Link: http://www.computerwoche.de/a/print/noimages/2551161

Vertrauensfrage Mitarbeiterdatenschutz

Wenn der Chef "mal über die Schulter" schaut...

Datum: 26.12.2013
Autor(en): Stanislav Wittmann

Videoüberwachung, Mithören von Telefongesprächen, fremder Zugriff auf eigene E-Mails - für viele Mitarbeiter Horrorszenarien. Doch was davon ist sogar erlaubt? Wo liegen die Grenzen der Kontrolle? Was können Arbeitnehmer und Arbeitgeber tun, wenn diese Grenzen überschritten werden?

Es ist zwar ein schmaler Grat, die Überwachung und Kontrolle von Arbeitnehmern können in bestimmten Fällen aber berechtigt sein. So ermittelte die Unternehmensberatung **Corporate Trust**[1] in ihrer Studie **"Industriespionage 2012"**[2], dass jeder zweite Fall von Datenklau in deutschen Unternehmen auf interne Mitarbeiter zurückzuführen ist.

Es stellt sich die Frage, ob einem Arbeitgeber bloße Verdachtsmomente ausreichen, gleich umfassende Überwachungsmaßnahmen einleiten zu dürfen. Das Bundesdatenschutzgesetz (BDSG) antwortet darauf ganz klar mit Nein. Demnach müssen bereits **"tatsächliche Anhaltspunkte" für eine Straftat**[3] vorliegen, um personenbezogene Daten erheben zu dürfen - und um nichts anderes geht es bei Maßnahmen wie der Video-, Telefon- oder E-Mail-Überwachung eines Mitarbeiters. Bei einem bloßen Verdacht sind Arbeitgebern die Hände gebunden - und das ist im Sinne der Verhältnismäßigkeit der Mittel auch gut so.

Der BR ist mit im Boot

Liegen konkrete Anhaltspunkte vor, ist zudem zu beachten, Daten nur in dem erforderlichen Maß zu erheben, das für den Beweis der Straftat ausreicht. In jedem Fall gilt es, vorher den Betriebsrat zu informieren, der in solch einem Fall **gemäß §87, Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG)**[4] ein Mitbestimmungsrecht besitzt. Informationspflichten gegenüber dem Betriebsrat gibt es prinzipiell für alle Fragen der betrieblichen Sicherheit und Ordnung, besonders wenn es um den **Schutz der Persönlichkeitsrechte der Mitarbeiter**[5] und **Änderungen im Betriebsablauf, die einseitig dem Wohl des Arbeitgebers dienen**[6], geht.

Dieses gewünschte Miteinander von Arbeitgeber und Belegschaft funktioniert nicht immer reibungslos, wie aktuellere Fälle von Mitarbeiterüberwachung **beim ADAC**[7] oder der **Handelsgruppe Rewe**[8] zeigen.

Kurzum: Es ist und bleibt ein Spannungsfeld zwischen den Interessen des Unternehmens und denen der Arbeitnehmer. Aber: Ohne gegenseitiges Vertrauen bleibt jedes Arbeitsverhältnis instabil.

Im Folgenden möchten wir anhand einer "Checkliste zum Mitarbeiterdatenschutz - Hürden und Grenzen der Überwachung" aufzeigen, welche Überwachungsmaßnahmen unter gewissen Umständen legitim sind und was es zu beachten gilt, wenn der Chef seinen Untergebenen "mal über die Schulter schaut."

Regelwerke erstellen

Grundsätzlich sind die Mitarbeiter bei jeder Art von Überwachungsmaßnahmen vorher zu informieren. Das legt das im Grundgesetz verankerte **Persönlichkeitsrecht**[9] fest. Es regelt unter anderem

- die informelle Selbstbestimmung,
- das Recht auf Gewährleistung der Vertraulichkeit und Integrität von IT-Systemen, sowie
- das Recht am eigenen Wort und am eigenen Bild.

Die Information darüber, dass Überwachungsmaßnahmen getroffen werden, soll in einer für jedermann verständlichen Form erfolgen. Also nicht per schriftlicher Mitteilung, die nur ein Fachanwalt ins Deutsche übersetzen kann. Idealerweise erfolgt neben einer schriftlichen Information auch die persönliche samt Erläuterung der wichtigsten Punkte. Dieses Vorgehen stärkt die Vertrauensbasis, auf der Arbeitgeber und -nehmer zusammen arbeiten und sensibilisiert alle Beteiligten im Bereich des Datenschutzes.

Darüber hinaus ist es als Arbeitgeber sinnvoll, sich juristischen Beistand zu holen - um wasserdichte Regeln aufzustellen und die Einführung von Überwachungsmaßnahmen selbst durch geschulte Kräfte überwachen zu lassen. Gesetzesverstöße, die hier begangen werden, können sonst nämlich ziemlich teuer werden - wie später in diesem Beitrag noch zu lesen sein wird.

Taschen- oder "Ehrlichkeitskontrollen"

Von Sportveranstaltungen, aus Discotheken und vom Flughafen ist sie wohlbekannt: die Taschendurchsuchung. Doch wie sieht es damit

im Betrieb aus? Plant der Arbeitgeber entsprechende Maßnahmen, beruft er sich vor allem auf **§859 Bürgerliches Gesetzbuch (BGB)**[10] - die Selbsthilfe des Besitzers. Demnach sind Taschenkontrollen in einem konkreten Verdachtsfall - beispielsweis bei Diebstahl - zulässig. Doch auch hier gilt: Eine vage Vermutung ist kein konkreter Verdacht. Finden derartige Kontrollen regelmäßig statt, ist wiederum vorab (!) der Betriebsrat zu informieren.

"Diebesfallen"[11] wie die Markierung diebstahlgefährdeter Gegenstände mit chemischen Substanzen (wie die Markierung von Geldscheinen in einer Supermarktkasse) dürfen ausschließlich als "Ultima Ratio" bei einem konkreten Verdacht eingesetzt werden.

Videoüberwachung

Die Videoüberwachung ist möglich und zulässig. Im Gegensatz zur NSA muss der Arbeitgeber gemäß **§6b BDSG**[12] jedoch darauf hinweisen, wo sich der Überwachungsbereich befindet, damit die Mitarbeiter wissen, welcher Bereich überwacht wird. Die genauen Anforderungen an Videoüberwachungsanlagen lassen sich in der **DIN 33450**[13] nachlesen. Auch hier gilt: Vor der Einführung von Überwachungskameras muss der Betriebsrat angehört werden - je früher diese Information erfolgt, desto besser. Wer als Arbeitgeber von Anfang an alle Karten auf den Tisch legt, hat eine viel größere Aussicht, seine Pläne in die Tat umzusetzen. Kommt eine verdeckte Videoüberwachung erst viel später ans Licht, bringt der Arbeitgeber die gesamte Belegschaft gegen sich auf, wie beispielsweise die nachgewiesenen Fälle in diversen deutschen Supermarktketten zeigen. Nachvollziehbare Pro-Argumente wie die Verhinderung von Straftaten oder die Beweissicherung gegen Vandalismus- oder Einbruchschäden können die Einführung unterstützen. Hier ist die soziale Intelligenz des Unternehmers gefragt.

Wer den Betriebsrat nicht mit einbezieht, hat bei möglichen späteren Gerichtsverfahren zudem ein Problem, weil er vorhandene Beweise nicht einsetzen darf (**Beweisverwertungsverbot**[14]). Wird also beispielsweise ein Arbeitnehmer ausschließlich aufgrund einer nicht mit dem Betriebsrat abgesprochenen Videoaufnahme, die ihn beim Diebstahl von Firmeneigentum zeigt, gekündigt, hat dieser Arbeitnehmer in einem von ihm angestrengten Kündigungsschutzverfahren vor dem Arbeitsgericht beste Karten auf eine Gehaltsnachzahlung und Wiedereinstellung.

Bei allen Möglichkeiten, die der Arbeitgeber hat, sind der Videoüberwachung aber auch Grenzen gesetzt. So sind Kameras von "intimen Bereichen" wie Umkleiden, Duschen oder Toiletten in jedem Fall fernzuhalten. Darüber hinaus sind nicht mehr benötigte Aufnahmen **unverzüglich zu löschen**[15]. Die willkürliche oder permanente Videoüberwachung ist ebenfalls unzulässig. Heimlich getätigte Aufzeichnungen, von denen der einzelne Mitarbeiter nichts weiß, sind nur bei einem konkreten Straftatverdacht zulässig.

Telefonüberwachung

Telefone anzuzapfen und Gespräche heimlich mitzuhören, ist in manchen Hollywood-Filmen gang und gäbe. In Deutschland ist solch ein Vorgehen grundsätzlich strafbar. **§201 des Strafgesetzbuches (StGB)**[16] sieht darin die Verletzung der Vertraulichkeit des Wortes. Zulässig ist es - genauso wie der **Einsatz von Wanzen in Büroräumen**[17] - nur bei "notwehrähnlichen Situationen". Heißt: Nur, wenn ein konkreter Straftatverdacht vorliegt, wie der Verdacht, dass Geschäfts- und Betriebsgeheimnisse weitergegeben werden, kann das Abhören von Telefongesprächen erlaubt sein.

Überwachung von E-Mails und Internetnutzung

Die **Internetnutzung am Arbeitsplatz**[18] ist ein heikles Thema. Mitarbeiter, die ihre privaten E-Mails vom Büro aus prüfen, sich auf News-Seiten herumtreiben oder zwischendrin kurz online shoppen, können auch juristisch zu einem Problem für das Unternehmen werden. Entscheidend ist, ob es allgemein gültige Richtlinien gibt oder etwas in den Arbeitsverträgen vorgeschrieben ist. Auf der sicheren Seite ist der Arbeitgeber nur, wenn er die private Internetnutzung von vornherein nicht gestattet. Jeder Verstoß gegen diese Auflage hätte für Mitarbeiter arbeitsrechtliche Konsequenzen - von der Abmahnung bis zur Kündigung. Auch dürfte der Arbeitgeber in diesem Fall die Internet- und E-Mail-Nutzung seiner Angestellten regelmäßig prüfen - nicht jedoch dauerhaft überwachen. Denn das wäre wieder ein unzulässiger Eingriff ins Persönlichkeitsrecht.

Die geschilderte Situation ist jedoch selten - viel häufiger existieren überhaupt keine Regelungen zur Internetnutzung. In diesem Fall greifen zusätzlich das **Telemediengesetz (TMG)**[19] und das **Telekommunikationsgesetz (TKG)**[20]. Demnach muss der Arbeitgeber das Fernmeldegeheimnis wahren - gibt es keine Richtlinien zur Internetnutzung am Arbeitsplatz, sind Kontrollen gemäß **§202a StGB**[21] deshalb grundsätzlich strafbar.

Was bleibt, ist der elegante Mittelweg der eingeschränkten privaten Internetnutzung. Viele Unternehmen gestatten ihren Mitarbeitern zumindest in den Pausen gewisse Freiheiten in der privaten Nutzung von E-Mail und Internet. Hier sollte die Verhältnismäßigkeit im Vordergrund stehen - die Arbeitsleistung nicht beeinträchtigt werden. Zwar gilt auch in diesem Fall das Fernmeldegeheimnis, dies jedoch mit Einschränkungen. Werden entsprechende Betriebs- respektive Dienstvereinbarungen getroffen, sind Kontrollen durchaus zulässig. Wiederum nur in begründeten Fällen und in dem erforderlichen Umfang. Und wieder ist der Betriebsrat einzuschalten.

In allen Fällen ist das BDSG einzuhalten. Weitere Informationen zum Thema bietet beispielsweise die **Bayerische Landesbehörde für den Datenschutz**[22].

Einsatz externer Detektive

"Ich bin dann mal krank." - Arbeitnehmer, die Krankheiten nur vortäuschen oder während ihrer Abwesenheit gar noch für die Konkurrenz tätig werden, können das Unternehmen teuer zu stehen kommen. Thorsten Hoth, langjähriger Unternehmer im Sicherheitsgewerbe,

berichtet aus seinem Berufsalltag: "In einem Fall betrieb ein Krankgemeldeter während seiner ‚Krankheit' nebenbei eine Tauchschule in Spanien. In einem anderen Fall erarbeitete sich ein Krankgemeldeter als Skilehrer in den Bergen einen lukrativen Zusatzverdienst."

In solchen Situationen trägt sich manch ein Arbeitgeber sicherlich mit dem Gedanken, eine externe Detektei mit Nachforschungen zu einem bestimmten "Dauerpatienten" zu beauftragen, um mögliche Betrugsfälle aufzudecken. Grundsätzlich ist der Einsatz von Detektiven nur als letztes Mittel gestattet. Nur wenn ein konkreter Straftatverdacht oder der Verdacht auf schwere Verfehlungen seitens des Arbeitnehmers im Rahmen seines Arbeitsverhältnisses vorliegen, ist eine Observierung rechtlich möglich. Auch hier das bereits erwähnte Beweisverwertungsverbot: Zu Unrecht erlangte Beweismittel sind bei Kündigungsschutz- oder Regressprozessen nicht verwertbar. Im Gegensatz zu anderen Überwachungsmaßnahmen hat der Betriebsrat **bei Detektiveinsätzen kein Mitbestimmungsrecht**[23].

Wichtig zu wissen ist aber, dass sich die Anforderungen an Detektiveinsätze derzeit in der Novellierungsphase befinden. Ein Punkt, der überarbeitet werden soll, ist beispielsweise die Frage, wie lange und an wie vielen Tagen observiert werden darf. Hoth macht deutlich, dass gute Ermittler eine Person über mehrere Tage hinweg observieren und entsprechende Beobachtungen protokollieren sollten, um Arbeitgebern stichhaltige, gerichtsfeste Beweise liefern zu können.

Konsequenzen bei Verstößen

Verstößt der Arbeitgeber im Zuge der Mitarbeiterüberwachung gegen geltende Gesetze, kann es teuer werden. Das **BDSG sieht Geldbußen bis zu 300.000 Euro vor**[24], bei ganz schlimmen Gesetzesverletzungen gar bis zu drei Jahre Freiheitsstrafe. Es greifen unter anderem folgende Paragrafen:

- **§43 BDSG**[25] - unbefugte Datenerhebung
- **§44 BDSG**[26] - Strafvorschriften
- **§ 201 StGB**[27] - Verletzung der Vertraulichkeit des Wortes
- **§202a StGB**[28] - Ausspähen von Daten
-

Der Datenschutzbeauftragte

Bei allen Möglichkeiten, die Unternehmen im Bereich der Überwachung ihrer Mitarbeiter besitzen, darf das Vertrauen in diese nicht zu kurz kommen. Ohne Vertrauen wird kein Arbeitsverhältnis Früchte tragen. Das sollen Arbeitgeber immer berücksichtigen.

Sind Mitarbeiter verunsichert, lassen sich der Betriebsrat oder der **Datenschutzbeauftragte (DSB)**[29] zu Rate ziehen, der bei mehr als neun Vollzeitbeschäftigten im Unternehmen gemäß **§4f BDSG**[30] zwingend vorgeschrieben ist. In Behörden ist ein DSB erst ab 20 Vollzeitstellen erforderlich, weil dort nicht das Bundes-, sondern das jeweilige Landesdatenschutzgesetz (LDSG) greift.

Der DSB ist dafür zuständig, Vorschläge für die Umsetzung des Datenschutzes in allen Vorhaben des Unternehmens zu erarbeiten. "Ein DSB tut gut daran, sich nicht als verlängerter Arm der Aufsichtsbehörde zu sehen", warnt Andreas Teuscher, Leiter Konzerndatenschutz/Informationssicherheit und Vorstand des **ISACA Germany Chapter e.V.**[31] "Er sollte sich eine gewisse Neutralität bewahren, denn allzu oft werden Datenschutzargumente vorgeschoben, um unliebsame Auskünfte nicht geben oder Änderungen an Systemen nicht vornehmen zu müssen."

Fazit

Datenschutz ist und bleibt ein sehr sensibles Thema. In jedem Fall sollen Unternehmen dafür Sorge tragen, dass eine wertebasierte Unternehmenskultur vorhanden ist, die Vertrauen schafft. Strikte Kontroll- und Überwachungsmaßnahmen erreichen meist das Gegenteil. Überwachungsmaßnahmen müssen die Interessen der Mitarbeiter berücksichtigen. Nur dann erfüllen sie ihre wahre Funktion - die Gewährleistung der Wettbewerbsfähigkeit unter dem Schutz der Persönlichkeitsrechte der Mitarbeiter. (sh)

Links im Artikel:

[1] **http://www.corporate-trust.de/**
[2] **http://www.corporate-trust.de/studie/studie-2012.html**
[3] **http://www.gesetze-im-internet.de/bdsg_1990/__32.html**
[4] **http://www.gesetze-im-internet.de/betrvg/__87.html**
[5] **http://dejure.org/gesetze/BetrVG/75.html**
[6] **http://www.gesetze-im-internet.de/betrvg/__80.html**
[7] **http://www.sueddeutsche.de/wirtschaft/ueberwachte-e-mails-spionageverdacht-beim-adac-1.1629727**
[8] **http://www.spiegel.de/wirtschaft/unternehmen/geheime-kameraueberwachung-auch-rewe-bespitzelt-mitarbeiter-a-897401.html**
[9] **http://de.wikipedia.org/wiki/Pers%C3%B6nlichkeitsrecht_%28Deutschland%29**
[10] **http://dejure.org/gesetze/BGB/859.html**
[11] **http://de.wikipedia.org/wiki/Diebesfalle**
[12] **http://www.gesetze-im-internet.de/bdsg_1990/__6b.html**
[13] **http://www.nasg.din.de/cmd?artid=76533394&bcrumblevel=1&contextid=nasg&subcommitteeid=54754424&level=tpl-art-**

detailansicht&committeeid=54739031&languageid=de

[14] **http://de.wikipedia.org/wiki/Beweisverbot**

[15] **http://www.gesetze-im-internet.de/bdsg_1990/__6b.html**

[16] **http://dejure.org/gesetze/StGB/201.html**

[17] **http://www.computerwoche.de/a/erst-beschenkt-dann-abgehoert%2C2550783**

[18] **http://de.wikipedia.org/wiki/Internetnutzung_am_Arbeitsplatz**

[19] **http://www.gesetze-im-internet.de/tmg/**

[20] **http://www.gesetze-im-internet.de/tkg_2004/**

[21] **http://dejure.org/gesetze/StGB/202a.html**

[22] **http://www.datenschutz-bayern.de/technik/orient/privmail.html**

[23] **http://dejure.org/dienste/vernetzung/rechtsprechung?Text=1%20ABR%2026/90**

[24] **http://www.gesetze-im-internet.de/bdsg_1990/__43.html**

[25] **http://www.gesetze-im-internet.de/bdsg_1990/__43.html**

[26] **http://www.gesetze-im-internet.de/bdsg_1990/__44.html**

[27] **http://dejure.org/gesetze/StGB/201.html**

[28] **http://dejure.org/gesetze/StGB/202a.html**

[29] **http://de.wikipedia.org/wiki/Datenschutzbeauftragter**

[30] **http://www.gesetze-im-internet.de/bdsg_1990/__4f.html**

[31] **http://www.isaca.de/**
