



12.7.2010

MITTEILUNG AN DIE MITGLIEDER

Betrifft: Petition 1198/2009, eingereicht von J.F.K., ungarischer Staatsangehörigkeit, zum Eindringen multinationaler Unternehmen in die Privatsphäre ihrer Beschäftigten

1. Zusammenfassung der Petition

Der Petent protestiert gegen die Praxis multinationaler Unternehmen, am Werkstor Taschenkontrollen durchzuführen und die Mitarbeiter während der Arbeit mit Kameras zu überwachen, sowie die Pflicht, bei der Bewerbung einen Lebenslauf vorzulegen. Dies stelle eine Verletzung der Menschenrechte dar, weshalb er vom Parlament Maßnahmen fordert, um diesen Praktiken Einhalt zu gebieten.

2. Zulässigkeit

Für zulässig erklärt am 1. Dezember 2009. Die Kommission wurde um Auskünfte gebeten (Artikel 202 Absatz 6 der Geschäftsordnung).

3. Antwort der Kommission, eingegangen am 12. Juli 2010

Die Petition

Der Petent beschwert sich über drei Praktiken multinationaler Unternehmen wie Jabil, Nokia und Sanmina in Ungarn: 1) tägliche Kontrollen der Mitarbeiter durch Taschenkontrolleure (oftmals mit Leibesvisitation) auf dem Gelände der multinationalen Unternehmen, 2) die Pflicht, bei der Bewerbung um eine Stelle im Voraus einen Lebenslauf vorzulegen, und 3) entwürdigende Videoüberwachung am Arbeitsplatz. Er gibt an, dass er keine Belege für seine Vorwürfe habe, erklärt jedoch dazu, dass die Mitarbeiter eine gesonderte Vereinbarung unterschreiben müssen, in der sie bestätigen, dass sie am Arbeitsplatz kein Mobiltelefon und keine Kamera benutzen. Er führt weiterhin an, dass es Regeln gebe, wonach Bilder und Töne für Ton- und Videoaufnahmen nicht kränkend und durch Schikanen anderer wiedergegeben

oder gegen den Willen der Betroffenen gemacht werden dürfen. Bei außergewöhnlicher Notwendigkeit und aus berechtigten Gründen dürfe jeder eine Aufnahme zur Beweissicherung anfertigen.

Der Petent vertritt die Ansicht, dass derartige Kontrollen demütigend seien, dass die Pflicht zur Vorlage seines Lebenslaufes im Voraus eine unzulässige Erfassung von Daten darstelle und dass das Verbot zur Verwendung eines Mobiltelefons mit Kamera an seinem Arbeitsplatz seine Menschenrechte verletze. Es ersucht darum, dass die Arbeitnehmer durch entsprechende Rechtsinstrumente vor den genannten Praktiken geschützt werden.

Die Anmerkungen der Kommission zur Petition

Die Datenschutzrichtlinie (*Richtlinie 95/46/EG*¹) gibt den rechtlichen Rahmen für die Verarbeitung personenbezogener Daten in allen Mitgliedstaaten vor. Wenn ein Mitgliedstaat seiner Umsetzungspflicht nicht nachgekommen ist, können die Bürger die direkte Anwendung einiger Bestimmungen dieser Richtlinie fordern. In diesem Sinne entschied der EuGH in der Rechtssache C-465/00², dass gewisse Bestimmungen wie z. B. Artikel 6 Absatz 1 Buchstabe c (Grundsätze in Bezug auf die Qualität der Daten: Daten müssen den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen) und Artikel 7 Buchstabe c und e (Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von Daten) direkte Wirkung haben.

Richtlinie 95/46/EG ist nur auf personenbezogene Daten anwendbar, die in ihren Geltungsbereich fallen. In Artikel 2 werden „personenbezogene Daten“ definiert als alle Informationen über eine bestimmte oder bestimmbare natürliche Person (betroffene Person). Als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

In Richtlinie 95/46/EG sind die Voraussetzungen für eine rechtmäßige Verarbeitung der Daten festgelegt. Sie begründet auch die Rechte der von der Verarbeitung personenbezogener Daten betroffenen Personen, um die Wahrung ihres Grundrechts auf den Schutz ihrer personenbezogenen Daten sicherzustellen. Die in Artikel 6 verankerten Grundsätze bilden die Grundlage für den Schutz personenbezogener Daten, da sie die Qualität der Datenverarbeitung betreffen: die Daten müssen für festgelegte eindeutige und rechtmäßige Zwecke erhoben und verarbeitet werden (Grundsatz der Zweckbindung), den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen (Grundsatz der Verhältnismäßigkeit) und wenn nötig auf den neuesten Stand gebracht werden (Artikel 6). Außerdem dürfen personenbezogene Daten nicht länger verarbeitet werden, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist.

¹ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31.

² EuGH C-465/00, C-138/01 und C-139/01, Rechnungshof / Österreichischer Rundfunk, 20.5.2003, Randnr. 98ff.

Nach Artikel 7 ist die Datenverarbeitung nur dann rechtmäßig, wenn

- a) die betroffene Person ohne jeden Zweifel ihre Einwilligung gegeben hat, oder
- b) die Verarbeitung zur Erfüllung eines für die betroffene Person bindenden Vertrags erforderlich ist, oder
- c) die Verarbeitung zur Erfüllung einer gesetzlichen Verpflichtung erforderlich ist, oder
- d) die Verarbeitung für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist, oder
- e) die Verarbeitung erforderlich ist für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, oder
- f) die Verarbeitung erforderlich ist im Interesse einer anderen Person, vorausgesetzt, dass die Interessen oder die Rechte und Freiheiten der betroffenen Person geschützt sind.

Die betroffene Person hat das Recht auf Information betreffs Zugang zu, Berichtigung und Löschung oder Sperrung ihrer personenbezogenen Daten sowie auf wirksame Rechtsbehelfe bei unrechtmäßiger Verarbeitung ihrer Daten. Diese Rechte können eingeschränkt werden, soweit dies beispielsweise nicht nur für die Sicherheit des Staates und die Landesverteidigung, sondern auch für die Ermittlung und Verfolgung von Straftaten erforderlich ist.

Die Verarbeitung wird durch unabhängige öffentliche Kontrollstellen überwacht und kontrolliert (Artikel 28), die in der Regel „Datenschutzbehörden“ genannt werden und die dafür zuständig sind, die Einhaltung der einzelstaatlichen Rechtsvorschriften zur Umsetzung der Richtlinie bei der Verarbeitung personenbezogener Daten auf nationaler Ebene zu überwachen.

Zwei Fragen sind zu klären, um die Anwendbarkeit der Datenschutzrichtlinie 95/46/EG festzustellen.

Die wichtigste Frage betrifft die verarbeiteten Daten und ob sie unter die Definition der „personenbezogenen Daten“ von Artikel 2 Buchstabe a fallen. Was den zweiten und dritten Vorwurf des Petenten betrifft, handelt es sich bei den Daten eines Lebenslaufes und den bei einer Videoüberwachung aufgezeichneten Daten um personenbezogene Daten im Sinne der Richtlinie 95/46/EG. Hinsichtlich des ersten Vorwurfs liegen Leibesvisitationen nicht im Geltungsbereich der Datenschutzrichtlinie.

Als zweite relevante Frage gilt es zu klären, wer die personenbezogenen Daten verarbeitet. Je nachdem, ob es sich um einen für die Verarbeitung Verantwortlichen oder lediglich um einen Datenverarbeiter handelt, müssen sie eine Reihe von Pflichten erfüllen. Multinationale Unternehmen wie Jabil, Nokia und Sanmina sind Rechtspersonen, die selbst den Zweck und die Mittel der Verarbeitung der von ihnen gesammelten personenbezogenen Daten bestimmen, wie z. B. die in einem Lebenslauf enthaltenen Angaben oder die durch Videoüberwachung erfassten Daten. Somit gelten sie als für die Verarbeitung Verantwortliche im Sinne der Richtlinie 95/46/EG, obwohl sie die Verarbeitung der personenbezogenen Daten an Verarbeiter delegieren/untervergeben könnten, die diese Aufgabe in ihrem Auftrag ausführen.

Erster Vorwurf: Kontrollen von Mitarbeitern durch Taschenkontrolleure (oft mit

Leibesvisitation)

Nach Maßgabe des Vertrages über die Europäische Union und des Vertrages über die Arbeitsweise der Europäischen Union verfügt die Europäische Kommission über keine allgemeine Befugnis, in Einzelfällen von angeblichen Verstößen gegen die Grundrechte tätig zu werden. Sie kann nur einschreiten, wenn Rechtsvorschriften der Europäischen Union betroffen sind.

Im Zusammenhang mit der Beschwerde des Petenten über Kontrollen der Mitarbeiter durch Taschenkontrolleure in Montagewerken sei darauf hingewiesen, dass diese Angelegenheit durch keine spezifischen EU-Rechtsvorschriften geregelt wird. Aus diesem Grunde ist es der Kommission nicht möglich, diesem ersten Vorwurf nachzugehen.

Zweiter Vorwurf: unrechtmäßige Datensammlung durch Abforderung eines Lebenslaufes von einem potenziellen künftigen Mitarbeiter

Stellen in Unternehmen werden heutzutage besetzt, nachdem interessierte und in Betracht kommende Bewerber ein Auswahlverfahren absolviert haben. Dazu gehört generell eine Vorauswahlphase auf der Basis der Lebensläufe, die von interessierten Bewerbern im Voraus eingereicht werden. Die Verarbeitung der in Lebensläufen enthaltenen Daten fällt in den Anwendungsbereich der Datenschutzrichtlinie 95/46/EG und unterliegt den Grundsätzen der Zulässigkeit, Notwendigkeit und Verhältnismäßigkeit (Artikel 6 der Richtlinie).

In den meisten Fällen lässt sich die Verarbeitung der in Form von Lebensläufen eingereichten Daten als rechtmäßig begründen, da sie

- mit Einwilligung der betroffenen Person erfolgt (Artikel 7 Buchstabe a),
- für die Erfüllung eines Arbeitsvertrages zwischen einem Arbeitgeber und einem Arbeitnehmer erforderlich ist (Artikel 7 Buchstabe b) oder
- Bestandteil des berechtigten Interesses ist, das vom Arbeitgeber wahrgenommen wird, um in Erfahrung zu bringen, welche Qualifikationen potenzielle künftige Mitarbeiter erworben haben, so dass die freie Stelle mit der am besten geeigneten Person besetzt wird (Artikel 7 Buchstabe f).

Die Verarbeitung personenbezogener Daten aus Lebensläufen muss im Verhältnis zu den berechtigten Zielen stehen und sollte insbesondere so erfolgen, dass das Eindringen in die Privatsphäre auf ein Mindestmaß beschränkt wird. Sofern ausreichende Sicherheitsvorkehrungen getroffen wurden, stünde eine derartige Verarbeitung der Daten im Einklang mit der Richtlinie 95/46/EG. Derartige Vorkehrungen könnten z. B. Folgendes beinhalten:

- Information der Mitarbeiter über die Identität des für die Verarbeitung Verantwortlichen und über die Zweckbestimmung der Überwachung sowie weitere Informationen, die notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten (Artikel 11);
- Information der betroffenen Person über ihr Berichtigungsrecht und – insbesondere für letztendlich nicht angenommene Bewerber – über ihr Recht auf Datenlöschung.

Der einfache Umstand, dass ein potenzieller Arbeitgeber ein Vorausexemplar des Lebenslaufs eines potenziellen Arbeitnehmers verlangt, kann nicht als unrechtmäßige Erfassung von Daten angesehen werden, wie vom Petenten geltend gemacht.

Dritter Vorwurf: Videoüberwachung am Arbeitsplatz

Videoüberwachung fällt in den Anwendungsbereich der Datenschutzrichtlinie 95/46/EG. Die Datenschutzgrundsätze, insbesondere die Grundsätze der Zulässigkeit, der Notwendigkeit und der Verhältnismäßigkeit (Artikel 6 der Richtlinie) gelten für jegliche Verarbeitung von personenbezogenen Daten aus der Videoüberwachung.

Die Artikel-29-Datenschutzgruppe¹ hat zwei Stellungnahmen zur Videoüberwachung am Arbeitsplatz² herausgegeben, die eine Orientierungshilfe dafür bieten, wie die Bestimmungen der Datenschutzrichtlinie auf die Videoüberwachung anzuwenden sind. Diesen Stellungnahmen zufolge hängt die Rechtmäßigkeit einer Videoüberwachung am Arbeitsplatz von mehreren Faktoren ab:

Erstens vom Zweck der Verarbeitung: Videoüberwachungssysteme können gerechtfertigt sein, wenn sie unter Einhaltung der angemessenen Schutzmaßnahmen eingesetzt werden, um Sicherheitsvorschriften in der Produktion oder am Arbeitsplatz zu erfüllen, oder aus Gründen des Schutzes. Den verschiedenen Interessen sollte fallweise und vor dem Hintergrund der konkreten Umstände Rechnung getragen werden.

Die Installation von Videoüberwachungsanlagen durch Unternehmen zur Erfüllung von Sicherheitsvorschriften der Produktion oder aus Gründen des Schutzes (zur Verhinderung des Diebstahls von elektronischen Erzeugnissen oder technologischen Forschungsergebnissen) kann insofern legitim sein, als sie für die Wahrung des berechtigten Interesses dieser Unternehmen („für die Verarbeitung Verantwortlicher“) notwendig ist, um die Sicherheit der Räumlichkeiten bzw. des Geländes zu gewährleisten oder den Diebstahl technologischer Forschungsergebnisse und Geschäftsgeheimnisse zu verhindern, wobei die Interessen der Arbeitnehmer dieses Interesse nicht überwiegen (Artikel 7 Buchstabe f).

Gleichfalls kann der Einsatz von Videoüberwachungssystemen gerechtfertigt sein, um ein lebenswichtiges Interesse der betroffenen Person zu schützen, wie z. B. der Schutz vor Arbeitsunfällen im Sinne des Arbeitsschutzes (Artikel 7 Buchstabe d) .

Zweitens von der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung: Der Einsatz von Videoüberwachungstechnik muss im Verhältnis zu den berechtigten Zielen stehen, und vor allem muss bei der Verarbeitung der Daten so vorgegangen werden, dass das Eindringen in

¹ Die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgruppe) wurde nach Maßgabe von Artikel 29 der Datenschutzrichtlinie 95/46/EG eingesetzt und besteht aus Vertretern der nationalen Datenschutzbehörden. Sie ist unabhängig und hat beratende Funktion für die Kommission.

² Stellungnahme 8/2001 (WP48) zur Verarbeitung personenbezogener Daten von Beschäftigten, Arbeitsdokument vom 25. November 2002 (WP67) zur Verarbeitung personenbezogener Daten aus der Videoüberwachung und Stellungnahme 4/2004 (WP89) zum Thema Verarbeitung personenbezogener Daten aus der Videoüberwachung.

die Privatsphäre auf ein Mindestmaß beschränkt ist. Die Interessen des Arbeitgebers bei der Installation von Videoüberwachungsanlagen müssen gegen die Interessen des Arbeitnehmers abgewogen werden, seine personenbezogenen Daten geschützt zu sehen. Das lässt sich nur durch geeignete Sicherheitsvorkehrungen erreichen. Nur dann stünde die Videoüberwachung im Einklang mit der Richtlinie 95/46/EG. Derartige Sicherheitsvorkehrungen könnten beispielsweise Folgendes beinhalten:

- keine Installation von Videoüberwachungstechnik auf Toiletten, in Duschräumen, Umkleieräumen und Freizeitbereichen;
- Unterrichtung der Mitarbeiter über die Identität des für die Verarbeitung Verantwortlichen und über den Zweck der Überwachung sowie Bereitstellung weiterer Informationen, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten;
- eine Begrenzung der Aufbewahrungsdauer der Videos;
- eine unabhängige Beaufsichtigung durch die nationalen Datenschutzbehörden, die dafür zuständig sind, die Einhaltung nationaler Datenschutzgesetze zur Umsetzung der Richtlinie 95/45/EG zu überwachen und die geeigneten Vorkehrungen zu treffen und Anforderungen zu stellen, damit das System rechtmäßig ist.

Außerdem ist der für die Verarbeitung Verantwortliche verpflichtet (Artikel 11), die Personen, die einen videoüberwachten Ort betreten, sichtbar, klar und eindeutig darüber zu informieren, dass sie beobachtet werden. Bei Videoüberwachungsanlagen am Arbeitsplatz sollten auch die Arbeitnehmervertreter davon in Kenntnis gesetzt werden.

Schlussfolgerungen

Was den ersten Vorwurf der Taschenkontrollen von Mitarbeitern, insbesondere Leibesvisitationen, betrifft, so fällt diese Angelegenheit nicht in den Anwendungsbereich des Unionsrechts, weshalb die Kommission diesem Vorwurf nicht nachgehen kann.

Was die anderen Vorwürfe betrifft, hat der Petent keine Belege vorgelegt, die nachweisen, dass die Tochtergesellschaften der multinationalen Unternehmen Jabil, Nokia und Sanmina gegen die Richtlinie 95/46/EG verstoßen haben.

Dem Petenten sei geraten, Vorwürfe, die er gegen diese multinationale Unternehmen erhebt und die im Zusammenhang mit einer Verletzung seiner Datenschutzrechte stehen, an die nationale Datenschutzbehörde in Ungarn zu richten:

Ungarischer Datenschutzbeauftragter
Nádor str. 22.
1051 Budapest
Tel.: (+36 1) 475 7100, (+36 1) 475 7186
Fax: (+36 1) 269 3541
E-Mail: adatved@obh.hu