Persönliche Verantwortung und Haftungsrisiken von IT-Verantwortlichen – Strafrechtliche Aspekte

Jürgen Wessing

Lehrbeauftragter für Strafprozeßrecht an der Heinrich-Heine-Universität Düsseldorf
Kanzlei Wessing II Verjans
Königsallee 74, 40212 Düsseldorf

1 Präambel

Die Nutzung von Computern, Internet und E-Mail im Geschäftsleben hat in den letzten Jahren rasant zugenommen. Der Einsatz dieser Informationssysteme geht einher mit der Vernetzung der Datenverarbeitung in den Betrieben. Waren in der Vergangenheit nur einzelne betriebliche Funktionen, wie Buchführung oder Gehaltsabrechnung in ein EDV-System integriert, verfügen heute zahlreiche Arbeitnehmer eines Unternehmens über einen an ein Netzwerk angeschlossenen Computer am Arbeitsplatz. Zumeist besitzt dieser durch das Internet auch Kontaktmöglichkeiten über den unternehmensinternen Bereich hinaus. Die explosive Entwicklung wirft nicht nur eine Vielzahl technischer, sondern auch rechtlicher Fragen auf. In den vergangenen Jahren wurden zahlreiche Rechtsvorschriften erlassen, die unmittelbare Handlungspflichten und Haftungsvoraussetzungen für den Bereich des Datenschutzes, der Datenverarbeitung und Datenübertragung festlegen. Diese Normen finden sich über die verschiedensten Gesetze verstreut und sind untereinander zum Teil disharmonisch. Die Neuigkeit des Rechtsgebietes und der zu regelnde hochkomplexe technische Hintergrund, der zudem noch ständig in Bewegung ist, begründet und entschuldigt zugleich die inhomogene Regelung des neuen Bereiches. Auch deshalb ist nur den Wenigsten der Umfang der strafrechtlichen Verantwortung bekannt, die den Einzelnen im EDV-Wesen treffen kann. In Unternehmen liegen aufgrund Arbeitsteilung und Delegation unterschiedliche Verantwortlichkeiten vor, da das Strafrecht an Pflichtenstellungen ansetzt, ist es von besonderer Wichtigkeit, zu wissen, wer sich und weshalb einer Strafdrohung ausgesetzt sieht.

Anliegen dieses Vortrages ist es angesichts des zeitlichen Rahmens nicht, eine umfassende Abhandlung des Computerstrafrechts zu geben, sondern ihr Gespür dafür zu entwickeln, welche Vorgehensweisen in der täglichen Arbeit eines IT-Verantwortlichen zu einer strafrechtlichen Verantwortung führen können, wo die Fallstricke liegen.

Die hier interessierende Frage der Gefährdung von mit Datenverarbeitung beschäftigten Personen wird deshalb in der Folge nur angerissen werden können. Es hat sich zu dem gesamten Bereich eine hoch kasuistische Rechtssprechung entwickelt, die neben den weit verteilten und zum Teil auch juristisch sehr zerklüfteten Vorschriften zu beachten ist. Ein Vortrag dieser Art kann keine Detailkenntnisse in umfassender Form vermitteln, er soll wesentliche Punkte beleuchten und ein Grund(problem)verständnis schaffen.

2 Persönliche Verantwortung und Haftungsrisiken von IT-Verantwortlichen

Um die persönliche Verantwortung und die Haftungsrisiken für Sie greifbar zu machen, müssen Begrifflichkeiten geklärt werden. Im Anschluß daran erfahren Sie einiges über Grundlagen und Aufbau des deutschen Strafrechtes ehe ich Sie mit ausgewählten konkreten Verantwortlichkeiten und Strafbarkeitsgefahren vertraut machen will.

2.1 Der Begriff des IT-Verantwortlichen

Wer „IT-Verantwortlicher“ ist, läßt sich nicht anhand einer Checkliste bestimmen. Der Begriff ist ebenso wie die Funktion – wie so vieles in dem jungen Bereich des EDV-Rechtes – neu und noch ohne eindeutige gesetzliche Kontur, es gibt keine verbindliche gesetzliche Definition. IT-Verantwortliche sind, im Sinne einer negativen Abgrenzung, jedenfalls nicht die großen kommerziellen Access-Provider oder Internet-Service-Provider (AOL, Compuserve, T-Online), welche in der öffentlichen Diskussion hauptsächlich wahrgenommen werden. Die eben Genannten sind Firmen, also juristische Personen, und können deshalb nach unserem Rechtsverständnis strafrechtliche Schuld persönlich gar nicht tragen. Sie können deshalb auch nicht IT-Verantwortliche im Sinne des Strafrechtes sein. IT-Verantwortlicher – auch im Sinne dieses Vortrages – ist notwendigerweise eine natürliche Person.

Mangels einer gesetzlichen Umschreibung muß ich hier versuchen, eine den weiteren Konsens wiedergebende Definition anzubieten: Danach ist IT-Verantwortlicher derjenige,

> der nach Vertrag, Funktion, Stellung oder tatsächlichen Möglichkeiten dafür einzustehen hat, daß Daten gespeichert, übertragen, verarbeitet, verändert oder die technischen Voraussetzungen hierfür geschaffen werden.

Diese Umschreibung auf das Wirtschaftsleben angewendet zeigt, daß im täglichen Umgang mit dem Medium Computer sowohl Unternehmensinhaber, Systemadministratoren, EDV-Betreuer oder – eingeschränkt – Datenschutzbeauftragte persönlich in strafrechtlicher Verantwortung stehen können.

2.1.1 Verantwortlichkeit nach innen

Als grobe Unterscheidung der wesentlichen Strafbarkeitsfelder kann die Verantwortungsrichtung dienen. Verantwortlichkeit nach innen liegt dann vor, wenn Rechtsgüter entweder des Unternehmens selbst oder von Mitarbeitern des Unternehmens strafrechtlich geschützt sind. Zumeist handelt es sich bei den in Frage kommenden Vorschriften um solche des allgemeinen Strafrechtes. Das sind diejenigen Vorschriften die sich im Strafgesetzbuch (StGB) finden. Sie werden als Kernstrafrecht bezeichnet und sind zu großen Teilen nicht klassisch computerbezogen, wenn auch einige Vorschriften des Strafgesetzbuches in der letzten Zeit der neuen Entwicklung angepaßt wurden. Zu benennen sind dabei insbesondere:

- § 202a StGB – Ausspähen von Daten
- § 263a StGB – Computerbetrug

- § 269 StGB – Fälschung beweiserheblicher Daten
- § 274 Abs. 2 StGB – Elektronische Urkundenunterdrückung
- § 303a StGB – Datenveränderung
- § 303b StGB – Computersabotage

Neue Regelungsstrukturen des Strafrechtes stellen diese Vorschriften nicht dar, der Gesetzgeber hat mit Ihnen bereits seit langem geregelte „normale“ Straftatbestände an die technische Entwicklung anpassen wollen.

2.1.2 Verantwortlichkeit nach außen

Die strafbewehrten Pflichten eines IT-Verantwortlichen nach außen werden meist durch Normen des sogenannten Nebenstrafrechtes geregelt. Diese Vorschriften finden sich überwiegend in für den Bereich des EDV-Wesens speziell erlassenen Gesetzen wieder. Sie sind im allgemeinen Annex zu den in letzter Zeit vielfach neu geschaffenen und wieder geänderten Spezialgesetzen zur Regelung neuer Formen der Datenverarbeitung und elektronischer Kommunikation. Die wesentlichsten Gesetze in diesem Bereich sind:

- BDSG = Bundesdatenschutzgesetz
- MDStV = Mediendienste-Staatsvertrag
- TDDSG = Teledienste-Datenschutzgesetz
- TDSV = Telekommunikations-Datenschutzverordnung
- TDG = Teledienstgesetz
- TKG = Telekommunikationsgesetz

Die Strafvorschriften und Regelungen von Ordnungswidrigkeiten innerhalb dieser Gesetze sind zumeist so aufgebaut, daß sie auf andere Regelungen des Gesetzes verweisen und deren Mißachtung unter Strafe stellen. Die klassische Formulierung lautet „Wer entgegen… wird mit… bestraft“. Hinter „entgegen“ findet sich dann eine im Gesetz vorher definierte Vorschrift. Bei der Kompliziertheit der Regelungen und den zugrunde liegenden unendlich komplexen technischen Vorgängen fragt sich der Strafrechtler, ob das verfassungsrechtliche Gebot der Bestimmtheit aller Strafnormen noch eingehalten ist.

2.2 Die strafrechtliche Verantwortlichkeit im Allgemeinen

In der Folge sollen sie – weil zum Verständnis notwendig – mit einigen wesentlichen Grundlagen strafrechtlichen Denkens bekannt gemacht werden, um die Ansatzpunkte der Strafbarkeit im Allgemeinen kennenzulernen. Unser Rechtssystem kennt den sogenannten „materiellen“ Teil des Strafrechtes (das Strafgesetzbuch und die Strafvorschriften innerhalb der Nebengesetze), daneben gibt es den prozessualen Teil (im Wesentlichen die Strafprozeßordnung). Das materielle Strafrecht regelt, was verboten ist, welche Verhaltensweisen mit einer Sanktion belegt werden sollen. Aus dem Prozeßrecht ergibt sich, unabhängig von den einzelnen Tatbeständen, ob es überhaupt zu einem Strafverfahren und damit einer Verurteilung kommen kann und auf welchem Wege eine Entscheidung, sei es eine Einstellung oder ein freisprechendes oder verurteilendes Urteil gefunden werden kann.

2.2.1 Täterschaft und Teilnahme

Im Strafrecht gilt der Grundsatz der Eigenverantwortlichkeit der Person (daß Unternehmen als Rechtspersonen grundsätzlich nicht Gegenstand des Strafrechtes sind, wurde bereits gesagt). Der Grund für eine Strafbarkeit liegt darin, daß eine Person als Täter eine Straftat selbst, durch einen anderen oder zusammen mit einem anderen begeht (vgl. § 25 StGB). Selbst – als Alleintäter – erfüllt eine Person den Tatbestand eines Strafgesetzes, wenn sie vollständig und ohne Beteiligung eines anderen handelt. Wer eine Straftat „durch einen anderen begeht", ist ein sogenannter mittelbarer Täter. Diese Konstellation zeichnet sich dadurch aus, daß ein anderer vom Täter quasi als Werkzeug benutzt wird. Der Täter gestaltet dabei im Hintergrund das Tatgeschehen kraft überlegenen Wissens oder Willens, wohingegen das Werkzeug, auch Tatmittler genannt, oftmals gutgläubig ist, also gar nicht weiß, daß es gerade ein Delikt begeht. Ein solcher „Täter hinter dem Täter" ist auch derjenige, der durch Organisationsstrukturen bestimmte Rahmenbedingungen ausnutzt und durch regelhafte Abläufe andere Personen zur angestrebten Tatbestandsverwirklichung führt. Entwickelt wurde diese sogenannte „Täterschaft kraft Tatherrschaft" für organisatorische Machtapparate, doch hat die Rechtsprechung schon länger anerkannt, daß diese Grundsätze auch für unternehmerische Betätigungen gelten. Sind an einer Tat Mehrere beteiligt und verwirklichen sie einen gemeinsamen Tatplan arbeitsteilig, liegt Mittäterschaft vor. Voraussetzung ist, daß die Mittäter jeweils an der Ausübung der Tatherrschaft – im Planungs-, Organisations- oder Ausführungsstadium – beteiligt sind. Zwar erfüllen Mittäter nicht alle Tatbestandsmerkmale in ihrer eigenen Person, jedoch werden ihnen die Tatbeiträge ihrer Tatgenossen wie eigene zugerechnet.

Neben der Täterstrafbarkeit gibt es in unserem Strafrechtssystem auch eine Verantwortung des Teilnehmers: Gelingt es einer Person, in einem anderen den Entschluß zur Begehung einer Straftat hervorzurufen, ist er ein sogenannter Anstifter (§ 26 StGB). Dieses Hervorrufen des Tatentschlusses kann durch Überreden, Anregen oder die Erteilung eines Rates[1] geschehen, aber auch durch Drohung oder eine Täuschung. Der Anstifter wird grundsätzlich wie ein Täter bestraft. Daneben macht sich strafbar, wer als Teilnehmer an einer fremden Straftat dem Täter in körperlicher oder physischer Hinsicht vorsätzlich Hilfe leistet (§ 27 StGB) und so die Handlung oder den Erfolgseintritt erleichtert[2]. Dafür ist jede Förderung der Haupttat ausreichend. Die Rechtsprechung geht sogar so weit, eine so genannte psychische Beihilfe zu kennen. Diese soll dann gegeben sein, wenn der Täter sich durch die innere und äußere Zustimmung des Beihelfers in seinem Tun bestätigt fühlen kann, so daß eine Beihilfe auch dann in Frage kommt, wenn die Tat ohne den Zuspruch des Gehilfen gleichermaßen begangen worden wäre. Eine Strafbarkeit wegen Teilnahme ist ohne eine rechtswidrige Haupttat nicht möglich – im juristischen Fachjargon heißt dies „Akzessorietät". Da das Unrecht des Teilnehmers weniger schwer wiegt, als eine Täterschaft, wird eine Teilnahme milder bestraft.

All diese Differenzierungen entfallen, wenn es sich um Ordnungswidrigkeiten handelt, dort gilt der sogenannte „Einheitstäterbegriff", der alle Handlungsformen des Strafrechtes vereint.

[1] Tröndle/Fischer § 26 Rn. 4

[2] Tröndle/Fischer § 27 Rn. 2 m.w.N., Rn. 2c

2.2.2 Strafbarkeit durch aktives Tun oder Unterlassen

Die Strafbarkeit des Einzelnen setzt ein bestimmtes Verhalten voraus. Das Gesetz kennt aktives Tun oder Unterlassen einer rechtlich gebotenen Handlung. Nun ist schon nach allgemeinem Verständnis Handeln eben nicht dasselbe wie „etwas nicht tun“. Um als Anknüpfungspunkt für Strafbarkeit zu dienen, muß das Unterlassen die gleiche rechtliche Qualität wie ein Handeln haben. Deshalb ist Voraussetzung für eine Strafbarkeit des Unterlassenden, daß er rechtlich dafür einzustehen hat, daß der strafrechtlich relevante Erfolg nicht eintritt. Er muß eine so genannte Garantenstellung innehaben. Diese Garantenstellung fliegt einem nicht zu, sondern sie entsteht aus dem Gesetz, vertraglichen Vereinbarungen und bestimmten Verhaltensweisen. Im Rahmen der sich aus dieser Garantenstellung ergebenden Pflichten wird zwischen Beschützergaranten und Überwachergaranten unterschieden. Den Beschützergaranten obliegen die Obhutspflichten für ein bestimmtes Rechtsgut, für dessen Bestand und Sicherheit sie zu sorgen haben. Der Überwachergarant ist für bestimmte Gefahrenquellen verantwortlich, ihn treffen aufgrund dessen Sicherungspflichten gegenüber jedermann. Hierzu gehören die allgemeine Verkehrssicherungspflicht, die Pflicht zur Beaufsichtigung Dritter sowie die Garantenstellung aus pflichtwidrigem gefährdendem Vorverhalten. Soweit durch eine ungenügende Ausfüllung einer dieser Pflichten ein Verletzungserfolg entsteht, resultiert daraus eine Unterlassenstrafbarkeit.

2.2.3 Organe, Vertreter und Beauftragte im Sinne des § 14 StGB, § 9 OWiG

Da unser Strafrecht von dem Gedanken geprägt ist, daß Pflichtenstellungen Verantwortlichkeiten auslösen, andererseits aber juristische Personen – GmbH's, AG's, Vereine und andere – Träger von Pflichten sein, jedoch nicht bestraft werden können, mußte eine Transfernorm geschaffen werden. Das Strafrecht enthält in § 14 StGB eine Vorschrift, die die strafrechtliche Verantwortung von Firmen und Körperschaften, ganz allgemein: die Verantwortung von juristischen Personen, auf deren vertretungsberechtigte Personen und Beauftragte erweitert. Im Ordnungswidrigkeitenrecht existiert die Parallelvorschrift des § 9 OWiG. Werden im delegierten Verantwortungsbereich Straftaten begangen, so machen die nun verantwortlichen Personen sich selbst strafbar. Sowohl die Delegation von Verantwortungsbereichen als auch von Einzelaufgaben auf einen Dritten begründet die strafrechtliche Haftung für die korrekte Erfüllung beziehungsweise Durchführung der zu erledigenden Tätigkeit. Dies gilt auch, wenn ein externer EDV-Berater mit der System- und Netzwerkpflege betraut wird. Mit der Erfüllung dieser Aufgabe wird er in Pflichten des Unternehmens eingebunden, ihm wird die Verantwortung auch in strafrechtlicher Hinsicht für diesen Pflichtenkreis übertragen – er wird in unserem Sinn IT-Verantwortlicher.

Organe von Gesellschaften – Geschäftsführer, Vorstände – sind kraft ihrer Organstellung in der Verantwortung ihrer Gesellschaften. Dabei ist es völlig ohne Bedeutung, ob die Anstellungsverträge arbeitsrechtlich wirksam geschlossen sind oder nicht – der registerrechtliche Eintritt in die Organstellung reicht aus, um die Pflichtenstellung über § 14 StGB zu gründen. Vom Gesetzgeber nicht vorgesehen, aber von der Rechtsprechung erkannt wurde, daß die Steuerung von Gesellschaften tatsächlich auch erfolgen kann, ohne daß die steuernde Personen die Stellung eines im Gesetz vorgesehenen Organs innehat. Die Rechtssprechung

hat dazu die Rechtsfigur des sogenannten „faktischen Geschäftsführers“ entwickelt. Wer sich also in einem bestimmten Gebiet, welches einem Organ vorbehalten ist, „breit macht“ und letztlich das eigentliche Organ verdrängt, tritt in dessen Pflichtenstellung ein. Umgesetzt auf die IT-Verantwortung bedeutet dies, daß jede Person in Organverantwortung einer juristischen Person jedenfalls IT-Verantwortlicher ist. Alle Verpflichtungen, die das Gesetz der juristischen Person auferlegt, sind von ihm bei Meidung von Strafbarkeit zu erfüllen. Neben den Organverantwortlichen gibt es die vertretungsberechtigten Gesellschafter, die ebenso behandelt werden.

Weiter von Bedeutung ist der zweite Absatz des § 14 StGB, wonach derjenige, der Aufgaben wahrnimmt, die eigentlich dem Inhaber eines Unternehmens obliegen, ebenso behandelt wird, wie der Inhaber selbst. Die Vorschrift ist das Einfallstor strafrechtlicher Verantwortung für alle Personen, denen von den eigentlich Verpflichteten Verantwortung zugewiesen wurde. Eine Einschränkung existiert: Es muß sich um betriebsbezogene Aufgaben handeln, zudem muß der Auftrag ausdrücklich vorliegen, eine faktische Betriebsleiterschaft oder Vertreterschaft gibt es im strafrechtlichen Sinne nicht.

Aus der gesetzlichen Regelung des § 14 Abs. 2 StGB wird gleichzeitig deutlich, daß Verantwortung auch delegiert werden kann. In einer arbeitsteiligen Wirtschaft ist dies nicht anders denkbar. Mit der Delegation der Aufgabe wird ein Teil der in der Aufgabe liegenden Pflichten mit übergeben. Allerdings auch nur ein Teil, eine Restverantwortung aus der Position des Unternehmensleiters ist nicht delegierbar. Überwachungs- und Kontrollpflichten bleiben in der Unternehmensspitze grundsätzlich immer.

2.3 Die persönliche Verantwortung des IT-Verantwortlichen

Die individuelle Verantwortlichkeit eines mit EDV-Aufgaben im Unternehmen Befaßten richtet sich mithin einerseits nach seiner gesellschaftsrechtlichen Position, andererseits nach seiner vertraglichen Aufgabe. Nicht jeder im IT-Bereich Tätige ist schon deshalb strafrechtlich verpflichtet, sondern nur derjenige Mitarbeiter, Betriebs- oder Behördenangehörige, der originär und ausdrücklich Leitungsaufgaben im IT-Bereich übertragen erhalten hat. Diese Aufgaben kann er wieder unterübertragen, diese Subdelegation muß aber genauso ausdrücklich geschehen. Wer schlicht im IT-Bereich tätig ist, ist nicht IT-Verantwortlicher, auch wenn ihn Strafbarkeiten treffen können, die sich aus allgemeinen Grundsätzen ergeben. Auch externe, nicht dem Unternehmen angehörige Personen können IT-Verantwortliche sein, wenn sie vertraglich die Aufgaben eines IT-Verantwortlichen übernommen haben.

2.3.1 Delegation von Führungsverantwortung

Unternehmen aber auch Behörden sollten so organisiert sein, daß möglichst eine effiziente Arbeitsteilung und Dezentralisierung gesichert sind. Die Führung umfaßt nicht nur die Besorgung bestimmter Geschäfte, sondern die verantwortliche Leitung in ihrer Gesamtheit. Damit trifft die Unternehmensführung, so sie zur Steuerung oder Kommunikation oder Werbung EDV einsetzt, automatisch auch eine IT-Verantwortlichkeit. Die kraft der Führungsverantwortung anfallenden Aufgaben müssen aber nicht in eigener Person wahrgenommen werden. Sie können auf andere Personen delegiert werden. Da der Delegierende

damit nicht mehr in der Lage ist, alle Ge- und Verbote selbst einzuhalten, muß er kraft seiner Organisationsgewalt sicherstellen, daß durch die zur Erledigung berufenen Personen die Verhaltensanforderungen erfüllt werden. Dies gilt auch für die IT-Verantwortlichkeit. Die Anforderungen beginnen mit der Auswahl der Personen, auf die Verantwortlichkeit übertragen werden soll. Es muß darauf geachtet werden, daß der zukünftige Mitarbeiter – oder auch der in eine neue Verantwortungsposition versetzte Mitarbeiter – dafür auch geeignet ist. Das bedeutet, daß im Rahmen der Stellenausschreibung eindeutig festgelegt sein muß, welche Aufgaben zu erfüllen sind und diese mit dem Leistungsprofil verglichen werden müssen. Damit ist es allerdings nicht für alle Zeiten getan, der Unternehmensleiter muß überprüfen, ob die Aufgaben auch tatsächlich korrekt erfüllt werden. Erst wenn dies geschehen ist, kann man bezüglich der delegierten Aufgaben von strafrechtlicher Risikofreiheit ausgehen. Wenn sich allerdings im laufenden Betrieb Zweifel hinsichtlich des normgemäßen Verhaltens der Untergebenen aufdrängen, kann nicht bis zum nächsten turnusmäßigen Überprüfungstermin gewartet werden. Der Organverantwortliche muß dann sofort und unmittelbar handeln, da in Krisenzeiten die volle Verantwortung wieder an die Führungspersonen fällt.

In Krisen- und Ausnahmesituationen, in denen das Unternehmen als Ganzes betroffen ist, gilt der Grundsatz der Generalverantwortung und Allzuständigkeit der Geschäftsleitung. Die delegierte Verantwortung fällt zurück. Ein Führungsverantwortlicher hat in der Krise alles ihm Mögliche und Zumutbare zu tun, um den drohenden Schaden abzuwenden[3]. Unabhängig von einer Krise gilt eine gesteigerte Verantwortung bei der Auswahl und Überwachung, wenn mit der zu besetzenden Stelle ein erhöhtes Gefährdungspotential für die öffentliche Sicherheit verbunden ist.

Der Gedanke der Führungsverantwortung findet sich auch in den allgemeinen Bußgeldtatbeständen des Ordnungswidrigkeitenrechtes wieder. Danach handelt ordnungswidrig, wer als Inhaber eines Betriebes oder Unternehmens seine Aufsichtspflichten verletzt (§ 130 OWiG). Die Verantwortlichkeit des Betriebsinhabers wird insoweit über das reine Handeln ergänzt. Über die Erweiterung der Verantwortlichkeit auf Vertreter und Beauftragte (§ 9 OWiG) trifft die Verpflichtung zur Bußgeldzahlung auch den IT-Verantwortlichen, der nicht gleichzeitig Betriebsinhaber ist.

2.3.2 Handlungsverantwortung

Handelt ein IT-Verantwortlicher selbst, trifft ihn dafür die persönliche Verantwortung nach den allgemeinen Vorschriften. In dem hier interessierenden Bereich handelt es sich so weitaus überwiegend um Strafnormen, die nur vorsätzlich begehbar sind. Der Täter muß Wissen und Wollen was er tut. Fahrlässigkeitsstrafbarkeiten interessieren also weniger, soweit es diesen Vortrag angeht. Eine Beurteilung des strafrechtlich relevanten Handelns findet nach den Ihnen bereits nähergebrachten Tatbeteiligungsformen der Täterschaft (§ 25 StGB) und Teilnahme (§§ 26, 27 StGB) statt.

In all diesen Handlungsformen kann auch der IT-Verantwortliche sich strafbar machen.

[3] BGH NStZ 1990, 587 – Lederspray-Entscheidung (Erdal); BGH NStZ 1993, 488 – Mauerschützen-Fall

2.3.3 Die besondere Stellung des Datenschutzbeauftragten

Nicht unerwähnt bleiben darf bei der Bestimmung der persönlichen Verantwortlichkeiten die besondere Stellung des Datenschutzbeauftragten. Die ihm gesetzlich zugewiesene Rolle rechtfertigt eine andere Beurteilung seiner Funktion. Kennzeichen der Tätigkeit des Datenschutzbeauftragten ist, daß ihm weder Leitungs- noch ausführende Funktionen zustehen. In seiner Funktion nimmt er Aufgaben wahr, die vor allem im öffentlichen Interesse liegen. Er befindet sich damit außerhalb der Verantwortungstragung im Unternehmen – vorausgesetzt ihm wurden nicht arbeitsvertraglich Leitungsfunktionen zugewiesen – was vermieden werden sollte. Da dem Beauftragten lediglich die Aufsicht über den ordnungsgemäßen Umgang mit den personenbezogenen Daten der Mitarbeiter und die Einhaltung der datenschutzrechtlichen Vorschriften obliegt, resultieren aus seiner Stellung im Unternehmen für ihn persönlich keine Strafbarkeitsrisiken, wenn andere Gesetze des EDV-Wesens verletzt werden.

2.4 Mögliche Strafbarkeitsrisiken

Die Strafbarkeitsrisiken für einen IT-Verantwortlichen bilden die verschiedenen Nutzungsmöglichkeiten eines EDV-Systems ab. Bei der Netzwerkpflege und Überwachung stellen sich andere Problematiken und Anforderungen, als bei der Darstellung des Unternehmens in der Öffentlichkeit oder der Kommunikation auf elektronischem Wege. Sie sollen in der nötigen Kürze dargestellt werden.

2.4.1 Verantwortung in lokalen Firmennetzen

Unternehmen und Behörden haben ihre Computerarbeitsplätze meist innerhalb einer geschossenen Benutzergruppe vernetzt (Corporate Networks). Die Unterschiedlichkeiten in Art und Weise des Aufbaues und des Betreibens können strafrechtliche Unterschiede erheblichen Ausmaßes hervorrufen. Die Gesetzgebung hat kein einheitliches Regelwerk geschaffen, wie mit und in Netzen zu verfahren ist, vielmehr finden sich Strafnormen mit Netzbezug in vielen Gesetzen verstreut, häufig als Annex .

Verantwortungsunterschiede durch unterschiedliche Strukturen von lokalen Firmennetzen

Je nach dem, ob den Mitarbeitern auch eine private Nutzung des Netzzugangs gestattet ist, wird das Unternehmen bereits als Anbieter von Telekommunikationsdiensten, Telediensten oder Mediendiensten eingeordnet. Daran knüpfen sich rechtliche Konsequenzen.

Die Einordnung eines lokalen Firmennetzes in die unterschiedlichen Dienstearten orientiert sich an der Konzeption der erbrachten Netz-„Dienstleistung“. Spezielle Normen des Nebenstrafrechts legen durch sogenannte Legaldefinitionen, sprich rechtlich verbindliche Umschreibungen, fest, welche bestimmten Voraussetzungen erfüllt sein müssen, damit eine Netzleistung in den Anwendungsbereich des jeweiligen Gesetzes fällt.

- § 3 Nr. 24 TKG
  normiert den Begriff des Telekommunikationsdienstes und bestimmt ganz allgemein, daß darunter die Übertragung von Signalen über Telekommunikationsnetze zu verstehen ist. Daß dies – wie die Vorschrift formuliert – „in der Regel“ gegen Entgelt erfolgt, bedeutet gerade nicht, daß dies zwingend vorausgesetzt wird.
- § 2 Abs. 1 TDG
  legt den Geltungsbereich des Teledienstgesetzes fest und bezeichnet als Teledienste alle elektronischen Kommunikations- und Informationsdienste zur individuellen Nutzung.
- § 2 Abs. 1 MDStV
  beschreibt Mediendienste als an die Allgemeinheit gerichtete Informations- und Kommunikationsdienste

Allgemein gesprochen richten sich *Mediendienste* also in ihrer Ausgestaltung an eine Vielzahl von Adressaten, bei ihnen steht in Anlehnung an den Rundfunk das Senden im Vordergrund. *Telekommunikations- und Teledienste* dienen in erster Linie der individuellen Interaktion und Kommunikation. Daß diese Abgrenzung nicht trennscharf ist und den rechtlichen Charakter des zu betrachtenden Netzwerkes nicht unbedingt klarer werden läßt, zeigt bereits die Tatsache, daß der einzelne Nutzer technisch gesehen immer individuell kommuniziert – auch beim Aufrufen einer bestimmten Seite und des Herunterladens ihres Inhaltes in den Arbeitsspeicher. Da die Haftungsbestimmungen der in Rede stehenden Gesetze weitgehend inhaltsgleich sind, ist es an dieser Stelle jedoch nicht notwendig, diese juristischen Feinheiten weiter zu vertiefen.

Nicht nur die Art eines Dienstes ist entscheidend für die Frage, ob ein Gesetz Anwendung findet. Auch der Erbringer des Netzdienstes muß die jeweiligen gesetzlich beschriebenen Eigenschaften haben, um als Diensteanbieter qualifiziert zu werden.

- § 3 Nr. 6 TKG
  bezeichnet einen Diensteanbieter als jemanden, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt.
- § 2 Nr. 2 TDSV
  enthält neben einer beispielhaften Aufzählung eine ähnlich allgemeine Definition für den Begriff des Diensteanbieters.
- § 3 Nr. 1 TDG
  will als Diensteanbieter die natürlichen und juristischen (also GmbH's, AG's etc.) Personen erfassen, die Teledienste zur Verfügung stellen oder den Zugang dazu vermitteln.
- § 2 Nr. 1 TDDSG
  ist inhaltsgleich mit dem Begriff des Diensteanbieters im Teledienstegesetz.
- § 3 Nr. 1 MDStV
  bestimmt für den Bereich der Mediendienste, daß Diensteanbieter jede natürliche oder juristische Person ist, die eigene oder fremde Mediendienste zur Nutzung bereithält oder den Zugang dazu vermittelt.

Die Eigenschaft, Diensteanbieter zu sein, kann sich für ein Unternehmen oder eine Behörde nur ergeben, wenn sie „geschäftsmäßig“ Netzdienste erbringen. Dies darf hier nicht als Teilnahme am geschäftlichen Leben, also Betreiben eines Geschäftes verstanden werden. Die Geschäftsmäßigkeit als Abgrenzungskriterium orientiert sich vielmehr daran, ob das lokale Netzwerk und die Verbindung „nach draußen“ zum Internet den Mitarbeitern auch für den privaten Gebrauch zur Verfügung gestellt wird. Ist das private Surfen und Mailen untersagt, ist das lokale Netzwerk nur aus eigenem Unternehmensinteresse eingerichtet. Dem Unternehmer ist in diesem Fall nicht daran gelegen, einem Anderen einen Netzzugang zur Verfügung zu stellen. Vielmehr möchte er nur den betrieblichen Ablauf des Geschäftsalltags technisch optimieren – um selbst einen Nutzen davon zu haben. Bei untersagter privater und lediglich erlaubter dienstlicher Nutzung bleibt das Unternehmen selbst alleiniger Nutzer und unterfällt damit nicht den Regeln der angesprochenen Normwerke.

Materielle Strafnormen des Netzbetreibers – Datenschutz

Die rechtlichen Konsequenzen und Verpflichtungen, die sich für ein Unternehmen aus der Qualifizierung als Anbieter von Telekommunikations-, Tele- oder Mediendiensten ergeben, sind in den jeweiligen Spezialgesetzen genau beschrieben. Es würde zu weit führen, und ist auch nicht Sinn dieses Vortrages, die umfangreichen Tatbestandskataloge in ihren Einzelheiten darzustellen, so daß ich mich darauf beschränke, einen Überblick zu geben:

- Das Telekommunikationsgesetz (TKG) regelt den Umgang mit der Telekommunikationsinfrastruktur und legt die den Diensteanbieter gegenüber der Regulierungsbehörde für Telekommunikation treffenden Verpflichtungen fest. Die Behörde ihrerseits achtet darauf, daß die Interessen der Nutzer gewahrt, der Wettbewerb der Telekommunikation und die öffentliche Sicherheit gewährleistet sind.
- Die Telekommunikations-Datenschutzverordnung (TDSV), das Teledienst-Datenschutzgesetz (TDDSG) und der Staatsvertrag über Mediendienste (MDStV) stellen umfassende Datenschutzbestimmungen auf, die den Umgang mit den personenbezogenen Daten der Nutzer bei der Erhebung, Verarbeitung und Nutzung ihrer Daten durch den Diensteanbieter regeln.

Als nicht EDV-spezifischer Regelungskomplex schützt das Bundesdatenschutzgesetz (BDSG) den Einzelnen davor, daß er durch den Umgang Dritter mit seinen persönlichen Daten – insbesondere auch beim Einsatz von Datenverarbeitungsanlagen – in seinem Persönlichkeitsrecht verletzt wird. Wegen der spezifischen Fähigkeiten von elektronischer Datenverarbeitung ist der IT-Verantwortliche regelmäßig in der Gefahr, Datenschutzverletzungen zu begehen.

Damit der Netzbetreiber angehalten wird, die auferlegten Verpflichtungen zu erfüllen, finden sich in den jeweiligen Gesetzen eigene materielle Strafnormen in Form von Bußgeld- und Strafkatalogen, die Versäumnisse diesbezüglich ahnden[4].

Art und Höhe der Sanktion variieren je nach verletzter Verhaltenspflicht beziehungsweise Norm. Die Spannbreite der Strafen reicht dabei von Geldbußen für Ordnungswidrigkeiten,

[4] §§ 148, 149 TKG, § 9 TDDSG, § 17 TDSV, § 24 MDStV, §§, 44 BDSG

die bis zu € 500.000,– betragen können, sowie Geld- und bis zu zweijährigen Freiheitsstrafen bei Erfüllung eines Straftatbestandes.

2.4.2 Rechtswidrige IT-Nutzung durch Mitarbeiter

Eine den Mitarbeitern eingeräumte technische Möglichkeit, auf unzählige Internetseiten zugreifen zu können, birgt auch für den IT-Verantwortlichen strafrechtliche Risiken. Im weltweiten Netz gibt es vielfache Gelegenheiten, sich strafbare Inhalte zu verschaffen. Der Zugriff beispielsweise auf (kinder-)pornographische und volksverhetzende Internetseiten oder die Speicherung solcher Informationen durch die Beschäftigten kann auch für den IT-Verantwortlichen zum „Problem“ werden, denn das Kernstrafrecht und ganz besonders die EDV-spezifischen Gesetze des Nebenstrafrechts enthalten eine Vielzahl von Haftungs- und Zurechnungsregeln. Dabei hat der Gesetzgeber in den strafrechtlichen Nebengesetzen vielfach für Diensteanbieter„Erleichterungen“ im Vergleich zum allgemeinen Strafrecht geschaffen, die die technischen Möglichkeiten und den begrenzten zumutbaren Aufwand für eine inhaltliche Kontrolle der Daten bei der Frage nach der strafrechtlichen Verantwortung berücksichtigen – unjuristisch: wer Diensteanbieter ist, haftet nur eingeschränkt strafrechtlich für Fehlverhalten Dritter.

Spezialgesetzliche Zurechnung an den IT-Verantwortlichen als Diensteanbieter

Das TDG und der MDStV enthalten ein besonderes Haftungssystem, das eine abgestufte Verantwortlichkeit, je nach tatsächlichem Verantwortungs- und Einflußbereich, für den Anbieter von Tele- oder Mediendiensten vorsieht, Unterschieden wird dabei grundsätzlich zwischen eigenen Informationen des Dienstanbieters, die er zur Nutzung bereithält, und fremden Informationen.

Die Verantwortlichkeit für eigene Inhalte ergibt sich aus den „allgemeinen Gesetzen“ (so bestimmt in: § 6 Abs. 1 MDStV, § 8 Abs. 1 TDG), also aus dem Strafgesetzbuch und den Nebengesetzen. Für fremde Informationen, die der Anbieter zur Nutzung bereithält oder die in seinem Kommunikationsnetz übermittelt werden, ist der IT-Verantworliche nur dann verantwortlich:

- wenn er die Übermittlung veranlaßt hat,
- wenn er den Adressaten ausgewählt
- und wenn er die übermittelten Informationen ausgewählt oder verändert hat.

Ausnahme: Der Diensteanbieter ist voll verantwortlich, wenn er mit dem Nutzer – also dem Mitarbeiter – absichtlich zusammen arbeitet, um rechtswidrige Handlungen zu begehen (§ 7 Abs. 1 S. 2 MDStV, § 9 Abs. 1 S. 2 TDG), eine Gesetz gewordene Selbstverständlichkeit.

Werden fremde Informationen auf dem Server des Diensteanbieters gespeichert, ist dieser grundsätzlich nur verantwortlich, wenn er von deren Inhalt Kenntnis hat und nicht unverzüglich nach Kenntniserlangung die rechtswidrigen Informationen entfernt oder sperrt. Diese Haftungsfreistellung, die sicherstellen soll, daß Provider nur als Mittler anzusehen

sind und von einer Inanspruchnahme verschont bleiben, findet aber auf Corporate Networks in Unternehmen ausdrücklich keine Anwendung. Dort ist der Mitarbeiter als Nutzer nämlich dem Unternehmer als Diensteanbieter unterstellt oder wird von ihm beaufsichtigt (§ 9 S. 2 MDStV, § 11 S. 2 TDG). Den Unternehmer trifft die Verantwortung in solch einem Fall nach den allgemeinen Vorschriften des Strafrechts, ohne sich auf diese Privilegierungen – die eine Strafbarkeit nur bei konkretem Wissen vorsehen – berufen zu können.

Zurechnung nach den allgemeinen Vorschriften

Erfüllt das Unternehmen oder eine Behörde nicht die Eigenschaft eines Diensteanbieters im dargestellten Sinn, kommt eine Zurechnung von strafrechtlich relevantem Verhaltens der Mitarbeiter nur nach den allgemeinen Strafvorschriften in Betracht. Die einzelnen Erscheinungsformen von Täterschaft und Teilnahme sowie die Arten strafbaren Verhaltens in Form von Tun oder Unterlassen kennen Sie bereits vom Beginn meiner Ausführungen.

Die bloße Bereitstellung des Netzzugangs macht den IT-Verantwortlichen nicht zum Mittäter (§ 25 Abs. 2 StGB) wenn der Mitarbeiter die technische Infrastruktur zum Aufrufen strafbarer Netzinhalte nutzt. Es liegt kein bewußtes und gewolltes arbeitsteiliges Zusammenwirken vor. Es fehlt auch die sog. Tatherrschaft, da über den Einwahlknotenpunkt das Abrufen bestimmter Inhalte technisch nicht verhindert werden kann. Der IT-Verantwortliche hat keine Einwirkungsmöglichkeit auf die Datenspeicher, die die strafbaren Inhalte bereithalten. Es wäre zwar denkbar, daß die technischen Möglichkeiten beim Mitarbeiter erst den Entschluß zum Abrufen der strafbaren Inhalte wecken, von einer Anstiftung (§ 26 StGB) kann dennoch nicht gesprochen werden.

Eine Beihilfe (§ 27 StGB) scheidet aus, wenn der Unternehmer nicht weiß und nicht will, daß ein Mitarbeiter sich die entsprechenden Inhalte verschafft. Ein Nachweis eines Gehilfenvorsatzes ist nur denkbar, wenn der Unternehmer konkrete Anhaltspunkte dafür hatte oder es gebilligt hätte, daß über das Netzwerk des Betriebes strafbare Inhalte abgerufen werden. Eine Garantenpflicht, die eine Unterlassenstrafbarkeit begründet, weil der Netzzugang aufrechterhalten wurde, besteht nicht[5]. Die strafrechtliche Gefahr geht hier nicht von der technischen Infrastruktur des Einwahlknotenpunkts aus, sondern von den abrufbaren Inhalten[6].

Anders ist die Rechtslage, wenn ein Arbeitnehmer strafbare Inhalte auf dem Server des Unternehmens speichert. Der IT-Verantwortliche hat nun die technischen Möglichkeiten, den Datenspeicher auf strafbare Inhalte zu kontrollieren. Ihm kommt auf Grund seiner Leitungsfunktion eine Erfolgsabwendungspflicht zu und damit auch Verantwortung für die Verhinderung strafbaren Verhaltens. Aufgrund seiner Weisungsbefugnis und der Sachherrschaft über den Server als „Gefahrenquelle“ beherrscht der IT-Verantwortliche das Geschehen. Die Menge der zu kontrollierenden Daten schließt eine strafrechtliche Verantwortung nicht aus[7]. Zwar müssen nicht alle Daten geprüft werden, jedoch solche, die Anlaß zur Prüfung geben, weil der Inhalt möglicherweise strafbar ist.

[5] LG München, NJW 2000, 1051 (allerdings ohne Begründung)

[6] MüKo-Freund § 13 Rn. 148

[7] Vassilaki, NStZ 2000, 535, 536 mit Hinweis auf BVerfGE 77, 356ff

Die bisherigen Entscheidungen zu dieser Problematik betrafen nur kommerzielle Provider[8], mit den diesbezüglichen Fragen im Unternehmen scheint sich die Rechtsprechung noch nicht beschäftigt zu haben, so daß die weitere Entwicklung abzuwarten bleibt.

2.4.3 Datenmanipulation

IT-Verantwortliche haben – meist arbeitsvertraglich festgeschrieben – den Bestand der Daten sicherzustellen und diese vor einem Zugriff von „außen“ zu schützen. Dafür stehen vielfältige technische Lösungen (Firewalls, Virenprogramme etc.) zur Verfügung, die alle ein Charakteristikum in sich vereinen: Sie bieten – und damit erzähle ich Ihnen nichts Neues – im Zuge der rasanten Entwicklung des Computerwesens nur zuverlässig Schutz, wenn sie auf dem aktuellsten Stand in puncto Technik und Software sind. Andernfalls besteht in verstärktem Maß die Gefahr der Infiltration des unternehmenseigenen Netzwerkes durch Viren, Trojaner, Dialer oder andere schädliche Programme.

Auch das Strafrecht trägt dem Interesse an einem unversehrten Datenbestand Rechnung und zieht denjenigen strafrechtlich zur Verantwortung, der rechtswidrig Daten löscht, unterdrückt oder unbrauchbar macht (§ 303 a StGB). Selbstredend wird nicht jede Umgestaltung von Daten durch das Strafrecht erfaßt, da andernfalls die Datenverarbeitung per se inkriminiert wäre. Das Gesetz trifft allerdings keine weitere Präzisierung, da es keine Angaben darüber macht, wem die Daten zugeordnet sein müssen. Jedenfalls ist die Veränderung eigener Daten damit nicht gemeint. Im Bereich der Frage, wann Daten „fremd“ sind, ist ebenfalls viel unausgegoren, für die Beurteilung wird teilweise auf das Eigentum am Datenträger oder die Vornahme der Speicherung abgestellt. Daneben muß die Datenveränderung „rechtswidrig“ sein. Dies läßt sich wohl am ehesten als „unbefugt“ umschreiben. Die Unternehmensdaten sind aber für den IT-Verantwortlichen fremde Daten, den Unternehmer einmal ausgenommen.

Sie sehen, hier sind eindeutige Differenzierungen schwierig. Aufgrund der dargestellten Ungenauigkeiten bei der Anwendung der Vorschrift gibt es deshalb nicht wenige Strafrechtler – mich eingeschlossen – die daran zweifeln, ob die Norm dem verfassungsrechtlichen Bestimmtheitsgrundsatz gerecht wird.

Ungeachtet dieser Unsicherheiten liegt ein „Verändern“ dann vor, wenn gespeicherte Daten inhaltlich umgestaltet werden oder bereits bestehenden Dateien oder Programmen weitere Daten hinzugefügt werden. Ob die Gebrauchstauglichkeit der Daten dabei gemindert wird, ist unerheblich, so daß auch Dialer-Programme, wo eine zusätzliche DFÜ-Verbindung errichtet und statt der bisher verwendeten Standardverbindung zum Zugang in das Internet genutzt wird, dem strafrechtlich relevanten Bereich unterfallen.

Wesentlich verschärft ist die strafrechtliche Haftung, wenn die Datenverarbeitungsanlage eines fremden Betriebes oder fremden Unternehmens betroffen ist (§ 303b StGB). Das Haftungsrisiko besteht nicht nur für Personen, die nicht dem Unternehmen angehören und lediglich vertraglich die Aufgaben eines IT-Verantwortlichen übernommen haben, wie die

[8] LG München, NJW 2000, 1051 – Compuserve; Generalbundesanwalt, NJW-CoR 1998, 154 – „Radikal“

Formulierung „fremder Betrieb“ beziehungsweise „fremdes Unternehmen“ vermuten läßt. Die Fremdheit ist im Rahmen der Vorschrift wirtschaftlich zu verstehen. Entscheidend ist, wem der Betrieb oder das Unternehmen gehört, wessen Geld „drin steckt“. Damit ist ein Betrieb oder Unternehmen nicht nur für einen Außenstehenden fremd, sondern auch für Betriebs- und Unternehmensangehörige.

Das Delikt kann nicht nur durch aktives Handeln verwirklicht werden: Der IT-Verantwortliche hat, da er für Bestand und Sicherheit der Daten zu sorgen hat, eine Garantenstellung inne. Er hat also rechtlich dafür einzustehen, daß ein bestimmter „Erfolg“ nicht eintritt, was ihn zum potentiellen „Unterlassungstäter“ macht. Nimmt er nicht regelmäßige Updates der Sicherheitssoftware vor und kommt es dadurch zu einer Datenmanipulation, trifft ihn eine Unterlassensstrafbarkeit (§ 13 StGB). Strafbar ist er allerdings nur unter der Voraussetzung, daß er vorsätzlich gehandelt hat. Unterläßt er es wissentlich, sich zu vergewissern ob neue Sicherheits-Updates erhältlich sind und diese gegebenenfalls zu installieren, nimmt er zumindest billigend in Kauf, daß es zu einem Verletzungserfolg kommt. Diesen sogenannten bedingten Vorsatz läßt die Rechtsprechung für eine Strafbarkeit genügen. : Die rechtswidrige Datenveränderung wird mit bis zu zwei Jahren Freiheitsentzug bestraft.

Ist die Datenverarbeitung für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung, kann ein Fall der Computersabotage vorliegen (§ 303b Abs. 1 Nr. 1 StGB). Für den IT-Verantwortlichen hat dies einschneidende Folgen. Die Strafandrohung in diesem Fall ist mit bis zu fünf Jahren Freiheitsstrafe deutlich erhöht.

Einmal mehr muß ich als Strafrechtler an dieser Stelle meine Bedenken anbringen, ob mit der Norm der strafrechtliche Bestimmtheitsgrundsatz gewahrt bleibt. Bei der heutigen zentralen Bedeutung der Datenverarbeitung wird eine Vielzahl von Handlungsweisen erfaßt, für welche die Strafdrohung der Vorschrift mehr als überzogen erscheint. Zwar ist eine Verfolgung der Tat grundsätzlich von einem Strafantrag des Betriebseigentümers abhängig, aber die Staatsanwaltschaft kann von sich aus einschreiten, sollte sie es aufgrund eines besonderen öffentlichen Interesses für geboten halten.

2.4.4 Strafbarkeit bei der Überwachung von E-Mail-Nutzung und Internetzugang

Die im Rahmen meiner Ausführungen bereits aufgezeigte mögliche strafrechtliche (Mit-)Verantwortung des IT-Verantwortlichen für eine rechtsmißbräuchliche Verwendung des IT-Zugangs durch den Nutzer macht es für Unternehmen und Behörden erforderlich, sicherheitsstrategische Überlegungen anzustellen, wie dieses Risiko vermieden werden kann. Die Palette der technisch zur Verfügung stehenden Möglichkeiten reicht dabei vom einfachen Virenprogramm über Firewalls bis zu komplexen Filterlösungen, bei denen aufgerufene Seiten mit Datums- oder Zeitangaben festgehalten werden. Was technisch möglich ist, ist allerdings nicht automatisch rechtlich zulässig. Das Strafgesetzbuch setzt hier Grenzen. Umfang und Zulässigkeit der Maßnahmen sind dabei wiederum davon abhängig, ob den Nutzern auch eine private oder nur dienstliche Verwendung des E-Mail-Systems und des Internetzugangs eingeräumt wurde. Im Zusammenhang mit einer erlaubten privaten Verwendung des Netzes wird der Nutzer – wie schon erwähnt – durch das Fernmeldegeheimnis geschützt. Dieses wird durch die Strafnorm des § 206 StGB abgesichert,

die zum einen die unbefugte Mitteilung von dem Fernmeldegesetz unterliegenden Tatsachen, zum anderen das Unterdrücken von Sendungen sanktioniert. Erfaßt werden davon alle an Dritte gerichtete E-Mails, nicht nur während des Übermittlungsvorgangs, sondern auch nach der Speicherung auf dem Mailserver. Daten – aufgrund ihrer informationstechnologischen Struktur auch E-Mails – erfahren darüber hinaus durch § 202a StGB einen strafrechtlichen Schutz vor unbefugter Einsichtnahme.

Installation von Spam-Filtern

Unternehmen werden von ungewollter E-Mail-Werbung in zunehmendem Maße überschwemmt. Um diesem Übel Herr zu werden, ist der Einsatz von Spam-Filtern ein technisch probates Mittel. Werden die Nachrichten ausgefiltert, ohne daß der Adressat (Mitarbeiter) darauf Einfluß nehmen kann, besteht für den IT-Verantwortlichen die Gefahr, sich wegen der Verletzung des Fernmeldegeheimnisses (§ 206 Abs. 2 Nr. 2 StGB) verantworten zu müssen. Danach ist es strafbar, durch technische Eingriffe „unbefugt“ in den Vorgang des Aussendens, Übermittelns oder Empfangens von Nachrichten einzugreifen und zu verhindern, daß die E-Mail ihr Ziel vollständig oder überhaupt erreicht.

Ob der Eingriff ohne Befugnis erfolgt, ist für die Frage der Strafbarkeit entscheidend. Eine Befugnis fehlt grundsätzlich, wenn kein Einverständnis des Betroffenen vorliegt. Dessen Einwilligung kann nur im Vorfeld eingeholt werden, eine nachträgliche Genehmigung ist bedeutungslos. Die Erteilung des Einverständnisses kann über eine Betriebsvereinbarung erreicht werden, zu welcher der Betriebsrat seine Zustimmung erteilen muß (§ 87 Abs. 1 Nr. 6 BetrVG). In Unternehmen ohne Betriebsrat bedarf es Einzelvereinbarungen mit den Mitarbeitern.

Fehlt die Einwilligung des Mitarbeiters, darf diese nicht ohne weiteres unterstellt werden. Es ist davon auszugehen, daß der Mitarbeiter daran interessiert ist, alle an ihn adressierten E-Mails zu erhalten. Nur in Ausnahmefällen darf der IT-Verantwortliche ein Einverständnis voraussetzen. Eine solche sogenannte mutmaßliche Einwilligung läßt das Strafrecht gelten, wenn eine Handlung im Interesse des Betroffenen erfolgt und dieser vermutlich einwilligen würde, aber nicht rechtzeitig – also im Voraus – einwilligen kann. Wegen der Schäden, die eine virenverseuchte E-Mail anrichten kann, darf deshalb angenommen werden, daß der Mitarbeiter sein Einverständnis zur Filterung dieser Mail erteilt hätte.

Liegen weder ein ausdrückliches noch ein mutmaßliches Einverständnis vor, können E-Mails nur ausgefiltert werden, wenn ein sogenannter – im Strafgesetzbuch oder einem Gesetzeswerk des Nebenstrafrechts ausdrücklich geregelter – Rechtfertigungsgrund vorliegt. Die Rechtsordnung sieht dann bei eigentlich strafbaren Handlungen von einer Sanktion ab, wenn die Straftat begangen wurde, um ein anderes Rechtsgut vor Schaden zu bewahren, das in der konkreten Situation schützenswerter ist.

Gesondert beurteilt werden muß der Einsatz eines Spam-Filters, wenn unerwünschte E-Mails bereits anhand der IP-Adresse des Absenders erkannt und blockiert werden, bevor die eingehenden Daten auf dem Mailserver gespeichert werden. Bei der Verwendung derartiger sogenannter „Blacklists“ sollen die geschützten Interessen des Empfängers nicht berührt sein, da die bloße Adressierung einer E-Mail noch kein Recht an ihren Daten

begründet. Auch der Absender soll nicht in seinem Recht an der Unversehrtheit der Daten verletzt sein: Spam-Mails werden ohne oder gegen den Willen des Eigentümers einer Datenverarbeitungsanlage an diese übertragen. Sie unterliegen deshalb dem alleinigen Verfügungsrecht des Eigentümers des Speichermediums[9]. Dies sind zugegebener Maßen juristische Feinheiten und aufgrund der schnell fortschreitenden technischen Entwicklung, mit der die rechtliche Fortschreibung der Thematik naturgemäß nicht Schritt halten kann, nicht verbindlich. Gleichwohl wollte ich diesen Gedanken nicht unerwähnt lassen.

Zur Minimierung des Strafbarkeitsrisikos bietet sich – neben der Einholung eines Einverständnisses der Mitarbeiter zur Löschung – eine „Quarantäne"-Lösung an. E-Mails, die im Verdacht stehen, Spam-Inhalte aufzuweisen oder virenverseucht zu sein, sollten außerhalb der Mailboxen in „externen" Ordnern abgespeichert werden. Dem ursprünglichen Empfänger wird dann – ebenfalls per E-Mail – lediglich mitgeteilt, wo er die an ihn adressierte verdächtige E-Mail einsehen kann. Anschließend entscheidet dieser selbst, ob er die Nachricht löschen oder abrufen möchte (OLG Karlsruhe, Beschl. v. 10.01.2005, 1 Ws 152/04). Eine aus meiner Sicht wenig praktikable Lösung.

Kenntnis der Einloggdaten und Zugriffsmöglichkeit auf Mailboxen

Die automatisierte Erfassung von Verbindungs- und Inhaltsdaten, auch und gerade in Erfüllung von Überwachungsaufgaben ermöglicht dem IT-Verantwortlichen die Zuordnung dieser Daten zu einer bestimmten Person. Dabei ist für ihn erkennbar, welchen Inhalt (beispiellsweise bei E-Mails) diese Daten verkörpern. Der IT-Verantwortliche gelangt somit an Informationen, die eigentlich nicht für ihn bestimmt sind. Das Sich-Verschaffen von Daten, sanktioniert grundsätzlich § 202a StGB. Teilt der IT-Verantwortliche die aus der Überwachung gewonnenen Informationen dem Unternehmensinhaber mit, ist wiederum das Fernmeldegeheimnis – wie Sie bereits wissen ist dieses durch § 206 StGB geschützt – tangiert.

Ein Blick auf den Wortlaut der Norm des § 202a StGB zeigt, daß die betreffende Person sich die Daten unbefugt verschaffen muß. Was „unbefugt" bedeutet, haben Sie heute im Rahmen dieses Vortrages schon erfahren. Darüber hinaus fordert das Gesetz eine besondere Sicherung gegen unberechtigten Zugang. Eine solche Sicherung liegt vor, wenn Vorkehrungen getroffen sind, die geeignet und dazu bestimmt sind, den Zugriff auf die Daten für andere als den Berechtigten auszuschließen Die vorhandenen Technologien bieten dem IT-Verantwortlichen aber gerade eine uneingeschränkte Kontrollmöglichkeit der Daten und des Datenflusses. Ein Paßwort oder Verschlüsselungssoftware bieten zwar grundsätzlich Schutz vor mißbräuchlichen Zugriffen und gegen unautorisierte Veränderungen, allerdings ist der Sinn dieser Vorrichtungen, wenn sie in Unternehmen verwendet werden, nicht, die Kenntnisnahme durch den IT-Verantwortlichen zu unterbinden. Aus Sicht des Unternehmers ist deren Hauptfunktion, Zugriffe von außerhalb des Unternehmens auf die betriebliche E-Mail-Kommunikation zu verhindern. Auch sollen unautorisierte Mitarbeiter „ihre Nase nicht überall hineinstecken können". Der Unternehmer kann über Paßwörter und Verschlüsselungssoftware disponieren. Dies ergibt sich schon aus seiner Weisungsbefugnis gegenüber den einzelnen Mitarbeitern, aber auch aus Praktikabilitätsgründen – bei

[9] Tröndle/Fischer § 303a Rn. 7

Ausscheiden eines Mitarbeiters, im Krankheits- oder Urlaubsfall muß auf E-Mails zugegriffen werden können. Delegiert der Unternehmer die Überwachung des E-Mail-Verkehrs auf seinen IT-Verantwortlichen gilt für diesen dasselbe, das heißt gegenüber diesem besteht keine besondere Zugangssicherung.

Selbstverständlich gelten diese Grundsätze nur für E-Mail-Anschlüsse, die der Unternehmer seinen Mitarbeitern zur ausschließlichen geschäftlichen Nutzung oder zur gemischten – also zusätzlich noch privaten – Nutzung eingerichtet hat. Erlaubte separate und private, durch ein Paßwort geschützte E-Mail-Accounts seiner Mitarbeiter darf der Unternehmer nicht einfach „durchleuchten".

Fehlende Einbeziehung des Betriebsrates

Bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, kommt dem Betriebsrat – soweit ein solcher vorhanden ist – ein Mitbestimmungsrecht zu. Über die Installation von Sicherheits- und Überwachungssoftware ist der Betriebsrat zu informieren. Diese Informations- und Mitwirkungsrechte bestehen nicht nur auf dem Papier, sondern haben bei Verletzung durch den Unternehmensinhaber Konsequenzen: Er begeht dann eine Ordnungswidrigkeit, die mit einer Geldbuße bis zu € 10.000,– geahndet werden kann (§ 121 BetrVG). Besteht im Unternehmen kein Betriebsrat, muß der Arbeitgeber seine Mitarbeiter aus datenschutzrechtlichen Gründen über die technischen Maßnahmen persönlich informieren (§ 33 BDSG), andernfalls droht ihm ein Bußgeld in Höhe von bis zu € 25.000,– (§ 43 Abs. 1 Nr. 8 BDSG).

2.4.5 Präsentation des Unternehmens im Netz

Die Präsentation des Unternehmens im Netz berührt verschiedene strafrechtliche Vorschriften bezüglich einerseits des Inhaltes sowie andererseits der Art und Weise der Darstellung.

Inhaltsverantwortung

Das Internet stellt eine Fülle von Informationen zur Verfügung. Allerdings ist die Möglichkeit, sich Informationen oder Daten beschaffen zu können, nicht gleichbedeutend mit dem Recht, diese Inhalte für sich nutzbar zu machen. Die Einfügung von „aus dem Netz gezogenen" Logos, Tabellen oder Landkarten in eigene Internetauftritte ist nicht ohne weiteres zulässig und unterliegt urheberrechtlichen Beschränkungen. Bei der Außendarstellung des Unternehmens durch einen eigenen Internetauftritt oder Serien-E-Mails sind wettbewerbsrechtliche Vorschriften zu beachten. Verstöße gegen diese Bestimmungen sind oftmals mit materiellen Strafnormen sanktioniert.

Ungenehmigte Vervielfältigung

Eine Verwertung oder Bearbeitung urheberrechtlich geschützter Werke ist in anderen als den gesetzlich zugelassenen Fällen unter Strafe gestellt (§ 106 Abs. 1 UrhG). Von diesem strafrechtlichen Schutz werden Computerprogramme und Datenbanken ebenso erfaßt

wie literarische Werke, Lichtbilder und Musik. Eine gesetzlich erlaubte Nutzung für Jedermann ist die Ausnahme. Die ausschließlichen Rechte des Urhebers über das von ihm geschaffene Werk werden nur in gewissem Umfang eingeschränkt, wenn dies im Interesse der Allgemeinheit liegt; etwa für die Rechtspflege (§ 45 UrhG) oder den Kirchen-, Schul- und Unterrichtsgebrauch (§ 46 UrhG). In allen anderen Fällen hängt die Berechtigung von der Zustimmung des Urhebers ab, er besitzt das alleinige Verwertungsrecht (§ 15 Abs. 1 UrhG).

Im Online-Bereich ist die unberechtigte Vervielfältigung (§ 16 UrhG) von besonderer Relevanz. Lediglich für den privaten Gebrauch ist es zulässig, einzelne Vervielfältigungen eines Werkes herzustellen (§ 53 UrhG). Internetspezifische Handlungsweisen sind die Speicherung auf einem Datenträger, auch die nur vorübergehende, und die Digitalisierung eines ursprünglichen Bild-, Text- oder Tonwerkes. Das Herunterladen („Downloading“) von Werken aus dem Internet führt zur Speicherung der jeweiligen Daten im Arbeitsspeicher oder auf der Festplatte und stellt damit eine Vervielfältigung dar. Auch bei der Bereitstellung eines Werkes in digitaler Form auf einem Internet-Server („Uploading“) wird ein Werk vervielfältigt. Das Setzen eines Links ist ebenfalls eine urheberrechtlich relevante Handlung. Zwar wird das „verlinkte“ Werk selbst nicht vervielfältigt, allerdings wird durch das Anklicken des Links die Internetseite im Cache des Rechners gespeichert und es kommt so zu einer Vervielfältigung. Dann erst erfolgt die Sichtbarmachung auf dem Bildschirm. In der Präsentation einer Internetseite liegt aber im Regelfall die Zustimmung des Berechtigten, daß auf die Seite verwiesen wird. Keine Vervielfältigung ist die bloße Sichtbarmachung eines Werkes auf dem Bildschirm[10].

Öffentliche Bekanntmachungen im Internet – strafbare Werbung

Für Unternehmen ist die Außendarstellung ein wichtiger Faktor zur Gewinnung neuer Kunden und der Anpreisung der eigenen Produkte. Neben dem Fernsehen entdecken immer mehr Unternehmen auch das Internet als Präsentationsplattform. Im Netz ist Werbung zwar geographisch grenzenlos, doch wettbewerbsrechtliche Vorschriften sind dennoch einzuhalten. Ganz allgemein gesprochen muß Werbung wahr sein. Niemand darf durch unwahre Angaben in öffentlichen Bekanntmachungen in die Irre geführt werden, damit der Anschein eines besonders günstigen Angebots entsteht (§ 16 Abs. 1 UWG).

Eine Irreführung liegt vor, wenn eine Werbeaussage objektiv unrichtig ist. Es genügt auch eine mißverständliche Aussage, die bei einer „verständigen Durchschnittsperson“ eine unrichtige Vorstellung hervorruft[11]. Ausreichend ist ein vermeintlich sachlicher Kern, selbst wenn er in Wahrheit nur die Meinung des Werbenden wiedergibt. Wird für einen Domainnamen ein Gattungsbegriff verwendet, z.B. „Mitwohnzentrale.de“[12], ist dies nicht automatisch irreführend. Allerdings kann sich eine Irreführungsgefahr ergeben, wenn sich aus der Verwendung des Gattungsbegriffs und dem Internetauftritt für den Adressatenkreis die Behauptung einer Monopolstellung ergibt (OLG Hamm MMR 2003, 471 – Tauchschule Dortmund). Die Vermeidung einer solchen eventuellen Irreführung läßt sich durch einen aufklärenden Hinweis auf der ersten sich öffnenden Internetseite vermeiden.

[10] BGH NJW 1991, 1231 – „Betriebssystem“
[11] Lettl, Das neue UWG, Rn. 412
[12] BGHZ 148, 1

Daneben ist die Absicht erforderlich, den Anschein eines besonders günstigen Angebots beim Adressaten hervorzurufen. Dafür muß die Leistung günstiger dargestellt werden, als sie tatsächlich ist[13]. Worin das Günstige des Angebots besteht, ist gleichgültig. Es kann im Preis, der Güte der Ware, der besonderen Herkunft oder anderer angepriesener Vorteile, die sich auf die angebotene Ware oder Leistung beziehen, liegen. Zwar wird der IT-Verantwortliche die inhaltliche Gestaltung des Internetauftritts nur selten eigenverantwortlich übernehmen, jedoch macht er sich als Teilnehmer (Beihilfe, § 27 StGB) strafbar, wenn er die Inhalte ins Netz stellt, obwohl er weiß, daß die Angaben irreführend oder unzutreffend sind.

Verbindung zu anderen Webseiten durch Links

Häufig wird auf Webseiten durch Hyperlinks eine Verknüpfung zu anderen Internetseiten hergestellt. Dabei gibt es zwei unterschiedliche Grundformen des Hyperlinks – den aktivierbaren Link und den automatischen Link. Während bei Ersterem der Nutzer per Mausklick auf eine andere Webseite geführt wird, erfolgt bei der zweiten Variante die Weiterleitung ohne sein Zutun. Häufig wird der Nutzer gar nicht erkennen, daß es sich nicht um das Angebot der aufgerufenen Seite, sondern um einen eingebetteten fremden Inhalt handelt. So unterschiedlich die Erscheinungsformen des Links sind, so differieren auch die strafrechtlichen Risiken. Zu unterscheiden ist deshalb die Haftung des Linksetzers durch Verbreitungshandlungen als Gehilfe oder Täter sowie die strafrechtliche Verantwortung durch das Unterlassen späterer Kontrollen.

Verweisung auf eigene Inhalte

Links auf weitere eigene Internetseiten des Linksetzers bereiten hinsichtlich der Zurechnung als eigene Inhalte und damit der Begründung der strafrechtlichen Verantwortung keinerlei Probleme. Selbiges gilt auch bei der – für den Nutzer unbemerkten – automatischen Weiterleitung auf eine fremde Webseite, da der Linksetzer die verlinkte Webseite in seinen eigenen Internetauftritt integriert und sich den Inhalt damit praktisch zu eigen macht. In beiden Fällen ist der Linksetzer als Täter des jeweils einschlägigen Delikts zu behandeln.

Zugänglichmachen und Verbreiten fremder Inhalte durch Verweisung

Bringt der IT-Verantwortliche aktivierbare Links an und weiß er gleichzeitig, daß auf der Internetseite, auf die verwiesen wird, strafbare Inhalte abrufbar sind, trifft ihn eine strafrechtliche Verantwortung.

Im Bereich bestimmter Strafgesetze, beispielsweise Pornographie (§ 184 Abs. 1, 2 StGB) oder Volksverhetzung (§ 130 Abs. 2 StGB), kann bereits allein durch die Verweisung auf den fremden Inhalt und nicht erst durch das inhaltliche Anbieten die strafbare Handlung erfüllt sein. Diese Straftaten werden auch als Verbreitungsdelikte bezeichnet. Der Linksetzer wird als Täter bestraft, denn durch den Link hat er dem jeweiligen Nutzer den fremden Inhalt zugänglich gemacht. Nach der Rechtsprechung muß der Nutzer nicht einmal von

[13] Baumbach/Hefermehl-*Bornkamm*, § 16 Rn. 18

den Inhalten Kenntnis nehmen, die Möglichkeit hierzu reicht für eine Strafbarkeit des Linksetzers aus.

Ferner kommt bei Straftaten, die nicht das reine Zugänglichmachen sanktionieren, eine Verantwortung des Linksetzers zum Tragen, wenn er bewußt auf den rechtswidrigen Inhalt verweist und dadurch die Tat gefördert hat. Ihn trifft als Gehilfe dann eine Strafbarkeit wegen Beihilfe (§ 27 StGB). Hat er mit dem „Anbieter" des strafbaren Inhalts zusammengearbeitet, kann ihn sogar eine mittäterschaftliche Verantwortung treffen (§ 25 Abs. 2 StGB).

Verantwortung bei unterlassener späterer Kontrolle

Eine andere Beurteilung ist geboten, wenn der Inhalt, auf den verwiesen wird, erst nach dem Setzen des Links in strafrechtlich relevanter Weise verändert wird oder es sich um eine dynamische Verweisung, etwa den Link zu einer Online-Ausgabe einer Zeitschrift, handelt. Anknüpfungspunkt für eine Strafbarkeit ist dann die unterlassene Entfernung des Links[14]. Grundsätzlich wird durch das Setzen eines Links keine Pflicht verletzt, da darin keine gefahrbegründende Handlung zu sehen ist. Vielmehr sind Links Bestandteile des Internet als Kommunikationsmittel. Allerdings wird durch Hyperlinks die Verbreitung von rechtswidrigen Inhalten gesteigert, sie – nicht nur die strafbaren Inhalte – stellen eine „Gefahrenquelle" dar. Da der Linksetzer jederzeit die technische Möglichkeit hat, die Links zu entfernen, beherrscht er diese Gefahrenquelle. Hieraus leitet sich eine Verantwortlichkeit in Form einer Garantenstellung ab. Ihm obliegt die Verpflichtung, die Inhalte, auf die er verweist, zu kontrollieren[15], da der Link ja nicht nur bei seiner Errichtung sondern während der gesamten Zeit seiner Existenz für eine erhöhte „Gefahr" der Verbreitung sorgt.

Allerdings sagt das Bestehen der Kontrollpflicht noch nichts über deren Ausmaß aus. Links sind ein nützliches Kommunikationswerkzeug, deshalb kann dem Linksetzenden nicht die ständige Kontrolle aller Inhalte, auf die er verweist, auferlegt werden. Die Pflicht muß auf ein zumutbares Maß beschränkt werden, schon um die Effizienz des Internet als Kommunikationsmedium aufrecht zu erhalten. So kommt der Linksetzer seiner Pflicht in ausreichendem Maß nach, wenn er bei der Einrichtung des Links die Inhalte der Seite, auf die verwiesen wird, überprüft hat. Drängen sich später förmlich Umstände auf, die auf strafbare Inhalte schließen lassen, ist eine neuerliche Kontrolle der Inhalte notwendig. In allen anderen Fällen ist es ausreichend, aber auch unbedingt nötig, sich von den Inhalten auf die verwiesen wird, ausdrücklich zu distanzieren und auf deren fremde Urheberschaft hinzuweisen. Durch einen derartigen sogenannten Disclaimer läßt sich eine Strafbarkeit vermeiden·Diesen Gedanken spiegelt auch § 9 Abs. 1 TDG wider, der für Diensteanbieter im Sinne des TDG eine Verantwortlichkeit für fremde Inhalte ausschließt. Eine bloß zivilrechtliche Haftungsfreizeichnungsklausel, in der lapidar auf die eigene Verantwortung des Autors verwiesen wird, ist nicht ausreichend (LG Hamburg, NJW-CoR 1998, 302). Eine strafrechtliche Haftung kommt bei Verwendung eines Disclaimers also frühestens ab dem Zeitpunkt in Betracht, in welchem positive Kenntnis von den neuen, jetzt strafbaren Inhalten gegeben ist oder sich deren strafbarer Inhalt zumindest aufdrängt.

[14] Barton, Multimediastrafrecht, Rn. 311

[15] Barton, aa0

Erlauben Sie mir diesbezüglich folgenden Hinweis. Eine Möglichkeit, wie ein Disclaimer rechtlich wirksam formuliert werden kann, finden Sie auf der Homepage meiner Kanzlei unter http://www.strafrecht.de/de/links/index.php. Eine Alternative hierzu bietet http://www.e-recht24.de/muster-disclaimer.htm.

Links auf weitergehenden Ebenen

In der Realität sieht es so aus, daß der gesetzte Link auf eine Webseite verweist, die ihrerseits mit Links zu weiteren Internetadressen Zugang vermittelt. Alleine durch das Benutzen der Links auf den aufgerufenen Internetseiten kann man sich – zumindest theoretisch – durch das gesamte Internet bewegen. Würde man auch hier noch eine Pflicht zur Überprüfung bejahen, würde dies letztlich bedeuten, den Linksetzer für den Inhalt des gesamten Internets in die strafrechtliche Haftung zu nehmen. Dies ist ersichtlich unzumutbar. Unerkannte und ungewollte Weiterverweisungen auf einer zweiten oder weitergehenden Verweisungsebene sind damit nicht mehr zurechenbar, es sei denn, daß derjenige, der den ersten Link gesetzt hat, die weiteren Verweisungen und die jeweiligen Internetseiten noch realisiert und erkennt, daß diese der „Eingang" zu Internetseiten mit strafbaren Inhalten sind.

2.4.6 Strafbarkeit bei der Nutzung von Software – Lizenzen

Urheberrechtsverletzungen aufgrund ungenehmigter Vervielfältigungen sind nicht auf das bereits angesprochene „Uploaden" oder „Downloaden" im Online-Bereich beschränkt. Auch Programme, die im Unternehmen verwendet werden, sind urheberrechtlich geschützt (§ 2 Abs. 1 Nr. 1, 69a ff. UrhG). Hat ein Unternehmen ein Computerprogramm gekauft, darf dieses grundsätzlich nur „bestimmungsgemäß" (§ 69d Abs. 1 UrhG) benutzt werden. Geregelt ist die bestimmungsgemäße Benutzung in Individualvereinbarungen oder Allgemeinen Geschäftsbedingungen. Danach dürfen Programme meist nur auf einem einzigen Rechner installiert werden. In diesen Fällen spricht man von einer „Einzelplatzlizenz". Selbst das zusätzliche Installieren des Programms auf dem Laptop des Eigners des „Ursprungsrechners" ist von einer einzelnen Lizenz nicht gedeckt. Dies gilt unabhängig davon, ob die Software im privaten oder geschäftlichen Bereich genutzt wird. Die Vervielfältigung von EDV-Programmen ist nur mit Einwilligung des Berechtigten, sprich des Softwareanbieters, als Inhaber des alleinigen Verwertungsrechts zulässig (§69 d Abs. 1 UrhG). Lediglich die Anfertigung einer Sicherungskopie ist ohne Zustimmung möglich. Dies ist für den bestimmungsgemäßen Gebrauch, insbesondere um bei Programmfehlern reagieren zu können, erforderlich (§ 69d Abs. 1 UrhG). Wenn der Softwarehersteller eine Sicherungskopie mit dem Programm mitgeliefert hat, darf eine zusätzliche Kopie jedoch nicht angefertigt werden. In Unternehmen besteht aber regelmäßig das Bedürfnis, die Software mehreren Arbeitnehmern zur Verfügung zu stellen. Dazu muß das betreffende Programm auf mehreren PC-Arbeitsplätzen installiert werden. Folglich ist eine „Mehrplatzlizenz" erforderlich oder es ist für jeden Computer eine eigene „Einzelplatzlizenz" zu erwerben, andernfalls liegt eine strafbewehrte unberechtigte Verwendung der Software vor (§ 106 Abs. 1 UrhG).

Die Strafbarkeit des IT-Verantwortlichen richtet sich auch hier nach den allgemeinen Erscheinungsformen von Täterschaft und Teilnahme, sowie der Art der Tatbegehung in Form von Tun oder Unterlassen. Ein sogenannter bedingter Vorsatz, die billigende Inkaufnahme eines strafrechtlichen Erfolges reicht für eine Strafbarkeit aus. Überprüft das IT-Verantwortliche bei einer Neuinstallation wissentlich nicht, ob eine Lizenz für das betreffende Software-Produkt vorliegt, greift die strafrechtliche Haftung bereits ein.

Von besonderer praktischer Relevanz ist die Frage, ob der IT-Verantwortliche auch für Urheberrechtsverletzungen anderer Mitarbeiter in der strafrechtlichen Verantwortung steht. Den IT-Verantwortlichen trifft – wie bereits mehrfach angesprochen – im Rahmen seiner ihm zugewiesenen Leitungs- und Überwachungsfunktion eine Erfolgsabwendungspflicht zur Verhinderung strafbaren Verhaltens anderer Mitarbeiter. Kommt er dieser Pflicht nicht nach, macht er sich wegen Unterlassens strafbar.

Der IT-Verantwortliche hat die Sachherrschaft über den Unternehmensserver als „Gefahrenquelle“ inne und kann kontrollieren, welche Programme auf den einzelnen PC-Arbeitsplätzen installiert sind. Zwar müssen – ähnlich wie bei der Speicherung strafbarer Netzinhalte – nicht alle Programme auf ihre Lizenz geprüft werden, jedoch solche, die Anlaß zur Prüfung geben, etwa weil sie neu hinzugefügt wurden. Zur Verhinderung diesbezüglicher „unliebsamer“ Überraschungen sollte Mitarbeitern arbeitsvertraglich untersagt werden, selbständig Software auf ihren PC-Arbeitsplätzen zu installieren.

Erstellt ein Mitarbeiter Raubkopien eines für das Unternehmen lizenzierten Programms, beispielsweise zur Verwendung auf seinem privaten Computer, kommt eine Strafbarkeit (diesmal in Form der Beihilfe, § 27 StGB) des IT-Verantwortlichen nur in Betracht, wenn er konkrete Anhaltspunkte für die Aktivitäten des Mitarbeiters gehabt und diese gebilligt hätte. Das bloße Bereitstellen der Soft- und der Hardware im Unternehmen macht ihn auch nicht zum Mittäter (§ 25 Abs. 2 StGB). Ausnahme wiederum: Bewußtes und gewolltes Zusammenwirken mit dem Mitarbeiter.

2.4.7 Strafrechtliche Verantwortung im In- und Ausland

Das Internet ist ein weltumspannendes Netzwerk und erlaubt Kontaktmöglichkeiten über die Staatsgrenzen hinaus. Dies muß nicht nachteilig sein: Ist nämlich deutsches Strafrecht nicht anwendbar, wird die Tat von deutschen Ermittlungsbehörden nicht weiter verfolgt und das Verfahren eingestellt. Auf der anderen Seite ergeben sich durch diese strafrechtlichen Freiräume auch unbekannte Risiken. Da eine Information, die in das Internet eingestellt worden ist, sofort weltweit abgerufen werden kann, ist kaum zu beurteilen, ob dadurch in anderen Staaten Straftatbestände verwirklicht werden. Ausländische Rechtsordnungen sollen aber nicht Gegenstand dieses Vortrags sein, so daß ich mich darauf beschränke, die Anwendbarkeit des deutschen Strafrechts zu erörtern.

In Deutschland gilt das so genannte – in § 3 StGB verankerte – Territorialitätsprinzip. Danach sind alle Taten der Strafgewalt des deutschen Strafrechts unterworfen, wenn sie innerhalb des deutschen Staatsgebiets begangen wurden. Dies gilt unabhängig davon, wer sie begeht oder wer das Opfer ist. Reine Auslandstaten werden nur unter bestimmten Voraussetzungen nach deutschem Strafrecht verfolgt.

Zwar ist der Tatort im Strafgesetzbuch definiert (§ 9 StGB), jedoch ist die Unterscheidung, ob es sich um eine In- oder Auslandstat handelt, nicht immer einfach zu treffen. Dies liegt daran, daß es mehrere Anknüpfungspunkte für die Beurteilung gibt: Der Ort der Handlung, der Ort an dem bei einem Unterlassen hätte gehandelt werden müssen und der Ort, an dem der Tatbestandserfolg eingetreten ist oder eintreten hätte sollen. Es wird also zwischen Handlungs- und Erfolgsort unterschieden. Üblicherweise ist der Handlungsort der Ort, von welchem aus die Dateien ins Netz gestellt wurden, wo sie abgerufen werden oder die Speicherung erfolgt. Erfolgsort ist – ohne in die im einzelnen umstrittenen Details zu gehen – allgemein gesprochen der Ort, an dem eine Rechtsgutsverletzung oder -gefährdung eingetreten ist. Handlungs- und Erfolgsort können auch auseinanderfallen, so daß ein und dieselbe Tat an mehreren Orten begangen werden kann. Für die Anwendung der deutschen Strafnormen genügt es, wenn einer dieser Orte in Deutschland liegt. Dieser Grundsatz heißt „Ubiquitätsprinzip".

Deutschland ist zweifellos Tatort, wenn sowohl das Netzangebot in Deutschland eingespeist wurde, als auch der Zugriff in Deutschland erfolgt. Werden strafrechtlich relevante Inhalte im Ausland in das Internet eingespeist, ist aufgrund des weltumfassenden Charakters des Internet auch ein Zugriff auf diese Seiten in Deutschland möglich. Der tatbestandliche Erfolg tritt damit in Deutschland ein, so daß deutsches Strafrecht zur Anwendung gelangt. Werden die Netzangebote mit in Deutschland verbotenen Inhalten in Deutschland ins Netz eingespeist, aber im Ausland abgerufen, ist aufgrund der strafbaren Tätigkeit des Einspeisens Tatort wiederum Deutschland (Generalbundesanwalt NJW-CoR 1998, 175). Selbst wenn die Netzangebote im Ausland in das Internet eingespeist werden und der Zugriff nur im Ausland erfolgt, ist unter bestimmten Voraussetzungen das deutsche Strafrecht anwendbar: Diese reinen Auslandstaten werden in Deutschland verfolgt, wenn sie sich gegen bestimmte inländische oder international geschützte Rechtsgüter richten, oder wenn sie von einem Deutschen begangen werden oder sich gegen einen Deutschen richten. In den beiden letztgenannten Fällen muß die Tat allerdings auch im Ausland unter Strafe stehen.

2.5 Strafprozessuale Folgen: Sicherstellung, Einziehung und Verfall

Eine mögliche Strafbarkeit des IT-Verantwortlichen hat nicht nur für diesen persönlich Auswirkungen. Auch das Unternehmen ist im Rahmen der behördlichen Ermittlungen von Einschränkungen betroffen, wenn Computer oder Datenträger sichergestellt werden. Nach einer Verurteilung ist sogar eine endgültige Einziehung oder Unbrauchbarmachung von Hard- und Software möglich.

2.5.1 Sicherstellung zur Beweissicherung

Bei der Sicherstellung zur Beweissicherung handelt es sich um strafprozessuale Folgen einer Tat. Dementsprechend ist diese Art der Sicherstellung nicht im materiellen Strafrecht, sondern im prozessualen Strafrecht – der Strafprozessordnung und hier § 94 StPO geregelt. Danach dürfen Gegenstände, die als Beweismittel von Bedeutung sein können, sichergestellt werden. Werden die Sachen nicht freiwillig herausgegeben, erfolgt eine förmliche

Beschlagnahme. Die Sicherstellung kann auf mehrere Arten[16] vollzogen werden: Die Ermittlungsbehörden können die Sachen in amtlichen Gewahrsam verbringen oder die Gegenstände an Ort und Stelle belassen und mit einer Versiegelung versehen. Als weitere Möglichkeit kann gegenüber dem Gewahrsamsinhaber das Verbot ausgesprochen werden, über die betreffende Sache zu verfügen oder sie zu verändern. Beweismittel können nur körperliche Gegenstände sein. Eine Sicherstellung von Computern oder Datenträgern, sogar der gesamten EDV-Anlage[17], ist damit ohne weiteres möglich. Daten in Computern sind für sich genommen keine körperlichen Gegenstände. Ihre Sicherstellung kann deshalb nur durch Sicherstellung von Ausdrucken oder Datenträgern erfolgen. Auch das Anfertigen von Kopien[18] oder das Überspielen auf behördliche Datenträger[19] ist zulässig. Dieselben Grundsätze gelten auch bei Ermittlungen im Internet, allerdings ist ein Zugriff auf noch nicht abgerufene E-Mails, die sich noch im Speicher des Mailbox betreibenden Providers befinden, nicht möglich. Aufgrund der Bedeutung des Fernmeldegesetzes in unserer Rechtsordnung dürfen die Ermittlungsbehörden nur bei einer richterlichen Überwachungsanordnung (§ 100a StPO) zugreifen.

2.5.2 Sicherstellung zur Einziehung

Bei einer Verurteilung sieht das Strafgesetzbuch als Tatfolge die Möglichkeit vor, die Gegenstände, die der Täter zur Begehung oder Vorbereitung der Tat gebraucht hat, einzuziehen (§ 74 StGB). Um zu verhindern, daß der Täter nicht zwischenzeitlich über die Gegenstände verfügt und sie so dem staatlichen Zugriff entzieht, können die Sachen bis zu einem Abschluß des Verfahrens sichergestellt werden (§ 111b Abs. 1 StPO). Die Sicherstellungsmöglichkeiten entsprechen dabei denjenigen bei der Sicherstellung zur Beweissicherung (§ 111c Abs. 1 StPO), die ich Ihnen soeben vorgestellt habe.

2.5.3 Einziehung

Hat der IT-Verantwortliche eine vorsätzliche Straftat begangen, können Gegenstände, die der zur Tatbegehung gebraucht hat, – wie soeben bereits angedeutet – eingezogen werden (§ 74 Abs. 1 StGB). Hierbei handelt es sich um eine „Nebenstrafe“, also eine materielle Straffolge, die neben die eigentliche Geld- oder Freiheitsstrafe des Täters tritt. Dementsprechend sind die einschlägigen Normen wiederum im Strafgesetzbuch (§§ 74ff StGB), als dem materiellen Teil des Strafrechts zu finden. Gebraucht hat der Täter einen Gegenstand zur Tatbegehung, wenn er ihn tatsächlich eingesetzt hat. Von einem Tatwerkzeug spricht das Gesetz, wenn der Gegenstand die Begehung der Tat in irgendeiner Weise gefördert hat. Allerdings muß der Gegenstand nach Ansicht des Täters, als das eigentliche Mittel zur Verwirklichung eines Straftatbestandes eingesetzt worden sein. Wird ein Computer lediglich als „Schreibmaschine“ verwendet, um etwa einen beleidigenden Brief zu verfassen[20], handelt es sich nicht um ein der Einziehung unterliegendes Tatwerkzeug. Die

[16] im Einzelnen: Löwe-Rosenberg-*Schäfer*, StPO, § 94 Rn. 5
[17] Löwe-Rosenthal-*Schäfer,*StPO, § 94 Rn. 27 m.w.N.
[18] Löwe-Rosenthal-*Schäfer*, StPO, § 94 Rn. 14
[19] LG Köln, NStZ 1995, 54, 55
[20] OLG Düsseldorf, NJW 1993, 1485

Beleidigung war hier nicht von der Verwendung des Computers abhängig. Etwas anderes gilt für die in diesem Vortrag dargestellten computer- und internetspezifischen Straftaten. Eine Möglichkeit zur Tatbegehung ist erst durch den Einsatz des Computers möglich, so daß dieser als Tatwerkzeug der Einziehung unterliegt. Eine Einziehung ist jedoch nur möglich, wenn das Tatwerkzeug, in diesem Fall der Computer, demjenigen gehört, der die Straftat begangen hat (§ 74 Abs. 2 Nr. 1 StGB). Soweit der Computer nicht im Alleineigentum des verurteilten IT-Verantwortlichen steht, kommt eine Einziehung nur in Betracht, wenn alle, die ein Recht an diesem Computer haben, an der Tat beteiligt waren[21] oder vom einzuziehenden Gegenstand eine besondere Gefährlichkeit ausgeht (§ 74 Abs. 2 Nr. 2 StGB). Als Folge der Einziehung geht das Eigentum an der Sache auf den Staat über (§ 74e Abs. 1 StGB).

2.5.4 Unbrauchbarmachung

Enthalten Datenträger – Disketten, Festplatten – einen Inhalt, dessen vorsätzliche Verbreitung den Tatbestand eines Strafgesetzes verwirklichen würde, können sie unbrauchbar gemacht werden (§ 74d Abs. 1 S. 2 StGB). Unter solche Inhalte fallen alle gewaltverherrlichenden Darstellungen und harte Pornographie. Bei vielen Datenträgern, die als Vorlage für eine Vervielfältigung dienen sollen, reicht das Löschen des Inhalts nicht aus, da dessen Rekonstruktion durch so genannte „Undo-Programme“ möglich bleibt. Zwar können die Datenträger mit einer entsprechenden Software weiterbearbeitet und endgültig unlesbar gemacht werden, was in der Praxis jedoch nicht geschieht, da Datenträger auch eingezogen werden (§ 74d Abs. 1 S. 1 StGB) können.

2.5.5 Verfall

Die einschneidenste strafprozessuale Maßnahme ist der Verfall, für das Strafgesetzbuch geregelt in den §§ 73 ff StGB, für das Ordnungswidrigkeitenrecht in § 29a OWiG geregelt. Danach kann der Staat in bestimmten Fällen das „Erlangte“ herausverlangen. Das ist nicht der Saldo aus beispielsweise Preis und Warenwert, sondern der erlangte Geldbetrag brutto. Aufwendungen sind nicht abzugsfähig. Was dies für eine Firma bedeutet, die durch unlautere Werbung im Internet große Mengen einer hochwertigen Ware verkauft hat, lässt sich leicht vorstellen.

Eine Steigerung erfährt diese Gefährdung aus dem strafrechtlichen Bereich noch dadurch, dass – nur bei dem Vorwurf von Straftaten – der Verfall auch durch Beschlagnahme noch während eines Ermittlungsverfahrens gesichert werden kann. Da heute fast alle Gesetze einen Bereich „Ordnungswidrigkeiten und Strafvorschriften“ kennen, eine existenzbedrohende Gefahr. Das Gesetz bezeichnet den Verfall nicht als Strafe, sondern eine „Nebenfolge“. In der wirtschaftlichen Realität stellt der Verfall jedoch oft genug die härteste Sanktion dar.

[21] Sch/Sch-*Eser*, StGB, § 74 Rn. 22

2.6 Schutzmöglichkeiten

Zwar sind die strafrechtlichen Risiken erheblich,. gleichwohl müssen Sie vor der strafrechtlichen Verantwortung nicht kapitulieren, bei der Beachtung einiger Verhaltensregeln stehen Sie als IT-Verantwortlicher nicht „mit einem Bein im Gefängnis".

- Eine ordnungsgemäße Wahrnehmung der Sicherungs- und Überwachungspflichten, bietet Gewähr dafür, daß eigene Versäumnisse erkannt oder Verstöße von unterstellten Mitarbeitern aufgedeckt werden.
- Ständige Anpassung der betrieblichen Organisation und der technischen Einrichtungen des Unternehmens an alle Möglichkeiten der Sicherheitskontrolle in den Bereichen Internet und E-Mail.
- Machen Sie Gebrauch von allen Freizeichnungsmöglichkeiten („Disclaimern") im Internet und übernehmen dazu bewährte Texte.
- Umgehende Information der Geschäftsleitung bei der Feststellung von Mißständen.
- Zur eigenen Entlastung sollte der IT-Verantwortliche dies dokumentieren und sich von seinen Vorgesetzten gegenzeichnen lassen.
- Eine freiwillige Selbstkontrolle im Unternehmen, durch Einholung des Einverständnisses der Mitarbeiter zur Überwachung von Internet- und E-Mail-Nutzung, ermöglicht es, „schwarze Schafe" ausfindig zu machen.
- Bestellung und beste Ausstattung eines Datenschutzverantwortlichen.
- Ein Pflichtenheft zur Selbstkontrolle und Überwachung der Personen, auf die Pflichten delegiert wurden, sollte selbstverständlich sein.
- Sofortiges Einschreiten bei Warnzeichen oder gar erkannten Fehlern.

Durch die Ausgliederung der Verantwortung auf externe Fachunternehmen läßt sich das Haftungsrisiko für die IT-Verantwortlichen in der Führungsetage weiter minimieren.

3 Fazit

Es ist vor dem Hintergrund einer über viele Gesetzte verstreuten Ge- und Verbotslage von enormer Wichtigkeit, daß Sie mit geschärftem Gespür auch für strafrechtliche Anforderungen Ihre täglichen Aufgaben angehen, denn der Mißbrauch von Informationstechnologien und der rechtswidrige Umgang mit Daten rücken zunehmend in den Blickpunkt der Gerichte. Oftmals lauern strafrechtliche Risiken dort, wo man sie nicht vermutet. Wie das „Compuserve-Urteil" zeigt, endet dabei die Verantwortung nicht an den Landes- oder Betriebsgrenzen. Dem weltumspannenden Charakter des Internet müssen auch Sie als IT-Verantwortliche Rechnung tragen.