**Andrea Mondini**
**lic. iur., Schellenberg Wittmer Rechtsanwälte, Zürich, www.swlegal.ch**

# Internet und E-Mail am Arbeitsplatz

Die übermässige Nutzung von Internet und E-Mail am Arbeitsplatz kann die Produktivität eines Unternehmens beeinträchtigen und Sicherheitsrisiken zur Folge haben. Welche Massnahmen sollen Unternehmen ergreifen, um solche Missbräuche zu bekämpfen und welche rechtliche Grenzen haben Sie dabei zu beachten?

## 1. Ausgangslage

Dank einer technisch und organisatorisch durchdachten Nutzung von Internet und E-Mail können Unternehmen erhebliche Produktivitätsgewinne und Kosteneinsparungen erzielen. Doch durch die übermässige private Nutzung von Internet und E-Mail am Arbeitsplatz stehen diesen positiven Effekten Risiken und Bedrohungen gegenüber, welche mögliche Produktivitätsgewinne gefährden können.
Die übermässige Nutzung der Kommunikationsmittel eines Unternehmens für private Zwecke ist nicht nur von finanzieller Relevanz; eine Betrachtung drängt sich auch unter dem Aspekt der IT-Security auf, da der private Datenverkehr mit erhöhten Sicherheitsrisiken technischer Art (z.B. Computerviren), der übermässigen Beanspruchung von Speicherkapazitäten oder einer Blockierung des elektronischen Arbeitsplatzes verbunden sein kann. Vor diesem Hintergrund stellt sich die Frage, inwiefern und in welchem Umfang Arbeitgeber nach schweizerischem Recht die Nutzung von Internet und E-Mail zu privaten Zwecken am Arbeitsplatz dulden müssen und welche rechtlichen Schranken, insbesondere aus dem Arbeitsrecht, der Datenschutzgesetzgebung und dem Strafrecht, im Zusammenhang mit Schutzmassnahmen zu beachten sind.

## 2. Überblick: Präventive und repressive technische Massnahmen

Um die Möglichkeiten zur Risikobegrenzung aufzuzeigen, sind technische Fragen klar von

rechtlichen Fragen über die Zulässigkeit der privaten Nutzung abzugrenzen. In technischer Hinsicht sind präventive technische Schutzmassnahmen und repressive Überwachungsmassnahmen zu unterscheiden.

*Präventive technische Schutzmassnahmen* werden mit dem Ziel implementiert, Risiken zu minimieren und die Funktionstüchtigkeit und Sicherheit einer IT-Infrastruktur zu gewährleisten. Zu den wichtigsten präventiven technischen Schutzmassnahmen gehören der Passwortschutz, Zugriffsschutz, die Verschlüsselung besonders schützenswerter Daten, Antivirusprogramme, Sperrung des Zugangs zu bestimmten Websites, DiskquotaManagers, Backups und Firewalls. Schutzmassnahmen dieser Art sind aus rechtlicher Sicht nicht nur erlaubt, sondern erwünscht, da dadurch illegale Aktivitäten (z. B. Verbreitung von Computerviren, Computersabotage, Verletzung von Geschäftsgeheimnissen, Missbrauch von persönlichen Daten) präventiv verhindert werden sollen.

*Repressive technische Überwachungsmassnahmen* dienen dazu, etwaige Missbräuche im Nachhinein festzustellen und zu sanktionieren. Hier sind die Überwachung des Netzwerkes und des E-Mail-Verkehrs, die Bildschirmüberwachung oder gar die Tastatur- und Mausüberwachung von Bedeutung. Rechtlich sind repressive Überwachungsmassnahmen dieser Art nur in beschränktem Umfang zulässig. Entscheidend ist hier jedoch die abschreckende Wirkung, auf die im Zusammenhang mit arbeitsrechtlichen Mitteln zur Durchsetzung einzugehen ist.

Bereits an dieser Stelle ist festzuhalten, dass präventive technische Schutzmassnahmen stets Vorrang gegenüber repressiven Überwachungsmassnahmen haben sollten. Technische und organisatorische Schutzmassnahmen im Sinne der Prävention (z. B. um unerwünschtes Surfen im Internet in Grenzen zu halten und das Unternehmen vor technischem Schaden zu schützen) setzen aber gleichzeitig voraus, dass der Arbeitgeber technische Installationen regelmässig aktualisiert und bezüglich Sicherheitsstandards in angebrachter Art und Weise konfiguriert.

## 3. Rechtliche Schranken der Überwachung im Allgemeinen

Rechtliche Schranken der Überwachung von Arbeitnehmern ergeben sich insbesondere aus dem Arbeitsrecht, der Datenschutzgesetzgebung und dem Strafrecht. Zudem wird der Privatbereich vom Fernmeldegeheimnis erfasst. Ob, und wenn ja, in welchem Umfang die private Nutzung unternehmenseigener Kommunikationsmittel überhaupt erlaubt oder aber teilweise oder gänzlich verboten ist, sollte im Einzelfall Gegenstand eines Nutzungsreglements sein (vgl. 4).

Informatikmittel sind technisch in der Lage, durchgeführte Aktivitäten fortlaufend zu protokollieren. Die laufende, *anonyme* Überwachung der Funktionstüchtigkeit und Sicherheit eines IT-Systems ist rechtlich ohne weiteres zulässig. Auch die anonyme Überwachung des Surfverhaltens zur Erstellung von Statistiken ist erlaubt. Die Überwachung ist dann «anonym», wenn sie keine Rückschlüsse auf das Surfverhalten der einzelnen Arbeitnehmer erlaubt.

Hingegen ist die *personenbezogene,* heimliche, permanente Überwachung von Arbeitnehmern in der Schweiz rechtlich verboten (Art. 26 ArGV3).

Sinn und Zweck dieses Verbotes ist es, Arbeitnehmer vor ständiger, gezielter Verhaltensüberwachung zu schützen. Bildschirmüberwachung, Tastatur- und Mausüberwachung sowie so genannte «Spionprogramme» verletzen die Persönlichkeits- und Geheimsphäre der betroffenen Arbeitnehmer und sind deshalb nicht zulässig. Zudem wird der Persönlichkeitsschutz eines Arbeitnehmers vom Datenschutzgesetz und vom Arbeitsvertragsrecht erfasst. Zu den unzulässigen Überwachungen gehört auch die personenbezogene Auswertung der Protokollierungen ohne vorherige Information der Arbeitnehmer. Die Überwachung des Surfverhaltens zur Identifikation einer Person ist zudem nur ausnahmsweise bei Missbrauchsverdacht oder -feststellung zulässig, und dies nur in Fällen, in denen ein Missbrauch mit technischen Schutzmassnahmen nicht verhindert werden kann: Technische präventive Schutzvorkehrungen haben auch hier Vorrang. Eine solche Überwachung sollte pseudonym durchgeführt werden, indem Arbeitnehmern Pseudonyme (z. B. Zahlenfolgen) zugeordnet und vorerst in dieser nicht namentlichen Form IT-seitig erfasst werden. Bei Feststellung von Missbräuchen können diese Protokollierungen anhand einer Korrespondenzliste, welche die Zuordnung sichtbar macht und nur den Personalverantwortlichen bekannt ist, namentlich ausgewertet werden. Entscheidend ist dabei die Möglichkeit, Benutzerdaten in pseudonymisierter Form vorderhand ohne Einbezug der Personalverantwortlichen zu protokollieren.

Voraussetzung für eine personenbezogene Überwachung ist somit die Feststellung eines Missbrauchs bzw. eines entsprechenden Verdachts und die vorherige Information der Arbeitnehmer. Letztere wird in der Praxis durch einen entsprechenden Vorbehalt in einem schriftlichen Überwachungsreglement sichergestellt.

## 4. Empfohlene arbeitsrechtliche Mittel: Nutzungs- und Überwachungsreglement

Jeder Arbeitgeber hat ein arbeitsvertragliches *Weisungsrecht* (Art. 321d OR) und kann frei entscheiden, in welchem Umfang Internet und E-Mail am Arbeitsplatz zur Verfügung stehen und wie diese elektronischen Hilfsmittel zu nutzen sind. Entsprechend gross ist der rechtliche Spielraum: Der Arbeitgeber darf die Nutzung komplett verbieten, einschränken oder umgekehrt für bestimmte Aufgaben vorschreiben. Arbeitnehmer haben folglich keinen rechtlichen Anspruch auf die private Nutzung netzbasierter Anwendungen am Arbeitsplatz.

Um klare Verhältnisse zu schaffen, ist Arbeitgebern zu empfehlen, in Ausübung ihres Weisungsrechts ein *Nutzungs- und Überwachungsreglement* zu erlassen, das die Schranken des zu geschäftlichen und privaten Zwecken jeweils tolerierten Internet- und E-Mail-Gebrauchs festhält. Selbstverständlich können die Nutzung bzw. die Überwachung zusammen in einem einzigen Reglement oder getrennt geregelt werden.

### 4.1 Nutzungsreglement: Gebrauch nach dem Willen des Arbeitgebers

Der Erlass eines *Nutzungsreglements* ist zwar nicht obligatorisch, bietet jedoch dem Arbeitgeber eine Möglichkeit, klare Verhältnisse zu schaffen und vom rechtlichen Spielraum bezüglich der Einschränkungen der privaten Nutzung Gebrauch zu machen. Ob Arbeitnehmer das Recht haben, am Arbeitsplatz Internet und E-Mail für private Zwecke zu nutzen, hängt also in erster Linie vom Willen des Arbeitgebers ab, wobei der Umfang der Nutzungsberechtigung je nach Arbeitnehmerkategorie und den beruflichen Bedürfnissen unterschiedlich sein kann. Von Bedeutung ist zudem, dass der Verstoss gegen ein solches Reglement einen Rechtfertigungsgrund für die Identifikation einer fehlbaren Person darstellt (vgl. 3). In einem Reglement kann z. B. vorgesehen werden, dass am Arbeitsplatz der Download von Filmen und Musik untersagt oder dass die private E-Mail-Nutzung auf kurze, dringende Mitteilungen zu beschränken ist.

Auch wenn die allgemeine Sorgfalts- und Treuepflicht des Arbeitnehmers (Art. 321a OR) den angemessenen Umgang mit Mitteln des Arbeitgebers erfordert, besteht bei den Arbeitnehmern ohne Nutzungsreglement Unklarheit über die Befugnis zum Gebrauch von Internet- und E-Mail zu privaten Zwecken. Im Weiteren sollte das Nutzungsreglement konkret und klar sein, sodass die Grenzen der erlaubten privaten Nutzung am Arbeitsplatz unmissverständlich daraus hervorgehen. Andernfalls ist es in

der Praxis kaum möglich, eine Nutzung mit Blick auf private Zwecke für erlaubt oder unerlaubt zu erklären und damit einen Missbrauch festzustellen, der wiederum Voraussetzung für allfällige Sanktionen ist.

### 4.2 Überwachungsreglement: Möglichkeit der personenbezogenen Auswertung bei Missbrauch

Im Gegensatz zum Nutzungsreglement ist der Erlass eines *Überwachungsreglements* zwingend vorausgesetzt, sofern sich der Arbeitgeber die Möglichkeit vorbehalten will, Protokollierungen personenbezogen auszuwerten: Die damit stattfindende Überwachung kann einen Eingriff in die Privatsphäre des Arbeitnehmers darstellen. Durch einen entsprechenden Hinweis im Reglement genügt der Arbeitgeber dem Erfordernis, die Arbeitnehmer über die Möglichkeit dieses Eingriffes in Fällen eines Missbrauchs oder Missbrauchsverdachts in Kenntnis zu setzen. An dieser Stelle ist festzuhalten, dass der Erlass eines solchen Reglements eine überaus wünschbare Sensibilisierung der Arbeitnehmer mit sich bringen kann – allein das Bewusstsein, dass bei Missbräuchen eine personenbezogene Überwachung möglich ist, mag eine präventive Wirkung auf das Verhalten der Arbeitnehmer haben.

## 5. Geschäftliche und private E-Mails

Ist die Nutzung von E-Mail zu privaten Zwecken in einem Unternehmen grundsätzlich erlaubt und sind *private* E-Mails auch als solche erkennbar, beispielsweise durch einen entsprechenden Vermerk in der Betreffzeile, so sind sie privater Briefpost am Arbeitsplatz gleichzusetzen und geniessen den gleichen umfassenden Schutz. Wird solche persönliche Post von Dritten geöffnet, bzw. E-Mails mit dem Vermerk «privat» gelesen, ist darin eine widerrechtliche Persönlichkeitsverletzung zu erblicken: Der Arbeitgeber darf auf Grund des Persönlichkeitsschutzes und des Verhaltensüberwachungsverbotes keine Einsicht in den Inhalt privater E-Mails des Arbeitnehmers haben; als privat gekennzeichnete E-Mails dürfen also nicht inhaltlich ausgewertet werden. Zudem wird der E-Mail-Verkehr vom Fernmeldegeheimnis erfasst. E-Mails, die als privat gekennzeichnet sind, dürfen in keinem Fall inhaltlich ausgewertet werden.

Anders zeigt sich die Situation bei *geschäftlichen* E-Mails: Hier ist der Arbeitgeber berechtigt, diese systematisch zu protokollieren, zu registrieren und mittels Backups zu sichern. Geschäftliche E-Mails stellen grundsätzlich Geschäftskorrespondenz dar, sodass grundsätzlich während 10 Jahren eine Aufbewahrungspflicht besteht (Art. 962 OR). Im Rahmen der Sicherung bzw. Archivierung stellen sich jedoch praktische Unterscheidungsprobleme, die rechtlich nur gelöst werden können, indem der Arbeitgeber in einem Reglement allgemein bekannt gibt, dass grundsätzlich alle am Arbeitsplatz ausgetauschten E-Mails archiviert werden, also auch private E-Mails erfasst werden. Damit haben es die Arbeitnehmer in der Hand, die Archivierung privater E-Mails durch Löschung oder gänzlichen Verzicht auf private E-Mail-Kommunikation zu verhindern.

Aus praktischer Sicht empfiehlt sich die Erarbeitung und Durchsetzung einer eigentlichen E-Mail Policy als Gesamtkonzept in Bezug auf den Empfang, die Archivierung, die Löschung sowie die Einsichtsrechte.

## 6. Verstösse und Sanktionen

### 6.1 Missbrauch durch den Arbeitnehmer

Ein Missbrauch durch den Arbeitnehmer kann gegen arbeitsvertragliche Vereinbarungen bzw. gegen ein vom Arbeitgeber erlassenes Nutzungsreglement verstossen. In letzterem Fall haftet der Arbeitnehmer für vorsätzlich oder fahrlässig herbeigeführte Schäden (Art. 321e OR), wobei der Arbeitgeber die Pflichtverletzung des Arbeitnehmers und den resultierenden Schaden beweisen muss, um arbeitsrechtliche Sanktionen wegen Verletzung des Nutzungsreglements aussprechen zu dürfen. Vorbehalten bleibt die strafrechtliche Verfolgung durch die zuständige Behörde, sofern ein Straftatbestand vorliegt (z. B. Rufschädigung, Betriebsspionage, sexuelle Belästigung oder Verbreitung von rassistischem oder pornografischem Material). Auch wenn keine Anzeigepflicht besteht, ist eine Anzeige durch den Arbeitgeber geboten, um eine Mittäterschaft auszuschliessen.

Der Arbeitgeber trägt die Verantwortung, die Arbeitnehmer über ihre (Unterlassungs-) Pflichten zu informieren und technisch sowie organisatorisch gute Umsetzungsvoraussetzungen für erlassene Reglemente zu schaffen, beispielsweise durch Schulungen.

### 6.2 Unzulässige Überwachung durch den Arbeitgeber

Hält der Arbeitgeber die Voraussetzungen zur Überwachung der Internet- und E-Mail-Nutzung der Arbeitnehmer nicht ein, kann der Arbeitnehmer Eingriffe und daraus folgende arbeitsrechtliche Sanktionen (z. B. missbräuchliche Kündigung) als widerrechtliche Persönlichkeitsverletzung gerichtlich anfechten und seine Ansprüche auf Feststellung der Widerrechtlichkeit und möglicherweise Schadenersatz gegen den Arbeitgeber vor dem Arbeitsgericht geltend machen. Kommt es zu einer Verletzung des Geheim- und Privatbereichs oder zu unbefugtem Beschaffen von Personendaten, kann dies auch strafrechtliche Folgen haben. Um eine unzulässige Überwachung durch den Arbeitgeber zu vermeiden, ist es notwendig, den Zweck, Inhalt und die Aufbewahrungsdauer der Protokollierungen sowie deren Verwendung klar zu regeln und sicherzustellen, dass Personendaten stets unter Einhaltung des Zweckbindungs- und Verhältnismässigkeitsprinzips bearbeitet werden. Dazu ist zu erwähnen, dass der Arbeitnehmer jederzeit Auskunft darüber verlangen kann, welche Art von ihn betreffenden Daten bearbeitet werden (Art. 8 Abs. 1 DSG).

## 7. Elektronische Signatur

Die elektronische Signatur ist ein digitales, mit einer Botschaft verbundenes Siegel, das mit einem Signierschlüssel erzeugt und durch einen Prüfschlüssel (public key) überprüft wird. Der Prüfschlüssel wird dabei von einer Zertifizierungsstelle beglaubigt. In der Schweiz schafft das Bundesgesetz über die elektronische Signatur einen rechtssicheren und vertrauensbildenden Rahmen für den elektronischen Geschäftsverkehr. Entscheidend ist dabei die rechtliche Anerkennung: Seit dem 1. Januar 2005 sind qualifizierte digitale Signaturen der eigenhändigen Unterschrift gleichgestellt, sofern und soweit diese sich auf ein qualifiziertes Zertifikat stützen, welches nur von einer anerkannten (in- oder ausländischen) Zertifizierungsstelle herausgegeben werden kann.

Auch wenn elektronische Signaturen in der Praxis verbreitet sind, gibt es noch keine *rechtsgültige* elektronische Signatur im Sinne des genannten Gesetzes, da es in der Schweiz bis heute keine anerkannte Anbieterin von Zertifizierungsdiensten gibt. Entsprechend erhält die gesetzlich gültige elektronische Signatur erst dann rechtliche Relevanz,wenn eine Anbieterin von Zertifizierungsdiensten vom Bund anerkannt wird. Die entscheidenden

Qualitäten der elektronischen Signatur im Sinne des neuen Gesetzes beziehen sich auf die Integrität einer Nachricht (Unveränderbarkeit des Übermittlungswegs), die Authentizität (richtiger Kommunikationspartner) und die Nichtabstreitbarkeit (verbindliche Absendung).

Die Verwendung von E-Mail im täglichen Geschäftsverkehr hat insofern einen direkten Zusammenhang zur elektronischen Signatur, als dass elektronisch zu signierende Dokumente sinnvollerweise per E-Mail oder andere netzbasierte Dienste übermittelt werden, weshalb die Ausführungen zu Nutzungs- und Überwachungsreglementen auch in diesem Zusammenhang relevant sind. Die Praxis wird zeigen, ob und allenfalls wie rasch qualifizierte elektronische Signaturen Anwendung finden und welche Auswirkungen dies auf Haftungsregeln und auf unternehmensinterne Reglemente bezüglich des Umgangs mit Kommunikationsmitteln hat.

## 8. Fazit

Um klare Verhältnisse zu schaffen und gegen Missbräuche vorgehen zu können, drängt sich für Unternehmen der Erlass eines schriftlichen Nutzungs- und Überwachungsreglements auf, worin verbindliche Regeln für die Nutzung von E-Mail und Internet am Arbeitsplatz festgehalten und der Umfang der tolerierten Nutzung zu privaten Zwecken definiert werden. Der Erlass eines Überwachungsreglements und der Vorbehalt bestimmter Massnahmen ist zudem eine zwingende Voraussetzung, um Schritte wie die *personenbezogene* Auswertung von Protokolldaten überhaupt einleiten zu dürfen. Konkret lassen sich die Voraussetzungen der rechtlich heiklen personenbezogenen Überwachung wie folgt zusammenfassen: Einerseits müssen präventive technische und organisatorische Schutzmassnahmen (Passwort, Verschlüsselung usw.) ergriffen worden sein, die in jedem Fall Vorrang vor Überwachungsmassnahmen haben. Andererseits sind rechtliche Massnahmen zu treffen, nämlich der Erlass eines Nutzungs- und Überwachungsreglements. In jedem Fall ist eine personenbezogene Überwachung nur bei Missbrauch oder Missbrauchsverdacht zulässig. Die laufende Bildschirm-, Maus- oder Tastaturüberwachung und der Einsatz von «Spionprogrammen» sind generell unzulässig. Bezüglich privater E-Mails sollte in einem solchen Reglement festgehalten werden, dass alle E-Mails, die nicht als «privat» bezeichnet sind, als Geschäftskorrespondenz behandelt werden und dass somit die Archivierung privater E-Mails möglich ist. Insgesamt hat der Arbeitgeber seine Bemühungen primär auf die technische Prävention zu konzentrieren, um unerwünschtem oder gar illegalem Gebrauch einen Riegel vorzuschieben und das Unternehmen vor technischem Schaden zu schützen. Konsequent eingesetzt vermag die präventive Wirkung dieser Massnahmen den Einsatz repressiver Mittel wie die personenbezogene Überwachung weit gehend zu ersetzen. ■

aus CH-D Wirtschaft 4.2005