Licht im „Compliance-Dickicht“? BAG schärft Konturen zur Zulässigkeit interner Ermittlungen

EINFÜHRUNG

Interne Ermittlungen sind mittlerweile fester Bestandteil der unternehmerischen Praxis. Neben der breiten Palette altbekannter Pflichtverstöße durch Mitarbeiter (Unterschlagung von Betriebsmitteln, Vortäuschen einer AU, „Vorbereitung“ späterer Konkurrenztätigkeiten etc.), ist dies vor allem auf die Compliance-Bewegung zurückzuführen, indem die erweiterten Verhaltensvorgaben für Unternehmen und Mitarbeiter auch einen erhöhten Ermittlungsaufwand nach sich gezogen haben.

Gleichwohl sehen sich Unternehmen aufgrund des Fehlens klarer rechtlicher Vorgaben zur Zulässigkeit interner Ermittlungen oftmals mit der Frage konfrontiert, ob einzelne Ermittlungsmaßnahmen zulässig und wie diese in ihrer Gesamtheit aufeinander abzustimmen sind. Verschärft wird dieses Problem mit Blick auf die Vielzahl möglicher Maßnahmen (z. B. Videoüberwachungen, E-Mail-Kontrollen, Detektei) und vor allem die Rechtsfolgen unzulässiger Ermittlungen, die von Beweisverwertungsverboten in späteren Kündigungsschutz- oder Schadensersatzprozessen über eine Strafbarkeit bzw. Ordnungswidrigkeit bis hin zu möglichen Schmerzensgeldansprüchen der Mitarbeiter reichen können – dazu kommen unter Umständen noch erhebliche Reputationsschäden für die betroffenen Unternehmen.

In diesem Zusammenhang schafft das neueste Urteil des Bundesarbeitsgerichts („BAG“) vom 19. Februar 2015 zumindest einiges an Klarheit, indem es insbesondere die Konturen zur Zulässigkeit interner Ermittlungen zu repressiven Zwecken mit Blick auf den hierfür erforderlichen Verdacht weiter geschärft hat.

SACHVERHALT

BAG, URTEIL VOM 19.02.2015 - 8 AZR 1007/13

Die Klägerin war bei der Beklagten seit Mai 2011 tätig und ab dem 27. Dezember 2011 arbeitsunfähig erkrankt, zunächst mit Bronchialerkrankungen. Für diese Zeit reichte sie sechs AU-Bescheinigungen, zunächst vier eines Facharztes für Allgemeinmedizin, dann zwei weitere einer Fachärztin für Orthopädie ein. Der Geschäftsführer der Beklagten bezweifelte das Vorliegen eines – zuletzt durch die Klägerin mitgeteilten – Bandscheibenvorfalls und schaltete einen Detektiv ein, der sie an vier Tagen überwachte und hierbei sowohl Bild- als auch Videoaufnahmen, u.a. beim Besuch eines Waschsalons, erstellte. Auf die folgende Kündigung der Beklagten hin erhob die Klägerin Kündigungsschutzklage und beantragte zudem die Verurteilung der Beklagten zur Zahlung eines Schmerzensgeldes nach gerichtlichem Ermessen, wobei sie selbst EUR 10.500 für angemessen hielt.

ENTSCHEIDUNG DES BAG

Das Arbeitsgericht hatte der Kündigungsschutzklage stattgegeben, die Schmerzensgeldklage jedoch abgewiesen, wohingegen das LAG Hamm die Beklagte zu einer Zahlung von Schmerzensgeld in Höhe von EUR 1.000 verurteilte. Das BAG bestätigte dieses Urteil. Zur Begründung stellt es darauf ab, dass ein Arbeitgeber, der wegen des Verdachts einer vorgetäuschten AU einem Detektiv die Überwachung eines Arbeitnehmers übertrage, rechtswidrig handele, wenn sein Verdacht nicht auf konkreten Tatsachen beruhe. Dies sei vorliegend der Fall, da der Beweiswert der AU-Bescheinigungen weder dadurch erschüttert gewesen sei, dass sie von unterschiedlichen Ärzten stammten, noch durch eine Änderung im Krankheitsbild oder weil der Bandscheibenvorfall zunächst hausärztlich behandelt worden sei. Eine solche rechtswidrige Verletzung des allgemeinen Persönlichkeitsrechts könne ebenfalls einen Schmerzensgeldanspruch begründen, wobei die vom LAG angenommene Höhe des Schmerzensgeldes revisionsrechtlich nicht zu beanstanden sei.

PRAKTISCHE BEDEUTUNG DER ENTSCHEIDUNG

Das BAG führt mit dieser Entscheidung, die bislang lediglich in Form einer Pressemitteilung vorliegt, seine Rechtsprechung zu internen Ermittlungen fort, bewertet deren Zulässigkeit aber erstmals ausdrücklich am Maßstab des § 32 Abs. 1 S. 2 BDSG. Zuvor hatte es die Frage, ob eine Ermittlungsmaßnahme in Form einer Spind-Untersuchung als datenschutzrechtlich relevante „Datenverarbeitung“ zu begreifen sei, noch offen gelassen (BAG v. 20-06.2013 – 2 AZR 546/12). Dennoch hatte es schon hier anklingen lassen, Ermittlungsmaßnahmen – bei denen es regelmäßig um die Gewinnung und Verwertung von personenbezogenen Daten i.S.d. § 3 Abs. 1 S. 1 BDSG geht – im Grundsatz als relevante Datenverarbeitung anzusehen und damit einer datenschutzrechtlichen Beurteilung zu unterwerfen. Hier hatte das BAG gleichfalls klargemacht, dass dies aufgrund des § 32 Abs. 2 BDSG auch unabhängig davon gelte, ob die Ermittlungen rein tatsächliche Handlungen (z. B. bei der Beobachtung durch eine Detektei) oder automatisierte Datenverarbeitungen (z. B. bei der Herstellung von Bild- oder Videoaufnahmen) beträfen (BAG a.a.O.).

Die maßgebliche Vorschrift des § 32 Abs. 1 S. 2 BDSG setzt auf der ersten Stufe zu dokumentierende tatsächliche Anhaltspunkte voraus, die den Verdacht einer Straftat durch den Mitarbeiter begründen. Nach allgemeiner Auffassung sind hierfür tatsächliche Anhaltspunkte jedenfalls im Sinne eines Anfangsverdachts erforderlich. Indem das BAG die Unzulässigkeit der Ermittlungen vorliegend bereits mit dem Fehlen eines Verdachts begründet, macht es deutlich, dass es diese „Einstiegshürde“ sehr ernst nimmt und auch verhältnismäßig hohe Begründungsanforderungen an

einen Tatverdacht stellt. Dennoch wird es hier auf den Einzelfall ankommen. Denn der dem Urteil zugrunde liegende Sachverhalt weist vor allem die Besonderheit auf, dass die in derartigen Fällen regelmäßig vorliegende AU-Bescheinigung einen gegenteiligen Beweiswert aufweist, den es aufgrund konkreter Anhaltspunkte erst einmal zu entkräften gilt. Dies kann etwa dann gelingen, wenn der Mitarbeiter widersprüchliche Angaben zur AU macht oder einer Aufforderung zu einer Begutachtung durch den medizinischen Dienst der Krankenkasse nicht nachkommt (LAG Hamm v. 11.07.2013 – 11 Sa 312/13), erfordert aber im Vergleich zu anderen Fallkonstellationen erhöhte Begründungsanforderungen. Bevor einzelne Ermittlungsmaßnahmen eingeleitet werden, ist in der Praxis allerdings in jedem Einzelfall notwendig, die gegebenen Verdachtsmomente mit Blick auf die genannten Maßstäbe sorgfältig zu bewerten und dies ebenfalls – gemäß den weiteren gesetzlichen Anforderungen des § 32 Abs. 1 S. 2 BDSG – zu dokumentieren.

Auf der zweiten Stufe müssen Ermittlungsmaßnahmen, kurz gesagt, erforderlich und verhältnismäßig sein und die Interessen des Mitarbeiters hinreichend berücksichtigen. Auch wenn das BAG vorliegend keine Abwägungsentscheidung mehr treffen musste, hatte es sich in einigen Vorgängerentscheidungen gerade an dieser Stelle – auch wenn der Abwägungsvorgang hier noch ausschließlich an die Grundrechte anknüpfte – äußerst zurückhaltend gezeigt. Eine heimliche Videoüberwachung hält es nur dann für zulässig, wenn „weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft sind, die verdeckte Videoüberwachung damit das praktisch einzig verbleibende Mittel darstellt und sie insgesamt nicht unverhältnismäßig ist“ (BAG v. 21.06.2012 – 2 AZR 153/11). Daran anknüpfend hatte das BAG auch eine heimliche Spind-Kontrolle insbesondere mit dem Hinweis für unzulässig erklärt, dass als „milderes Mittel“ ebenfalls eine derartige Kontrolle in Anwesenheit des Mitarbeiters in Betracht komme (BAG v. 20.06.2013 – 2 AZR 546/12).

Für die Praxis bedeutet dies, mit Blick auf die Eingriffsintensität der jeweils zur Verfügung stehenden Ermittlungsmaßnahmen eine Art „Treppe“ für das weitere Vorgehen zu bilden. E-Mail-Kontrollen, Video- oder eine umfassende Detektivüberwachung wären hierbei im Grundsatz erst auf höheren „Stufen“ zu verorten, wobei auch innerhalb einzelner Maßnahmen (z.B. E-Mail-Kontrolle) die Eingriffsintensität stufenweise erhöht werden kann (z.B. Beschränkung auf ausgewählte Zeiträume, anschließende Einschränkung auf Betreffzeile etc.). In Betracht kommt mit Blick auf die genannten BAG-Entscheidungen aber auch ein stufenweises Vorgehen, das die Ermittlungsmaßnahmen zunächst auf bestimmte Verdächtige begrenzt (BAG v. 21.06.2012 a.a.O), oder – falls weniger intensive Ermittlungsschritte auf den ersten Stufen nicht möglich sind – eine offene Durchführung der Maßnahme gegenüber dem Betroffenen (BAG v. 20.06.2013 a.a.O.). Darüber hinaus können bei einzelnen Maßnahmen aber auch weitergehende Sondervorschriften zu beachten sein, wie z.B. spezielle Grundrechte wie die Unverletzlichkeit der Wohnung gemäß Art. 13 GG (BAG v. 20.06.2013 a.a.O.). Letztlich ist mit Blick auf die Interessenabwägung aber auch daran zu denken, einen vorhandenen Betriebsrat oder betrieblichen Datenschutzbeauftragten miteinzubeziehen, wenngleich allein eine fehlende Beteiligung des Betriebsrats noch nicht zu einem Beweisverwertungsverbot führen soll (BAG v. 13.12.2007 – 2 AZR 537/06). Auch in diesem Zusammenhang ist aber zu empfehlen, das Vorgehen – auch wenn hier keine entsprechende gesetzliche Verpflichtung besteht – zu Beweiszwecken schriftlich zu dokumentieren.

Insgesamt ist festzuhalten, dass sich mit Blick auf die genannten rechtlichen Anforderungen jedwede schematische Lösungen bei der Vorbereitung und Durchführung von Ermittlungsmaßnahmen verbieten. In jedem Einzelfall kommt es darauf an, abhängig vom konkreten Verdacht, dem Ermittlungsziel und den zur Verfügung stehenden Mitteln ein jeweils maßgeschneidertes Maßnahmenpaket zu entwerfen. Ansonsten besteht angesichts der neuen Rechtsprechung nicht nur die Gefahr, dass man sich den „teuren“ Ergebnissen der Ermittlungen für ein späteres Kündigungsschutz- oder Schadensersatzverfahren beraubt, sondern auch Schmerzensgeldansprüchen von Mitarbeitern oder den Gefahren einer Strafbarkeit ausgesetzt sein kann. Denn parallel zum BAG hat auch der BGH in letzter Zeit mit Blick auf GPS-gestützte Bewegungsprofile durch eine Detektei unmissverständlich klargestellt, dass derartige – im Einzelfall datenschutzrechtlich unzulässige – Ermittlungsmaßnahmen strafbar sein können (BGH v. 04.06.2013 – 1 StR 32/13).■

ANSPRECHPARTNER

Dr. Thilo Mahnhold
t.mahnhold@justem.de

Dr. Daniel Klösel
d.klösel@justem.de

www.justem.de