Internet und Arbeitnehmerdatenschutz

Datenschutz: Was tun, wenn die Personaldaten in den USA lagern? Wie kann man im Internet eine Berichtigung durchsetzen? Was geschieht mit Daten, die beim „Crowdworking" anfallen?

von **Wolfgang Däubler**

Unser Datenschutzrecht kennt eine „verantwortliche Stelle". Für Arbeitnehmer ist dies das Unternehmen, für das sie tätig sind. Diese verantwortliche Stelle muss Auskünfte geben und unrichtige Angaben ergänzen oder löschen. Sie darf Informationen nur insoweit erheben, weiterverarbeiten und an Dritte übermitteln, als dies insbesondere zur Durchführung des Arbeitsverhältnisses erforderlich ist (§ 32 Abs. 1 Satz 1 BDSG).

Das Unternehmen als geschlossene Einheit

Wir haben uns alle an dieses „Verantwortungsmodell" gewöhnt, das dem BDSG zugrunde liegt. Datenschützer kümmern sich um die Probleme, die hier anfallen:

- Was darf alles in der elektronischen Personalakte stehen?

- Welche Auswertungen sind im Rahmen von Personinformationssystemen zulässig? Dürfen Betriebsdaten über den Fortgang von Aufträgen oder über das Ein- und Ausschalten des Computers mit den in der Personalabteilung verfügbaren Daten zusammengeführt werden, um so die Leistung des Einzelnen besser beurteilen zu können?

- Wann ist eine offene, wann eine verdeckte Kontrolle durch Videokameras zulässig?

- Darf der Arbeitgeber Bewegungsprofile im Betrieb erstellen, also festhalten, wer zu welchem Zeitpunkt in eine sicherheitsrelevante Abteilung gegangen und sie wieder verlassen hat?

- Dürfen die Inhalte von Telefongesprächen aufgezeichnet und ausgewertet werden? Wie verhält es sich bei E-Mails?

Dies sind nur Beispiele. Sie zeigen, wie groß die Aufgabe ist, wenn man für einen wirksamen Datenschutz in Betrieb und Unternehmen sorgen will. Dabei sind Betriebsräte besonders gefordert, weil sie ein Mitbestimmungsrecht bei allen diesen Fragen haben; da die Kontrollmöglichkeit durch den Arbeitgeber immer im Hintergrund steht, greift in aller Regel § 87 Abs. 1 Nr. 6 BetrVG ein.

Die Öffnung nach außen

Seit etwa zehn bis fünfzehn Jahren gewinnt das Internet wachsende Bedeutung auch für Arbeitnehmer. Einer der ersten, vergleichsweise harmlosen Schritte war, dass Arbeitgeber und Dienststellenleitungen bestimmte Angaben über ihre Beschäftigten ins Netz stellten.[1] Dies konnte der besseren Orientierung der Kunden oder der Bürger, aber auch Werbezwecken dienen. Ob der Arbeitgeber dabei ein Foto einstellen darf, ist ein is heute nicht ganz unwichtiger Streitpunkt.[2] Der Bezug zum Arbeitsverhältnis und zur verantwortlichen Stelle liegt aber immer noch auf der Hand.

Bestimmte Arbeitnehmergruppen sehen sich auf „Plattformen“ einer öffentlichen Beurteilung ihrer Leistungen ausgesetzt. Dies gilt etwa für Lehrer oder Ärzte und andere Freiberufler, deren zufriedene oder unzufriedene Kunden ihre Meinung zum Besten geben. Bislang ist dies keine Massenerscheinung, aber für die Betroffenen kann es eine erhebliche Belastung darstellen, öffentlich als „nicht besonders motiviert“ oder „schlecht vorbereitet“ dargestellt zu werden.[3] Wie kann sich der Betroffene wehren? Den Plattformbetreiber verklagen? Muss der Arbeitgeber auf seine Kosten einen Anwalt zur Verfügung stellen?

Die Benutzung von E-Mails nimmt rapide zu; sie ersetzen oft die früher geführten Telefongespräche. Was mit ihnen geschieht, wenn sie den betrieblichen Computer verlassen haben, bleibt eher unklar. Früher hätte man auf das Telekommunikationsgesetz und auf das Telemediengesetz verwiesen, die für einen umfassenden Schutz des Fernmelde- besser: des Telekommunikationsgeheimnisses sorgen. § 13 Abs. 6 Telemediengesetz gibt sogar das

[1] S. bereits OVG Nordrhein-Westfalen, Beschluss vom 20.1.2000 – 1 A 128/98,PVL – PersR 2000, 456
[2] Überblick über den Diskussionsstand bei Däubler, Internet und Arbeitsrecht, 4. Aufl. 2013, Rn. 369a - 369c
[3] S. etwa den Sachverhalt der Spickmich-Entscheidung BGH, 23.6.2009 – VI ZR 196/08 – NJW 2009, 2888

Recht, im Internet anonym zu bleiben oder sich eines Pseudonyms zu bedienen. Heute gelten diese Vorschriften zwar unverändert weiter. Gleichwohl setzt sich dem Vorwurf der Naivität aus, wer die Möglichkeit illegaler Eingriffe ignoriert, gewissermaßen nach dem Motto: „Also schloss er messerscharf, dass nicht sein kann was nicht sein darf“. Doch auch davon ganz abgesehen: Der deutsche wie der europäische Datenschutz stoßen an Grenzen. Außerhalb Europas sieht die Welt ganz anders aus.

Weit verbreitet sind auch die Recherche im Internet und der E-Commerce. Wie ist das Wetter am Ziel der für morgen geplanten Reise? Wie sieht der Internet-Auftritt einer möglichen neuen Partnerfirma aus? Gibt es bei E-Bay ein günstiges Angebot für einen besseren Schreibtisch, für den der Arbeitgeber nicht allzu viel Geld ausgeben möchte? Was sagt ein „Think Tank“ aus den USA über die Zukunft des Euro? Dieses und vieles mehr „ergoogelt“ man sich; früher musste man sich dafür tagelang mühen oder kam nie ans Ziel. Auf der anderen Seite kann man nicht ausschließen, dass jede Anfrage bei der benutzten Suchmaschine oder bei einem sonstigen Adressaten gespeichert wird. Wer im Netz ein Buch kauft, bekommt die Mitteilung, dass sich „viele“, die dieses Buch gleichfalls erworben haben, auch die drei folgenden Bücher angeschaut hätten. Das funktioniert ersichtlich nicht ohne umfassende Speicherung und Auswertung aller Vorgänge. Geschieht es nur zu so harmlosen Zwecken wie hier, besteht kein Grund zur Aufregung. Doch was geschieht, wenn sich Rückschlüsse auf eine unerwünschte politische Haltung ziehen lassen? Oder wenn ersichtlich wird, an welchen Fragen die Forschungs- und Entwicklungsabteilung eines Unternehmens arbeitet? Wenn nicht nur Menschen, die über eine bessere Werbung entscheiden, aus den Milliarden Daten, die täglich anfallen, die für sie relevanten Informationen herausziehen können, dann haben wir ein Problem. Die Stichworte „Google“ und „NSA“ genügen.

Arbeit wird weiter „nach außen“ verlagert, wenn der Einzelne im Auftrag seines Arbeitgebers soziale Netzwerke nutzt oder in ihnen durch eigene Beiträge präsent ist. Er schreibt beispielsweise dort seine dienstlichen E-Mails und bereichert die Fan-Seite seines Arbeitgebers, indem er die Firmenprodukte mit subtilem oder offenem Lob versieht. Auch der private Account kann für dienstliche Zwecke eingesetzt werden. Mittelbar ist dies sogar dann der Fall, wenn die eigene Person bei LinkedIn oder Xing im „Profil“ angepriesen und zugleich auf die Stellung im Arbeitgeberunternehmen hingewiesen wird.

Bewegliche Arbeitsmittel und bewegliche Arbeitskräfte

Smartphone und Tablet Computer bringen eine neue Qualität. Die mit ihrer Hilfe geleistete Internet-Arbeit ist nicht an bestimmte Tageszeiten und nicht an bestimmte Orte gebunden. Der Arbeitnehmer ist jederzeit erreichbar – im Grunde nur beschränkt durch soziale Konventionen, wonach man andere nicht wegen absoluter Kleinigkeiten nachts um 2 Uhr oder am Sonntag anruft. Je nach Anlass wird sich der Chef aber Ausnahmen genehmigen. Das Arbeitszeitrecht tritt fast ganz in den Hintergrund, da es in der Praxis schwer vorstellbar ist, dass der Angerufene seinem Arbeitgeber erklärt, die in dem Gespräch liegende Extra-Arbeit sei für ihn nicht akzeptabel oder am Sonntag sei er nicht zur Arbeit verpflichtet. Von wo aus der Einzelne ins Internet geht, ist unerheblich; auch im Hotelzimmer oder im Ferienappartement können die notwendigen Dinge erledigt werden. Diese flexible Einsatzmöglichkeit schafft einen zusätzlichen Anreiz, Arbeit aus dem traditionellen Betrieb heraus ins Internet zu verlegen.

Einen noch größeren Schritt hinein in eine neue Arbeitswelt stellt das „Crowdworking“ dar, aus Sicht der Unternehmen auch „Crowdsourcing“ genannt. Kleine Aufgaben wie das Einlesen handschriftlicher Angaben in den Computer werden über das Internet an die Arbeitskräfte vergeben, die bei einer im Prinzip weltweiten Ausschreibung das preiswerteste Angebot gemacht haben. Allerdings können auch komplexe Arbeitsprozesse in kleine, überschaubare Teile zerlegt und diese dann im Internet ausgeschrieben werden. Die Durchschnittseinkommen von Crowdworkern werden auf zwei bis drei US-Dollar pro Stunde geschätzt, gesuchte Spezialistentätigkeiten einmal ausgenommen. Das mag für einen Inder auskömmlich sein, für einen Westeuropäer ist es im wörtlichsten Sinne ein Hungerlohn.[4] Datenschutzrechtlich ist von Bedeutung, dass sich die gesamte Arbeit im Netz abspielt und damit vielfältigen Zugriffen ausgesetzt ist.

Verlagerung in die Cloud

Auch in Zeiten, als das Unternehmen im Prinzip noch eine geschlossene Einheit war, gab es die Auslagerung in Form der Auftragsdatenverarbeitung. Ein Rechenzentrum übernahm die gespeicherten Daten und sorgte für ihre Sicherung, doch blieb die Weisungsbefugnis beim Auftrag gebenden Unternehmen. Nunmehr sucht sich der Auftragnehmer einen oder mehrere

[4] Näher dazu Benner (Hrsg.), Crowdwork – zurück in die Zukunft? Perspektiven digitaler Arbeit, 2014

Unterauftragnehmer, die gerade Kapazität frei haben, die dann ihrerseits wieder die Dienste anderer Unternehmen in Anspruch nehmen. Dies schafft einen Zustand der Unübersichtlichkeit, der mit dem Ausdruck „cloud“ zutreffend umschrieben ist.[5] Die Folge ist, dass weder die verantwortliche Stelle noch der Betroffene weiß, wo im Augenblick seine Daten gespeichert sind und wer faktisch über sie verfügen kann.

Datenschutz als Ausnahmetatbestand

Sobald Arbeitnehmerdaten ins Internet geraten oder dort zur Entstehung kommen, ergeben sich für den Betroffenen mindestens drei gravierende Probleme.

- Es wird unklar, wo seine Daten gespeichert sind und wer dort auf sie zugreifen kann. Was in durchaus legaler Weise ins Internet gestellt wurde, kann von beliebigen Menschen und Organisationen „abgegriffen“ und gespeichert werden. Um wen es sich dabei handelt, lässt sich vom Betroffenen nicht kontrollieren. Sein informationelles Selbstbestimmungsrecht steht auf dem Papier. Er kann nicht mehr beurteilen, wer was wann und bei welcher Gelegenheit über ihn weiß.[6]

- Auch wo ein Datenfluss an sich nachvollziehbar ist, bleibt oft zweifelhaft, welche Rechtsordnung für die Datenverarbeitung maßgebend ist. Wenn beispielsweise Google seine europäischen Aktivitäten von Irland aus betreibt, ist dann irisches Datenschutzrecht anwendbar?[7] Oder muss stattdessen auf das wirkliche Entscheidungszentrum in den USA abgestellt werden?[8] Letzteres hätte zur Folge, dass nach § 1 Abs. 5 BDSG deutsches Recht anwendbar ist, soweit die Erhebung, Verarbeitung oder Nutzung im Inland erfolgt. Auch dann bleiben allerdings Unsicherheiten, wenn die verantwortliche Stelle keinerlei „technische Mittel“ im Inland besitzt und der Einzelne lediglich auf eine Website zugreift, die von einem Server in den USA aus betrieben wird. Auch gibt es Länder, die über keinerlei Datenschutzrecht verfügen. Wie soll man mit einer Datenverarbeitung umgehen, die dort stattfindet?

[5] Näher Däubler, Gläserne Belegschaften? 6. Aufl. 2014, Rn. 507r
[6] So die Formulierung in der Volkszählungsentscheidung des BVerfG (v. 15.12.1983 – 1 BvR 109/83 u. a., BVerfGE 65, 1, 43)
[7] Dafür OVG Schleswig-Holstein 22.4.2013 – 4 MB 11/13, DuD 2013, 463
[8] So etwa KG Berlin, Urteil v. 24.4.2014 – 5 U 42/12, DuD 2014, 417

- Was kann der Betroffene in dem unwahrscheinlichen Fall tun, dass er Kenntnis davon erhält, wer mit seinen Daten Schindluder getrieben hat? Natürlich kann er mit Hilfe eines E-Mails protestieren und Löschung des unerlaubt Erlangten einfordern, doch wie will er das durchsetzen? Soll er einen Prozess in den USA, in China oder in Indien, vielleicht gar in Ghana oder in Neu-Guinea führen? Nicht mal Michael Kohlhaas hätte das versucht. Das „Recht auf Vergessenwerden" ist hier nur ein schwacher Ausgleich. Nach der Rechtsprechung des Europäischen Gerichtshofs[9] kann der Betroffene zwar von einem Suchmaschinenbetreiber wie Google verlangen, dass er nicht mehr auf die illegal erworbene oder nach europäischen Maßstäben zu löschende Information hinweist. Dies erschwert den Zugriff, schließt ihn aber nicht definitiv aus: Andere Wege zu der „Quelle" sind nicht verschlossen.

Was kann man tun? Schon die Probleme zu erkennen, ist keine Selbstverständlichkeit, weshalb es kaum Lösungsvorschläge gibt.[10] Man kann eine internationale Konvention fordern, doch müssten alle Staaten mitwirken, weil einzelne Unternehmen sonst in die „datenschutzfreien Zonen" ausweichen würden. „Möglichst wenig Daten ins Netz!" ist ein guter Grundsatz, der aber schnell an seine Grenzen stößt, wenn im Wesentlichen im Internet gearbeitet wird. Ein eingebautes „Verfallsdatum" bei allen personenbezogenen Daten oder eine konsequente Verschlüsselung würden uns sicher einer Lösung näher bringen, doch liegen auch hier Wunsch und Wirklichkeit noch weit auseinander.

[9] EuGH 13.5.2014 – C-131/12, CuA 6/2014 S. 30
[10] Weiterführend jedoch Schaar, Überwachung total. Wie wir in Zukunft unsere Daten schützen, 2014