CASTON

SINCE 1988 · INTERNATIONAL LAW & BUSINESS INFORMATION · WWW.CASTON.INFO

COMPACT

E-Mail und Internet am Arbeitsplatz

Monika Sekara, Rechtsanwältin, Fachanwältin für IT-Recht in Hannover

No. 290 – Mai 2010

Viele Arbeitgeber bieten ihren Beschäftigten neben einer rein betriebsbedingten auch die Möglichkeit zur privaten Nutzung von E-Mail- und Internetdiensten an. Betriebsvereinbarungen oder Diensteinweisungen bestimmen die Grenzen für diese Privatnutzung sowie die Verwendung von hierdurch entstehenden Protokolldaten. Aufgrund der aktuellen Rechtsentwicklungen werden Arbeitgeber und Betriebsräte vor besondere Herausforderungen gestellt. Über die Privatnutzung anfallende Protokolldaten dürfen nur ausnahmsweise ausgewertet werden. Der Kurzaufsatz zeigt auf, wie Unternehmen mit der Problematik umgehen und eigene Lösungen finden können.

Erfassen von Protokolldaten im Unternehmen

In den meisten Unternehmen werden Protokolldateien erfasst, die infolge der Nutzung des E-Mail-, Intranet- oder Internetdienstes anfallen können. Bei Protokolldaten handelt es sich um personenbezogene Daten. Erfolgt keine anonymisierte Erfassung, ist davon auszugehen, dass ein Unternehmen alle erfassten Protokolldaten jeweils einem bestimmten Rechner bzw. Arbeitsplatzsystem und insofern auch einem bestimmten Beschäftigten zuordnen kann.

Die technischen Verfahren zur Erfassung solcher Protokolldaten sind je nach Dienst (E-Mail, Internet oder Intranet) unterschiedlich. In Abhängigkeit von den jeweiligen Einstellungen können alle oder bestimmte Aktionen auf einem Computersystem in sog. Protokolldateien (oder Logdateien) erfasst werden und zwar unbemerkt vom Nutzer und ohne die Arbeit zu stören. Die Protokollierung beginnt bereits mit der Anmeldung am System. Eine Protokollzeile enthält in der Regel detaillierte Informationen über Datum und genaue Uhrzeit (sog. Timestamp) und das dem Kommunikationsvorgang zugrunde liegende Ereignis.

In rechtlicher Hinsicht bestimmt sich der Umgang mit Protokolldaten nach unterschiedlichen gesetzlichen Vorschriften. Je nach Inhalt des Dienstes können andere Gesetze und daraus folgende rechtliche Anforderungen gelten. Bei der Erbringung von Telekommunikationsdienstleistungen gehen die datenschutzrechtlichen Bestimmungen des Telekommunikationsgesetzes (TKG) dem Bundesdatenschutzgesetz (BDSG) als speziellere Regelungen (sog. „lex specialis“) vor.

Arbeitgeber als Dienstanbieter nach TKG

Bietet ein Unternehmen den Beschäftigten neben einer rein betriebsbedingten auch die Möglichkeit zur privaten Nutzung der E-Mail- und Internetdienste an, ist es ein Dienstanbieter im Sinne des TKG. Der Arbeitgeber muss insbesondere das Fernmeldegeheimnis und die datenschutzrechtlichen Pflichten nach TKG einhalten. Telekommunikation meint den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mit Telekommunikationsanlagen. Eine Kommunikation, die per E-Mail geführt wird, erfüllt diese Voraussetzungen. Das TKG ist auch anwendbar auf Verträge über den Zugang

zum Internet (sog. Accessproviderverträge) sowie Internettelefonie und Voice over IP.

„Dienstanbieter“ ist nach der gesetzlichen Definition jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt. Das geschäftsmäßige Erbringen von TK-Diensten ist das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht. Hierbei kommt es weder auf ein gewerbliches Handeln noch darauf an, ob die Telekommunikationsdienste für die Öffentlichkeit erbracht werden. Es muss ein mit einer gewissen Häufigkeit, auf Dauer angelegtes und an Dritte gerichtetes Angebot von Telekommunikationsdiensten sein. Bei einer erlaubten privaten Nutzung der betrieblichen Kommunikationsmittel sind die Beschäftigten „Dritte“ im Sinne des TKG. Sie werden in diesem Fall nach ganz überwiegender Meinung nicht mehr der betrieblichen Sphäre zugerechnet. Etwas anderes gilt hingegen, soweit eine private Nutzung verboten ist und die Beschäftigten nur zu einer dienstlichen Kommunikation befugt sind. In diesem Fall erfolgt die Nutzung ausschließlich zu betrieblichen Zwecken und kann mangels Außenwirkung daher nur der betrieblichen Sphäre des Arbeitgebers zugerechnet werden. Die Beschäftigten sind dann im Verhältnis zum Unternehmen keine Dritten.

Das TKG findet keine Anwendung bei Protokolldaten über die rein betriebsbedingte Kommunikation.

Datenschutz bei Privatnutzung von Internet und E-Mail

Protokolldaten über die gestattete Privatnutzung der E-Mail- und Internetdienste durch Beschäftigte sind Verkehrsdaten im Sinne des TKG. Das TKG unterscheidet insbesondere zwischen Bestandsdaten und Verkehrsdaten. Bestandsdaten sind Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über TK-Dienste erhoben werden. Dazu gehören Vor- und Nachname, Titel und akademische Grade, Anschrift, Teilnehmernummer und sonstige Kontaktinformationen, Informationen über Art und Inhalt des Vertragsverhältnisses und Bonität.

Verkehrsdaten sind Daten, die bei der Erbringung eines TK-Dienstes anfallen. Das TKG regelt, welche Verkehrsdaten ein Dienstanbieter zu welchen Zwecken erheben, verarbeiten und nutzen darf. Zu den Verkehrsdaten gehören: Die Nummer oder die Kennung der beteiligten Anschlüsse; Beginn und Ende einer Verbindung sowie deren Endpunkte, nach Datum und Uhrzeit und – soweit für die Abrechnung relevant – die übermittelten Datenmengen; Art des in Anspruch genommenen TK-Dienstes; sonstige Verkehrsdaten, die zum Aufbau und zur Aufrechterhaltung der Telekommunikation und zur Entgeltabrechnung notwendig sind. Diese Verkehrsdaten dürfen nur für Zwecke verwendet werden, die ein Gesetz vorsieht oder zum Aufbau weiterer Verbindungen erforderlich sind. Nach dem Ende einer Telekommunikationsverbindung dürfen die zu diesen Zwecken erhobenen Verkehrsdaten nur verwendet werden, um: Entgelte ordnungsgemäß zu ermitteln und mit den Teilnehmern abzurechnen; Einzelverbindungsnachweise zu erstellen; Störungen oder Fehler an TK-Anlagen zu erkennen, einzugrenzen oder zu beseitigen; Auskünfte über die Inhaber von Anschlüssen zu erteilen, von denen bedrohende oder belästigende Anrufe ausgingen.

Die für die Entgeltabrechnung benötigten Daten darf der Anbieter höchstens sechs Monate speichern. Eine längere Speicherfrist ist nur erlaubt, wenn der Teilnehmer gegen die Rechnung Einwände erhoben hat und diese noch abschließend geklärt werden müssen. In allen anderen Fällen ist ein TK-Anbieter verpflichtet, Verkehrsdaten nach Beendigung einer Verbindung unverzüglich zu löschen. Der Anbieter muss unter Berücksichtigung der technischen Gegebenheiten die Löschung ohne schuldhaftes Zögern vornehmen. Nach derzeitiger Praxis erfolgt die Löschung in der Regel innerhalb von 24 Stunden.

Maßgaben für Unternehmen und Betriebsräte

Die in einer Betriebsvereinbarung oder Dienstanweisung geregelte Nutzung von ITK-Systemen im Unternehmen verfolgt grundsätzlich das Ziel, die Arbeitserledigung und die aufgabenbezogene individuelle Kommunikation zu unterstützen sowie die Effektivität zu steigern. Die Protokolldaten dienen Unternehmen oft dazu, um das Erreichen dieser Ziele zu überprüfen und die Verletzung von arbeitsrechtlichen Ver-

pflichtungen und sonstigen Missbrauch zu verhindern bzw. zu ahnden. Mit dem Zugeständnis der Privatnutzung möchte der Arbeitgeber zusätzlich das Gefühl der Verbundenheit der Beschäftigten mit dem Unternehmen steigern.

Die Betriebsvereinbarung

Problematisch ist der Fall, wenn Unternehmen intern gar nicht oder nur in wenigen Fällen gegenüber Beschäftigten die Nutzung von Telefon, Fax, Internet und E-Mail abrechnen und interne Regelungen (z. B. Betriebsvereinbarungen) es gestatten, dass Protokolldaten auch über eine Abrechnung hinaus in unbegrenztem Umfang u. a. für interne Ermittlungsmaßnahmen verwendet werden dürfen.

Außerhalb von Abrechnungen darf ein Arbeitgeber Protokolldaten über die Privatnutzung nur speichern und auswerten (z. B. für interne Ermittlungen), wenn hierfür eine gesetzliche Erlaubnis besteht. Als solche kann nach herrschender Meinung eine Betriebsvereinbarung gelten. Die in einer Betriebsvereinbarung vorgesehenen Regelungen zur Erfassung und Verwendung von Protokolldaten müssen jedoch mit höherrangigem Recht, insbesondere mit dem Arbeitnehmerdatenschutz nach BDSG, vereinbar sein.

Beachtung des Arbeitnehmerdatenschutzes

Die Betriebsvereinbarung muss sowohl hinsichtlich der rein betrieblichen Nutzung als auch hinsichtlich der Privatnutzung von E-Mail, Internet und Intranet die Vorgaben umsetzen, die sich aus dem gesetzlichen Arbeitnehmerdatenschutz ergeben. Ein Arbeitgeber darf die Daten seiner Beschäftigten verwenden, wenn der Arbeitgeber seine im Zusammenhang mit der Durchführung des Beschäftigungsverhältnisses stehenden Rechte wahrnimmt, z. B. ein Weisungsrecht ausübt. Dazu können auch Maßnahmen gehören, die zur Verhinderung von Straftaten oder sonstigen Rechtsverstößen im Arbeitsverhältnis erforderlich sind. Zielen diese auf die Erfassung und Auswertung von Protokolldateien ab, sind die Maßnahmen nach einer Verhältnismäßigkeitsabwägung auf einen angemessenen Umfang zu begrenzen. Strikt untersagt ist nach einem kürzlich ergangenen Urteil des Bundesverfassungsgerichts die Speicherung von personenbezogenen Daten auf Vorrat zu unbestimmten oder noch nicht bestimmten Zwecken.

Nach dem Grundsatz der Verhältnismäßigkeit müssen die Regelungen zu Protokollierungen und Kontrollen in einer Betriebsvereinbarung: 1.) geeignet sein, um die aus der Betriebsvereinbarung folgenden Zwecke zu erreichen; 2.) erforderlich sein, indem es keine weniger einschneidenden Mittel gibt, um diese Zwecke zu erreichen; 3.) die Datensicherheit gewährleisten, die vorgesehene Datenverwendung nach Zeitraum und Menge beschränken und insgesamt transparent gestaltet sein.

Die Reichweite des Fernmeldegeheimnisses

Der Schutz des Fernmeldegeheimnisses kommt nur in Bezug auf die erlaubte private Nutzung von E-Mail und Internet im Unternehmen in Betracht. Die rein geschäftlich geführte Kommunikation fällt nicht in den Anwendungsbereich des TKG.

Das Fernmeldegeheimnis schützt zum einen die Inhalte der Telekommunikation und zum anderen die Vertraulichkeit der näheren Umstände der unkörperlichen Übermittlung von Informationen an individuelle Empfänger mit Hilfe der TK-Techniken. Daten zu Diensten der elektronischen Post (E-Mail) unterliegen dem Fernmeldegeheimnis ebenso wie Daten zum Internetzugang und zu aufgerufenen Internetseiten. Jede Erfassung, Kenntnisnahme, Aufzeichnung, Speicherung und Verwertung von privaten Kommunikationsdaten sowie jeder Abgleich mit anderen Daten, jede Auswertung ihres Inhalts und Übermittlung an Dritte stellt einen Engriff in dieses geschützte Recht dar. Der Schutz bleibt bestehen, solange der Kommunikationsvorgang nicht abgeschlossen ist. Dies ist z. B. der Fall, wenn der zugangsgesicherte Kommunikationsinhalt in einem E-Mail-Postfach auf einem Internetserver gespeichert ist, auf das der Nutzer nur über eine Internetverbindung zugreifen kann. Die auf dem Mailserver eines Providers gespeicherten E-Mails befinden sich nämlich nicht im Herrschaftsbereich des Kommunikationsteilnehmers, sondern in demjenigen des Providers. Hier besteht der Schutz des Fernmeldegeheimnisses fort, auch wenn der Kommunikationsteilnehmer vom Inhalt der E-Mail bereits Kenntnis genommen hat, diese aber beim Provider gespeichert bleibt.

Für den E-Mailverkehr im Unternehmen folgt daraus, dass **kein** nachwirkender Schutz des Fernmeldege-

heimnisses für diejenigen E-Mails gilt, die ein Beschäftigter des Unternehmens nach dem Abschluss einer Übertragung selbst den innerbetrieblichen Speichermedien zuführt. Gemeint sind E-Mails bei denen es dem Beschäftigten selbst obliegt, nach Erhalt oder Versendung einer E-Mail darüber zu entscheiden, ob die E-Mail samt der in ihr enthaltenen Verbindungsdaten dauerhaft an einer bestimmten Stelle im System ggf. geschützt gespeichert oder durch Entfernen aus dem Eingangs- oder Ausgangspostfach endgültig gelöscht werden soll. Derart auf den IT-Systemen eines Unternehmens gespeicherte E-Mails unterliegen der Beschlagnahme durch Strafverfolgungsbehörden und müssen unter Umständen an Behörden herausgegeben werden (z. B. auch im Rahmen einer steuerlichen Außenprüfung).

Bislang unbeantwortet blieb in der Rechtsprechung die Frage, ob und wann ein Übertragungsvorgang abgeschlossen ist, wenn E-Mails dauerhaft auf dem E-Mail-Server eines Unternehmens verbleiben und dort automatisch gespeichert und archiviert werden, ohne dass der Teilnehmer sie mit Öffnen des E-Mailprogramms auf einen lokalen Arbeitsplatzrechner abruft und danach selbst über die Speicherung entscheidet.

Zusammenfassung

Sowohl bei privater als auch rein betriebsbedingter Kommunikation dürfen Protokolldaten nicht ohne jeden Anlass ausgewertet werden. Vielmehr sollten Maßnahmen erst bei tatsächlichen Anhaltspunkten auf eine Straftat eingeleitet werden. Nicht strafbare Verstöße gegen arbeitsvertragliche Verpflichtungen dürfen von solchen Ermittlungsmaßnahmen nicht erfasst werden. Insbesondere der systematische Abgleich von Beschäftigtendaten mit anderen Quellen (sog. „Rasterabgleich“) ist nur zulässig, wenn tatsächliche Anhaltspunkte für das vorliegen einer bereits begangenen Straftat vorliegen. Im konkreten Einzelfall ist stets diejenige Ermittlungsmaßnahme zu wählen, die im Verhältnis zu anderen Maßnahmen den gleichen Ermittlungserfolg mit weniger einschneidenden Folgen herbeiführt. Eine Verwendung von Protokolldaten kommt nur zum Schutze überragend wichtiger Rechtsgüter in Betracht, nämlich zur Ahndung von schweren Straftaten oder zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person.

caston.info

Daily News und Datenbank im Internet. Mehrere tausend Beiträge zu Recht & Wirtschaft International finden Sie kostenfrei im Internet bei www.caston.info. Dort können Sie nach Schlagwort und Sachgebieten recherchieren. Unsere Titelliste erhalten Sie auch per Mail.

HERAUSGEBER
HERFURTH & PARTNER Rechtsanwaltsgesellschaft mbH
Luisenstr. 5, D-30159 Hannover
Fon0511-30756-O
Fax 0511-30756-10
Mail info@herfurth.de,
Web www.herfurth.de

Hannover · Göttingen · Brüssel ·
Member of the ALLIURIS GROUP, Brussels

REDAKTION HANNOVER
Redaktion: Ulrich Herfurth, Rechtsanwalt, zugelassen in Hannover und Brüssel (verantwortlich); Philipp Neddermeyer, Rechtsanwalt (D);
unter Mitarbeit von Sibyll Hollunder-Reese, M.B.L. (HSG), Rechtsanwältin; Angelika Herfurth, Rechtsanwältin (D); Jens-Uwe Heuer, Rechtsanwalt (D); Thomas Gabriel, Rechtsanwalt (D); JUDr. Yvona Rampáková, Juristin (CR); Dr. Jona Aravind Dohrmann, Rechtsanwalt (D); Marc-André Delp, M.L.E., Rechtsanwalt (D); Tatiana Getman, Rechtsanwältin (D); Monika Sekara, Rechtsanwältin und Fachanwältin für Informationstechnologierecht (D); Pen-Wen Lin, Rechtsanwältin (D); Maimiti Cohen-Solal, Avocat (FR), Attorney at Law (New York/USA); Alexia Calleja Cabeza, Abogada (ES) ; Prof. Dr. jur. Frank-Rüdiger Jach, Hochschulprofessor (D); Dr. jur. Christiane Trüe LL.M. (East Anglia), Rechtsanwältin (D), Uzunma Bergmann, Attorney at Law (New York/USA), Solicitor (England & Wales), Advocate and Solicitor (Nigeria).

KORRESPONDENTEN AUSLAND
u. a. Amsterdam, Athen, Bratislawa, Brüssel, Budapest, Bukarest, Helsinki, Istanbul, Kiew, Kopenhagen, Lissabon, London, Luxemburg, Mailand, Madrid, Oslo, Paris, Prag, Sofia, Stockholm, Warschau, Wien, Zürich,
New York, Sao Paulo, Moskau, Kairo, Tunis, Dubai, Peking, Hongkong, Tokio, New Delhi, Bangkok, Singapur, Sydney.

VERLAG
CASTON GmbH
Law & Business Information
Luisenstr. 5, D-30159 Hannover,
Fon 0511 - 30756-50
Fax 0511 - 30756-60
Mail info@caston.info
Web www.caston.info

Alle Angaben erfolgen nach bestem Wissen; die Haftung ist auf Vorsatz und grobe Fahrlässigkeit beschränkt. Wiedergabe, auch auszugsweise, nur mit Genehmigung der Herausgeber.