

# E-Mail- und Internetüberwachung am Arbeitsplatz

Wo liegen die Grenzen für den Arbeitgeber, welche unternehmensinternen Vorschriften und Massnahmen sollten Unternehmen für eine rechtskonforme Kontrolle der E-Mail- sowie Internetnutzung ihrer Arbeitnehmer vorsehen und wie können sie diese kontrollieren?

■ Von Dr. iur. Reto Fanger, Rechtsanwalt

Unternehmen haben ein legitimes Interesse daran, den Missbrauch ihrer ICT-Infrastruktur durch ihre Arbeitnehmer zu verhindern. Um ein allfälliges regelwidriges Verhalten von Mitarbeitenden aufdecken und daraus sich ergebende arbeitsrechtliche Sanktionen ableiten zu können, führen Unternehmen interne Untersuchungen durch. Wo liegen – ausgehend von der Rechtsprechung des Bundesgerichts sowie den aktuellen gesetzlichen Grundlagen – die Grenzen der Kontrolle von E-Mail-Kommunikation und Internetnutzung?

## Bundesgerichtliche Rechtsprechung

### Urteil zu widerrechtlich erlangtem Beweismaterial

Das Bundesgericht hatte in seinem Entscheid BGE 139 II 7 aus dem Jahr 2013 festgehalten, dass der verdeckte

Einsatz von Überwachungsprogrammen zur Kontrolle der Informatikaktivitäten eines Arbeitnehmers zur Bestätigung eines missbräuchlichen Gebrauchs für dienstfremde Zwecke unzulässig oder zumindest unverhältnismässig sei. Es sei zwischen dem öffentlichen Interesse an der Wahrheitsfindung und dem privaten Interesse des Arbeitnehmers am Schutz seiner Persönlichkeit abzuwägen. Das Bundesgericht taxierte den so gesammelten Beweis als widerrechtlich erlangtes Beweismittel und verneinte dessen Verwertung im Arbeitsprozess, weshalb die Grundlage für die Entlassung des Arbeitnehmers dahinfiel.

### Urteil zur fristlosen Entlassung zweier Angestellter

Mit Entscheid 8C\_87/2016 erachtete das Bundesgericht im Jahr 2017 die fristlose Entlassung von zwei SBB-

Angestellten für gerechtfertigt, die sich während ihrer Arbeitszeit bis zu vier Stunden täglich auf Internetseiten mit pornografischem und teilweise strafrechtlich relevantem Inhalt aufhielten, obwohl nach Feststellung der intensiven Nutzung dieser Websites die Daten der zwei Verdächtigten ohne vorherige schriftliche Information ausgewertet worden waren. Die fristlose Entlassung sei gerechtfertigt, da die beiden Arbeitnehmer durch Sperrfenster sowie die Richtlinie auf die Unrechtmässigkeit ihres Verhaltens hingewiesen worden waren und aus eigenem Verschulden diese nicht gelesen oder den Link zur Richtlinie nicht konsultiert hätten. Bei einer gewissen Schwere des Verstosses genügt daher bereits ein Warnfenster mit Sperrhinweisen, damit die Arbeitgeber ihren Informationspflichten nachkommen und den Eingriff rechtfertigen können.





## Gesetzliche Grundlagen

Sowohl bei der Überwachung des E-Mail- wie auch des Internetverkehrs sind in aller Regel Personendaten betroffen, was zur Anwendbarkeit des Datenschutzgesetzes (DSG) führt.

### Personendaten

Personendaten liegen nach Art. 3 lit. a DSG immer dann vor, wenn sich Informationen auf eine bestimmte oder bestimmbar Person beziehen. Die Bestimmtheit einer Person liegt dann vor, wenn aus der Information selbst ersichtlich ist, dass es sich genau um diese Person handelt. Bestimmbarkeit einer Person ist gegeben, wenn aufgrund zusätzlicher Informationen auf sie geschlossen werden kann, sofern die Identifizierung mit vertretbarem Aufwand möglich ist. Dies trifft sowohl auf die Randdaten wie Absender/Nutzer, Adressaten/besuchte Websites, Zeitpunkt und Dauer der Kommunikation/Nutzung wie auch auf Inhalte von Mails bzw. besuchten Websites zu, sofern diese Randdaten oder Inhalte nicht anonymisiert sind.

### Das Bearbeiten

Das Bearbeiten umfasst gemäss Art. 3 lit. e DSG jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten. Die Form der entsprechenden Informationen, beispielsweise als Zeichen, Wort, Bild, Ton oder deren Kombination, sowie die Beschaffenheit des Datenträgers sind dabei unerheblich, sofern sich die Angaben einer oder mehreren Personen zuordnen lassen. Eine nicht anonymisierte Überwachung der E-Mail- und/oder Internetnutzung durch den Arbeitgeber ist daher immer eine Bearbeitung von Personendaten.

Gestützt auf die arbeitsrechtliche Spezialbestimmung zum DSG von Art. 328b Obligationenrecht (OR) darf der Arbeitgeber Daten über den Arbeitnehmer nur bearbeiten, soweit sie des-

sen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrags erforderlich sind.

Diese Bestimmung setzt die Fürsorgepflicht des Arbeitgebers im Bereich der Datenbearbeitung um und darf als relativ zwingende Norm nicht zu Ungunsten des Arbeitnehmers abgeändert werden. Erforderlich im Sinne von Art. 328b OR ist die Datenbearbeitung, wenn diese vom Arbeitgeber zur Erfüllung seiner gesetzlichen oder arbeitsvertraglichen Pflichten oder für den Vertragsvollzug benötigt werden.

### PRAXISBEISPIEL



Von legitimen betrieblichen Interessen kann man unter anderem ausgehen bei der Gewährleistung ungestörter betrieblicher Abläufe, der Qualitätssicherung, der Optimierung der Arbeitsorganisation und der Produktivität, beim Schutz betrieblicher Vermögenswerte, bei der Kontrolle der Arbeitsleistung und Weisungsbefolgung sowie beim Interesse an der Erfüllung vertraglicher und gesetzlicher Pflichten. Alle diese Interessen betreffen insbesondere auch die Art und das Ausmass der E-Mail- und Internetnutzung durch die Arbeitnehmer.

### Überwachungs- und Kontrollsysteme

Nach Art. 26 Abs. 1 Verordnung 3 zum Arbeitsgesetz (ArGV 3) dürfen Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, nicht eingesetzt werden. Dies gilt allerdings nicht für Leistungs- und Sicherheitskontrollen: Für diesen Zweck sind die Überwachungs- oder Kontrollsysteme aber so zu gestalten und anzuordnen, dass sie die Gesundheit und die Bewegungsfreiheit der Arbeitnehmer dadurch nicht beeinträchtigen.

Art. 26 ArGV 3 verbietet nach Auffassung des Bundesgerichts ein Überwachungssystem nur dann, wenn es allein oder vorwiegend bezweckt, das Verhalten der Arbeitnehmer an sich zu überwachen, während die Rechtslehre teilweise strengere Anforderungen



aufstellt. Generell kann festgehalten werden, dass die ständige und damit systematische Verhaltensüberwachung der Mitarbeitenden mit Überwachungs- und Kontrollsystemen nicht zulässig ist, während die Zulässigkeit hingegen zu bejahen ist, wenn die Kontrolle für andere Zwecke wie beispielsweise zur Leistungs- und Sicherheitskontrolle eingesetzt wird, sofern dadurch Gesundheit und Bewegungsfreiheit der Mitarbeiter nicht beeinträchtigt sind.

### Rechtfertigungsgrund für die Bearbeitung

Personendaten dürfen sodann gestützt auf Art. 4 Abs. 1 DSG nur rechtmässig bearbeitet werden. Damit es nicht zu einer widerrechtlichen Persönlichkeitsverletzung kommt, bedarf das Bearbeiten von Personendaten eines Rechtfertigungsgrunds (Art. 13 Abs. 1 DSG). Die Zustimmung der Mitarbeitenden hilft hier oftmals nicht weiter, da es im Arbeitsverhältnis meist an der erforderlichen Freiwilligkeit einer solchen Einwilligung mangeln dürfte.

Ein Rechtfertigungsgrund für die Kontrolle von E-Mail- und Internetnutzung kann sich allerdings in Branchen mit Überwachungsverpflichtungen bereits aus dem Arbeitsvertrag allein ergeben, während sich Arbeitgeber in Branchen ohne Überwachungsverpflichtungen oftmals auf ein überwiegendes privates Interesse berufen können.



## Grundsatz der Verhältnismässigkeit

Weiter hat die Kontrolle der E-Mail- und Internetnutzung nach Art. 4 Abs. 2 DSG dem datenschutzrechtlichen Grundsatz der Verhältnismässigkeit zu entsprechen und darf nur nach Treu und Glauben erfolgen. Für die Datenauswertung im Rahmen solcher Kontrollen hat dies zur Folge, dass nur Auswertungen vorgenommen werden dürfen, die für die Missbrauchsaufdeckung geeignet sind, und dass der Arbeitgeber bei den Auswertungsformen das in Bezug auf die Persönlichkeitsrechte der Mitarbeiter mildestmögliche Vorgehen zu wählen hat.

## Das Bearbeitungsreglement

Nach dem Grundsatz der Zweckbindung gemäss Art. 4 Abs. 3 DSG darf das Unternehmen Personendaten nur für diejenigen Zwecke verwenden, welche bei der Beschaffung den Mitarbeitern bekannt gegeben wurden. Diesem Grundsatz kommt der Arbeitgeber im Bereich der Kontrolle der E-Mail- und Internetnutzung durch den Erlass eines Überwachungsreglements und durch die regelkonforme Datenbearbeitung nach. In diesem Reglement wird festgehalten, welche Auswertungen für welche Zwecke mit welchen Daten (Logfiles etc.) durchgeführt werden. Die Verwendung der Personendaten durch den Arbeitgeber für einen nicht im Bearbeitungsreglement erwähnten

Zweck verstösst demnach gegen den Grundsatz der Zweckbindung und somit gegen das Datenschutzgesetz.

## Transparenzprinzip

Die Kontrolle der E-Mail- und Internetnutzung und deren Zweck müssen schliesslich für die Mitarbeiter gemäss Art. 4 Abs. 4 DSG erkennbar sein, weshalb sie der Arbeitgeber vorgängig über Art, Umfang und Zweck der Überwachung informieren muss. Diese Informationspflicht der Arbeitnehmer ergibt sich überdies auch aus dem Erkennbarkeitsgebot.

Zusammenfassend kann man daher festhalten, dass eine stichprobenweise Randdatenauswertung zu Sicherheitszwecken und unter Einhaltung der datenschutzrechtlich erforderlichen Nutzungsweisungen zulässig ist, während eine private Auswertung einzig unter Einhaltung der einschlägigen strafrechtlichen Anforderungen von Art. 179<sup>bis</sup> und 179<sup>quinquies</sup> StGB möglich ist, auch dies wiederum unter Beachtung des Verhältnismässigkeits-, Zweckbindungs- sowie Transparenzprinzips. Dies hat zur Folge, dass der Einsatz sogenannter Compliance-Software oder von Spyware zur Kontrolle der E-Mail-Kommunikation und Internetnutzung unzulässig ist, da solche Tools diesen Anforderungen nicht gerecht zu werden vermögen.

## Unternehmensinterne Vorschriften und Massnahmen

Arbeitgeber können mit betrieblichen Reglementen über die E-Mail- und Internetnutzung, die auf die unternehmensspezifische Situation abgestimmt sind, klare Verhältnisse schaffen. Gleichzeitig kann so den datenschutzrechtlichen Anforderungen bezüglich Treu und Glauben, Transparenz sowie Vorhersehbarkeit der Datenerhebung Rechnung getragen werden.

Abgesehen von der betriebsspezifisch zulässigen E-Mail- und Internetnutzung sind in diesen Reglementen auch Vorgehen und Art der Überwachung festzuhalten, wie auch die daraus

sich ergebenden Sanktionen bei Missbrauch. Werden die Arbeitnehmer im Reglement aufgefordert, ihre privaten und geschäftlichen Daten zu trennen, können künftige Überwachungsmassnahmen allenfalls zureichend gerechtfertigt werden.

Neben diesen Vorschriften hat der Arbeitgeber weitere organisatorische sowie technische Massnahmen gegen eine missbräuchliche Nutzung zu treffen, sei es die Information und Sensibilisierung der Arbeitnehmenden oder der Einsatz aktueller Firewalls und Nutzungsfilter – dies alles neben allgemeinen technischen Massnahmen wie Zugriffs- und Antivirenschutz sowie Back-ups.

## Vorgehen bei internen Untersuchungen

Erweist sich eine Überwachung aufgrund festgestellter technischer Unregelmässigkeiten als erforderlich, ist diese zunächst anonymisiert und nach weiterer Eingrenzung des Kreises möglicher Verdächtiger pseudonymisiert durchzuführen. Erst bei klaren Hinweisen auf Missbrauch oder ein Risikoverhalten darf personenbezogen überwacht werden. Dabei kann der Arbeitgeber wie folgt vorgehen:

- Analyse der Verdachtsmomente
- Planung der internen Untersuchungen
- Durchführung der internen Untersuchungen
- Berichterstellung
- bedarfsweiser Beizug der zuständigen Strafverfolgungsbehörden inklusive Berichterstattung

## AUTOR



**Dr. iur. Reto Fanger** ist Rechtsanwalt (ADVOKATUR FANGER – Anwaltsboutique für ICT-, Daten-, Medien- und Arbeitsrecht, Luzern;

[www.advokatur-fanger.ch](http://www.advokatur-fanger.ch)), Partner der Swiss Business Protection AG ([www.swissbp.ch](http://www.swissbp.ch)), Dozent an der Hochschule Luzern, Lehrbeauftragter an der Universität Luzern sowie Co-Organisator und -Tagungsleiter des Lucerne Law & IT Summit (LITS).