Zeitschrift für Datenrecht und Informationssicherheit

digma

www.e-digma.ch

1. Jahrgang, Heft 1, April 2001

fokus: Internet am Arbeitsplatz

report: Neuer Standard für Online-Datenschutz

forum: Datensicherheit ist Chefsache

Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rolf Oppliger
Rainer J. Schweizer

Schulthess §

Was darf die Chefin, was die Angestellte?

Arbeits- und datenschutzrechtliche Schranken der technischen Überwachung der Internet-Nutzung am Arbeitsplatz

Dr. Beat Rudin, Geschäftsführer der Stiftung für Datenschutz und Informationssicherheit, Basel, Datenschutzbeauftragter des Kantons Basel-Landschaft (1992–2001)
stiftung.datenschutz@bluewin.ch

Wer Internet und E-Mail am Arbeitsplatz nutzen darf und in welchem Umfang, entscheidet die Arbeitgeberin. Über den Umfang der zulässigen Überwachung entscheidet dagegen das Gesetz.

Die neuen Kommunikationstechnologien erobern Privatwirtschaft und Verwaltung. Kaum mehr ein Unternehmen und kaum mehr eine Verwaltung können es sich leisten, sich von der weltweiten Kommunikation abzukapseln. Sie nutzen das Internet als wertvolles und hilfreiches Mittel zur Informationsbeschaffung und die E-Mail als modernes, billiges Mittel der weltweiten Kommunikation. Doch nach der ersten Euphorie wird schnell erkannt: Wenn wir das Fenster zur Welt so weit öffnen, kann auch Unerwünschtes durch das Fenster hereinkommen oder hinausgelangen. Damit wird der Ruf laut nach Überwachung – und die technischen Mittel dazu sind auf dem Markt[1]. Doch wie weit darf die Arbeitgeberin[2] sie einsetzen? Wie weit hat sich die Arbeitnehmerin eine solche Überwachung gefallen zu lassen?

In der Firma ist einiges los. Anna A. lädt gerade ein Last-minute-Angebot der Crossair herunter. Bernhard B. lässt in einem E-Mail an einen Bekannten seinem Ärger über das schlechte Arbeitsklima freien Lauf. Christine C. beweist einer Kollegin aus dem Sportverein, dass die Firma das Produkt Così tatsächlich ohne den Zusatz von Cyclotoxoclomat herstellt, und mailt ihr einen Auszug aus dem internen Produktionsbeschrieb. Daniel D. verkürzt sich die Kaffeepause, indem er sich ein paar Bildchen mit jungen Mädchen herunterlädt – wobei er zwar die Geschäfts-E-Mail-Adresse, aber selbstverständlich die Nummer seiner privaten Kreditkarte angibt. Erika E. mag schon gar nicht in den Pausenraum gehen, weil sie seit zwei Stunden mit einem interessanten Typen chattet. Felix F. schliesslich leitet per E-Mail die Internet-Adresse einer Website, auf der «bewiesen» wird, «dass die Juden Amerika wirtschaftlich total beherrschen», an eine Bekannte weiter, die ihm das gestern nicht hatte glauben wollen.

Muss die Geschäftsinhaberin Gisela G. das alles dulden?

1. Pflichten der Arbeitnehmerin

Für die Arbeitnehmerin ergeben sich aus dem Arbeitsvertrag und den entsprechenden Regeln des *Obligationenrechts*[3] Pflichten. Sie muss die ihr übertragenen Arbeiten sorgfältig ausführen und die berechtigten Interessen der Arbeitgeberin in guten Treuen wahren. Dazu gehören namentlich die Nutzung der Arbeitszeit für die Arbeitsleistung – nicht für private Zwecke – sowie die Vermeidung von Sicherheits- oder Haftungsrisiken. Die Umschreibung der Arbeitsleistung im Rahmen des Arbeitsvertrages obliegt primär der Arbeitgeberin und sie darf dazu allgemeine Anordnungen erlassen – z.B. über die Nutzung der Infrastruktur – und der Arbeitnehmerin besondere Weisungen erteilen, welche diese nach Treu und Glauben zu befolgen hat[4]. Die Arbeitnehmerin darf insbesondere auch Fabrikations- und Geschäftsgeheimnisse nicht anderen mitteilen[5] und ist schliesslich dafür verantwortlich[6], wenn sie der Arbeitgeberin absichtlich oder fahrlässig Schaden zufügt.

Die Geschäftsinhaberin Gisela G. will alles unternehmen, um diese Pflichten durchzusetzen, den Missbrauch des Internets und seiner

Dienste zu verhindern und gegen Arbeitnehmerinnen, die sich nicht an die Regeln halten, Sanktionen zu ergreifen. Sie verlangt deshalb von ihrer Informatikchefin Isabelle I., dass sie das Nutzungsverhalten aller Angestellten protokolliert und ihr die Protokolle wöchentlich aushändigt.

Müssen die Arbeitnehmerinnen sich das gefallen lassen?

2. Gesetzlicher Schutz der Arbeitnehmerin

Die Arbeitnehmerin treffen nicht nur Pflichten, die Gesetzgebung hat auch verschiedene Bestimmungen zu ihrem Schutz aufgestellt. Für das privatrechtliche Arbeitsverhältnis legt das *Obligationenrecht* fest, dass die Arbeitgeberin die Persönlichkeit der Arbeitnehmerin zu achten und zu schützen, auf deren Gesundheit gebührend Rücksicht zu nehmen und für die Wahrung der Sittlichkeit zu sorgen hat[7]. Sie hat zum Schutz von Leben, Gesundheit und persönlicher Integrität der Arbeitnehmerin diejenigen Massnahmen zu treffen, die nach der Erfahrung notwendig, nach dem Stand der Technik anwendbar und den Verhältnissen des Betriebes angemessen und zumutbar sind. Insbesondere aber darf die Arbeitgeberin Daten über die Arbeitnehmerin nur bearbeiten, soweit sie deren Eignung für das Arbeitsverhältnis betreffen[8] oder zur Durchführung des Arbeitsvertrages erforderlich sind[9]. Im Übrigen gelten die Bestimmungen des Datenschutzgesetzes[10].

Insbesondere die Unabänderlichkeit zuungunsten der Arbeitnehmerin[11] markiert deutlich, welches Gewicht die Gesetzgebung dieser Regelung einräumt.

Das *Bundesdatenschutzgesetz* (DSG)[12] stellt unter anderem Grundsätze auf für das Bearbeiten von Personendaten. So dürfen Personendaten nur rechtmässig beschafft werden. Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein. Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Zweckbindungsgebot)[13]. Wer Personendaten bearbeitet, hat die Pflicht, sich über deren Richtigkeit zu vergewissern[14]. Ohne Rechtfertigungsgrund dürfen Personendaten nicht entgegen diesen Grundsätzen oder gegen den ausdrücklichen Willen der betroffenen Personen bearbeitet werden[15]. Als Rechtfertigungsgründe gelten neben dem Gesetz und der Einwilligung der betroffenen Personen ein überwiegendes privates oder öffentliches Interesse[16]. Ein überwiegendes Interesse der Person, welche die Daten bearbeitet, fällt insbesondere dann in Betracht, wenn Personendaten in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags bearbeitet werden[17].

Eine weitere strenge Bestimmung zum Schutz der Arbeitnehmerin enthält die *Arbeitsverordnung 3*[18]: Sie verbietet – in weitgehender Übereinstimmung mit den Richtlinien der Internationalen Arbeitsorganisation ILO in Genf[19] – den Einsatz von Überwachungs- und Kontrollsystemen zur Überwachung des Verhaltens am Arbeitsplatz. Sind solche Systeme nötig, so müssen sie so eingesetzt werden, dass sie die Gesundheit und Bewegungsfreiheit der Arbeitnehmerinnen nicht beeinträchtigen.

Wenn eine Leistungsüberwachung zur Verhaltensüberwachung führt, etwa weil sie permanent stattfindet, dann ist sie verboten.

Es wird allerdings schwierig sein, die Grenze zwischen (erlaubter) Leistungs- oder Sicherheitsüberwachung und (verbotener) Verhaltens- und Bewegungsüberwachung scharf zu ziehen, weil das Verhalten eben in Leistung zum Ausdruck kommen oder sicherheitsrelevant sein kann. Die arbeits- und datenschutzrechtlichen Verbote zeigen aber klar den Vorrang. Wenn eine Leistungsüberwachung zur Verhaltensüberwachung führt, etwa weil sie permanent stattfindet, dann ist sie verboten. Ein Betrieb kann sich somit selbst gegen unerwünschtes oder rechtswidriges Verhalten nicht mit permanenter technischer Überwachung der Arbeitnehmerinnen schützen[20].

Ausserdem stellt das *Strafgesetzbuch* bestimmte Handlungen unter Strafe[21], etwa das unberechtigte Öffnen einer verschlossenen Schrift, das Abhören und Aufnehmen fremder Gespräche oder das unbefugte Aufzeichnen im Privat- und Geheimbereich einer Person. Die Anwendbarkeit dieser Bestimmungen auf die hier behandelten Sachverhalte ist aber zurzeit im Detail noch nicht gesichert.

3. Wann ist die Überwachung zulässig?

Inwieweit ist angesichts dieser gesetzlichen Vorschriften die technische Überwachung der Arbeitnehmerinnen am Arbeitsplatz überhaupt zulässig? Die folgenden Punkte können als gesicherte Eckpfeiler angesehen werden:

| Erlaubt ist es, über eine Arbeitnehmerin Daten zu erfassen, die für die Eignungsbeurteilung bzw. zur Durchführung des Arbeitsvertrages erforderlich sind.

˙ Widerrechtlich ist es, eine Arbeitnehmerin systematisch und permanent mit technischen Mitteln zu überwachen.

| Erlaubt ist eine System- oder Netzwerküberwachung, solange sie sich nicht auf die einzelne Arbeitnehmerin bezieht, also mit anonymisierten oder pseudonymisierten Daten arbeitet oder auf andere Weise sichergestellt ist, dass die Daten nicht zur Überwachung der Arbeitnehmerin verwendet werden.

˙ Widerrechtlich ist die technische Überwachung des Verhaltens einer Arbeitnehmerin am Arbeitsplatz.

| Erlaubt ist die Regelung der (privaten) Nutzung von Internet und E-Mail.

˙ Widerrechtlich ist das Lesen von privaten E-Mails, auch dann, wenn die private Nutzung des E-Mail-Systems verboten ist.

Die Arbeitgeberin hat zu entscheiden, für welche Funktionen, für welche Zwecke und in welchem Rahmen die Internetnutzung sinnvoll und erlaubt ist.

| Die Strafuntersuchungsorgane können auf Grund einer gerichtlichen Anordnung auch private E-Mails lesen oder personenbezogene Auswertungen vornehmen.

Die Frage, ob und welche Überwachungsmassnahmen im weiten Feld zwischen diesen sicheren Eckwerten zulässig sind, muss durch Abwägung der berechtigten Interessen der Arbeitgeberin und Arbeitnehmerin beantwortet werden.

4. Taugliche Lösung in drei Schritten

Wie können die berechtigten Interessen der Arbeitgeberin gewahrt werden, ohne dass die ebenso berechtigten Interessen der Arbeitnehmerin verletzt werden? Eine taugliche Lösung[22] kennt drei Schritte:

■ Konfliktsituationen sollen von allem Anfang an mit rechtlichen, organisatorischen und technischen Präventionsmassnahmen möglichst verhindert werden (siehe 5 und 6).

■ Viele Interessen der Arbeitgeberin können bereits mit einer nicht personenbezogenen Überwachung des Systems gewahrt werden (siehe 7).

■ Personenbezogen darf eine Überwachung erst erfolgen, wenn die nicht personenbezogene Systemüberwachung klare Anhaltspunkte für Missbrauch oder Risikoverhalten ergibt (siehe 8).

5. Rechtlich-organisatorische Prävention

Die Arbeitgeberin kann mit rechtlichen und organisatorischen Massnahmen präventiv darauf hinwirken, dass Konfliktsituationen gar nicht erst entstehen.

Es obliegt der Arbeitgeberin, über die Zulassung der Nutzung neuer Kommunikationsmittel zu entscheiden. Es gibt kein «Recht auf Internet am Arbeitsplatz». Die Arbeitgeberin hat zu entscheiden, für welche Funktionen, für welche Zwecke und in welchem Rahmen die Internetnutzung sinnvoll und erlaubt ist. Wichtig ist aber auch, dass die Arbeitgeberin nicht bloss die entsprechenden Mittel zur Verfügung stellt, sondern gleichzeitig auch ihre Nutzung klar regelt. Beispiele:

■ Die Arbeitgeberin kann den *Nutzungszweck* bestimmen. Sie kann die Nutzung des Internets generell verbieten oder erlauben; sie kann sie generell für Geschäftszwecke erlauben und für private Zwecke verbieten; sie kann die private Nutzung auf Zusehen hin erlauben, sie auf eine «nicht übermässige» Nutzung beschränken, etwa bezüglich der Arbeitszeit oder der Systemkapazität auf ein «vernachlässigbares Mass». Sie kann die Nutzungsberechtigung – etwa bei Nichteinhaltung der Regeln – auch wieder entziehen.

■ Die Arbeitgeberin kann die Nutzung nicht nur vom Zweck, sondern auch vom *Inhalt* her beschränken. Sie kann z.B. bestimmte Nutzungen verbieten, so das Aufrufen von Websites mit rechtwidrigem (rassendiskriminierendem, pornografischem) Inhalt[23].

■ Die Arbeitgeberin kann die Nutzung einzelner *Dienste* speziell regeln, etwa den Besuch von Chat Rooms oder das Abonnieren von (vielleicht auch bloss kostenpflichtigen) News Groups verbieten – eventuell mit der Möglichkeit, dass in begründeten Fällen Ausnahmen bewilligt werden können.

■ Die Arbeitgeberin kann bestimmte *Aktivitäten* einschränken oder verbieten, etwa den Versand von Werbung, von Kettenbriefen oder das Versenden zu grosser Dateien. Sie kann das Öffnen von Programmen aus dem Internet und die Installation von nicht angemeldeten Programmen untersagen. Sie darf auch etwa

Finanztransaktionen (Telebanking, Börsengeschäfte usw.), den Eintrag der Firmenadresse in Internet-Datenbanken, die Verwendung von Firmenpasswörtern, die automatisierte Weiterleitung von E-Mails und Ähnliches verbieten. Zu regeln ist insbesondere auch das Vorgehen, das bei Verdacht auf Missbrauch oder bei Risikoverhalten zum Tragen kommt.

Solche Weisungen müssen den Arbeitnehmerinnen auch bekannt sein. Je einschneidender die Regelung und die vorgesehenen Kontrollmassnahmen sind, umso höher sind die Anforderungen an die *«Publizität» der Weisungen*. Bei einem absoluten Verbot privater Nutzung ist es ungenügend, wenn dieses bloss in einem «Weisungs-Ordner» enthalten ist. Eine Lösung stellt etwa das Einrichten einer «Begrüssungsseite» dar, welche die Arbeitnehmerin bei jedem Einloggen ins System an die wichtigsten Regeln erinnert und nur durch ein akzeptierendes Klicken passiert werden kann.

Was gilt, wenn solche Weisungen fehlen? Ohne ausdrückliche Regelung darf davon ausgegangen werden, dass die nicht übermässige private Nutzung des Internets und seiner Dienste erlaubt ist und keine präventive Überwachung erfolgt. Besteht nur für das private Telefonieren am Arbeitsplatz eine ausdrückliche Regelung, kann allenfalls davon ausgegangen werden, dass diese sinngemäss auch für die Internet-Nutzung gilt. Eine ausdrückliche Regelung empfiehlt sich aber auf jeden Fall.

Allerdings kann auch das Verbot, private E-Mails zu versenden, nicht verhindern, dass eine Arbeitnehmerin private E-Mails erhält, insbesondere bei transparenten E-Mail-Adressen (vorname.name@firma.ch). Unter Umständen kann – auf organisatorischer Ebene – der Verzicht auf die Einrichtung persönlicher E-Mail-Konten und die Einrichtung unpersönlicher Konten (support@firma.ch) das Problem des Eingangs privater E-Mails entschärfen. Bei solchen Konten muss nicht damit gerechnet werden, dass private E-Mails eingehen.

6. Technische Präventionsmassnahmen

Mitarbeiterinnen können bestehende Regeln verletzen und das Internet missbräuchlich nutzen oder durch ihr Risikoverhalten die Sicherheit gefährden. Somit können – trotz rechtlicher Regeln und organisatorischer Massnahmen – Konfliktsituationen entstehen. Es geht deshalb darum, durch technische Präventionsmassnahmen solches Verhalten im Voraus weitgehend auszuschliessen.

6.1. Sicherheit im Allgemeinen

Vorweg ist festzuhalten, dass es heute als Standard eines verantwortungsbewussten Umgangs mit Informationstechnologie gelten müsste, dass die Frage der *Informatiksicherheit* in einem Betrieb oder einer Verwaltungsstelle – gerade bei Netzwerken – systematisch angegangen wird. Mit einem Konzept, das auf einem «baseline approach» basiert[24], kann mit vernünftigem Aufwand Missbrauch oder Risikoverhalten von Anfang an verunmöglicht oder wenigstens erschwert werden – etwa dann, wenn Disketten- oder CD-Laufwerke ausgebaut oder gesperrt werden, oder wenn die Installation von Programmen durch die Benutzerinnen gesperrt wird. Dazu gehören im hier interessierenden Zusammenhang etwa auch der Einsatz und die Konfiguration einer Firewall, die Installation einer immer im Hintergrund aktiven, durch die Benutzerinnen nicht deaktivierbaren und periodisch aktualisierten Virenwächter-Software oder die Einstellungen der Zugangsprogramme (Browser)[25]. Wo auf diese Weise ein risikobehaftetes oder missbräuchliches Verhalten bereits verunmöglicht werden kann, braucht man gar nicht mehr zu versuchen, solchem Verhalten mit technischen Überwachungsmassnahmen auf die Spur zu kommen.

Personenbezogen darf eine Überwachung erst erfolgen, wenn die nicht personenbezogene Überwachung klare Anhaltspunkte für Missbrauch oder Risikoverhalten ergibt.

Wenn man sich vor Augen hält, dass die Mehrzahl der sicherheitsrelevanten Vorfälle «von innen» kommt, sind Sicherheitsüberprüfungen für Mitarbeiterinnen, die in sensitiven Bereichen eingesetzt werden, unabdingbar. Die Rede ist von Bereichen, wo es um heikle Daten geht, oder von solchen, die für die Sicherheit relevant sind, etwa Systemadministratorinnen oder ähnliche Schlüsselpositionen. Logischerweise reicht eine einmalige Sicherheitsüberprüfung nicht. Solche Überprüfungen sind vielmehr regelmässig durchzuführen.

Der Bedarf nach Sicherheitsüberprüfungen ist kein Freipass für eine unbeschränkte Erhebung von Daten über Personen, die in solchen Schlüsselpositionen arbeiten. Sicherheitsüberprüfungen sind – datenschutzrechtlich betrachtet – Datenbearbeitungen. Sie müssen deshalb den Grundsätzen des Datenschutzrechts (siehe 2) genügen, also insbesondere rechtmässig und verhältnismässig sein. Das bedeutet erstens, dass die rechtlichen Grund-

lagen geschaffen werden müssen[26]. Zweitens muss sich die Überprüfung auf Personen beschränken, die aufgrund ihres Zugangs zu Informationen oder Systemen ein Sicherheitsrisiko darstellen können, und es müssen ihr drittens klare Grenzen gesetzt werden bezüglich der Daten, die zur Beurteilung des Risikos bearbeitet werden dürfen[27].

6.2. Spezifische Massnahmen

Es ist der Arbeitgeberin unbenommen, technische Präventionsmassnahmen wie Sperrungen oder automatisiertes Anfügen von Zusätzen vorzusehen.

- Die Arbeitgeberin kann beispielsweise die Nutzung des Internets und des E-Mail-Systems ganz oder teilweise sperren oder mit Filtern versehen. Sie kann den Zugang zu bestimmten URL-Adressen oder Diensten sperren oder die Grösse der übertragbaren Dateien limitieren.
- Die Arbeitgeberin darf den über ihre Systeme oder mit ihren Adressen versandten E-Mails automatisiert Informationen anfügen, etwa Vorbehalte zur Rechtswirkung des Inhalts, zur Vertraulichkeit usw., solange dabei die Inhalte nicht eingesehen oder aufgezeichnet werden.

Solange also in einem Unternehmen Nutzungsdaten nur ohne einen Personenbezug erhoben werden, entstehen keine datenschutzrechtlichen Probleme.

7. Nicht personenbezogene Überwachung

Auch mit der Kombination von rechtlichen, organisatorischen und technischen Präventionsmassnahmen kann ein Missbrauch oder eine Gefährdung der Sicherheit nicht ganz ausgeschlossen werden. Dem Schutz der Interessen der Arbeitgeberin dient – als nächster Schritt – eine *«nicht personenbezogene Systemüberwachung»*. Darunter fallen zwei verschiedene Sachverhalte:

7.1. Überwachung ohne Personendaten

Das Datenschutzgesetz – aber auch die anderen erwähnten gesetzlichen Vorschriften – regeln bloss das Bearbeiten von Personendaten, also von Angaben, die sich auf bestimmte oder bestimmbare Personen beziehen. Zur Bestimmbarkeit genügt es, dass durch die Kombination mit zusätzlichen Informationen – z.B. durch die Arbeitgeberin – darauf geschlossen werden kann, um wen es sich handelt[28]. In einem Unternehmen sind Personen beispielsweise über ihre Funktion («Chefin Rechtsdienst»), über ihre Personalnummer, ihre AHV-Nummer, aber auch über fest zugeteilte IP-Adressen oder Benutzerkennungen im Unternehmensnetzwerk bestimmbar – erst recht über «sprechende» (z.B. «supmeiem» für Marianne Meier in der Support-Abteilung).

Sobald auf die Verwendung solcher identifizierender Informationen verzichtet wird, die dahinter stehenden Personen also nicht (mehr) bestimmbar sind, muss eine Bearbeitung dieser Daten nicht mehr den Voraussetzungen des Datenschutzgesetzes genügen. Solange also in einem Unternehmen Nutzungsdaten nur ohne einen Personenbezug erhoben werden, entstehen keine datenschutzrechtlichen Probleme.

- Die Arbeitnehmerin darf beispielsweise statistische Erhebungen – welche URL-Seiten werden aus dem Unternehmen heraus an einem Tag abgerufen? – durchführen, die dazu dienen, das System zu optimieren (z.B. für das Cache-Management).
- Die Arbeitgeberin kann die Internet-Nutzung protokollieren, solange dabei die Nutzerinnen nicht bestimmbar werden, also keinerlei Daten über die Arbeitnehmerinnen – auch nicht über ausschliesslich genutzte Arbeitsstationen oder feste IP-Adressen – aufgezeichnet werden. Zulässig sind beispielsweise Erhebungen für die Kapazitätsplanung, welche Datenmengen von einem Abteilungsserver – nicht aber von einer Arbeitsstation aus, welche einer Nutzerin zugeordnet werden kann – abgerufen werden.
- Die Arbeitgeberin darf den Datenverkehr über ihre Systeme vollautomatisiert nach Inhalten scannen, die auf Gefahren (Systemüberlastung usw.) oder Missbrauch (Geheimnisverrat, Betrügereien usw.) hindeuten, solange die Inhalte oder die nicht anonymisierten Auswertungen nicht gespeichert werden und keinen weiteren Personen – auch nicht den Systemadministratorinnen – zugänglich sind[29].

Allerdings sind gegenüber einem solchen Vorgehen Bedenken und Zweifel in verschiedener Hinsicht angebracht. Vermag ein solches Vorgehen die Bedürfnisse einer wirkungsvollen Systemüberwachung überhaupt zu erfüllen? Und kann ein Zugriff auf die Inhalte wirkungsvoll ausgeschlossen werden, wenn zugleich die Beweise für allfällig begangene Straftaten zuhanden der Strafuntersuchungsbehörden gesichert werden sollten? Hier müssten wohl die entsprechenden Tools im Sinne von PET («Privacy Enhancing Technologies») erst entwickelt werden.

7.2. Überwachung ohne «Blick auf Personen»

Eine Systemüberwachung kann aber auch nicht personenbezogen sein, wenn zwar mit Personendaten gearbeitet wird, aber der Zweck der Datenbearbeitung nicht auf die Personen gerichtet ist[30]. In diesem Fall dürfen also zum Zweck der Systemüberwachung Personendaten bearbeitet werden, aber eben nur zu diesem Zweck. Das datenschutzgesetzliche Zweckbindungsgebot schliesst die Verwendung dieser Daten für andere Zwecke aus, also auch für die Überwachung der Arbeitnehmerinnen.

Das bedeutet, dass eine Aufzeichnung der Nutzungsdaten – z.B. IP-Adresse und User ID – für die Systemüberwachung zulässig ist. In analoger Anwendung der Bestimmungen für die Datenbearbeitung zu den Zwecken von Wissenschaft und Forschung müssen aber die Daten, sobald es der Bearbeitungszweck – hier eben die Systemüberwachung – erlaubt, anonymisiert werden und dürfen bei Auswertungen oder bei der Bekanntgabe dieser Daten die Arbeitnehmerinnen nicht mehr bestimmbar sein.

8. Personenbezogene Überwachung

8.1. Grundsätzliches Verbot

Es ist der Arbeitgeberin grundsätzlich nicht erlaubt, E-Mails und Internet-Zugriffe der Arbeitnehmerin zu speichern, zu überwachen oder zu kontrollieren, weil sie dabei auf private Inhalte und Informationen stossen und das Verhalten der Arbeitnehmerin überwachen kann.

Das heisst aber, dass – umgekehrt formuliert – die Überwachung erlaubt ist, wenn ausgeschlossen werden kann, dass private Inhalte gespeichert und überwacht werden. Konkret bedeutet das Folgendes:

- Bei unpersönlichen E-Mail-Konten einer Funktionsstelle (support@firma.ch) dürfen ein- und ausgehende Mails gespeichert und überwacht werden, weil hier nicht mit privaten E-Mails gerechnet werden muss. Stellt sich ein Mail trotzdem als privat heraus, muss es möglichst ungelesen an die Empfängerin weitergeleitet werden und es sind alle Kopien zu löschen.
- Der Postausgang eines persönlichen E-Mail-Kontos (vorname.name@firma.ch) darf nur überwacht werden, wenn und soweit dies aus betrieblichen Gründen unerlässlich ist (z.B. zur Dokumentation von Geschäftsvorgängen), der Versand privater E-Mails gänzlich verboten ist oder garantiert ausgeschlossen werden kann, dass private E-Mails überwacht werden[31].
- Der Posteingang eines persönlichen E-Mail-Kontos (vorname.name@firma.ch) darf nicht überwacht werden, weil der Eingang privater E-Mails nicht ausgeschlossen werden kann, es sei denn, dass private E-Mails von der Überwachung garantiert ausgeschlossen werden können[32].
- Internet-Zugriffe einer bestimmten Arbeitnehmerin dürfen nur unter der kumulativen Voraussetzung überwacht werden, dass (und soweit) dies aus betrieblichen Gründen unerlässlich ist (z.B. zur Leistungskontrolle) und die private Internet-Nutzung absolut verboten ist. Eine systematische und lückenlose Überwachung der Internet-Zugriffe einer Arbeitnehmerin ist in der Regel aber nicht erforderlich und damit nicht zulässig. Selbst für eine Leistungskontrolle wird eine Stichprobenkontrolle an ein paar Tagen pro Monat genügen.

Die Arbeitgeberin hat anzukündigen, dass sie die Internet-Zugriffe und Dienste-Nutzung künftig personenbezogen kontrollieren und Verstösse disziplinarisch sanktionieren werde.

8.2. Bei konkreten Anhaltspunkten

Eine Ausnahme vom grundsätzlichen Verbot der Überwachung von E-Mails und Internet-Zugriffen ist möglich, wenn konkrete Anhaltspunkte für Missbrauch vorliegen. Dabei ist zu unterscheiden zwischen «bloss» arbeitsvertragswidrigem, aber nicht strafbarem Handeln einerseits[33] und strafbarem Verhalten anderseits[34]. Anhaltspunkte können sich etwa dann ergeben, wenn beim automatisierten, nicht personenbezogenen Scannen von Internet-Zugriffen der Zugriff auf rechtswidrige Inhalte oder – wenn die private Nutzung verboten ist – auf Inhalte, die nichts mit geschäftlicher Nutzung zu tun haben können, festgestellt wird.

Auch wenn Anhaltspunkte für ein «bloss» *arbeitsvertragswidriges, aber nicht strafbares Handeln* vorliegen, darf die Arbeitgeberin nicht beliebig aufzeichnen und auswerten. Es ist vielmehr ein «Kaskadensystem» von Massnahmen angezeigt:

- Voraussetzung ist, dass den Arbeitnehmerinnen die Nutzungsregeln bekannt sind: welche Arten der Nutzung des Internets und seiner Dienste sind erlaubt, welche nicht?
- Wird bei der nicht personenbezogenen Systemüberwachung ein Missbrauch festgestellt, sind die Arbeitnehmerinnen mit Verweis auf die geltenden Nutzungsregeln darauf hinzuweisen, dass das nicht geduldet werden kann. Die Arbeitgeberin hat anzukündigen, dass sie die Internet-Zugriffe und Dienste-Nutzung

künftig personenbezogen kontrollieren und Verstösse disziplinarisch sanktionieren werde.
- Ab diesem Zeitpunkt dürfen während einer angemessenen Zeit (z.B. während eines Monats) an zufällig ausgewählten Tagen die Zugriffe personenbezogen protokolliert werden.
- Die ab der Mitteilung der Überwachungsankündigung erstellten Protokolle dürfen durch die Verantwortlichen[35] ausgewertet werden, soweit dies geeignet und erforderlich ist, um die fehlbare Arbeitnehmerin zu eruieren und die Verstösse zu sanktionieren.
- Wenn die «Täterinnen» erwischt worden sind oder die personenbezogene Überwachung keine Verstösse mehr zu Tage bringt, ist die personenbezogene Auswertung einzustellen und wieder auf das erlaubte «Normalniveau» (nicht personenbezogene Systemüberwachung: siehe 7) «herunterzufahren».

Selbstredend hat die Sanktionierung in den Formen und Verfahren zu erfolgen, die dafür vorgesehen sind. Die Tatsache, dass jemand wegen eines Verstosses gegen die Nutzungsregeln bestraft worden ist, darf im Sinne einer Generalprävention bekannt gemacht werden, selbstverständlich aber nicht der Name der bestraften Arbeitnehmerin.

Der «Beweiswert» der Resultate einer technischen Überwachung in einem Sanktionierungsverfahren darf allerdings nicht überschätzt werden. Über unverdächtige Links kann die Arbeitnehmerin auf Seiten stossen, deren rechtswidriger Inhalt erst zu erkennen ist, wenn die Seite schon heruntergeladen ist[36]. Wer sich in einem Chat Room anmeldet und nicht wieder aussteigt, kann im Laufe eines Tages Tausende von Hits «produzieren», ohne Arbeitszeit zu «vergeuden».

Bei Verstössen gegen die E-Mail-Regeln ist zu beachten, dass die Arbeitnehmerin nicht dazu gezwungen werden kann, private E-Mails zugänglich zu machen.

Eine praktikable Lösung könnte so aussehen, dass nach der Androhung der künftigen Überwachung mit der Arbeitnehmerin zusammen die aufgezeichneten E-Mails anhand der E-Mail-Adressen durchgegangen werden und sie den geschäftlichen Zusammenhang plausibel machen muss.

Die in diesem Zusammenhang oft geäusserte Befürchtung, man könne so nicht mehr gegen Arbeitnehmer vorgehen, welche Kolleginnen mit E-Mails sexuell belästigen, ist grundlos. Wer durch elektronische Post belästigt wird, kann solche E-Mails für die (Rück-)Verfolgung zum Absender zur Verfügung stellen, damit die Arbeitgeberin ihrer gesetzlichen Pflicht zum Schutz vor sexueller Belästigung nachkommen kann.

Wenn Anhaltspunkte für *rechtswidriges, insbesondere strafbares Handeln* vorliegen, kommt der staatliche Strafanspruch ins Blickfeld. Die Arbeitgeberin hat in diesen Fällen die *Strafverfolgungsorgane* einzuschalten. Sie können mit ihren untersuchungsrichterlichen Kompetenzen die nötigen Überwachungsmassnahmen anordnen – in diesem Fall auch die retrospektive Auswertung bestehender Protokollierungen.

Auf Grund des staatlichen Strafanspruchs, der die Selbstjustiz ersetzen will, liegt es nicht im Belieben der Arbeitgeberin, die Strafverfolgungsorgane einzuschalten oder nicht – auch wenn in der Praxis solche Fälle oft aus Angst vor einem Imageverlust lieber unter dem Deckel gehalten werden und Lösungen «im gegenseitigen Einvernehmen» getroffen werden.

8.3. Andere Gründe

Schliesslich ist der Vollständigkeit halber noch darauf hinzuweisen, dass auch andere Gründe eine Speicherung und Überwachung von Internet-Zugriffs- und E-Mail-Daten erlauben können.
- Bei einem Backup von Daten auf dem Mail-Server werden selbstverständlich Personendaten mitgesichert. Eine solche Speicherung ist erlaubt, doch dürfen die Sicherheitskopien für nichts anderes verwendet werden als für den Fall einer Daten-Wiederherstellung. Sie dürfen

Kurz und bündig

Die Arbeitgebenden dürfen die Internet-Nutzung regeln: Es gibt kein «Recht auf Internet am Arbeitsplatz». Sie können Missbrauch und Risikoverhalten bis zu einem gewissen Grad auch mit organisatorischen und vor allem technischen Präventivmassnahmen unterbinden. Die arbeits- und datenschutzrechtlichen Bestimmungen lassen hingegen eine technische Überwachung der Arbeitnehmenden nur in sehr restriktivem Rahmen zu. So sind die Systeme grundsätzlich nicht personenbezogen zu überwachen. Erst wenn die nicht personenbezogene Systemüberwachung konkrete Anhaltspunkte für Missbrauch oder Risikoverhalten ergibt, darf zur personenbezogenen Überwachung geschritten werden. Diese muss allerdings angekündigt oder angedroht werden, muss verhältnismässig, d.h. umfangmässig, inhaltlich und zeitlich auf das erforderliche Mindestmass beschränkt sein. In private E-Mails kann – auch wenn privates Mailen verboten ist – nicht Einblick verlangt werden. Besteht der Verdacht auf strafbare Handlungen, sind die Strafuntersuchungsbehörden beizuziehen, die gestützt auf eine richterliche Anordnung weitergehende Kompetenzen erhalten können.

also insbesondere nur unter den gleichen Voraussetzungen ausgewertet werden wie die ursprünglichen Daten.

■ Es ist denkbar, dass in bestimmten Arbeitsverhältnissen Internet-Zugriffe oder E-Mails für Leistungsabrechnungen erfasst werden müssen, etwa wenn Leistungen an Kundinnen weiterverrechnet werden müssen (z.B. Internet-Recherchen im Auftrag, Bearbeitung von E-Mails durch Support Call Centers).

9. Technik ersetzt Personalführung nicht

Ob private Nutzung absolut verboten oder in angemessenem Masse geduldet wird, ob die Nutzung überwacht wird oder auf die Selbstverantwortung der Arbeitnehmerinnen gebaut wird – wie ein Unternehmen oder eine Behörde mit der Nutzung des Internets und seiner Dienste umgehen, hat viel mit Unternehmenskultur zu tun. Ein absolutes Verbot der privaten Nutzung – daran ist aber nicht zu rütteln – ist zulässig. Allerdings ist eine solche Lösung wohl eher praxisfremd, weil damit Verstösse geradezu vorprogrammiert sind. Ausserdem ist eine Kontrolle, ob eine private Nutzung vorliegt, nur unter sehr engen Voraussetzungen zulässig und im Aufwand-Nutzen-Vergleich kaum verhältnismässig. Wer sich in der internetnutzenden Arbeitswelt umhört, wird schnell auch gewahr, dass zwar etliche Unternehmen und Behörden sehr restriktive Regelungen kennen, aber die Einhaltung kaum überwachen. Man hat dann – wenn es einmal nötig werden sollte – die nötigen Verbote zur Hand. Allerdings leidet so die Glaubwürdigkeit von Regelungen der Arbeitgeberin generell.

Der Eindruck täuscht wohl nicht, dass in vielen Fällen, wo die technische Überwachung forciert wird, ein Manko auf anderem Gebiet ausgeglichen werden soll. Mit technischen Mitteln wird versucht, mangelnde Personalführung zu kompensieren. Seien wir ehrlich: Wenn heute eine Arbeitnehmerin stundenlang zum Vergnügen chatten oder im Internet surfen kann, ohne dass die Arbeitsleistung darunter offensichtlich leidet, was hat sie dann früher während der Arbeitszeit gemacht, als sie noch keinen Internet-Zugang hatte? Zu Recht wehren sich die Informatikerinnen gegen den Versuch, ihnen die Rolle der Aufseherinnen zuschieben zu wollen. Die gesetzlichen Regeln lassen den Unternehmen und Behörden als Arbeitgeberinnen nur einen engen Spielraum für zulässige technische Überwachung. ■

Fussnoten und Links

1 Fast jedes Netzmanagementtool kann als auch zur Überwachung und/ oder Kontrolle der Useraktivitäten eingesetzt werden, z.B. Sniffer Pro (von Network Associates) oder eTrust Intrusion Detection Software (von Computer Associates). Vgl. auch ROLF OPPLIGER/MARCUS HOLTHAUS, Totale Überwachung ist technisch möglich , in: digma 2001, 14 ff.

2 Unter «Arbeitnehmerin» werden Arbeitnehmer, unter «Arbeitgeberin» Arbeitgeber selbstverständlich mitverstanden.

3 Bundesgesetz vom 30. März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) (OR, SR 220), im Internet abrufbar unter http://www.admin.ch/ch/d/sr/c220.html.

4 Art. 321d Abs. 2 OR.

5 Art. 321a Abs. 4 OR.

6 Art. 321e Abs. 1 OR.

7 Art. 328 OR.

8 Damit sind – nach MATTHIAS SCHWAIBOLD, Art. 328b/ Art. 362 OR Rz. 9, in: in: URS MAURER/ NEDIM PETER VOGT (Hrsg.), Kommentar zum schweizerischen Datenschutzgesetz, Basel/ Frankfurt a.M. 1995 – Daten über die persönliche und berufliche Qualifikation der Arbeitnehmerin gemeint, also die Voraussetzungen, derer sie vernünftigerweise bedarf, um ihre Arbeit machen zu können, also Angaben über die Schulbildung, Berufsausbildung, allfällige Zusatzqualifikationen wie Sprachkenntnisse, Auslanderfahrung, berufsbegleitende Ausbildungen. Weitere Angaben können bei so genannten Tendenzbetrieben, die also ideelle oder weltanschauliche Ziele verfolgen, dazu gehören.

9 Mit «Durchführung» ist weniger gemeint als mit «Erfüllung» (MATTHIAS SCHWAIBOLD [Fn. 8], Art. 328b/ Art. 362 OR Rz. 10): Es bezieht sich nur auf die äusserlich-organisatorische Seite des Arbeitsverhältnisses, während mit Erfüllung auch die inhaltliche Seite – die eigentliche Arbeitsleistung – gemeint wäre.

10 Art. 328b OR.

11 Art. 362 Abs. 1 OR: Von Art. 328b OR darf weder durch Abrede noch durch Normalarbeitsvertrag oder Gesamtarbeitsvertrag zuungunsten der Arbeitnehmerin abgewichen werden.

12 Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG-, SR 235.1), im Internet abrufbar unter http://www.admin.ch/ch/d/sr/c235_1.html.

13 Art. 4 DSG.

14 Art. 5 Abs. 1 DSG.
15 Art. 12 Abs. 2 lit. a und b DSG.
16 Art. 13 Abs. 1 DSG.
17 Art. 13 Abs. 2 lit. a DSG.
18 Art. 26 der Verordnung 3 vom 18. August 1993 zum Arbeitsgesetz (Gesundheitsvorsorge, ArGV 3, SR 822.113), im Internet abrufbar unter http://www.admin.ch/ch/d/sr/c822_113.html.
19 Vgl. dazu Leitfaden des Eidgenössischen Datenschutzbeauftragten für die Bearbeitung von Personendaten im Arbeitsbereich, Bern 1994, 21 f. (abrufbar über http://www.edsb.ch unter Publikationen | Merkblätter). Vgl. nun auch Protection of Workers' Personal Data, An ILO code of practice, Geneva 1997.
20 7. Tätigkeitsbericht des Eidgenössischen Datenschutzbeauftragten 1999/2000 (TB EDSB 1999/2000), 31 ff.
21 Art. 179 ff. des Schweizerischen Strafgesetzbuches vom 21. Dezember 1937 (StGB, SR 331.0), im Internet abrufbar unter http://www.admin.ch/ch/d/sr/c311_0.html.
22 Vgl. dazu auch DAVID ROSENTHAL, Rechtsgutachten zur Internetnutzung [und deren Überwachung] am Arbeitsplatz (Juni 2000), im Internet abrufbar unter http://www.rvo.ch/docs/internetarbeitsplatz.pdf.
23 Möglich wären auch engere Grenzen, etwa das Verbot, Websites mit unethischem, unmoralischem, beleidigendem Inhalt usw. aufzurufen. Hier drohen aber im Streitfall unergiebige Diskussionen, was unethisch, unmoralisch oder beleidigend ist.
24 Etwa nach dem IT-Grundschutzhandbuch des (deutschen) Bundesamtes für Sicherheit in der Informationstechnik (aktuelle Version: IT-Grundschutzhandbuch 2000, Köln 2000); http://www.bsi.de/gshb/deutsch/menue.htm.
25 Vgl. dazu etwa die Aktion Safer surf des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (http://www.rewi.huberlin.de/Datenschutz/DSB/SH/material/themen/safesurf/safer/sitemap.htm).
26 Im privatrechtlichen Arbeitsverhältnis auf vertraglicher Ebene, im öffentlichrechtlichen durch Gesetz. Im Bund bieten etwa die Art. 19 ff. des Bundesgesetzes vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (BWIS, SR 120, im Internet abrufbar unter http://www.admin.ch/ch/d/sr/c120.html) eine gesetzliche Grundlage für bestimmte Sicherheitsüberprüfungen, konkretisiert in der Verordnung vom 20. Januar 2000 über die Sicherheitsüberprüfungen (PSPV, SR 120.4, abrufbar unter http://www.admin.ch/ch/d/sr/c120_4.html). Auf kantonaler Ebene scheinen die gesetzlichen Grundlagen weitgehend zu fehlen; vgl. aber beispielsweise § 2 Abs. 2 der kantonalzürcherischen Verordnung vom 8. Oktober 1997 über den Flughafen (LS 748.21), im Internet abrufbar unter http://www.kanton.zh.ch (über Gesetze | ZH-Lex | Aktuelle Fassungen | Band 9).
27 Vgl. als Illustration etwa zu den Sicherheitsüberprüfungen im nachrichtendienstlichen Umfeld: Vorkommnisse in der Untergruppe Nachrichtendienst des Generalstabs («Bellasi-Affäre»), Bericht der Geschäftsprüfungsdelegation der eidgenössischen Räte vom 24. November 1999, in: BBl 2000, 586 ff, insb. 610 f. (im Internet abrufbar unter http://www.admin.ch/ch/d/ff/2000/586.pdf); dazu ebenfalls 7. Tätigkeitsbericht des Eidgenössischen Datenschutzbeauftragten 1999/2000 (TB EDSB 1999/2000), 81 ff. (abrufbar über http://edsb.ch/pdf/t7d.pdf).
28 Vgl. dazu URS BELSER, Art. 3 Rz. 6, in: URS MAURER/ NEDIM PETER VOGT (Hrsg.), Kommentar zum schweizerischen Datenschutzgesetz, Basel/ Frankfurt a.M. 1995.
29 Mehr darf ein Unternehmen nur tun, wenn die unter 8.2 beschriebenen Voraussetzungen erfüllt sind.
30 Mit den Bestimmungen für Datenbearbeitungen zu den Zwecken von Wissenschaft und Forschung regeln die Datenschutzgesetze eine vergleichbare Konstellation; vgl. etwa Art. 22 DSG oder § 12 des basellandschaftlichen Gesetzes vom 7. März 1991 über den Schutz von Personendaten (Datenschutzgesetz/ DSG, SGS 162), im Internet abrufbar unter http://www.baselland.ch/docs/recht/sgs_1-2/162.0.htm.
31 Ein solcher Ausschluss ist höchstens bei stark formalisierten Abläufen möglich, wenn etwa durch das E-Mail-System vollautomatisiert nur solche E-Mails zur Überwachung ausgesondert werden, welche über bestimmte Merkmale (z.B. durch eine Geschäftsreferenz oder Bearbeitungsnummer) eindeutig als geschäftliche E-Mails identifiziert werden können. Die Arbeitnehmerin muss darüber vorgängig informiert sein.
32 Ein solcher Ausschluss muss wiederum durch das E-Mail-System aufgrund bestimmter Merkmale vollautomatisiert erfolgen, nicht etwa durch Dritte. Bereits die Tatsache, dass eine Arbeitnehmerin von einer bestimmten Absenderin elektronische Post erhält, ist eine Information, welche die Arbeitgeberin nichts angeht. Eine solche Aussonderung ist höchstens bei stark formalisierten Abläufen möglich, durch eine eindeutige Identifizierung als geschäftliches E-Mail anhand einer Geschäftsreferenz oder Bearbeitungsnummer.
33 Z.B. ein Verstoss gegen die unternehmensinternen Nutzungsweisungen, etwa durch privates Mailen trotz Verbot.
34 Z.B. durch Weiterverbreiten von pornografischen oder rassendiskriminierenden Inhalten, Verletzung von Geschäftsgeheimnissen, Betrug, Verbreiten von Computerviren usw.
35 Diese Auswertung ist Teil der Personalführung, nicht technisches Auszählen. Die Zuständigkeit dafür ist klar zu regeln. Sie gehört hierarchisch weit oben angesiedelt, sei es in der Geschäftsleitung oder bei Linienvorgesetzten der Verdächtigten.
36 Augenfällig etwa durch entsprechende Bilder (z.B. pornografische Darstellungen, rassendiskriminierende Karikaturen), weniger augenfällig bei Texten, deren (z.B. rassendiskriminierende) Natur sich vielleicht erst bei sorgfältiger Lektüre erkennen lässt.

Weitere Links

- Eidgenössischer Datenschutzbeauftragter, Internet- und E-Mail-Überwachung am Arbeitsplatz, Für öffentliche Verwaltungen und Privatwirtschaft, April 2001, im Internet abrufbar unter http://edsb.ch/pdf/leit_7.pdf
- Commission Nationale de l'Informatique et des Libertés (CNIL), La cybersurveillance des salariés dans l'entreprise, Rapport d'Etude et de consultation publique, Paris, März 2001, im Internet abrufbar unter http://www.cnil.fr/thematic/docs/entrep/cybersurveillance.pdf