gestattet worden ist. Am besten stellt sich der Arbeitgeber dann, wenn er die Einwilligung in die private Nutzung mit einem Widerrufsvorbehalt versehen hat. Dann kann er nach billigem Ermessen entscheiden, was in der Regel einen sachlichen Grund wie beispielsweise Störungen im System oder eine unangemessene Kostenbelastung voraussetzt. Wurde der Widerruf nicht vorbehalten, ist eine Änderung in der Regel nur mit Zustimmung der Beschäftigten oder über eine Änderungskündigung möglich. Liegt eine betriebliche Übung vor, d.h. eine über einen längeren Zeitraum gewährte private Nutzung ohne entsprechenden Vorbehalt, kann diese entweder dadurch beseitigt werden, dass über einen längeren Zeitraum keine Privatnutzung mehr praktiziert wird oder aber dass durch Rundschreiben darauf hingewiesen wird, dass sich der Arbeitgeber künftig vorbehält, die private Nutzung jederzeit zu widerrufen. Sofern sich die Arbeitnehmer – wovon in aller Regel auszugehen ist – hiergegen nicht verwahren, führt dies dann auch zu einer Änderung des Status quo.

### **2.4. Missbrauchsfälle**

Auch wenn die private Nutzung gestattet ist, muss sich dies in einem angemessenen zeitlichen Rahmen bewegen. Was die Rechtsprechung bereits für ausschweifendes privates Telefonieren entschieden hat, nämlich eine Verletzung der Arbeitspflicht, gilt auch für ausschweifendes Surfen im Internet. Es empfiehlt sich zweckmäßiger Weise hier von vornherein eine zeitliche und inhaltliche Beschränkung vorzunehmen, da dann die Frage, wann ein ausschweifendes Surfen vorliegt, abschließend und eindeutig geregelt ist. Wird dann gegen diese Regelung verstoßen, zieht dies auf jeden Falle eine Abmahnung und im Wiederholungsfalle eine Kündigung nach sich.

Großes Interesse findet auch ein zweiter Missbrauchsfall: Der Arbeitnehmer verschafft sich über seinen auch für private Zwecke nutzbaren Anschluss Zugang zu Pornodateien oder Seiten mit rechtsradikalen Inhalten. Hier ist zu differenzieren, ob hierdurch betriebliche Belange berührt werden; wenn die strafbaren Dateien nur individuell konsumiert werden, sich der Vorgang jedoch nicht auf die Arbeitsleistung ausgewirkt und auch nicht andere Beschäftigte belästigt wurden, soll dies nicht der Fall sein. Dieser Fall wäre dann vergleichbar demjenigen, wenn der Arbeitnehmer zu Hause an seinem privat genutzten PC entsprechende Dateien heruntergeladen hätte. Anders liegt es natürlich in einem vom Arbeitsgericht Braunschweig entschiedenen Fall: Hier hatte der Leiter eines Kindergartens sich Kinderpornographie über das Internet verschafft, was eine außerordentliche Kündigung gerechtfertigt hat. Hier war auf Grund dieses Sachverhalts vom Wegfall der Eignung des Arbeitnehmers, weiterhin als Leiter eines Kindergartens zu fungieren, auszugehen. Ebenfalls wurde die fristlose Kündigung eines Krankenhausarztes bestätigt, der auf seinem Arbeitsplatzrechner 9.000 Kinderpornodateien abgespeichert und ausgedruckt hatte.

Ist von vornherein die Internetnutzung nur auf dienstliche Zwecke beschränkt und war dies eindeutig geregelt, kommt bei einem Verstoß sofort eine Abmahnung in Betracht. Eine fristlose Kündigung ohne Abmahnung wird nur dann in Betracht kommen, wenn eine erhebliche Dauer der Nutzung vorliegt oder andere Verstöße hinzukommen.

### **3. Pflichtverstöße bei Internetnutzung**

Neben den vorgenannten Fällen der unerlaubten Internetnutzung bzw. Nutzung des Internets über den eingeräumten Gebrauch hinaus gibt es auch noch andere Pflichtverstöße.

Im Einzelnen sind hier zu nennen:

#### **3.1. Nichtnutzung**

Sofern der Arbeitgeber anordnet, dass künftig die gesamte Korrespondenz über e-mail abgewickelt wird, unternehmensinterne Kommunikation über e-mail erfolgt oder Reisekostenabrechnungen, Materialanforderungen und ähnliches mehr nur noch über Internet zu erfolgen hat, ist der Arbeitnehmer verpflichtet, dieser Weisung nachzukommen. Verstößt er hiergegen oder erhält beispielsweise von unternehmensinternen Informationen deswegen

keine Kenntnis, weil er e-mails nicht abrufen, rechtfertigt dies eine Abmahnung, im Wiederholungsfalle die fristlose Kündigung. Voraussetzung hierfür ist allerdings, dass der Arbeitnehmer durch eine entsprechende Schulung/Unterrichtung in die Lage versetzt wurde, entsprechend mit der Technik umzugehen. Zulässig sind auch Weisungen, dass e-mails innerhalb bestimmter Termine zu bearbeiten sind.

### **3.2. Fehlerhafte Nutzung**

Häufiger werden die Fälle sein, in denen mit der Technik unsachgemäß umgegangen wird. Hier kommen wir in den Bereich der Datensicherheit.

Soweit lediglich das Passwort vergessen wird, ist dies weniger gravierend. Gravierender hingegen ist es, wenn das Passwort weitergegeben wird. Vergleichbar sind auch die Fälle, in denen gegen die entsprechende Anweisung verstoßen wurde, dass das Passwort in regelmäßigen Abständen zu ändern ist oder aber leicht zu entschlüsselnde Passwörter gewählt werden. Kommt es hierdurch zum Zugang zu vertraulichen Daten (Personalakten, Betriebsgeheimnissen) stellt dies eine erhebliche Gefährdung der Vertraulichkeit dar, die eine Abmahnung rechtfertigt. Fehler können auch darin liegen, dass entgegen betrieblichen Anweisungen keine Sicherungskopien hergestellt oder die Datensicherung nicht durchgeführt wird. Besteht hier eine eindeutige und klare Arbeitseinweisung und ist der Arbeitnehmer entsprechend eingewiesen, rechtfertigt auch dies eine Abmahnung oder sonstige arbeitsvertragliche Konsequenzen.

Gleiches gilt hinsichtlich des unsorgfältigen Umgangs mit externen Dateien. Sei es, dass ungeprüfte Dateien aus dem Internet heruntergeladen werden, sei es, dass Attachments bei e-mails geöffnet werden oder sei es, dass Datenträger von Dritten ohne vorherige Prüfung in den Computer eingelegt werden. Gleiches gilt, wenn entsprechende Warnungen des Systemadministrators vor gefährlichen e-mails ignoriert werden. Bei all diesen Vorfällen handelt es sich um Verstöße des Arbeitnehmers gegen arbeitsvertragliche Pflichten, die bei einer entsprechenden Schwere des Verstoßes eine Abmahnung, ggf. sogar eine fristlose Kündigung rechtfertigen können. Wichtig in diesem Zusammenhang ist es, dass entsprechende Anweisungen entsprechend dokumentiert werden und den Mitarbeitern auch das entsprechende know-how vermittelt wird, um diese Anweisung richtig umsetzen zu können.

### **3.3. Schadensersatzansprüche des Arbeitgebers**

Neben den arbeitsvertraglichen Konsequenzen stellt sich auch die Frage, inwieweit der Arbeitgeber Schadensersatzansprüche gegenüber dem Arbeitnehmer geltend machen kann, der gegen seine Pflichten verstoßen hat. Dies setzt zunächst voraus, dass der Arbeitnehmer durch fahrlässiges Verhalten den Schaden herbeigeführt hat. Hierbei gelten die von der Rechtsprechung entwickelten Grundsätze über die Arbeitnehmerhaftung. Diese weicht von der „normalen“ Haftung in Vertragsverhältnissen ab:

Danach haftet ein Arbeitnehmer bei leichter Fahrlässigkeit gegenüber dem Arbeitgeber überhaupt nicht. Die Rechtsprechung begründet dies damit, dass der Arbeitgeber unter dem Gesichtspunkt des von ihm zu tragenden Betriebsrisikos den Schaden allein zu übernehmen habe. Bei mittlerer Fahrlässigkeit des Arbeitnehmers ist der entstandene Schaden zwischen Arbeitnehmer und Arbeitgeber aufzuteilen. Hierbei sind alle Umstände der Schadensentstehung einschließlich der wirtschaftlichen Situation und des Verdienstes des Arbeitnehmers zu berücksichtigen. Häufig wird von der Rechtsprechung die Auffassung vertreten, dass hier eine wirtschaftliche Belastung des Arbeitnehmers, die über den Betrag von zwei bis drei Monatsgehältern hinaus geht, nicht mehr mit Treu und Glauben vereinbar ist. Wenn es möglich und branchenüblich ist, das eingetretene Risiko durch eine Versicherung einzugrenzen, neigen manche Arbeitsgerichte dazu, die Haftung des Arbeitnehmers auf den Betrag des bei solchen Versicherungen üblichen Selbstbehaltes zu beschränken. Besteht beispielsweise eine Betriebsunterbrechungsversicherung, die in einigen Branchen durchaus üblich ist und beträgt hier der Selbstbehalt des Arbeitgebers 10.000 Euro, wird in aller Regel eine Haftung des Arbeitnehmers über diesen Betrag hinaus abzulehnen sein. Eine vollständige Haftung des Arbeitnehmers kommt jedoch bei grob fahrlässigem oder gar vorsätzlichem Verhalten in Betracht. Groß fahrlässig handelt derjenige, der die naheliegendsten Überlegungen nicht anstellt und völlig außer Acht lässt, was jeder vernünftig Denkende in der betreffenden Situation berücksichtigt hätte. Gerade hier zeigt sich, wie wichtig es ist, Verhaltensregeln für den Umgang mit Internet und Intranet schriftlich festzulegen. Wenn ein Mitarbeiter gegen eindeutige klare Regelungen verstößt und – zusätzliches Kriterium - trotz einer entsprechenden Schulung/Einweisung nicht in der Lage ist, diesen Anweisungen nachzukommen, wird es einfacher sein, ihm grob fahrlässiges Verhalten nachzuweisen.

In der Rechtsprechung ist bisher lediglich ein Fall zu diesem Komplex entschieden worden, bei dem eindeutig vorsätzliches Verhalten vorlag. Hier ging es um einen Informatiker, dessen Arbeitsvertrag auslaufen sollte. Dieser installierte einen Virus im System, dem die ansonsten zu Wartungsarbeiten herangezogene Softwarefirma hilflos gegenüber stand. Hier wurde dann der betreffende Mitarbeiter zum Ersatz des entstandenen Schadens verurteilt. Abzuwarten bleibt, ob die Gerichte – wie in Aufsätzen zu dem Thema vertreten -, in den Fällen, in denen trotz ausdrücklicher Virenwarnung ein Attachment geöffnet wird, tatsächlich Schadensersatzansprüche des Arbeitgebers bejahen werden. Festzuhalten ist jedenfalls, dass solche arbeitsvertraglichen Schadensersatzansprüche leichter durchsetzbar sind, wenn konkrete Regelungen getroffen werden und hierin auch ganz gezielt bereits auf mögliche Schadensersatzansprüche hingewiesen wird. Dies hat zumindest die erzieherische Wirkung, dass die Arbeitnehmer angesichts des bestehenden Risikos gewissenhafter mit Computer und Internet umgehen werden. Ob diese dann in der Praxis auch tatsächlich durchgesetzt werden, steht dann ja auf einem anderen Blatt.

In einem kleinen Exkurs sei auch darauf hingewiesen, dass Haftungsansprüche nicht nur gegenüber Arbeitnehmern bestehen können, sondern auch gegenüber Geschäftsführern und Vorständen bzw. Aufsichtsräten durchgesetzt werden können. Geschäftsführer und Vorstände haben die Verpflichtung, Schaden von dem durch sie vertretenen Unternehmen abzuwenden. Hierzu gehört auch, dass entsprechende Vorkehrungen getroffen werden, um Vermögensschäden für das Unternehmen durch Betriebsspionage, Datenausfall, Betriebsunterbrechungen und ähnliche Vorfälle zu verhindern. Hier wird man auf jeden Fall verlangen können, dass zumindest durch entsprechende klare Regelungen und Vereinbarungen das Risiko von Datenmissbrauch und Angriffen von außen und innen auf ein vertretbares Maß reduziert wird. Auch Aufsichtsräte trifft eine entsprechende Verpflichtung, die sich aus einer gesteigerten Überwachungspflicht gegenüber dem Vorstand ergibt.

### **3.4. Bruch der Vertraulichkeit/Geheimnisverrat**

Gravierender sind die Folgen, wenn ein Mitarbeiter sich Informationen zu Bereichen im Intranet verschafft, zu denen er keinen Zugang haben dürfte und es sich hierbei um betriebsensible Daten handelt. In einem durch das LAG Schleswig-Holstein entschiedenen Fall hatte sich eine Sekretärin das Passwort ihres Chefs verschafft und sich mit dessen Hilfe in das betriebsinterne Informationssystem eingeloggt und der Führungsebene vorbehalten

Daten zur Kenntnis genommen. Hier hat das LAG eine Kündigung ohne jegliche Abmahnung für gerechtfertigt gehalten. Sicherlich wird man bei einer Interessenabwägung immer zu berücksichtigen haben, welche Informationen sich der betreffende Mitarbeiter auf diesem Wege verschafft hat, generell wird man jedoch dieser Rechtsprechung folgen müssen, schließlich erfolgt die Schaffung von durch Passwörtern geschützten Bereichen nicht ohne sachlichen Grund. Auf jeden Fall empfiehlt es sich hier, sämtliche Mitarbeiter nach § 5 Bundesdatenschutzgesetz auf das Datengeheimnis zu verpflichten: Dies erhöht zum einen die Hemmschwelle für den Arbeitnehmer und erleichtert zum anderen im Falle eines Verstoßes vertragliche Sanktionen. Überdies schreibt das BDSG eine solche Verpflichtung vor.

In einem anderen durch das Verwaltungsgericht Frankfurt/Main entschiedenen Fall wurde die fristlose Kündigung eines Systemadministrators bestätigt: dieser hatte personenbezogene Daten ausgespäht und in einem anderen Zusammenhang verwendet. Glimpflich lief die Sache für einen bayerischen Polizeibeamten ab, der sich über die Polizeidatenbank in mindestens drei Fällen Informationen verschafft hatte, die er dann zu privaten Zwecken verwendet hatte. Hier hatte das Gericht – es ging um die strafrechtliche Verantwortlichkeit – lediglich eine Ordnungswidrigkeit nach dem bayerischen Datenschutzgesetz und keinen strafrechtlichen Tatbestand in Anwendung gebracht. Ob auf die Verurteilung wegen der Ordnungswidrigkeit eine Kündigung gestützt werden konnte, ist leider nicht bekannt geworden.

Etwas anderes gilt in den Fällen, in denen betriebliche Daten auf einem privaten Datenträger überspielt werden. Nach einer Entscheidung des sächsischen Landesarbeitsgerichtes soll dies auf jeden Fall eine fristlose Kündigung rechtfertigen. Ebenfalls eine fristlose Kündigung wurde bei folgendem Sachverhalt für berechtigt angesehen:

Hier hatte ein Bankkassierer unter Verwendung der Geheimnummer eines Anderen das in der Bank bestehende Vier-Augen-Prinzip verletzt und anschließend sogar noch versucht, sein Handeln durch die Vernichtung von Dokumenten zu verschleiern. Bei einem derart gravierenden Fall ist dem Arbeitgeber auf keinen Fall zuzumuten, weiter mit dem Arbeitnehmer zusammenzuarbeiten.

Aus Arbeitgebersicht sollte auf jeden Fall in einer der Regelungen im Arbeitsvertrag bzw. in einer Betriebsvereinbarung festgehalten werden, dass sowohl das Einbringen privater

Datenträger in das Computernetzwerk wie auch das Überspielen geschäftlicher Daten auf private Datenträger ausdrücklich untersagt ist.

### **3.5. Dialer-Programme und Pornoseiten**

Ein Hauptdiskussionspunkt in den letzten Monaten ist die Nutzung von sog. Pornoseiten im Internet oder aber auch – die meist unfreiwillige – Verwendung sog. Dialer-Programme, bei denen der Internetzugang dann über eine 0190-Nummer hergestellt wird. Während es hier zur konkreten Nutzung durch das Internet noch relativ wenige Gerichtsentscheidungen gibt, existiert bereits eine umfangreiche Rechtsprechung zur vergleichbaren Problematik des Telefonsex. In diesem Bereich war die Rechtsprechung eher uneinheitlich, es gab einige Gerichte, die gerade bei erheblichen Kosten der jeweiligen Telefongesellschaft keinen Zahlungsanspruch wegen der Sittenwidrigkeit des hinter dem Telefonvertrages stehenden Vertragsverhältnisses zugesprochen hatten. Hingegen haben andere Gerichte die Auffassung vertreten, dass Telefonverbindungen wertneutral seien und die dahinter stehenden evtl. sittenwidrigen Telefonsexverträge sich auf das Verhältnis des Netzbetreibers zum Kunden nicht auswirken. Dies hat vor allem den Hintergrund, dass es auch eine Reihe seriöser Anbieter gibt, die über 0190-Telefonnummern ihre Kosten vereinnahmen.

Diese Streitfrage hat nun der Bundesgerichtshof durch ein Grundsatzurteil vom 22.11.2001 dahingehend entschieden, dass erhöhte Telefongebühren unabhängig von dem dahinterstehenden Vertrag zu entrichten sind. Diese Rechtsprechung lässt sich auch auf den Internetzugang übertragen, der mittels 0190-Telefonnummern hergestellt wird. Dies bedeutet, dass ein Arbeitnehmer, der sich in ein solches Dialer Programm bewusst einwählt, gegen seine arbeitsvertraglichen Verpflichtungen verstößt und infolgedessen – je nach Schwere des Verstoßes – abgemahnt oder sogar fristlos gekündigt werden kann. Etwas anderes wird dann gelten, wenn sich die Dialer Programme ohne entsprechende Ankündigung quasi selbst installieren und der Arbeitnehmer hierauf keinen Einfluss hat. Hier besteht auch die Möglichkeit, den Vertrag wegen arglistiger Täuschung anzufechten.

Von Interesse ist auch die Frage, wie sich der Besuch von Internetseiten mit pornographischem Inhalt in arbeitsrechtlicher Hinsicht beurteilt. Solange der Besuch dieser Seiten keinen Bezug zur Tätigkeit aufweist, wird im Schrifttum noch überwiegend die Auffassung vertreten, dass es sich hier um ein rein privates Verhalten handle und – solange

weder andere belästigt noch der Arbeitgeber geschädigt wird – arbeitsrechtliche Sanktionen nicht zu befürchten sind. Der Arbeitgeber, der ein solches Verhalten unterbinden will, ist daher gut beraten, entsprechende betriebliche Anweisungen zu erlassen. Wird gegen diese dann verstoßen, kann dies auch arbeitsrechtlich sanktioniert werden.

## **4. Regelungsvorschläge für Datensicherheit und Internetnutzung**

### **4.1. Einzelvertragliche oder betriebliche Regelung?**

Hier stellt sich zunächst die Frage, ob es sinnvoll ist, die Regelungen im Arbeitsvertrag zu treffen oder aber hierzu die Form einer Betriebsvereinbarung zu wählen. Eine arbeitsvertragliche Regelung beinhaltet, dass bei jedem Arbeitsvertrag, der neu eingegangen wird (zweckmäßiger Weise in der Anlage) eine detaillierte Regelung hinsichtlich des Umgangs mit dem Computer, Internetzugang und Internetnutzung getroffen wird. Bei bereits bestehenden Arbeitsverträgen ist diese Zusatzvereinbarung entweder einvernehmlich (Annahme durch den Arbeitnehmer) zu treffen oder aber im Wege der Änderungskündigung durchzusetzen. Dies erfordert – je nach Unternehmensgröße – einen erheblichen Arbeitsaufwand. Zweckmäßiger ist es daher, die Regelung im Rahmen einer Betriebsvereinbarung zu treffen. Dies setzt wiederum voraus, dass ein Betriebsrat vorhanden ist. Sollte ein Betriebsrat nicht existieren, besteht die Möglichkeit, die Regelung im Rahmen einer Betriebs- oder Arbeitsordnung zu treffen, die dann den Arbeitnehmern zur Kenntnis gebracht wird. Zweckmäßiger Weise empfiehlt es sich in diesem Falle, in die jeweiligen Arbeitsverträge den Passus aufzunehmen, dass der Umgang mit Computer und Internet/e-mail-Nutzung durch eine entsprechende Betriebsordnung geregelt wird, die in der jeweiligen Fassung Bestandteil des Arbeitsvertrages ist.

### **4.2. Inhalt der Regelung**

Der Regelungsbereich im Arbeitsvertrag, durch Betriebsordnung oder Betriebsvereinbarung ist weitgehend identisch, so dass diese Punkte einheitlich dargestellt werden sollen. Hinsichtlich der Betriebsvereinbarung ergibt sich lediglich noch die zusätzliche Notwendigkeit, die Dauer der Betriebsvereinbarung und eine Kündigungsmöglichkeit zu regeln.

Im wesentlichen sind folgende Punkte zu nennen:

- **Geltungsbereich**

Hier ist anzugeben, für welche Mitarbeiter und an welchen Unternehmensstandorten die Regelung gelten soll.

- **Nutzung Internet/e-mail**

Hier ist zu regeln, ob auch die private Nutzung gestattet ist. Wenn die private Nutzung gestattet wird, sollten Beschränkungen aufgenommen werden, in welchem zeitlichen Umfang bzw. zu welchen Zeiten (Pausen etc.) die Nutzung zulässig ist. Bei der Internetnutzung/e-mail-Nutzung empfiehlt sich darüber hinaus inhaltliche Beschränkungen vorzunehmen. Denkbar ist beispielsweise folgende Formulierung:

„Das Recht zur Internetnutzung/e-mail-Nutzung darf nicht missbraucht werden. Ein Missbrauch liegt insbesondere dann vor, wenn strafbare, diffamierende, rassistische, gewaltverherrlichende, sexistische oder (bei e-mails) den Empfänger belästigende Inhalte übermittelt werden.“

- **Herunterladen von Dateien/Öffnen von e-mails**

Hier sollte generell festgelegt werden, dass Dateien zu privaten Zwecken nicht heruntergeladen werden dürfen und beim Herunterladen von Dateien zu geschäftlichen Zwecken diese nur von seriösen Seiten heruntergeladen werden dürfen. Ferner empfiehlt sich der Zusatz, dass in Zweifelsfällen vorab über den Netzwerkadministrator oder einen fachlich versierten Mitarbeiter eine Überprüfung vorzunehmen ist. Eine gleiche Regelung sollte für Attachments von e-mails getroffen werden, wenn diese von einem unbekanntem Absender stammen oder sonst zu Misstrauen Anlass geben.

- **Passwort**

Hier empfiehlt sich eine Regelung mit folgenden Punkten:

- Regelmäßiger Wechsel des Passwortes
- Verbot der Weitergabe des Passwortes
- Haftung bei Weitergabe des Passwortes
- Wahl eines Passwortes unter Verwendung von Sonderzeichen
- Sichere Aufbewahrung des Passwortes, insbesondere nicht auf dem Rechner

- **Verwendung fremder Datenträger**

Verbot, geschäftliche Daten auf private Datenträger zu überspielen und Verbot von privaten Datenträgern an Überspielung auf Firmenrechner/Netzwerk ohne vorherige Freigabe durch Netzwerkadministrator vorzunehmen

- **Dokumentation**

Die Verpflichtung, geschäftserhebliche e-mails auszudrucken, sollte ebenfalls geregelt sein.

- **Verschlüsselung**

Die Anordnung, e-mails mit vertraulichem Inhalt oder mit personenbezogenen Daten Dritter nur verschlüsselt zu versenden, empfiehlt sich ebenfalls.

- **Regelung für Abwesenheit**

Eine Regelung, dass bei Urlaubsabwesenheit bzw. plötzlich eintretender Abwesenheit bei dienstlicher Post dafür gesorgt wird, dass diese durch eine andere Person bearbeitet werden kann, sollte ebenfalls getroffen werden. Dies kann durch eine automatische Weiterleitung oder aber durch Einschaltung des Postmasters, dann eine entsprechende Weiterleitung vorzunehmen, erfolgen.

- **e-mail-Kontrolle durch Arbeitgeber/Internetkontrolle durch Arbeitgeber**

Hier sollte eine Regelung getroffen werden, in welchen Fällen des Verdachts eines Missbrauchs der Arbeitgeber berechtigt ist, eingehende e-mails (auch privaten Inhalts) oder Aufzeichnungen über die Internetnutzung auszuwerten.

- **Verpflichtung auf das Bundesdatenschutzgesetz**

Zuletzt sollte jeder Mitarbeiter auf das Datengeheimnis nach § 5 des Bundesdatenschutzgesetzes (Verbot personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen) verpflichtet werden.

## **5. Kontrollmöglichkeiten des Arbeitgebers**

### **5.1. Sinn und Zweck einer Kontrolle**

Aus den USA ist bekannt, dass mittlerweile dort bestimmte Überwachungsprogramme eingesetzt werden, die sämtliche Aktivitäten am Computer aufzeichnen und alle besuchten Internetadressen ebenso festhalten wie die Nutzungszeiten des Computers. Ferner sollen in den USA 27 % aller Unternehmen die e-mails ihrer Beschäftigten systematisch überwachen. Es ist anerkannt, dass der Arbeitgeber das grundsätzliche Recht besitzt, die Erfüllung der Arbeitsaufgaben durch seine Mitarbeiter zu kontrollieren. Fraglich ist lediglich, ob und welcher technischer Mittel man sich hierzu bedienen darf und ob die Herstellung einer totalen Transparenz des Arbeitnehmersverhaltens zulässig ist.

Für eine solche Kontrolle sprechen einige Argumente:

- Die Kosten werden in Grenzen gehalten und eine Systemüberlastung wird verhindert.
- Durch die Überwachung von e-mails kann der Verrat von Geschäftsgeheimnissen auf diesem Wege verhindert werden.
- Es besteht die Möglichkeit, sich gegen Wirtschaftsspionage zu schützen
- Durch die Überwachung der Kommunikation mit Dritten kann korrektes und freundliches Verhalten der Arbeitnehmer gegenüber Kunden überwacht werden.

Es sprechen demzufolge einige Argumente dafür, die Computernutzung zu überwachen.

### **5.2. Zulässigkeit der Kontrolle**

Hieran knüpft die Frage an, ob und in welchem Umfang eine solche Kontrolle zulässig ist.

## **Überblick über die gesetzlichen Regelungen**

Ausgangspunkt ist die Frage, ob das sog. Telekommunikationsgeheimnis gilt. Dieses ist an die Stelle des früheren Fernmeldegeheimnisses getreten. Telekommunikation wird in § 3 Nr. 16 Telekommunikationsgesetz (TKG) als der „technische Vorgang des Aussendens,

Übermitteln und Empfangs von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen“ definiert. In diesem Zusammenhang unterscheidet man im Telekommunikationsrecht drei verschiedene Schichten:

- a) Die erste Schicht betrifft die Technik der Informationsübermittlung, also den Datentransport (hier gilt das Telekommunikationsgesetz [TKG])
- b) Die zweite Ebene betrifft die übermittelten Dienste: hier greift das Teledienstegesetz (TDG) bzw. bei redaktionell bearbeiteten Texten, die der öffentlichen Meinungsbildung dienen sollen, der zwischen den Bundesländern geschlossene Mediendienstestaatsvertrag ein.
- c) In der dritten Schicht geht es um den Inhalt der vermittelten Informationen, hier ist das allgemeine Recht maßgeblich, wie es auch sonst für alle öffentlichen Verlautbarungen (Presse, Rundfunk usw.) gilt.

In datenschutzrechtlicher Hinsicht wird hier differenziert, ob eine dienstliche oder eine private Nutzung vorliegt. Bei einer rein dienstlichen Nutzung gelangt das Teledienstedatenschutzgesetz (TDDSG) nicht zur Anwendung, bei einer privaten Nutzung hingegen ist es in vollem Umfang anzuwenden. Da die Abgrenzung zwischen privater und dienstlicher Nutzung in der Praxis fast nicht durchzuführen ist, besteht eigentlich nur die Möglichkeit, beide Nutzungsarten strikt zu trennen.

## Persönlichkeitsschutz des Mitarbeiters

Soweit bei einer rein dienstlichen Nutzung von Einrichtungen der Telekommunikation das Telekommunikationsgesetz und das Teledienstedatenschutzgesetz nicht eingreifen, wird hier auf allgemeine Grundsätze des Persönlichkeitsschutzes im Arbeitsverhältnis zurückgegriffen. Hier finden sich in der Rechtsprechung und Literatur insbesondere im Hinblick auf die Vertraulichkeit von Telefongesprächen die entsprechenden Grundsätze, die sich auf Internetnutzung bzw. e-mail-Verkehr übertragen lassen:

Hiernach ist ein Mithören (Mitlesen von e-mails, Mitprotokollierung von Internetsurfen) nur dann zulässig, wenn der Eingriff gerechtfertigt ist. Hierfür ist ein überwiegendes schutzwürdiges Interesse des Arbeitgebers erforderlich. Rechtfertigungsgründe werden dann angenommen, wenn der Eingriff nach Inhalt, Form und Begleitumständen erforderlich ist und überdies das schonendste Mittel darstellt. Nach dieser Rechtsprechung wurde beispielsweise

das Mithören von Telefongesprächen in einem Callcenter während der Probezeit als zulässig erachtet, ebenso wurde eine Kontrolle durch versteckte Kameras bei erheblichen Warenverlusten für zulässig erachtet. Sofern lediglich bei Telefongesprächen deren Beginn und Ende, die vertelefontierten Einheiten und die angerufene Nummer festgehalten werden, liegt ein geringerer Eingriff in das Persönlichkeitsrecht des Arbeitnehmers vor. Dieses wird als zulässig erachtet. Diese Rechtsprechung lässt sich auf e-mails ohne weiteres übertragen, eine Kontrolle wie Zeitpunkt der Absendung und angeschriebene Adresse wird dem Arbeitgeber zugestanden, eine inhaltliche Kenntnisnahme nur bei ganz überwiegenden Arbeitgeberbelangen (z.B. begründeter Verdacht für strafbare Handlungen). Zu beachten ist in diesem Zusammenhang, dass aber durch entsprechende Betriebsvereinbarung oder arbeitsvertragliche Regelung das Fernmeldegeheimnis abbedungen und weitergehende Überwachungsmöglichkeiten eingeräumt werden können.

## Kontrolle bei privater Nutzung

Bei unerlaubter privater Mitnutzung finden das Telekommunikationsgesetz und das Teledienstschutzgesetz keine Anwendung. Dann ist lediglich das Bundesdatenschutzgesetz maßgeblich. Hier wird überwiegend die Auffassung vertreten, dass in diesen Fällen dann die äußeren Verbindungsdaten (Zeit, Internetadressen, e-mail-Adressen) zur Kenntnis genommen werden dürfen, eine Erhebung weiterer Daten jedoch unzulässig ist. Aber auch hier gilt, dass dann, wenn eine entsprechende Einwilligung des Arbeitnehmers erteilt ist, auch eine weitergehende Überwachung möglich ist.

Bei erlaubter privater Nutzung ist der Arbeitgeber hingegen zur Wahrung des Fernmeldegeheimnisses verpflichtet. D.h: er darf in der Regel nur die zur Abrechnung erforderlichen Daten und evtl. Daten zur Störungsbeseitigung erheben und verwenden.

# 2. Teil

## Datenschutz im Internet

### **1. Einführung in die Problematik**

Das Internet schafft neue Kommunikationsstrukturen, die einen neuen Wirtschaftszweig entstehen ließen. Durch das Internet sind zahlreiche neue Produkte und Marketingstrukturen entwickelt worden. Wenn auch die noch vor zwei Jahren vorhandene Euphorie einer gewissen Ernüchterung Platz gemacht hat, ist doch in zahlreichen Branchen das Netz zum unverzichtbaren Vertriebsweg geworden. Die E-Mail ist heute fast so selbstverständlich wie Telefon oder Fax.

Durch diese neue digitale Kommunikation entstehen aber auch Gefahren für die einzelnen Nutzer, die nach meiner Überzeugung noch viel zu sehr vernachlässigt werden.

Das Internet ist eine offene Plattform. Informationen, die im Netz versendet werden, sind für eine breite Öffentlichkeit zugänglich. Dies gilt nicht nur für Informationen, die auch zur Veröffentlichung bestimmt sind, sondern grundsätzlich auch für E-Mails. Sie müssen sich vergegenwärtigen, dass eine E-Mail allenfalls die Vertraulichkeit einer Postkarte genießt.

Diese Offenheit des Netzes steht in einem Konfliktverhältnis zum Datenschutz.

Viele Nutzer sind sich nicht der Möglichkeiten der Informationsgewinnung bewusst, die eine Kommunikation im Netz mit sich bringt. Wer im Netz surft, hinterlässt Spuren. Beim Besuch einer Web-Site wird die IP-Adresse des verwendeten Rechners bekannt. Ihr Access-Provider erfährt, welche Sites Sie besucht haben. Auf vielen Servern werden Protokolle erstellt, die neben Zugriffszeiten und Browsertyp auch festhalten, welche Vorlieben ein Surfer hat. Es ist durch die Verknüpfung solcher Informationen möglich, ein umfassendes Persönlichkeitsprofil des Nutzers zu erstellen.

Weiterhin ist festzustellen, dass auch die Nutzer des Netzes selbst, insbesondere im Bereich der E-Mail-Kommunikation nicht mit der gebotenen Sensibilität bei der Übertragung von Daten umgehen. Immer wieder kommt es vor, dass personenbezogene Informationen

ungeschützt und unverschlüsselt im Netz verschickt werden. Aus meiner Praxis ist mir folgender Fall bekannt: Ein Software-Unternehmen A vertreibt eine Buchhaltungssoftware, in der auch insbesondere die Lohnbuchhaltung integriert ist. Das Unternehmen B hat diese Software erworben und anfangs ein paar Probleme damit. Der Techniker des Unternehmens B rief daraufhin die Hotline von A an. Dort verabredete man, dass B per E-Mail das gesamte Programm einschließlich der Daten der Firma A zuschickt. Ohne jeden Skrupel wurden die Daten der Mitarbeiter über Familienstand, Einkommen, Adresse, Kontonummer, Krankheitstage usw. durch das Netz geschickt. Niemand weiß, auf welchen Datenbanken diese Informationen mittlerweile gespeichert sind.

## 2. Rechtliche Grundlagen

Dass dies nicht mit dem Leitbild des Datenschutzes übereinstimmt, ist offensichtlich. Das Bundesverfassungsgericht hat bereits in seinem Mikrozensus-Beschluss 1969 festgestellt, dass es mit der Menschenwürde nicht vereinbar ist, wenn der Staat für sich in Anspruch nehme, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren.<sup>1</sup>

Im Volkszählungsurteil vom 15.12.1983 hat das BVerfG aus der allgemeinen Handlungsfreiheit des Art.2 GG ein Recht auf informationelle Selbstbestimmung abgeleitet. Im Zeitalter der automatisierten Datenverarbeitung gäbe es kein belangloses Datum mehr, jedes personenbezogene Datum stehe unter dem Schutz des Grundgesetzes.<sup>2</sup>

Dabei ist der Datenschutz nicht nur ein hehres Ziel, bei dem es gilt, Orwellschen Schreckensvisionen vorzubeugen, sondern auch eine wirtschaftliche Notwendigkeit.

Umfragen belegen, dass viele Internet-Nutzer angeben, bei einer Inanspruchnahme des Netzes in ihrer Privatsphäre beeinträchtigt zu sein. Der damit verbundene Vertrauensverlust droht zu einem echten Hindernis für die Durchsetzung von E-Commerce zu werden. Es liegt deshalb auch im Interesse der im Netz agierenden Unternehmen, den Datenverkehr sicherer zu gestalten.

---

<sup>1</sup> BVerfG 27, 1

<sup>2</sup> BVerfG 65, 1; NJW 1984, 419 #

Man darf im World Wide Web die Möglichkeiten staatlicher Reglementierung nicht überbewerten. Dies würde seinem grenzenlosen Charakter aber auch dem Leitbild einer freiheitlichen Gesellschaftsordnung widersprechen. Allerdings stellt der Staat Leitlinien auf, die den Ausbau einer elektronischen Datenverkehrsordnung beschleunigen sollen.

Ausgehend von diesem Leitbild haben Bund und Länder bereits in den siebziger Jahren Datenschutzgesetze erlassen, die die Verarbeitung personenbezogener Daten mit einer strengen Zweckbindung verknüpfen. Der Datenschutz lässt sich kurz gesagt auf den Nenner bringen, dass die Verarbeitung von Daten nur dann erlaubt ist, wenn entweder ein bestimmter Zweck die Verarbeitung rechtfertigt oder der Betroffene in die Verarbeitung einwilligt.

Diese Gesetze wurden in den letzten 30 Jahren natürlich etliche Male reformiert und im Internetzeitalter durch spezialgesetzliche Regelungen ergänzt.

Über die Entscheidungen des BVerfG hinausgehend wenden sich diese Gesetze nicht nur an staatliche Stellen, sondern an jeden, der Daten erhebt und verarbeitet.

Nach der Legaldefinition des § 3 BDSG sind personenbezogen solche Daten, durch die eine Person eindeutig zu identifizieren ist. Da sind insbesondere natürlich die sog. Bestimmungsdaten wie Name, Anschrift, Sozialversicherungsnummer, Ausweis-, Konto-, Telefonnummer, KfZ-Kennzeichen.

Daneben gibt es aber eine Menge an Daten, durch die die Person zwar nicht bestimmt, aber bestimmbar ist. So kann über die IP-Adresse, mit der sich Ihr Computer im Netz anmeldet, auch im System der flexiblen IP-Adressenvergabe eine Identifizierung des Nutzers möglich. Werden solche Daten in sog. Log-Protokollen verknüpft, ist eine umfangreiche Auswertung des Nutzungsverhaltens möglich.

Das jeweils für den Datenschutz anzuwendende Recht orientiert sich nach dem sog. Schichtenmodell und ist von der Anwendungsebene abhängig. Man unterscheidet zwischen

Datentransport	—————▶	Telekommunikationsrecht ( TKG, TDSV)
Interaktion	—————▶	Online-Recht (TDDSG, MDStV)
Inhaltsebene	—————▶	Offline Recht (BDSG, allgemeine Regeln)

### 3. Teledienststedatenschutzgesetz (TDDSG)

Wir wollen uns hier ein wenig näher den Vorgaben des Teledienststedatenschutzgesetzes (TDDSG) widmen, das den Umgang mit personenbezogenen Daten im interaktiven Bereich, also z. B. beim Online-Banking oder im E-Commerce regelt.

Nach dem TDDSG bestehen zunächst folgende Informationspflichten des Diensteanbieters:

- Unterrichtung des Nutzers über die Verarbeitung von personenbezogenen Daten
- Identifizierung der für die Datenverarbeitung verantwortlichen Stelle
- Informationen über Weitervermittlung

Die Erhebung, Verarbeitung und Nutzung von Daten ist von der Art der Daten abhängig.

Man unterscheidet:

- Bestandsdaten
- Nutzungsdaten
- Abrechnungsdaten

Bestandsdaten sind solche, die für die Begründung eines Vertragsverhältnisses zwingend erforderlich sind, also Namen, Adresse, Bankverbindung usw.

Daraus folgt, dass die Verarbeitung von Bestandsdaten grundsätzlich auch ein Vertragsverhältnis zwischen dem Nutzer und der verarbeitenden Stelle voraussetzt. Dies wiederum bedingt die Unzulässigkeit der Datenverarbeitung zu Werbezwecken, der Übermittlung an Dritte und die Aufnahme in ein öffentliches Verzeichnis ohne die Einwilligung des Betroffenen.

Die Erhebung von Daten, die für das Vertragsverhältnis nicht notwendig ist, ist grundsätzlich unzulässig, wenn der Betroffene nicht einwilligt.

Nutzungsdaten geben Auskunft darüber, welche Web Sites der Benutzer aufgesucht hat . Nutzungsdaten können eine erhebliche Aussagekraft über den Nutzer erzeugen, insbesondere, wenn sie verknüpft werden. Die Verarbeitung dieser Daten ist grundsätzlich nur erlaubt, wenn sie zur

- Ermöglichung der Inanspruchnahme
- Abrechnung
- Missbrauchsaufklärung

notwendig ist oder der Betroffene einwilligt.

Eine Verarbeitung von Daten ist nur gestattet, wenn dies eine Rechtsvorschrift vorsieht oder wenn der Betroffene in die DV ausdrücklich schriftlich einwilligt. Dabei ist der Betroffene auf den genauen Zweck der Erhebung, Verarbeitung oder Nutzung hinzuweisen.

Zusammenfassend bleibt deshalb festzustellen, dass durch den Dienstanbieter nur solche Daten gesammelt und verarbeitet werden dürfen, die dem Zweck der Nutzung entsprechen oder in deren Verarbeitung der Nutzer eingewilligt hat. Dabei gilt das sog. Kopplungsverbot, das dem Anbieter untersagt, das Erbringen der Leistung von einer ansonsten unzulässigen Datenverarbeitung abhängig zu machen.

#### **4. Datenschutz beim E-Commerce**

Wachsende Bedeutung im Geschäftsleben hat der Handel im Internet. Dabei stellt sich insbesondere die Frage des Vertrauens zwischen Anbietern und Kunden. Umfragen belegen, dass Verbraucher durchaus bereit wären, mehr Bestellungen über das Internet aufzugeben, aber davor aus Sorge über den Umgang mit ihren Daten Abstand nehmen.

Grundsätzlich können Verträge auch über das Internet geschlossen werden. Willenserklärungen können auch per E-Mail oder per Mausklick abgegeben werden.

Um einen sicheren Vertragsschluss zu gewährleisten sind

- Authentizität
- Integrität
- Vertraulichkeit

zu gewährleisten.

Authentizität bedeutet, dass derjenige, der als Absender einer Nachricht auftritt, diese auch tatsächlich selbst abgesendet hat.

Integrität bedeutet, dass die Nachricht auch ohne Veränderung übermittelt wird.

Vertraulichkeit heißt in diesem Zusammenhang, dass die Nachricht auch nur von demjenigen geöffnet und gelesen werden kann, für den sie auch tatsächlich bestimmt ist.

Diese Kriterien werden in durch die Verwendung von kryptographischen Systemen erfüllt. In der Praxis wird dabei sehr häufig auf das Protokoll SSL zugegriffen, bei dem der Nutzer durch Überprüfung eines digitalen Zertifikates des Anbieters dessen Authentizität feststellen kann. Dadurch kann der Nutzer sicherstellen, dass er mit der richtigen Adresse verbunden ist, allerdings nicht umgekehrt. Außerdem hat er keine Kontrolle darüber, was mit seinen Daten nach der Übersendung geschieht.

Für beide Seiten sicherer ist deshalb das System der asymmetrischen Schlüssel. Dieses funktioniert in der Weise, dass für die Verschlüsselung und die Entschlüsselung unterschiedliche Schlüssel verwendet werden. Das wohl bekannteste System der asymmetrischen Schlüssel ist PGP, das für den privaten Gebrauch kostenlos im Internet downzuladen ist.

Dieses System funktioniert in der Weise, dass dem Empfänger zunächst ein sog. öffentlicher Schlüssel zugeschickt wird. Danach wird die Erklärung, mit dem sog. Privaten Schlüssel des Absenders verschlüsselt und versandt. Der Empfänger ist dann in der Lage, mit dem öffentlichen Schlüssel diese Erklärung zu öffnen. Allerdings kann man mit dem öffentlichen Schlüssel nicht auf den privaten schließen. Es ist also gewährleistet, dass die verschlüsselten Erklärungen mit dem privaten Schlüssel des Absenders versandt wurden. Sie ist die Urheberschaft des Absenders nachzuweisen.

Auf dem gleichen Grundprinzip basiert die digitale Verschlüsselung bzw. Signatur. Der Gesetzgeber hat mit dem Erlass des Signaturgesetzes und entsprechender Anpassung des Bürgerlichen Gesetzbuches die Möglichkeit geschaffen, mit der sog. elektronischen Form die vom Gesetz an zahlreichen Stellen geforderte Schriftform zu ersetzen. So kann etwa eine Bürgschaft oder ein Schuldanerkenntnis auch in digitaler Form abgegeben werden.

Dabei werden die Verschlüsselungssysteme auf einer Smart-Card installiert. Diese werden von zertifizierten Ausgabestellen vertrieben, die wiederum strengen Sicherheitsanforderungen entsprechen müssen.

Die Verwendung dieser Karte ist abhängig von der Kenntnis einer PIN. Erklärungen, die unter

Verwendung der digitalen Signatur abgegeben werden, sind letztlich auch dem Vertragspartner in gerichtsverwertbarer Weise zuzurechnen.

Leider haben sich die Möglichkeiten der digitalen Verschlüsselung nach dem Signaturgesetz nicht in dem Maße durchgesetzt wie dies zu erwarten gewesen wäre. Ich bin jedoch davon überzeugt, dass mit der wachsenden Bedeutung der Willenserklärung im Netz auch die digitale Signatur wichtiger wird. Dies wäre im Interesse einer sicheren Kommunikation und des Datenschutzes und damit auch der Sicherheit des Datenaustausches überhaupt dringend zu wünschen.

Vervielfältigung und Wiedergabe – auch auszugsweise- nur mit Zustimmung der Verfasser

Wir weisen ferner darauf hin, dass wir den Vortrag nach bestem Wissen erstellt haben, aber für die inhaltliche Richtigkeit keine Gewähr übernehmen können