Mitarbeiterüberwachung – Technische Möglichkeiten und rechtliche Grenzen

Sebastian Meyer

Rechtsanwälte Brandi Dröge Piltz Heuer & Gronemeyer
Adenauerplatz 1, D-33602 Bielefeld
meyer@bdphg.de

Schlagworte: Datenschutz, Telekommunikationsrecht, Ortung
Abstract: Mit relativ geringem Aufwand ist es mittlerweile möglich, das Arbeitsverhalten von Mitarbeitern zu überwachen – vor allem wenn ihnen vom Arbeitgeber ein Mobiltelefon und/oder ein Computer zur Verfügung gestellt werden. Nicht alles, was technisch möglich ist, muss rechtlich aber auch zulässig sein. Entsprechende Maßnahmen sind vor allem auf ihre datenschutzrechtliche Zulässigkeit zu prüfen.

1. Einführung

Die Überwachung von Mitarbeitern durch den eigenen Arbeitgeber wird in der Öffentlichkeit zurzeit nach Medienberichten über heimliche Videoaufnahmen bei mehreren Einzelhandelsunternehmen kontrovers diskutiert. In der öffentlichen Diskussion kommt dabei jedoch teilweise zu kurz, dass Arbeitgeber durchaus ein berechtigtes Interesse haben können, ihre Mitarbeiter zu kontrollieren. Andererseits können die Arbeitnehmer regelmäßig verlangen, dass sie nicht ohne besonderen Anlass und ohne konkrete Notwendigkeit rund um die Uhr überwacht werden. In diesem Spannungsverhältnis stehen alle Überwachungsmaßnahmen, so dass ihre Zulässigkeit stets im Einzelfall unter Berücksichtigung und Abwägung der widerstreitenden Interessen geprüft werden muss.

2. Ziel der Nutzung technischer Maßnahmen

Grundsätzlich können technische Überwachungsmaßnahmen verschiedenen Zwecken dienen. Im Rahmen der Prävention soll einem möglichen Fehlverhalten von Mitarbeitern vorgebeugt werden. Bei der Ermittlung

geht es dem Arbeitgeber um die Überprüfung, ob bereits ein Fehlverhalten stattfindet. Liegt das Fehlverhalten bereits in der Vergangenheit, kann im Wege der Reaktion versucht werden, dieses Fehlverhalten zu rekonstruieren. Je nach Einsatzzweck müssen unterschiedliche Vorgehensweisen und Techniken gewählt werden. Verfolgter Zweck und eingesetzte Technik müssen folglich korrespondieren. Dabei ist auch zu beachten, dass alle Überwachungstechniken umgekehrt von Dritten ebenfalls zur Informationsgewinnung genutzt werden können. Daher sollte der Arbeitgeber sich des Missbrauchsrisikos, das beispielsweise im Hinblick auf Werksspionage bestehen kann, immer bewusst sein.

Bei der Prävention ist vorrangiges Ziel zumeist die Abschreckung der Mitarbeiter. Es erfolgt daher typischerweise ein offener Einsatz technischer Maßnahmen, etwa die Installation von sichtbaren Videokameras. Sollen Beweise für ein aktuelles Fehlverhalten gesammelt werden, bietet es sich dagegen eher an, technische Kontrollmaßnahmen nicht offen anzuwenden, weil andernfalls der Erfolg der Maßnahme gefährdet würde. Geht es nur noch um die Rekonstruktion eines Fehlverhaltens, das in der Vergangenheit liegt und abgeschlossen ist, kommt es nicht mehr darauf an, verdeckt vorzugehen, sondern es kann der Einsatz technischer Maßnahmen (wieder) offen erfolgen.

3. Technische Möglichkeiten

Technische Überwachungsmaßnahmen sind nicht automatisch mit besonderem Aufwand verbunden. Oftmals lassen sich bereits gute Ergebnisse mit geringem Aufwand und ohne nennenswerte Kosten erzielen. Hierdurch ist die Versuchung der Nutzung der bestehenden technischen Möglichkeiten oftmals relativ hoch.

3.1 Abhören und Ortung von Mobiltelefonen

Bei einem Firmenhandy ist etwa das Abhören von Gesprächen, die in einem Raum stattfinden, kaum ein Problem. Die einfachste Lösung ist die Deaktivierung der Benachrichtigung für eingehende Gespräche und die Einschaltung der automatischen Rufaufnahme. Wird ein derart präpariertes Handy angerufen, kann der Anrufer die Gespräche in der Nähe des Mobiltelefons mithören, und zwar auch ohne Wissen des Handynutzers. Zur

Optimierung des Abhörens von Raumgesprächen gibt es für zahlreiche Mobiltelefone spezielle Software, die das Betriebssystem der Geräte manipuliert. Wird eine derartige Software auf dem Gerät vor Aushändigung an den Mitarbeiter installiert, ist für diesen das Mithören oder Abhören nicht feststellbar. Die Steuerung des Mobiltelefons kann über Steuerungscodes völlig unbemerkt vom Besitzer erfolgen. Technisch kaum zu bewältigen ist dagegen das Abhören von Mobilfunkverbindungen ohne Zugriff auf das Mobiltelefon selbst. Bei Übertragung des Gesprächs vom Mobiltelefon zum Sendemast erfolgt eine Verschlüsselung, so dass Mobilfunkgespräche als vergleichsweise abhörsicher gelten. Es ist allerdings möglich, mithilfe eines sogenannten IMSI-Catchers die Verschlüsselung zu umgehen. Der IMSI-Catcher simuliert eine eigene Funkzelle, in die sich alle Mobiltelefone in der Nähe einbuchen. Durch ein Steuerkommando wird von der simulierten Funkzelle dann die Verschlüsselung deaktiviert, so dass die Gespräche – die an die echte Funkzelle weitergeleitet werden – mitgehört werden können.

Eine weitere Möglichkeit, die sich durch die große Verbreitung von Mobiltelefonen ergibt, ist die Ortung von Personen, sofern diese ihr Handy mit sich führen. Für die Ortung ist die Nutzung des Mobiltelefons nicht erforderlich. Es genügt, dass dieses eingeschaltet ist und Netzempfang hat. Bei der GSM-Ortung kann die Cell-ID der Funkzelle abgefragt werden, in die sich das Mobiltelefon eingebucht hat. Abhängig von der Größe der Funkzelle, die je nach Region variiert, kann eine Ortung mit einer Genauigkeit von bis zu 300 Metern (in Ballungsräumen) vorgenommen werden. Durch eine Laufzeitmessung kann die Genauigkeit unter Umständen noch weiter erhöht werden. Der Service zur Ermittlung der Funkzelle wird von den Netzbetreibern angeboten. Die Abfrage ist ohne Wissen des Betroffenen möglich, die SIM-Karte muss lediglich einmalig für den Service freigeschaltet werden.

Eine genauere Ortung von Mobiltelefonen ist dann möglich, wenn die Geräte über ein eingebautes oder angeschlossenes GPS-Modul verfügen, was vor allem bei Smartphones oft der Fall ist. Für derartige Geräte gibt es Zusatzsoftware, die fortlaufend die Standortdaten des Gerätes erfasst und diese in festgelegten Intervallen überträgt. Die Genauigkeit liegt wie bei mobilen Navigationsgeräten bei 5 – 20 Metern. Bei Nutzung der GPS-Daten ist ein Live-Tracking möglich, bei dem live verfolgt werden kann, welche Wege der Telefonbesitzer zurücklegt. Alternativ kann auch nachträglich ausgewertet werden, welche Strecken der Telefonbesitzer regelmäßig zurücklegt und wo er sich etwa oft für längere Zeit aufhält.

3.2 Überwachung von PC-Aktivitäten

Auch bei Zugriff auf den PC eines Mitarbeiters lässt sich über den Betroffenen vieles in Erfahrung bringen. Zunächst können die E-Mails des Mitarbeiters von Interesse sein. Diese lassen sich auf Nutzerebene an ein anderes Account weiterleiten. Soll dies für den Mitarbeiter nicht erkennbar sein, können entsprechende Einstellungen bereits auf dem Mailserver vorgenommen werden, auf den der Mitarbeiter regelmäßig keinen ausreichenden Zugriff hat. Eine weitere Möglichkeit ist es oft, sich – bei Kenntnis des Passwortes – direkt als Benutzer anzumelden oder wenigstens Zugriff auf die Postfach-Dateien über einen anderen Nutzer zu erhalten.

Aussagekräftig ist außerdem oftmals der Umfang der Internetnutzung. Standardmöglichkeiten sind hierbei das Auslesen der History und die Kontrolle des Browser-Cache auf Nutzerebene. Am Server können die besuchten URLs archiviert werden. Weiterhin bietet sich wenigstens eine quantitative Auswertung des Nutzerverhaltens an. Durch Zusatzsoftware können sämtliche besuchte Internetseiten aufgezeichnet werden. Die Aufzeichnungen erfassen dabei auch etwaige Eingaben des Nutzers, was zum Beispiel bei der Chat-Nutzung von Bedeutung ist. Sämtliche Daten können entweder auf dem erfassten Computer gespeichert oder an ein anderes Gerät weitergeleitet werden.

Noch umfassender ist die Kontrolle sämtlicher Programmaktivitäten auf einem Computer (Monitoring). Eine Live-Kontrolle ist bereits durch die Einrichtung eines Remote-Access möglich. Wenn das Freigabeerfordernis für den Nutzer und die Informationsfunktionen abgeschaltet werden, kann dies auch unbemerkt vom Nutzer erfolgen. Spezielle Monitoring-Software lässt sich so konfigurieren, dass alle Aktivitäten zunächst aufgezeichnet werden, wobei eine spätere Wiedergabe im Zeitraffer erfolgt. Dabei kann eingestellt werden, dass eine Benachrichtigung oder Aufzeichnung bei bestimmten Aktionen des Nutzers erfolgt.

4. Rechtliche Grenzen

Bei der Prüfung der rechtlichen Zulässigkeit der zuvor aufgeführten Überwachungsmöglichkeiten ist eine Vielzahl von Rechtsgrundlagen zu beachten. Auf Seiten der betroffenen Mitarbeiter sind vielfach Grundrechte berührt, insbesondere das allgemeine Persönlichkeitsrecht. Aus arbeitsrechtlicher Sicht ist stets zu überprüfen, ob vom Arbeitgeber vorgesehene

Kontrollmaßnahmen der Mitbestimmung unterliegen und daher zustimmungspflichtig sind. Außerdem ist zu untersuchen, ob alle datenschutzrechtlichen Vorgaben eingehalten werden. Soweit durch die Überwachung in die Übertragung von Informationen eingegriffen wird, sind auch die Sondervorschriften des Telekommunikations- und Telemedienrechts zu berücksichtigen. Mitunter kann sich die Frage ergeben, ob der Arbeitgeber sich selbst strafbar macht, wenn er – sei es auch zur Abwehr oder Aufklärung von Verbrechen – seine Mitarbeiter zu weit gehend überwacht.

4.1 Mobiltelefone

Im Zusammenhang mit dem Abhören von Raumgesprächen durch ein Mobiltelefon wird etwa in Deutschland diskutiert, ob der Tatbestand der Verletzung der Vertraulichkeit des Wortes gem. § 201 Abs. 2 StGB erfüllt ist. Da die Vertraulichkeit des Gespräches nicht erforderlich ist, kommt die Vorschrift grundsätzlich in Betracht, wenn unbemerkt dienstliche Gespräche mitgehört werden. Eine Einwilligung der Betroffenen lässt jedoch die Strafbarkeit entfallen. Hieran wird es aber vermutlich regelmäßig fehlen, da die Einwilligung aller Beteiligten vorliegen muss. Es ist nicht ausreichend, wenn ein Mitarbeiter „eingeweiht" ist, während die übrigen Gesprächsteilnehmer nicht wissen, dass ihre Gespräche mitgehört werden. Eine ausdrückliche Einwilligung ist allerdings nicht zwingend erforderlich, denkbar und ausreichend ist eine konkludente Einwilligung. In der Rechtsprechung ist anerkannt, dass eine ausdrückliche Zustimmung nicht erforderlich ist, wenn aufgrund geschäftlicher Gepflogenheiten von einer Zustimmung auszugehen war.[1] Außerdem ist auch ohne ausdrückliche oder konkludente Einwilligung das Verhalten zumindest gerechtfertigt, wenn es zur Abwehr krimineller Handlungen geboten ist.[2]

Eindeutiger ist die Rechtslage im Hinblick auf die Nutzung von IMSI-Catchern. Diese dürfen von Strafverfolgungsbehörden in Erfüllung ihrer hoheitlichen Aufgaben eingesetzt werden. Für Deutschland ist dies ausdrücklich durch das Bundesverfassungsgericht entschieden worden.[3] Die Verwendung durch Privatpersonen ist dagegen unter keinen Umständen zulässig. Es würde ansonsten massiv in die bestehende Mobilfunk-Infrastruktur eingegriffen. Vor diesem Hintergrund läge bei dem privaten Einsatz

1 BVerfGE 34, 238.
2 BGH, NStZ 1982, 255.
3 BVerfG, NJW 2007, 351.

von IMSI-Catchern auch ein Verstoß gegen die Vorschriften des Telekommunikationsgesetzes vor.

Bei der Ortung unter Nutzung von Mobiltelefonen ist zu unterscheiden. Die Freischaltung von dienstlichen Mobiltelefonen für die Ortung durch den Arbeitgeber ist nicht zu beanstanden. Es werden insoweit nur die Voraussetzungen für eine spätere Ortung geschaffen, die nicht automatisch unzulässig sein muss. Zum Schutz seines Eigentums und weiterer wesentlicher Interesse ist dem Arbeitgeber die Möglichkeit einzuräumen.

Die Nutzung der Möglichkeit ist ohne Kenntnis des Betroffenen dagegen bedenklich. Vorab stellt sich allerdings die Frage, ob das Datenschutzrecht überhaupt Anwendung findet. Dies setzt voraus, dass personenbezogene Daten erhoben, gespeichert oder verarbeitet werden. Unmittelbar ist dies bei der Ortung nicht der Fall, da das Mobiltelefon und nicht der Telefonbesitzer geortet werden. Soweit aber – und das dürfte der Regenfall sein – das Telefon einem konkreten Mitarbeiter zugeordnet ist, können damit Rückschlüsse auf den Aufenthaltsort und die Tätigkeiten des Mitarbeiters gezogen werden. Die Bestimmbarkeit reicht nach dem Datenschutzrecht aus, so dass die Bestimmung von Standortdaten als Erhebung von personenbezogenen Daten anzusehen sein dürfte. Hierfür fehlt es bei einer heimlichen Ortung an der eigentlich erforderlichen Einwilligung des Betroffenen. Besteht gegen diesen jedoch ein konkreter Verdachtsmoment, dürfte bei Abwägung aller Umstände im Einzelfall eine Ortung ohne vorhergehende Information möglich sein, weil andernfalls eine Ermittlung gegen den Verdächtigen nicht möglich wäre. Sinnvoll könnte es sein, sich bereits bei Übergabe des Telefons das Recht einräumen zu lassen, bei bestimmten Anhaltspunkten eine Handyortung durchzuführen. Diese Anhaltspunkte sollten dann allerdings präzisiert werden. Eine anlassunabhängige jederzeitige Ortung ist nicht zulässig.

4.2 Kontrolle von E-Mail und Internet sowie Monitoring

Bei der Überwachung des Mailverkehrs einzelner Mitarbeiter ist danach zu differenzieren, ob die private Nutzung des E-Mail-Systems erlaubt ist oder nicht. Im Hinblick auf dienstliche E-Mails besteht ein berechtigtes Interesse des Arbeitgebers an einer Überprüfung der E-Mails; diese sind primär an das Unternehmen gerichtet und nicht an den einzelnen Mitarbeiter. Ebenso wie es dem Arbeitgeber freisteht zu entscheiden, wie die Eingangspost geprüft und bearbeitet wird, kann er Regelungen zum Umgang mit betrieblichen E-Mails einführen. Schützenswerte Belange der Betroffenen treten dahinter regelmäßig zurück.

Der Sachverhalt ist anders zu beurteilen, wenn der Arbeitgeber die private Nutzung erlaubt oder zumindest toleriert. Ihm ist dann bewusst, dass er durch die Kontrolle von E-Mails eventuell auch private Belange des Betroffenen erfährt, die besonders schutzbedürftig sind. In Deutschland wird in diesem Zusammenhang diskutiert, ob der Arbeitgeber als Access-Provider im Sinne von § 11 TMG anzusehen ist und inwieweit er dem Fernmeldegeheimnis gem. § 89 TKG unterliegt. Zur Vermeidung derartiger Schwierigkeiten ist Arbeitgebern zu empfehlen, strikt zwischen privater und dienstlicher Nutzung zu trennen.

Soweit sich die Überwachung des Arbeitgebers nicht auf die Mails beschränkt, sondern umfassender das Surfverhalten kontrolliert werden soll, kann dies zunächst bedenkenlos erfolgen, wenn nur eine anonymisierte Kontrolle am Server vorgenommen wird. In Bezug auf einen konkreten, einzelnen Nutzer soll es auch hier wieder auf die Unterscheidung zwischen dienstlicher und privater Nutzung ankommen. Die Interessenabwägung erfolgt ähnlich wie im Zusammenhang mit dem Einsatz von E-Mails.

Legt der Arbeitgeber ganze Nutzerprofile an, in denen die gesamte Computer-Nutzung erfasst wird, stellt sich die Frage der Verhältnismäßigkeit derartiger Maßnahmen. Im ersten Schritt ist zu untersuchen, ob nicht eine spätere Kontrolle bei einem konkreten Verdacht ausreicht (Erforderlichkeit). Dann stellt sich die Frage, ob selbst bei konkretem Verdacht nicht die Überwachung einzelner Bereiche wie E-Mail oder Internet ausreicht und damit die Erstellung von Nutzerprofilen überhaupt nicht notwendig war. Schließlich ist für den Arbeitgeber zu bedenken, dass er mitunter Gefahr läuft, über das Ziel hinauszuschießen. Erlangt er etwa aufgrund der Nutzung von Monitoring-Software Kenntnis von eigentlich verschlüsselt übertragenden Passwörtern oder PIN-Nummern, kann hierin möglicherweise ein Ausspähen von Daten gesehen werden, das mit Strafe bedroht ist. Im Regelfall dürfte ein derartiges Ausspähen vom Arbeitgeber aber nicht beabsichtigt gewesen sein.

5. Fazit

Durch die mitunter einfachen technischen Möglichkeiten besteht die Gefahr, dass Arbeitgeber voreilig und ohne ausreichende rechtliche Beratung zur Aufklärung von Verdachtsfällen der Versuchung unterliegen, ihre Mitarbeiter konsequent zu überwachen. Tatsächlich ist eine heimliche Kon-

trolle regelmäßig aber nur nach sorgfältiger Abwägung aller Aspekte im Einzelfall und unter Berücksichtigung zahlreicher rechtlicher Regelungen legal.