**Miescher & Partner**, Rechtsanwälte, Bielstrasse 9, 4502 Solothurn
032 623 26 36 **matthias.miescher@anwalt-so.ch**

# Mitarbeiterüberwachung am Arbeitsplatz

**Referat vom 15. September 2004**

## Einleitung

Die Nutzung von Kommunikationsmitteln über das Internet ist in den letzten Jahren weit verbreitet. E-Mail und Informationsbeschaffung auf anderen Websites gehören heute auch zu den alltäglichen Arbeitsmitteln im Geschäftsleben.

Welche Spielregeln gelten dort? Die Besonderheiten liegen darin, dass einerseits mit viel weniger Aufwand kommuniziert wird, andererseits aber auch technische Möglichkeiten bestehen, Mitarbeitende am Arbeitsplatz zu überwachen, ohne sichtbare Spuren zu hinterlassen. Interessen der Arbeitnehmer und Arbeitgeber widerstreben oft und es besteht ein riesiger Gegensatz zwischen „Können" und „Dürfen". Die nachfolgenden Ausführungen sind Spielregeln, die sich aus dem Gesetz und der Rechtsprechung ableiten lassen und im Arbeitsbereich klare Regeln über die gegenseitigen Rechte und Pflichten zwischen Arbeitnehmer und Arbeitgeber aufstellen.

## 1. Damit die Lösung fair ist, findet eine Interessenabwägung statt

Bei der Suche nach einer Lösung, welche die Überwachung am Arbeitsplatz regelt, muss es vor allem darum gehen, den Missbrauch zu bekämpfen (was für beide, Arbeitnehmer und Arbeitgeber gilt!):

### a. Die Interessen des Arbeitgebers:

Er will eine möglichst hohe **Produktivität** am Arbeitsplatz. Die neuen Technologien sollen zwar ausgeschöpft werden, aber exzessives Surfen während der Arbeitszeit ist unerwünscht.
Die **Kapazität des Netzwerks** ist beschränkt, und es darf zu keinen Ausfällen kommen.
Der **Ruf der Firma** muss gewahrt werden: man will nicht ins Gerede kommen im Zusammenhang mit Vorwürfen wegen Pornographie, Rassismus, etc.

### b. Interessen des Arbeitnehmers:

Mitarbeitende erwarten den **Schutz ihrer Persönlichkeit**, insbesondere die Wahrung der **Privatsphäre**
Auch sie wollen ihre Produktivität ausschöpfen und erwarten ein gutes Arbeitsklima, weshalb sie die neuen Technologien nutzen möchten

In diesem Spannungsfeld muss der Lösungsansatz gefunden werden, aber es gibt keine Lösung, welche für jeden Betrieb standardisiert richtig ist: der Grossbetrieb braucht eine andere Lösung als die kleine Unternehmung.

**Miescher & Partner**, Rechtsanwälte, Bielstrasse 9, 4502 Solothurn
032 623 26 36 **matthias.miescher@anwalt-so.ch**

## 2.Einige einschlägige Rechtsnormen

**- Art. 7 und 8 Datenschutzgesetz (DSG) und Verordnung**
regeln den Schutz der Daten vor unberechtigtem Zugriff. Dabei unterstehen Personendaten besonderem Schutz. Der Betrieb ist verpflichtet, technische Massnahmen nach dem Stand der Technik zu ergreifen, um die Daten zu schützen. Daneben wird geregelt, dass Angestellte Auskunft über die gespeicherten Daten sowie allenfalls deren Korrektur verlangen können.

**- Art. 26 Verordnung Nr. 3 zum Arbeitsgesetz (V3 ArbG)**
verbietet das dauernde Überwachen der Mitarbeiter (auch im Intra- oder Internet)

**- Art. 179$^{nonies}$ Strafgesetzbuch (StGB)**
stellt die Verletzung der Privatsphäre sowie das unbefugte Beschaffen von Daten unter Strafe

## 3.Regelungsspielraum formell

Rechtsnormen alleine genügen nicht: der Gesetzgeber hat nämlich ausdrücklich vorgesehen, dass der Betrieb – innerhalb der Rechtsnormen – eine eigene Regelung treffen darf. In welcher Form? Aus Beweisgründen sollen die Regelungen grundsätzlich schriftlich erfolgen. Dabei muss sichergestellt werden, dass der Mitarbeiter vorher Kenntnis über seine Rechte und Pflichten erhält und ihm dies auch nachgewiesen werden kann, etwa indem er das entsprechende Schriftstück datiert und unterzeichnet. Zu empfehlen ist, ihm dies auch noch mündlich zu erklären. Es bestehen folgende Varianten:

**- im Arbeitsvertrag**
Die etnsprechende Klausel wird in den Text des Vertrages aufgenommen. Wird sie neu eingeführt. müssen Nachträge oder neue Verträge erstellt und vom Mitarbeiter unterzeichnet werden. Diese Variante hat den Vorteul, dass mit jedem Itarbeitenden individuelle Lösungen gteroffen werden können.

**- separate, ev. individuelle Vereinbarung mit den Mitarbeitenden**
entsprechen einem Nachtrag (s. oben)

**- Mitarbeiterhandbuch/Betriebsreglement**
Wo solche Schriftstücke bestehen, kann der Passus dort aufgenommen werden. Hier ist sorgfältig darauf zu achten, dass jeder Mitarbeiter nachweislich Kenntis von dessen Inhalt hat. Der Vorteil liegt darin, dass die neuregelung nicht in einer Aenderung des Arbeitsvertrages nachgeführt werden kann.

**- allgemeines Nutzungs- und Ueberwachungsreglement**
Der Betrieb kann ein allgemeines Nutzungs- und Ueberwachungsregelement erlassen. Es ist in der Regel sehr umfassend und lässt sich deshalb nicht ohne weiteres in ein Mitarbeiterhandbuch integrieren. Eine gute Vorlage hat der eidg. Datenschutzbeauftragte ausgearbeitet (vgl. Internetadresse am Schluss).

**- laissez faire**
zwar weit verbreitet, aber leider nicht zu empfehlen ...

**Miescher & Partner**, Rechtsanwälte, Bielstrasse 9, 4502 Solothurn
032 623 26 36 **matthias.miescher@anwalt-so.ch**

## 4.Regelungsspielraum inhaltlich

Hier sind folgende Kriterien von Bedeutung:

- **Nutzung** festlegen:
Wer darf was im Intra- oder Internet? Die Bedürfnisse können je nach Funktion des Mitarbeitenden sehr unterschiedlich sein. Daraus leitet sich auch der Umfang der Nutzung ab: einige brauchen keinen Anschluss, andere sollen ihn nur beruflich, eingeschränkt oder eingeschränkt privat nutzen können. Solche Nutzungen können sowohl schriftlich als auch technisch definiert werden.

Interessant ist, dass der Betrieb individuell festlegen kann, was er als Missbrauch definiert und wie die damit verbundenen Konsequenzen aussehen.

- (Vor-)**Information** der Mitarbeitenden:
Dies ist ein zentraler Punkt: Die Mitarbeitenden müssen vorab informiert werden, dass eine Überwachung stattfindet, wenn ein Missbrauch oder Verdacht auf einen Missbrauch bei der Nutzung des Internets festgestellt wird. Diesen Vorgang kenne wir von vergleichbaren Handlungen, etwa die Aufnahme von Telefongesprächen oder Sitzungsgesprächen.

- **Ausnahme**: schwerer Missbrauch
Liegt eine Straftat vor, darf sofort überwacht werden. Allerdings sollen sich die Betreibe nicht als Untersuchungsrichter gebärden. Bei begründeten Verdacht sind die spezialisierten Polizeiorgane einzuschalten.

## 5.Ablauf der Überwachung der Internetnutzung (Surfen)

Wie findet die Überwachung statt? Es bestehen sowohl zeitlich gestaffelte Massnahmen als auch unterschiedliche Eingriffe in Bezug auf deren Intensität:

**Stufe 1**: Zuerst müssen **technische Mittel** vorgesehen und die **Mitarbeitenden sensibilisiert** werden:
Sie sollen die Folgen des Missbrauchs, aber auch das daraus resultierende Schadenpotential für sich selber und den Betrieb kennen

**Stufe 2:** Liegt ein **Missbrauch** (nach betrieblicher Definition unerlaubte Nutzung) vor, muss er anonymisiert oder mindestens pseudoanonymisiert festgestellt werden. Eine dauernde konkrete Überwachung eines Arbeitsplatzes ist unzulässig. Erlaubt ist hingegen die Auswertung der Zugriffsstatistiken. Wird ein Missbrauch festgestellt, darf konkret während beschränkter Zeit überwacht werden.

**Stufe 3**: Sind die Mitarbeitenden über die Möglichkeit der Überwachung **informiert**, ist eine Rückverfolgung nach der Stufe 2 zulässig.

**Miescher & Partner**, Rechtsanwälte, Bielstrasse 9, 4502 Solothurn
032 623 26 36 **matthias.miescher@anwalt-so.ch**

## Ueberwachung des Surfens

**Anonym** dürfen die Protokollierungen ständig ausgewertet werden.

**Pseudoanonym** dürfen Stichproben erhoben werden, sofern gewährleistet ist, dass die Korrespondenzlisten getrennt aufbewahrt werden.

**Namentlich** darf nur gezielt und für kurze Zeit überwacht werden. Bestätigt sich der Missbrauchsverdacht nicht, wird sofort abgebrochen.

Aus der Sicht der Mitarbeitenden stellen sich folgende Fragen:

**Wer überwacht den Überwacher?**
Ein Missbrauch kann auch seitens jener stattfinden, die sich im Betrieb um die neuen Technologien kümmern. Sei es aus Überreifer, Angst vor Zwischenfällen oder purem „Gwunder", lohnt es sich, Missbräuchen auch hier vorzubeugen, indem die Überwacher nach dem 4-Augen-Prinzip arbeiten. So können die Korrespondenzlisten einer anderen Person als jener, welche die Stichproben durchführt, anvertraut werden. Zudem lohnt es sich, klare schriftliche Weisungen zu erteilen und mit Konsequenzen zu versehen.

**Wie nimmt die Geschäftsleitung ihre Verantwortung wahr?**
Da der Schutz der Persönlichkeit der Mitarbeitenden direkt tangiert wird und sic h erhebliche Konsequenzen für das Betriebsklima ergeben können, sind solche Regelungen nicht einfach der IT-Abteilung zu überlassen. Die Geschäftsleitung muss ihre Verantwortung und Aufsicht wahrnehmen. Besteht ein Funktionendiagramm (in jeder Aktiengesellschaft eigentlich eine Selbstverständlichkeit!), sind die Kompetenzen zu regeln.

## Überwachung von E-Mails

Hier besteht eine klare Praxis des Bundesgerichts:

- Private Mails dürfen nicht überprüft werden, denn sie unterstehen wie Briefe dem Fernmeldegeheimnis
- Privat ist, was als Privat gekennzeichnet ist (nicht aber „fritz.muster@abc.ch"!)
- Speicherung der privaten Daten auf externen Servern sowie Verschlüsselung ist dringend empfohlen!
- Geschäftliche E-Mails dagegen dürfen protokolliert und gespeichert werden.

Spezielle Fragen ergeben sich zudem bei Ferienabwesenheiten, Todesfällen oder Kündigungen.

**Miescher & Partner**, Rechtsanwälte, Bielstrasse 9, 4502 Solothurn
032 623 26 36 **matthias.miescher@anwalt-so.ch**

## 6.Sanktionen

Der **Arbeitgeber** kann Verwarnen, Versetzen, den Lohn kürzen, Schadenersatz und Genugtuung geltend machen, den Zugang sperren oder gar Entlassen und im Extremfall das Arbeitsverhältnis fristlos auflösen.

Vorsicht: Die Kompetenzen und formellen Voraussetzungen sind zu beachten, besonders bei schweren Massnahmen wie der fristlosen Kündigung!

Der **Arbeitnehmer** kann verlangen, dass die Überwachung regelkonform durchgeführt, allenfalls gestoppt und Schadenersatz oder Genugtuung gezahlt wird.

Diese zivilrechtlichen sind nicht zu verwechseln mit strafrechtlichen Sanktionen. Für die Strafuntersuchung und die Strafzumessung sind aber die staatlichen Gerichte und Behörden zuständig. Das ist vor allem für den Arbeitgeber sehr unangenehm, weil er den Strafverfolgungsbehörden Einsicht in die Abläufe geben muss.

## 7.Weiterführende Fundstellen zu diesen Themen:

| | |
|---|---|
| ☞**www.edsb.ch** | **Website des eidg. Datenschutzbeauftragten** insbesondere Aufsatz **Leitfaden über Internet- und E-Mailüberwachung am Arbeitsplatz** |
| ☞**www.admin.ch/ch/d/sr** | **Systematische Gesetzessammlung** |

Matthias Miescher, Rechtsanwalt und Mediator SAV