Compliance und Schutz der Privatsphäre im Unternehmen

Von Dr. **Alexander Dix**, LL.M., Berlin*

Die Gegenüberstellung der Begriffe „Compliance“ und „Schutz der Privatsphäre“ erweckt den Eindruck, es handele sich dabei um ein Gegensatzpaar. Dieser Eindruck geht zurück auf die in der Öffentlichkeit stark diskutierten Vorfälle bei großen deutschen Unternehmen wie der Deutschen Telekom AG, der Deutschen Bahn AG und bei Airbus, um nur einige zu nennen.

Zur Erinnerung: Bei der Deutschen Telekom wurden systematisch Verbindungsdaten von Aufsichtsratsmitgliedern (in erster Linie von Arbeitnehmervertretern) analysiert, um herauszufinden, wer Informationen aus Aufsichtsratssitzungen an die Medien gegeben haben könnte (eine Straftat nach dem Aktiengesetz). Die Staatsanwaltschaft ermittelte zunächst gegen ehemalige Top-Manager der Telekom wegen Verletzung des Fernmeldegeheimnisses, stellte diese Ermittlungen später aber ein. Der ehemalige Leiter Konzernsicherheit wurde dagegen vom Landgericht Bonn zu einer Freiheitsstrafe von dreieinhalb Jahren verurteilt.

Auch bei der Deutschen Bahn AG wurde aus dem gleichen Grund systematisch und heimlich der E-Mail-Verkehr sämtlicher Bahn-Mitarbeiter daraufhin überwacht, ob diese Kontakt zu bahnkritischen Journalisten oder Mitarbeitern von Bundestagsabgeordneten aufgenommen hatten. Auch hier ermittelt die Staatsanwaltschaft. Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich hat ein Bußgeld gegen die Deutsche Bahn AG in Höhe von 1,1 Mio. Euro verhängt,[1] weil das Unternehmen außerdem über Jahre nahezu seine gesamte Belegschaft einem systematischen heimlichen Screening unterzogen hat, um herauszufinden, ob Mitarbeiter insbesondere bei Beschaffungen Vorteile angenommen oder gewährt haben. In die heimliche Überprüfung einbezogen wurden auch Ehepartner von Führungskräften. Außerdem wurden Mitarbeiterdaten über Jahre hinweg an ein privates Dienstleistungsunternehmen weitergegeben, das mit spezieller Software die Personal- und Kontodaten von Bahnbeschäftigen analysiert und mit Lieferantendaten abgeglichen hat. Die Deutsche Bahn, deren früherer Vorstandsvorsitzender im Zuge der Datenaffäre zurückgetreten ist, hat das Bußgeld mittlerweile gezahlt. Schließlich hat auch Airbus die Kontodaten von Mitarbeitern in ähnlicher Weise auf korruptive Zusammenhänge hin untersucht, was der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit als rechtswidrig beanstandet hat.

Was heißt eigentlich „Compliance“? Der Begriff hat sich seit den Finanzskandalen des Jahres 2001 in den USA (ENRON, WorldCom u.a.) weltweit eingebürgert, nachdem der US-Kongress in einer Reihe von Gesetzen (insbesondere dem Sarbanes-Oxley Act – SOX) insbesondere die Bilanz-Vorschriften verschärft hat. Entsprechende Gesetze wurden inzwischen weltweit – auch in Deutschland – von den Parlamenten verabschiedet. Auch untergesetzliche Regelungen wie der deutsche Corporate Governance Code sind in diesem Zusammenhang zu nennen. Zugleich wird der Kampf gegen die Korruption weltweit intensiviert, was bei zwei deutschen Unternehmen, die an der New Yorker Börse notiert waren (Daimler und Siemens), zu Ermittlungen der amerikanischen Börsenaufsicht Securities Exchange Commission und des Department of Justice geführt hat, die teilweise noch andauern.

Der Begriff „Compliance“ hat also Konjunktur. Er steht für „Rechts- oder Regeltreue“ und schließt die Überwachung der Rechtsbefolgung mit ein. Während anfangs das Bilanzrecht und Regeln gegen das Insider-Trading im Vordergrund standen, befassen sich Compliance-Abteilungen oder Compliance-Beauftragte in Unternehmen (soweit vorhanden) mittlerweile insbesondere mit der Korruptionsbekämpfung, aber auch mit der Aufdeckung des Verrats von Betriebs- und Geschäftsgeheimnissen. Vielfach wird „Compliance“ aber immer noch eindimensional missverstanden und nur bezogen auf bestimmte, als besonders wichtig angesehene Normbereiche.

Ein Beispiel: Im Sommer 2007 machte die New York Times die Tatsache öffentlich, dass das US-Schatzministerium regelmäßigen heimlichen Zugriff auf einen in den USA gelegenen Server des belgischen Unternehmens SWIFT hat, über den der gesamte weltweite Zahlungsverkehr elektronisch abgewickelt wird (auch soweit er keinerlei Bezug zu den Vereinigten Staaten hat). Zweck dieses Zugriffs sollte schon vor dem 11. September 2001 die Ermittlung von Finanzquellen terroristischer Organisationen sein. Nach amerikanischem Recht war dieser Zugriff rechtmäßig, allerdings wurde in Europa sowohl von Banken, vom Europäischen Parlament als auch von Datenschutzbehörden Kritik an dieser Praxis geübt, weil es insbesondere an einer unabhängigen Kontrolle darüber fehlt, ob die gewonnenen Daten tatsächlich nur zur Bekämpfung des Terrorismus verwendet werden. Dies hat mittlerweile dazu geführt, dass das Unternehmen SWIFT gegenwärtig seine internationale Infrastruktur der Datenverarbeitung in der Weise ändert, dass Daten über Finanztransaktionen mit ausschließlich europäischem Bezug nur in Europa (Schweiz) verarbeitet werden. Im Juni 2010 wurde ein Abkommen zwischen der Europäischen Union und der US-Regierung geschlossen, das den US-Behörden auch einen Zugriff auf in Europa belegene Daten ermöglicht. Dem hat das Europäische Parlament, das ein entsprechendes Abkommen zunächst abgelehnt hatte, u.a. deshalb zugestimmt, weil die Datenverarbeitung in den USA durch EUROPOL effektiv kontrolliert werde – eine Annahme, die nach den Erkenntnissen der Gemeinsamen Kontrollbehörde für EUROPOL nicht zutrifft[2]. Ich erwähne dieses Beispiel nur

* Der *Autor* ist Berliner Beauftragter für Datenschutz und Informationsfreiheit – Überarbeitete Fassung des Vortrages vom 22.10.2009.

[1] Es handelt sich um das bisher höchste Bußgeld, das eine einzelne deutsche Datenschutzaufsichtsbehörde seit Inkrafttreten des Bundesdatenschutzgesetzes 1978 verhängt hat.

[2] Vgl. dazu die Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder v. 17.3.2011 „Gravierende Defizite bei der Umsetzung des SWIFT-Abkommens“,

deshalb, weil ein Blick auf die Website von SWIFT im Herbst 2007 (kurz nachdem der Zugriff des US-Schatzministeriums bekannt geworden war) deutlich machte, welches eindimensionale Verständnis von „Compliance" in diesem international agierenden Unternehmen vorherrschte. Dabei handelte es sich mit Sicherheit nicht um einen Einzelfall. Das belgische Unternehmen SWIFT erwähnt auf seiner Homepage in einer eigenen Rubrik unter der Überschrift „Compliance" ausschließlich US-amerikanische Rechtsvorschriften (insbesondere zum Bilanzrecht, z.B. SOX). Europäische Regelungen etwa zum Datenschutz wurden nicht erwähnt.

Wenn man den Begriff „Compliance" wörtlich nimmt, muss er dagegen auf die Gesamtheit der für ein Unternehmen geltenden Rechtsregeln (einschließlich möglicher Verhaltenskodizes zur Good Corporate Governance) bezogen werden. Compliance ist stets mehrdimensional zu verstehen. Anders formuliert: Bei der Durchsetzung bestimmter Rechtsnormen dürfen nicht andere, gleichwertige Normen außer Acht gelassen werden.

Im Staat wie in Unternehmen wird Regelverstößen präventiv und repressiv begegnet. Dabei zeichnet sich im staatlichen Bereich seit längerem eine zunehmende Tendenz zu präventiven Maßnahmen ab, die Rechtsverstöße möglichst frühzeitig bereits im Vorfeld eines konkreten Verdachts unterbinden sollen. Das erscheint zwar zunächst plausibel, birgt aber die Gefahr, dass Eingriffe in Grundrechte von immer geringeren bzw. immer diffuseren Voraussetzungen abhängig gemacht werden, weil das Ziel der Prävention fast alles zu rechtfertigen scheint. Dabei wird vergessen, dass in einem Rechtsstaat personenbezogene Überwachungsmaßnahmen (Datenerhebungen) in der Regel nicht der bloßen Gewinnung von Verdachtsmomenten dienen dürfen, sondern sie voraussetzen. Wie es der ehemalige Vizepräsident des Bundesverfassungsgerichts, *Winfried Hassemer*, einmal sinngemäß formuliert hat: „Ich habe ein Recht darauf, vom Staat in Ruhe gelassen zu werden, solange ich mich regelkonform verhalte." Je größer die Streubreite staatlicher Überwachungsmaßnahmen wird, je mehr Unverdächtige ins Visier der Sicherheitsbehörden geraten, desto größer wird die Intensität der Grundrechtseingriffe.

Die Tendenz zu verstärkter Prävention durch verdachtsunabhängige Kontrollen lässt sich auch in Unternehmen beobachten. Das mag auch daran liegen, dass zumindest Großunternehmen zunehmend auch leitende Mitarbeiter beschäftigen, die früher bei staatlichen Sicherheitsbehörden tätig waren. Als Beispiele seien nur der ehemalige Chief Compliance Officer der Deutschen Bahn AG (früher Staatsanwalt mit dem Spezialgebiet Bekämpfung der Wirtschaftskriminalität) und der jetzige Leiter der Konzernsicherheit desselben Unternehmens (ehemaliger Polizeivizepräsident in Berlin) genannt. Auch frühere Mitarbeiter von Nachrichtendiensten sind von Unternehmen bereits mit vergleichbaren Aufgaben betraut worden.

http://www.datenschutz-berlin.de/content/deutschland/konferenz.

Um jedem Missverständnis vorzubeugen: Die Bekämpfung von Korruption, Wirtschaftsspionage und Geheimnisverrat in Unternehmen sind legitime und wichtige Ziele, die jeder Arbeitgeber verfolgen muss. Aber: Diese Ziele sind nur mit recht- und verhältnismäßigen Mitteln zu verfolgen und zu erreichen. Das Bundesarbeitsgericht hat in seiner neueren Rechtsprechung[3] unter ausdrücklicher Bezugnahme auf die Rechtsprechung des Bundesverfassungsgerichts betont, dass Eingriffe in das allgemeine Persönlichkeitsrecht der Arbeitnehmer durch schutzwürdige Belange anderer Grundrechtsträger gerechtfertigt sein und dabei insbesondere dem Grundsatz der Verhältnismäßigkeit genügen müssen. Im engeren Sinn verhältnismäßig sind nur solche Eingriffe, die nach einer konkreten Abwägung zwischen der Intensität des Eingriffs und des Gewichts der ihn rechtfertigenden Gründe angemessen sind. Dabei genießen weder das allgemeine Persönlichkeitsrecht der Arbeitnehmer noch die konkurrierenden Grundrechte des Arbeitgebers oder Dritter von vornherein Vorrang. Das Bundesarbeitsgericht zieht für die Beurteilung der Schwere des Eingriffs mehrere Gesichtspunkte heran, darunter insbesondere die Frage, wie viele Personen wie intensiv den Beeinträchtigungen durch Überwachung ausgesetzt sind, ob sie als Person anonym bleiben und welche Nachteile den Grundrechtsträgern aus der Überwachungsmaßnahme drohen oder von ihnen nicht ohne Grund befürchtet werden. Von erheblicher Bedeutung ist nach den Worten des Gerichts, „ob der Betroffene einen ihm zurechenbaren Anlass für die Datenerhebung geschaffen hat – etwa durch eine Rechtsverletzung – oder ob diese anlasslos erfolgt. Die Heimlichkeit einer in Grundrechte eingreifenden Ermittlungsmaßnahme erhöht das Gewicht der Freiheitsbeeinträchtigung. Den Betroffenen kann hierdurch vorheriger Rechtsschutz faktisch verwehrt und nachträglicher Rechtsschutz erschwert werden."[4] Im konkreten Fall erklärte das BAG deshalb die Regelung in einer Betriebsvereinbarung für nichtig, in der die Erstreckung der Videoüberwachung auf die gesamte Belegschaft eines Briefverteilzentrums für den Fall vorgesehen war, dass durch eine anlassbezogen räumlich beschränkte Überwachung kein Täter (z.B. Diebstahl einer Postsendung) überführt werden konnte. Dadurch wäre ein weit größerer Kreis unverdächtiger Arbeitnehmer in die Überwachung einbezogen worden, die hierzu durch ihr Verhalten keinen Anlass gegeben hätten.

Diese Rechtsprechung ruft etwas in Erinnerung, was eigentlich selbstverständlich sein sollte: Ein undifferenzierte, pauschale und anlasslose Überwachung ganzer Belegschaften ist durch nichts zu rechtfertigen. Das gilt sowohl für den Einsatz von Kameratechnik am Arbeitsplatz, die Überwachung der Internet-Nutzung wie auch für Datenabgleiche von Mitarbeiterdaten. Wohlgemerkt: Nicht die Tatsache, dass die Deutsche Bahn und Airbus die Daten von bestimmten Mitar-

[3] BAG, Beschl. v. 26.8.2008 – 1 ABR 16/07 (Videoüberwachung im Briefverteilzentrum).

[4] BAG, Beschl. v. 26.8.2008 – 1 ABR 16/07, Rn. 21, unter Verweis auf das Urteil des BVerfG (Urt. v. 11.3.2008 – 1 BvR 2074/05, 1 BvR 1254/07 = BVerfGE 120, 378 [402 f.] – Kfz-Kennzeichen-Scanning).

beitern mit denen von Lieferanten oder Vertragspartnern abgeglichen haben, ist rechtlich zu beanstanden, wohl aber die Tatsache, dass alle Mitarbeiter oder zumindest große Teile der Unternehmensbelegschaft einem solchen Abgleich unterworfen wurden.

Zuweilen halten die Unternehmen dem entgegen, sie seien durch das Strafgesetzbuch oder gar durch die Verfassung daran gehindert, Differenzierungen vorzunehmen. Beide Einwände sind nicht tragfähig. Zwar folgen aus dem Straftatbestand der Untreue (§ 266 StGB) eine Reihe von Pflichten für Unternehmensvorstände und auch Compliance-Beauftragte, die der Bundesgerichtshof gerade erst am Beispiel der Berliner Stadtreinigung[5] konkretisiert und verschärft hat. Die Vorstellung aber, der Untreue-Tatbestand verpflichte die Unternehmensleitung dazu, sämtliche Mitarbeiter regelmäßig präventiv einem pauschalen personenbezogenen Screening zu unterwerfen, um Schaden vom Unternehmen abzuwenden, ist abwegig. Ebenso wenig verfängt der Einwand, bei einer Beschränkung solcher Maßnahmen auf Beschäftigte in bestimmten, korruptionsanfälligen Unternehmensbereichen würden diese in verfassungswidriger Weise diskriminiert. Denn es ist gerade umgekehrt ein Gebot der Verfassung, informationelle Eingriffe in die Rechte der Arbeitnehmer an sachlichen Differenzierungsgründen zu orientieren.

Es bleibt also festzuhalten: Das Bundesdatenschutzgesetz lässt eine pauschale, anlasslose Überwachung von Arbeitnehmern zur Verdachtsgewinnung nicht zu.[6] Das gilt erst recht, wenn unternehmensfremde Dienstleister für solche Aufgaben eingeschaltet werden, die Überwachung also gewissermaßen „outgesourct" wird. Auch diese Praxis ist offenbar weit verbreitet, sei es, dass Personal- und Lieferantendaten in großem Umfang an spezialisierte Datenverarbeitungsunternehmen weitergegeben werden, die dann mit entsprechenden Software-Tools die Datenbestände durchforsten und Zusammenhänge aufdecken sollen. Schließlich werden Detekteien und Auskunfteien eingeschaltet, die ohne konkreten Anlass verdeckte Ermittlungen über leitende Angestellte und ihre Familienangehörigen anstellen sollen, um Hinweise darauf zu erhalten, ob die Pflicht zur Offenlegung von Beteiligungen an anderen Unternehmen verletzt wurde. Setzen solche Auftragnehmer – wie bei der Deutschen Telekom und der Deutschen Bahn – rechtswidrige Ermittlungsmethoden ein, so suchen die Auftraggeber sich mit dem Argument aus der Affäre zu ziehen, sie seien davon ausgegangen, dass ihre Auftragnehmer rechtskonform agieren würden.[7]

Es ist deshalb zu begrüßen, dass der neue Vorstand der Deutschen Bahn AG nicht nur das verhängte Bußgeld für die festgestellten Rechtsverstöße gezahlt, sondern darüber hinaus auch weitreichende Maßnahmen ergriffen hat, die darauf schließen lassen, dass eine grundlegende Änderung der Unternehmenskultur und -ethik beabsichtigt ist. Der Bahnvorstand hat erklärt, er wolle künftig jedenfalls im Bereich des Arbeitnehmerdatenschutzes Maßstäbe setzen und in seiner Praxis sogar über das vom Gesetz geforderte Mindestniveau des Datenschutzes noch hinausgehen. Wenn einer der größten Arbeitgeber in Deutschland ein signifikantes Bußgeld nicht nur bezahlt, um aus den negativen Schlagzeilen herauszukommen, sondern wenn damit eine Änderung der Unternehmensethik verbunden ist, dann kann auch das Ordnungswidrigkeitenrecht generell zu einem verbesserten Schutz der Privatsphäre von Arbeitnehmern und damit auch zu einer verbesserten Compliance im Sinne von „Rechtstreue" beitragen.

[5] BGH NJW 2009, 3173 m. Anm. *Stoffers*.

[6] So jetzt explizit der neue § 32 Abs. 1 S. 2 BDSG für die Verfolgung von Straftaten. Die Vorschrift trägt allerdings selbst nicht zur Klärung der Frage bei, inwieweit der Arbeitgeber zu präventiven Zwecken Beschäftigtendaten erheben darf. Auch deshalb hat die neue Bundesregierung angekündigt, den Beschäftigtendatenschutz durch eine neuerliche Änderung des Bundesdatenschutzgesetzes präzisieren zu wollen. Vorzugswürdig wäre dagegen – nicht nur aus systematischen Gründen – ein gesondertes Gesetz zum Beschäftigtendatenschutz, das seit Jahren überfällig ist.

[7] Dieses Argumentationsmuster verwenden offenbar auch bestimmte Medienunternehmen beim Ausspähen des Privatlebens von Politikern (z.B. in den Fällen Lafontaine und Müntefering), vgl. *Prantl*, Pontius Pilatus als Chefredakteur, Süddeutsche Zeitung v. 27./28.2.2010, S. 4.