

von Rechtsanwalt **Patrick Prestel**

# Überwachung und Kontrolle des Arbeitnehmers und die Konflikte mit dem Fernmeldegeheimnis und dem Datenschutz (7. Teil der neuen Serie der IT-Recht Kanzlei zu den Themen E-Mailarchivierung und IT-Richtlinie)

Im 7. Teil der [neuen Serie der IT-Recht Kanzlei zum Thema E-Mail Archivierung](#) wird auf das Parallelproblem der Überwachung und Kontrolle des Arbeitnehmers eingegangen. Auch hier ergeben sich Konflikte mit dem Fernmeldegeheimnis und dem Datenschutz.

Um zum Beispiel die Weitergabe von Betriebsgeheimnissen, eine unerlaubte private Nutzung des E-Mail-Systems, oder die Begehung von Straftaten durch den Arbeitnehmer aufzudecken und zu unterbinden, möchte und muss der Arbeitgeber den Arbeitnehmer kontrollieren und überwachen. Technisch gesehen greift der Arbeitgeber dabei auf den E-Mail-Server zu oder setzt einen Sniffer ein. Aber auch die Frage inwieweit der Arbeitgeber den Arbeitnehmer überwachen darf, sprich einzelne Mails lesen und das Abrufen von Internetseiten nachvollziehen darf, hängt vom TKG und dem BDSG ab.

## 1. Überwachung, bei einem Verbot der privaten Nutzung der E-Mail und Internetdienste

Das TKG gilt in diesem Falle nicht, da der Arbeitgeber kein Dienstanbieter im Sinne des TKGs ist. Aber dann gilt das BDSG. Gemäß § 4 BDSG dürfen personenbezogene Daten nur erhoben oder genutzt werden, wenn dies durch den Betroffenen oder durch Gesetz oder eine andere Rechtsvorschrift gestattet ist.

Für die Überwachung kommt innerhalb eines Betriebes § 32 BDSG als gesetzliche Gestattung im Sinne des § 4 BDSG zur Anwendung. Dieser erlaubt nach Abs.1 S.1 die Erhebung, Verarbeitung und Nutzung personenbezogener Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.

Erforderlich ist die Verwendung personenbezogener Daten dann, wenn keine objektiv zumutbare Alternative existiert. Die Erforderlichkeit ist anzunehmen, wenn die berechtigten Interessen des Arbeitgebers auf andere Weise nicht oder nicht angemessen gewahrt werden können. Es ist eine Interessensabwägung zwischen dem Datenschutz des Arbeitnehmers (Art. 2 I GG i.V.m. Art.1 I GG) und dem Schutz des eingerichteten und ausgeübten Gewerbebetriebes (Art. 14 I GG) vorzunehmen.

**a.**

Im Rahmen der Überwachung eines Arbeitnehmers wird beim E-Mailverkehr zwischen den Verbindungsdaten (Datum, Uhrzeit, Datenvolumen und wohl auch E-Mail-Adressen) und dem E-Mail-Inhalten differenziert. Während erstere nach der Rechtsprechung gespeichert werden können, ist dies bei Letzteren umstritten.

Denn zum Teil werden die Grundsätze zur Telefonüberwachung als Vergleichsmaßstab heran gezogen. Danach ist eine Überwachung der -Mail nicht möglich, da die Inhalte eines Telefonats durch den Arbeitgeber weder mitgeschnitten noch mitgehört werden dürfen.

Teilweise wird die E-Mail jedoch mit dem Geschäftsbrief gleichgesetzt wird. Danach kann der Inhalt einer E-Mail problemlos, ebenso wie der Inhalt eines Geschäftsbriefes, gelesen werden. Diese Ansicht ist unserer Auffassung auch richtig, da die E-Mail wie ein Geschäftsbrief später für Dritte abrufbar ist und dies dem Arbeitnehmer beim Verfassen bewusst ist. Die Flüchtigkeit des gesprochenen Worts wie bei einem Telefonat ist bei der E-Mail nicht gegeben.

**b.**

Hierbei ist jedoch auch zu beachten, dass die Kontrolle abgestuft im vorgenommen werden muss, um nicht unverhältnismäßig zu sein. Zunächst darf nur auf die Verbindungsdaten Zugriff genommen werden. Ist schon daran (z.B. an der Betreffzeile oder der Emailempfängeradresse) zu erkennen, dass ein Missbrauch vorliegt, ist eine Kenntnisnahme des Inhalts nicht mehr nötig.

**c.**

Eine Überwachung, insbesondere eine Compliance-Überwachung, ist hier also zulässig.

Schließlich bleibt jedoch eine systematische und lückenlose Überwachung des E-Mail-Verkehrs und der Internetnutzung ein unzulässiger Verstoß gegen das allgemeine Persönlichkeitsrecht nach Art. 2 I, 1 I GG, da diese nicht erforderlich ist. Denn regelmäßig wird der Arbeitgeber die Missbrauch auch durch eine stichprobenartige Kontrolle feststellen können.

**d.**

Allerdings verlangt § 32 I 2 BDSG für die Datennutzung zur Aufdeckung einer Straftat engere Voraussetzungen. Dafür müssen zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat. Weiter muss die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich sein und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung darf nicht überwiegen.

**e.**

Umstritten ist, ob das Lesen einer ausdrücklich mit Privat gekennzeichneten Email gegen § 202a StGB (Straftatbestand) und § 43 BDSG (Ordnungswidrigkeit) verstößt.

Teilweise wird vertreten, dass dieser Zugriff zulässig sein soll, denn die Emails im Bereich der Arbeitsmittel des Arbeitgebers sollen nicht mehr unter dem Schutz der Intim- oder Privatsphäre stehen. Vielmehr seien sie Teil des sozialen und beruflichen Auftretens.

Unseres Erachtens ist dies jedoch anders zu beurteilen. Denn die Kennzeichnung mit Privat begründet eindeutig die Zugehörigkeit zur Privatsphäre. Auch ein Vergleich zu einem normalen Brief führt zum gleichen Ergebnis. Denn ein in der Firma versendeter privater Brief, der als solcher gekennzeichnet ist,

darf ebenso nicht gelesen werden.

## 2. Überwachung bei Zulassung des privaten E-Mail-Verkehrs

Es gilt das TKG, da der Arbeitgeber Diensteanbieter ist. Können private Mails von den betrieblichen Mails nicht unterschieden werden, ist dem Arbeitgeber auch der Zugriff auf die geschäftlichen Emails versagt. Die Überwachung des privaten E-Mail-Verkehrs ist sowohl hinsichtlich der Verbindungsdaten als auch des Inhalts der E-Mails unzulässig. Denn dann gilt als spezielles Gesetz das TKG. In diesem gibt es keinerlei Rechtfertigungsgründe für das Lesen der Emails. Vielmehr kann das Lesen einer E-Mail durch den Arbeitgeber selbst eine Straftat nach § 206 StGB sein. Von der Unzulässigkeit des Lesens kann nur in ganz seltenen Fällen zur Missbrauchskontrolle (z.B. Verrat von Geschäftsgeheimnissen oder Begehung einer Straftat) und nur bei Vorliegen von konkreten Anhaltspunkten eine Ausnahme zugelassen werden. Folglich kann es auch hier zu einer Pflichtenkollision für den Arbeitgeber kommen: er darf nicht seine Compliancepflicht und ebenso den Datenschutz nicht verletzen. Eine Lösung des Konflikts ist auch hier über den rechtfertigenden Notstand nach § 34 StGB denkbar, allerdings kann nicht gesagt werden, wie die Abwägung durch ein Gericht ausfallen würde.

Die einzige Ausnahme hierbei ist der Fall einer rechtswidrigen Inanspruchnahme der Telekommunikationsanlage. Dann darf der Arbeitgeber dann gemäß § 100 III TKG Verkehrsdaten erheben und verwenden. Allerdings gilt dies erst, wenn dem Arbeitgeber zu dokumentierende, tatsächliche Anhaltspunkte für einen derartigen Missbrauch vorliegen.

Bei der Möglichkeit „Zugriff auf Web-Accounts“ (siehe [6. Teil der Serie](#) unter 4. „Zwischenlösungen“ a.) kann eine Kontrolle dennoch Möglich sein, wenn die Zulassung der privaten Nutzung zeitlich beschränkt wird. Dann ist der Arbeitgeber außerhalb dieser Zeit nicht (mehr) Telekommunikationsanbieter, sodass das Fernmeldegeheimnis nicht gilt und er stichpunktartig kontrollieren kann.

## 3. Beweisverwertungsverbot

Weiterhin ist fraglich, ob der Arbeitgeber, der durch eine Kontrolle einen Beweis für einen Missbrauch erlangt hat, diesen Beweis auch im Prozess verwenden darf. Denn im Prozessrecht gibt es bestimmte Beweisverwertungsverbote. Die herrschende Meinung differenziert danach, ob ein Beweismittel unter unverhältnismäßiger Verletzung von Grundrechten des Betroffenen erlangt wurde.

Bei der Missbrauchskontrolle von Internetnutzung ist das Wahrheitsermittlungsbedürfnis gegen das allgemeine Persönlichkeitsrecht des Arbeitnehmers abzuwägen. Das allgemeine Persönlichkeitsrecht wurde aber bereits bei der Prüfung der Rechtmäßigkeit der Kontrollmaßnahme im Rahmen des TKGs oder des BDSG berücksichtigt. Somit ergibt sich, dass ein Beweis, der rechtmäßig nach dem TKG oder dem BDSG erhoben wurde, auch verwertbar ist.

Autor:

**RA Patrick Prestel**