

Vertrauen ist gut – IT-Kontrolle nur ausnahmsweise besser

Keylogger (Tasten-Protokollierer), Screen-Capture (Bildschirmkopierer), Mouse-Recorder (Mausbewegungskopierer) – die technischen Möglichkeiten der Kontrolle von Aktivitäten der Mitarbeiter an betrieblichen IT-Mitteln wie PC, Tablet und Smartphone nehmen mit der voranschreitenden Digitalisierung der Arbeitsabläufe stetig zu. Der Orwellsche „Big Brother“ aus „1984“ lässt grüßen. Die Schwelle eines Einsatzes einer solchen (Dauer-) Überwachungssoftware ist niedrig angesiedelt, da die Programme auch als Free Download im Internet kostenfrei zur Verfügung stehen. Das in der Praxis zu beobachtende Interesse von Arbeitgebern, sich derartiger schnell einsetzbarer – früher vornehmlich von Hackern und Geheimdiensten eingesetzt – Aufklärungsmittel zu bedienen, liegt darin begründet, dass die steigenden Einsatzmöglichkeiten des IT-Equipments von den Mitarbeitern umfangreicher zu nicht betrieblichen Zwecken genutzt werden können. Während zu Beginn des Internetzeitalters die Gewöhnung an neue IT-Mittel im Vordergrund stand, bei der es auf Zwecksetzung und Dauer der Nutzung nicht entscheidend ankam, hat sich zwischenzeitlich vermehrt das Kostenbewusstsein durchgesetzt, wonach jede nicht dienstlich genutzte Zeit wirtschaftliche Einbußen mit sich bringt – „Zeit ist Geld“ – und zu vermeiden ist.



Da von außen für den Vorgesetzten bei einer IT-Tätigkeit regelmäßig nicht erkennbar ist, ob der Mitarbeiter dienstlich oder privat für sich selbst arbeitet, leisten Kontroll-Tools unauffällige effektive technische Hilfe. Ob diese Vorgehensweise jedoch auch rechtlich empfehlenswert ist, lässt sich auf der Grundlage der aktuellen Rechtsprechung des BAG (Urt. v. 27.7.2017 – 2 AZR 681/16, PM Nr. 31, NZA aktuell H. 15/2017, S. VI) grundsätzlich mit einem klaren Nein beantworten. Eine elektronisch basierte dauerhafte Überwachung ist danach wegen der Verletzung des Grundrechts auf informationelle Selbstbestimmung (Art. 2 I iVm Art. 1 I GG) und des § 32 BDSG (ab 25.5.2018: § 26 BDSG neu) im Regelfall unzulässig; mit ihr erlangte Beweise sind prozessual nicht verwertbar. Nur wenn zu dokumentierende, den zu kontrollierenden Mitarbeiter betreffende Tatsachen vorliegen, die einen Verdacht einer Straftat oder einer anderen schwerwiegenden Pflichtverletzung begründen, kommt der Einsatz einer „Spähsoftware“ im Rahmen der einzuhaltenden Verhältnismäßigkeit – also im Ausnahmefall – in Betracht.

Diese Rechtsprechung überrascht – angesichts der Judikate des BAG zur Videoüberwachung (z.B. BAG, NZA 2003, 1193) – nicht und ist richtig. In einem Rechtsstaat sind bekanntlich nicht nur staatliche Organe, sondern – über die Drittwirkung der Grundrechte im Privatrecht – auch Arbeitgeber zu einer grundrechtskonformen Vorgehensweise im Arbeitsverhältnis verpflichtet, was kürzlich auch der EGMR in seiner Entscheidung vom 5.9.2017 (Nr. 268/17) bestätigt. Dieses gilt erst recht in der Arbeitswelt 4.0 mit ihren steigenden Gefahren für das Persönlichkeitsrecht des Arbeitnehmers. Abgesehen von grundsätzlich möglichen Stichprobenkontrollen (vgl. hierzu exemplarisch *Oberthür*, in *Kramer*, IT-Arbeitsrecht, 1. Aufl. 2017, B Rn. 438 ff.) gilt für Arbeitgeber und die sie beratenden Anwälte als Orientierungsregel daher das obige jedenfalls in diesem Kontext zu modifizierende Sprichwort. Sorgfältige Prüfung der Sachlage und Augenmaß sind gefordert.

Fachanwalt für Arbeitsrecht Dr. Stefan Kramer, Brüggehausen + Kramer, Hannover