

Internet- und e-mail-Nutzung im Unternehmen

Rechtliche Rahmenbedingungen für Filtering, Schutz und Haftung

Dr Martin Brodey, LL.M.

A. Das Produkt

Zunehmend werden am Markt Sicherheitslösungen im Bereich von Internet- und E-Mail-Filtern angeboten, die unter dem Schlagwort "Content-Filtering" zusammengefasst werden können. Das Leistungsangebot von Internet-Filtersoftware umfasst Inhaltskontrolle (Blockierung unerwünschter Inhalte) und Zugriffskontrolle (statistische Berichte über Zugriffe auf Web-Seiten innerhalb des Netzwerks, individuelle Zugriffsstatistiken der Mitarbeiter, bis hin zur Live-Überwachung des Surfers der Mitarbeiter). E-Mail-Filterprogramme dienen dem Schutz vor Viren und der Verhinderung von Spam-Mail. E-Mails können nach bestimmten Worten, Bildern und Programmen gefiltert werden. Es ist möglich, über einzelne Nutzer von E-Mail-Diensten Berichte zu erstellen.

B. Das Thema

Welche rechtlichen Rahmenbedingungen existieren in Österreich für Content-Filtering?

C. Rechtsbereiche

Content-Filtering wirft Fragen im Zusammenhang mit folgenden Rechtsbereichen auf: Arbeitsrecht, Datenschutzrecht, Telekommunikationsrecht und Zivilprozessrecht.

Allgemein ist anzumerken, dass für die rechtliche Beurteilung der e-mail- und Internet-Nutzung am Arbeitsplatz noch keine einschlägige Judikatur existiert.

1. Arbeitsrecht

Kontrollmaßnahmen des Dienstgebers unterliegen in den meisten Fällen der **betrieblichen Mitbestimmung**. Gemäß § 96 Abs 1 Z 3 ArbVG (Arbeitsverfassungsgesetz) bedürfen Kontrollmaßnahmen und technische Systeme zur Kontrolle der Dienstnehmer, sofern diese Maßnahmen die **Menschenwürde berühren**, zu ihrer Rechtswirksamkeit der Zustimmung des Be-

triebsrates. In Betrieben, in denen kein Betriebsrat errichtet ist, kann eine entsprechende Kontrollmaßnahme nur mit Zustimmung der davon betroffenen Dienstnehmer eingeführt bzw verwendet werden. Diese Zustimmung kann, sofern keine schriftliche Vereinbarung mit dem Dienstgeber über deren Dauer vorliegt, jederzeit und ohne Einhaltung einer Frist schriftlich gekündigt werden (§ 10 Arbeitsvertragsrechtsanpassungsgesetz; "AVRAG").

Zur Auslegung des Begriffes der "**Menschenwürde**" werden üblicherweise die Grundrechte (Persönlichkeitsrechte) herangezogen. Grundsätzlich wird die Menschenwürde immer dann durch technische Kontrollsysteme oder sonstige Kontrollmaßnahmen berührt, wenn dadurch die vom Dienstnehmer in den Betrieb eingebrachte Privatsphäre, die ein Persönlichkeitsrecht darstellt, kontrolliert wird. Kontrollmaßnahmen, die die Menschenwürde verletzen, sind generell unzulässig (dh auch mit Zustimmung der Dienstnehmer), während Maßnahmen, die die Menschenwürde lediglich berühren, der Zustimmung der Dienstnehmer bedürfen.

Zu den Kontrollmaßnahmen, die regelmäßig Persönlichkeitsrechte **berühren**, gehören beispielsweise ständige Fernsehüberwachung, Multimomentkameras, Telefonabhöranlagen, Mikrofone, Glasscheiben, die nur von einer Seite durchsichtig sind, sowie Torkontrollen und Leibesvisitationen (vgl EA Wien 16.3.1981, Arb 9955). Zu **Telefonanlagen** sprach die Rechtsprechung aus, dass die Einführung eines elektronischen Telefonkontrollsystems, das die Nummern der angerufenen Teilnehmer systematisch und vollständig den jeweiligen Nebenstellen zugeordnet erfasst, jedenfalls die Menschenwürde berührt und daher nur mit Zustimmung des Betriebsrates bzw der einzelnen Dienstnehmer erfolgen kann (OGH 13.6.2002, 8 ObA 288/01 p). Der Dienstgeber soll aber in jedem Fall die Möglichkeit haben, eine missbräuchliche Verwendung seiner Telefonanlage zu bekämpfen. Dies könne etwa in der Weise erfolgen, dass der Umfang der Nutzung der Anlage in einer Vereinbarung festgelegt wird, und dass sich der Dienstgeber verpflichtet, die Rufdatenerfassung der vollständigen Rufnummern nur im Verdachtsfall, etwa bei überdurchschnittlich hohen Telefonkosten einer Nebenstelle, zu öffnen.

Kontrollmaßnahmen, die die Menschenwürde berühren, sind mit Zustimmung der Dienstnehmer zulässig, wenn sie aufgrund ihrer **Verhältnismäßigkeit** keine Verletzung von Persönlichkeitsrechten darstellen, insbesondere weil sie in adäquater und menschenwürdiger Form durchgeführt werden. Insbesondere darf den Dienstnehmern nicht das dauernde Gefühl potentieller Überwachung gegeben werden (EA Linz 19.12.1985, Arb 10481; EA Feldkirch 12.12.1986, Arb 10571).

Um Diskriminierungen einzelner Dienstnehmer zu vermeiden, müssen weiters im Rahmen der ausgeführten Kontrolle alle Dienstnehmer oder jene Dienstnehmergruppen, deren Kontrolle durch ihre Tätigkeit sachlich gerechtfertigt ist, formal **gleichbehandelt** werden.

Zusammenfassend geht die Rechtsprechung von einer grundrechtlich verankerten Pflicht zur umfassenden **Interessenabwägung** aus. Dabei steht das in Artikel 5 Staatsgrundgesetz normierte Grundrecht der Unverletzlichkeit des Eigentums des Dienstgebers den Persönlichkeitsrechten des Dienstnehmers auf Achtung seines Privatbereichs und seiner Geheimsphäre gegenüber. Ist die Verletzung der Menschenwürde nicht schon vorab offenkundig, ist zur Überprüfung, ob eine Kontrollmaßnahme zulässig ist, besagte Interessenabwägung zwischen den Interessen des Dienstgebers und des Dienstnehmers vorzunehmen (OLG Graz 22.9.1994, Arb 11259).

In die Interessenabwägung ist der bestehende **Arbeitsvertrag** einzubeziehen, der einerseits Fürsorgepflichten des Dienstgebers, andererseits aber auch Treuepflichten des Arbeitsnehmers nach sich zieht, die vom jeweiligen Inhalt des Arbeitsvertrag abhängen.

Kontrolle an sich verstößt gegen kein Persönlichkeitsgut des Dienstnehmers. Es gehört zum Wesen des Arbeitsverhältnisses, dass sich der Dienstnehmer der Kontrolle durch den Dienstgeber unterwirft. Der Dienstgeber ist jedoch verpflichtet, Eingriffe in Persönlichkeitsrechte des Dienstnehmers auf die schonendste noch zielführende Art vorzunehmen. Die grundrechtlich verankerten Persönlichkeitsrechte wirken, wenngleich durch den Arbeitsvertrag abgeschwächt und modifiziert, auch im dienstlichen Bereich fort und schützen dort den Dienstnehmer insbesondere vor Erniedrigung, Ungleichbehandlung und Willkür. Durch zu große über das für die Erreichung des Kontrollzwecks erforderliche Ausmaß hinausgehende Kontrolldichte bei der Arbeit kann jedenfalls die Menschenwürde berührt werden (OGH 13.6.2002, 8 ObA 288/01 p).

Die vorsorgliche Sperre des Zugangs zu bestimmten Internet-Inhalten oder des Downloads von Programmen ist hingegen arbeitsrechtlich unproblematisch, sofern keine Vereinbarung über die freie Nutzungsmöglichkeit des Internets besteht. In diesem Fall findet keine Kontrolle der Arbeitnehmer statt (*Thiele*, Internet am Arbeitsplatz, ecolex 2001, 614). Gleiches gilt für die vorsorgliche Überprüfung von (privaten oder dienstlichen) E-Mails oder aufgerufenen Internet-Seiten nach Viren.

2. Datenschutzrecht

Im Rahmen des Content-Filtering werden personenbezogene Daten iSv § 4 Z 1 Datenschutzgesetz (DSG) verarbeitet. Im Regelfall werden diese Daten am Server oder zumindest auf der Firewall des Arbeitgebers gespeichert. Damit hat der Arbeitgeber Zugriff auf personenbezogene Verbindungs- und Inhaltsdaten und unterliegt selbst als „Auftraggeber“ den Bestimmungen des DSG.

Er darf die Daten nur dann verarbeiten, wenn der Arbeitnehmer dieser Verarbeitung ausdrücklich **zustimmt** oder wenn überwiegende berechnigte Interessen zu seinen Gunsten existieren (§ 8 Abs 1 DSG). Das Vorliegen solcher überwiegenden Interessen wird im Regelfall zu verneinen sein (*Obereder*, e-mail- und Internetnutzung aus arbeitsrechtlicher Sicht, RdA 2001, 75).

Die Möglichkeit einer Interessenabwägung entfällt, wenn es sich um **sensible Daten** iSv § 4 Z 2 DSG handelt, das sind Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder Sexualleben. Da alleine durch das Erfassen der angewählten Seiten und e-mail-Adressen durch Filtersysteme schon persönliche Neigungen, Einstellung, Gesinnungen und Absichten ablesbar werden können, handelt es sich bei den dabei verarbeiteten Daten im Regelfall um „sensible“ (*Dellisch*, aaO, 3.1.).

Bei einem generellen Nutzungsverbot durch den Arbeitgeber kann datenschutzrechtlich von einer Zustimmung des betroffenen Dienstnehmers abgesehen werden. Diesfalls genügt im Rahmen des DSG die Mitteilung des Arbeitgebers, dass umfassend protokolliert und gegebenenfalls auch ausgewertet wird, weil bei einem Nutzungsverbot dem Arbeitgeber als Eigentümer des Betriebsmittels das Recht eingeräumt sein muss, die ausschließliche dienstliche Verwendung zu kontrollieren (*Dellisch*, aaO).

3. Telekommunikationsrecht

Nach dem TKG unterliegen Unternehmer dem Fernmeldegeheimnis, wenn sie Telekommunikationsdienste geschäftsmäßig für Dritte betreiben. Schutzgegenstand des Fernmeldegeheimnisses sind die übermittelten Nachrichten (Inhaltsdaten). Noch nicht geklärt ist die Frage, ob die am Server aufgezeichneten log-files als solche Inhaltsdaten angesehen werden können.

Die Strafbestimmungen des § 103 TKG sind nicht auf das Verhältnis Arbeitgeber – Arbeitnehmer anzuwenden (OGH 8 Ob A 288/01p). Es kommt aber eine Strafbarkeit nach § 119 und § 119a StGB in Betracht (Verletzung des Telekommunikationsgeheimnisses: zB bei Live-Screen-Shots; Missbräuchliches Abfangen von Daten: zB bei unerlaubter Überwachung zum Zweck der Verwendung als Beweis in Entlassungs-Prozess).

4. Zivilprozessrecht

Besteht eine Vereinbarung zwischen den Parteien über zulässige Kontrollmaßnahmen, wird auch hinsichtlich der durch diese zulässigen Kontrollmaßnahme gewonnenen Ergebnisse kein Beweisverbot bestehen (*Dellisch*, aaO).

Fraglich ist aber, ob der Arbeitgeber durch unzulässige Kontrolle erlangte Information über die e-mail- und Internet-Nutzung eines Arbeitnehmers in einem eventuellen Entlassungs-Verfahren als Beweismittel verwenden kann.

Grundsätzlich obliegt es dem Gericht im Rahmen der freien richterlichen Beweiswürdigung, die – wenn auch rechtswidrig gewonnenen – Beweise einzusehen und für die Entscheidungsfindung zu verwerten (OGH 1996, RdA 1996, 246; *Obereder*, aaO). In der Praxis wird in Entlassungsprozessen häufig von log-files zum Beweis eines Entlassungsgrundes Gebrauch gemacht.

5. Zusammenfassung

- Eine individuelle Kontrolle der Arbeitnehmer ist nur in sehr eingeschränktem Umfang zulässig.
- Wenn die nicht personenbezogene Systemüberwachung konkrete Anhaltspunkte für Missbrauch oder Risikoverhalten ergibt, darf zu personenbezogenen Kontrolle übergegangen werden. Diese muss allerdings angekündigt oder angedroht werden sowie verhältnismäßig sein. Betriebliche Mitbestimmungsrechte sind zu beachten.
- Das Haftungsrisiko eines Arbeitgebers bei Eröffnung der Internet- und e-mail-Nutzung am Arbeitsplatz ist überschaubar. Die Haftung kann durch geeignete Maßnahmen weitgehend begrenzt werden.
- Maßnahmen zum vorsorglichen Schutz vor illegalen Handlungen und Schäden des Netzwerks stehen keine rechtlichen Hindernisse entgegen.
- Prävention ist besser als Repression („Internet Policy“).