

Rechtsanwalt Wolf Klimpe-Auerbach  
Richter am Arbeitsgericht a. D.  
Im Stahlbühl 3  
74074 Heilbronn  
mail@klimpe-auerbach.de

## **Aufriss zum Fachforum 1, Compliance ohne Arbeitnehmerüberwachung**

### **A. Compliance als Managementpflicht?**

Der Begriff „Compliance“ stammt aus dem us-amerikanischen Handels- und Wirtschafts-(straf)recht und gewinnt zunehmend auch bei uns in Deutschland an Bedeutung. Er wird allerdings wie viele andere Anglizismen auch zur Beschreibung unterschiedlicher Sachverhalte eingesetzt, verliert dadurch deutlich an Konturen und gerät ins Beliebig.

Wertungsfrei übersetzt, dabei den rechtlichen und gesellschaftlichen Zusammenhang, in dem er in der juristischen Diskussion aber steht, auslassend heißt compliance „Einhaltung, Befolgung, Einverständnis“. Gebrauch wird der Begriff allgemein im Zusammenhang mit dem Einhalten oder dem Abweichen von staatlichen Regelungen. Wenn es sich dabei um Gesetze handelt, kann man auch von „Gesetzestreue“ sprechen.

„Compliance“ kann aber auch mit der Schaffung eines Arbeitsumfeldes umschrieben werden, in dem Mitarbeiter nicht versucht sein müssen, für das Unternehmen Straftaten zu begehen.<sup>1</sup>

In der Beratungspraxis wird compliance als Verpflichtung der Unternehmen beschrieben, rechtlich und organisatorisch umfassend sicher zu stellen, dass alle für sie maßgeblichen Gesetze und sonstigen sie zu einem bestimmten Verhalten verpflichtenden Normen beachtet werden.

Dazu gehören der öffentlich-rechtliche und (wirtschafts-)strafrechtliche Normenbestand, Regeln der Börsenaufsicht, der Banken- und Finanzdienstleistungsaufsicht, der Arbeitsschutzbehörden und sonstiger Aufsichtsbehörden.

Art. 406 Sarbanes-Oxley-Act (SOX) verpflichtet Unternehmen, die an einer US-amerikanischen Börse notiert oder die sonst noch zur Berichterstattung an die US-amerikanische Börsenaufsicht verpflichtet sind, zur Einführung von Compliance Richtlinien. Zusätzlich wurden angesichts anhaltender Skandale im Unternehmens und Bankenbereich die gesetzlichen Anforderungen für börsennotierte Unternehmen weiter verschärft, was zu erheblichen Strafzahlungen an die amerikanische Börsenaufsicht zur Folge hatte. Neben den Bestimmungen des SOX sind das Börsenregularien wie das „Listed Company Manual der New York Stock Exchange (NYSE) und der Foreign Corrupt Practice Act (FCPA). Verstöße gegen den FCPA führen zur Verhängung von Geld- und Haftstrafen und zur Sperre der Teilnahmeberechtigung an Wertpapiergeschäften in den USA.

---

<sup>1</sup> Göpfert, Landauer „Arbeitsstrafrecht“ und die Bedeutung von Compliance-Systemen: Straftaten „für“ das Unternehmen, NZA-Beil. 2011, 16

In Deutschland schreibt der Corporate Governance Kodex vor, dass der Vorstand einer börsennotierten Aktiengesellschaft für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen hat und dass er auf deren Beachtung durch die Konzernunternehmen hinwirkt.

Ziff. 4.1.3 des DCGK beschreibt erstmals 2007 Compliance und zwar wie folgt:

***„Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance).“***

Mit Abgabe der Entsprechenserklärung nach § 161 Aktiengesetz (AktG) ist der Vorstand einer AG zur Compliance verpflichtet und wird dafür in Haftung genommen. Auch der Aufsichtsrat ist angehalten, einen Prüfungsausschuss einzurichten, der sich insbesondere mit Fragen der Compliance beschäftigen soll (Ziff. 5.3.2 Kodex).<sup>2</sup>

Der Vorstand einer Aktiengesellschaft ist nach § 91 Abs. 2 AktG verpflichtet, ein Überwachungssystem zur Früherkennung von Risiken einzurichten, die den Fortbestand der Gesellschaft gefährden, § 93 Abs. 2 AktG sieht für Verstöße dagegen vor, dass der Vorstand in Haftung genommen wird.<sup>3</sup>

Führt man sich vor Augen, dass allein die Firma Siemens 2007 und 2008 wegen Verstoßes gegen den FCPA (systematische Bestechung, bzw. wegen mangelhafter Compliancestrukturen, die die Bildung schwarzer Kassen, und Korruption ermöglicht haben) an die Securities Exchange Commission 350mio US-Dollar und an das US Department of Justice 450 mio US-Dollar zahlen musste, an die Deutschen Behörden Bußgelder wegen Verstoßes gegen § 130 OWiG (Verletzung der Aufsichtspflichten des Vorstandes) in Höhe von € 395 mio und € 201 mio wegen Untreuedelikten im Zusammenhang mit der Bildung schwarzer Kassen<sup>4</sup>, liegen existenzgefährdende Risiken im Sinne des § 91 AktG und damit der Zwang zum Aufbau einer Compliance Struktur im Unternehmen auf der Hand. Das gilt nicht nur für Siemens! Allein die Bußgelder für Kartellverstöße in Deutschland und Europa übersteigen zweistellige Milliardensummen.

Im Rundschreiben 4/2010 (WA) des BAFIN - Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach §§ 31 ff. WpHG für Wertpapierdienstleistungsunternehmen (MaComp) ist unter AT 6 u. a. geregelt: Wertpapierdienstleistungsunternehmen nach § 33 Abs. 1 WpHG haben angemessene Grundsätze aufzustellen, Mittel vorzuhalten und Verfahren einzurichten, die darauf ausgerichtet sind, sicherzustellen, dass das Wertpapierdienstleistungsunternehmen selbst und seine Mitarbeiter den Verpflichtungen des WpHG nachkommen. Dies erfordert insbesondere die Einrichtung einer dauerhaften und wirksamen sowie prozessbegleitend als auch präventiv tätigen Compliance-Funktion, die ihre Aufgaben unabhängig wahrnehmen kann.<sup>5</sup>

---

<sup>2</sup> Mengel Compliance und Arbeitsrecht, 2 ff.; Maschmann AuA 2009, 72

<sup>3</sup> Mengel a. a. O., 4

<sup>4</sup> Pressemitteilungen der Staatsanwaltschaft München I und der SEC jeweils v. 15.12.2008; Mengel aa.aO. FN 3 m. w. Fallbeispielen

<sup>5</sup> Rundschreiben 4/2010 (WA) - Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach §§ 31 ff. WpHG für Wertpapierdienstleistungsunternehmen (MaComp); Geschäftszeichen:WA 31-Wp 2002-2009/0010 (Stand: 14. Juni 2011)

Außerhalb der Welt der Finanzdienstleister und börsennotierten oder der amerikanischen Börsenaufsicht unterliegenden Aktiengesellschaften lassen sich verstreut gesetzliche Bestimmungen zur Sicherung der Einhaltung des gesetzlichen Normenbestands finden, die sich als rechtliche Verpflichtung von Compliance-Maßnahmen interpretieren lassen.

So verpflichtet etwa § 12 AGG die Arbeitgeber, die erforderlichen Maßnahmen zum Schutze vor nach § 1 AGG verbotenen Benachteiligungen zu treffen, § 3 ArbSchG zu erforderlichen Maßnahmen des Arbeitsschutzes.

Nach § 6 AsiG müssen die Arbeitgeber Fachkräfte für Arbeitssicherheit bestellen.

Im Umweltschutzrecht wäre auf § 52 a Abs. 2 BimmschG hinzuweisen.

§ 4 f BDSG schreibt die Bestellung eines Datenschutzbeauftragten vor.

Eine in der Öffentlichkeit weithin unbekannte Vorschrift ist § 130 OWiG. Danach handelt ordnungswidrig und macht sich bußgeldpflichtig, wer als Betriebsinhaber die Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um Straftaten oder Ordnungswidrigkeiten im Betrieb zu verhindern. Diese Vorschrift gilt für nicht nur für börsennotierte Konzernunternehmen, sondern auch für Kleinbetriebe. Zwar ist in § 130 OWiG von compliance, keine Wort zu finden, sehr wohl aber davon, dass die Unternehmensverantwortlichen ihr Aufsichtspersonal sorgfältig auswählen, anleiten und überwachen müssen.<sup>6</sup> § 130 Abs. 1 OWiG i.V.m. § 30 OWiG droht Geldbußen bis zu EUR 1 Mio. an.

In diesem Zusammenhang sind auch steuerrechtliche Sanktionen bei compliance Versagen zu erwähnen. So droht § 370 AO Haft, Geldstrafe, Einziehung und Verfall an, nach § 4 Abs. 5 Nr. 10 EstG können Aufwendungen für Korruption nicht als Betriebsausgabe geltend gemacht werden.

Auf den Punkt gebracht bedeutet „Compliance“ somit die eigentlich selbstverständliche Verpflichtung der Unternehmen, die für jedermann gültigen Gesetze anzuerkennen und deren Bestimmungen einzuhalten. Dadurch sollen Haftungsrisiken des Unternehmens und seiner Mitarbeiter vermieden werden.

Über die Sicherstellung eines gesetzeskonformen Verhaltens hinaus wird Compliance noch gleichgesetzt mit dem Begriff „best practice“.

Für unser Forum von Bedeutung ist schließlich, dass mit compliance auch auf das (ethisch) korrekte Verhalten des Unternehmens und seiner Beschäftigten abgestellt wird. Dieses Ziel soll mittels Einführung von Ethik- und Verhaltensregeln der Beschäftigten (Codes of Conduct) erreicht werden.

Zwar sind Unternehmen noch nicht verpflichtet, komplexe und in sich geschlossene Compliance Systeme einzuführen. Wenn sie allerdings ihre Haftungsrisiken minimieren wollen, kann man ihnen dazu aber nur raten. Denn auch ohne Einrichtungszwang müssen die Unternehmen „die Einhaltung der für sie geltenden Gesetze mit öffentlich-rechtlichem bzw.

---

<sup>6</sup> Maschmann, AuA 2009, 72

strafrechtlichen Charakter sicherstellen, gesellschaftsrechtlich bestehen für die Unternehmensleitungen auch Verpflichtungen zur Einführung geeigneter Organisations- und Überwachungssystem zur Einhaltung der zwingenden Gesetze“.<sup>7</sup>

Zu welchen Maßnahmen sind denn Unternehmen gegenwärtig berechtigt und verpflichtet, wenn sie compliant, also gesetzestreu handeln und strafrechtliche sowie haftungsrechtliche Sanktionen vermeiden wollen?

Die korrekte juristische Antwort lautet: Das kommt darauf an.

Die konkrete Ausgestaltung einer akzeptablen Compliance-Organisation hängt von den Besonderheiten des jeweiligen Unternehmens, dem Geschäftsgegenstand und den damit verbundenen erhöhten Risiken ab.<sup>8</sup> Branchenübergreifend gehört dazu insbesondere

- die Bestimmung der Risiken des Unternehmens
- Beschreibung der Maßnahmen zur Vorbeugung
- Aufzählung der Maßnahmen zur Kontrolle und Aufklärung
- Darstellung der Maßnahmen zur Ahndung
- Evaluation des Vorgehens und fortlaufende Verbesserung der Compliance-Organisation.

In der Beratungspraxis wird demnach allgemein zur Wahrung der Gesetzestreue die folgende Abfolge empfohlen:

- „prevent“ : „Prevent“- Maßnahmen sollen Gesetzesverstöße schon im Ansatz zu verhindern,
- „detect“: „detect“-Aktionen sollen begangenes Unrecht aufdecken,
- „react“ : „react“-Handlungen haben für angemessene Sanktionen zu sorgen.<sup>9</sup>

Das alles muss in eine von den übrigen Sektionen des Unternehmens abgegrenzte eigenständige Abteilung eingebaut sein mit einem Compliance-Beauftragten/Verantwortlichen.

Die rechtlichen Anforderungen an die Errichtung und Erhaltung eines wirksamen Compliance-Systems laufen auf einen für alle Unternehmen für alle Mindeststandard hinaus:

„Es darf keine Einfallstore für (systematische) Regelverstöße im und aus dem Unternehmen heraus geben.“<sup>10</sup>

Rechtsverstöße, insbesondere von Straftaten, die aus dem Unternehmen heraus begangen werden und die zu erheblichen Nachteilen durch Eintritt von Haftungsrisiken oder Ansehensverlust führen können, sind zu verhindern.

Dabei sind nur solche Maßnahmen angebracht, die geeignet sind, unternehmens- bzw. betriebsbezogene Verstöße mit hoher Wahrscheinlichkeit zu unterbinden. Stehen mehrere

---

<sup>7</sup> Mengel a.a.O., 8

<sup>8</sup> Moosmayer, Compliance, Praxisleitfaden für Unternehmen, 2010 (da Moosmayer die Compliance Organisation von Siemens nach Aufkommen des auf Korruption und der Existenz schwarzer Kassen basierenden „Siemenssystems“ geleitet hat, ist das Werk stark „siemensorientiert“);

<sup>9</sup> Maschmann a. a. O.,

<sup>10</sup> Dann/Mengel, NJW 2010, 3265

gleichgeeignete Möglichkeiten zur Verfügung, ist auf das mildeste Mittel zurückzugreifen (Verhältnismäßigkeitsgrundsatz). Die Maßnahmen müssen objektiv zumutbar sein. Ziel kann weder eine Aufsicht um der Aufsicht willen noch die Verhinderung von Pflichtverletzungen um jeden Preis sein. Andererseits darf die Aufsicht nicht erst dann einsetzen, wenn bereits Missstände zutage getreten sind. Unzumutbar sind demnach Anforderungen, deren praktische Umsetzung lebensfremd ist, mit unverhältnismäßig hohen Kosten verbunden sind, die den Betriebsfrieden unzumutbar stören oder die von den Betriebsangehörigen als schikanös oder entwürdigend empfunden werden.

In der Hitze der Auseinandersetzungen um das Verhindern von Regelverstößen aus dem Unternehmen heraus wird oft übersehen, dass das **Compliancekonzept im Unternehmen selbst „compliant“** sein muss.

Das heisst. Verhindern, Aufdecken und Ahnden von Rechtsverstößen darf nicht mittels Verletzung der Persönlichkeitsrechte der Beschäftigten erfolgen. Verstöße müssen zur Schadenersatz- und Schmerzensgeldpflicht des Unternehmens führen, zudem sind sie strafbar, etwa wenn

- heimlich Gespräche aufgezeichnet werden, § 201 StGB,
- private E-Mails abgefischt werden, § 206 StGB, oder
- gegen den Datenschutzbestimmungen verstoßen wird, § 44 BDSG.<sup>11</sup>

Zudem sind Beweise, die rechtswidrig gewonnen worden sind, in einem späteren Gerichtsverfahren nicht verwertbar.<sup>12</sup>

Folgende compliance relevanten Regelungen sind arbeitsrechtlich von Bedeutung:

- Verschwiegenheitspflicht
- Nebentätigkeits- und Wettbewerbsregelungen
- Vermeidung von Interessenkonflikten
- Verbot der Annahme von Schmiergeldern ohne Rücksicht auf die Strafbarkeit
- Aufklärungspflichten
- Pflicht zur (internen) Anzeige (whistleblowing) bei drohendem Personenschaden oder schwerem Sachschaden
- Schadensabwendungspflicht im eigenen Arbeitsbereich und im Rahmen der persönlichen Möglichkeiten
- Schutzpflichten für überlassenen Besitz des Unternehmers
- Pflicht zu ethisch korrektem Verhalten
- Pflicht zur Einhaltung der betrieblichen Ordnung (Einfallstor zum einseitigen Erlass weitreichender Regelungen in betriebsratslosen Unternehmen (Würth!) und Betrieben (Schlecker!))

Einseitig durchsetzbar sind Regelungen, die Art und Weise des Erbringens der Arbeitsleistungen umfassen. Dabei handelt es sich um Maßnahmen oder Anordnungen, mit denen der Arbeitgeber die Arbeitspflicht unmittelbar konkretisiert und abfordert. Dieser Bereich unterliegt dem Weisungsrecht des Arbeitgebers nach § 106 GewO und ist im Kernbereich noch nicht einmal mitbestimmungspflichtig. Die Weisungen müssen sich aber im Rahmen billigen Ermessens bewegen, § 315 BGB. Das ist nur dann der Fall, wenn der Arbeitgeber die wesentlichen Umstände des Falls abgewogen und die beiderseitigen Interessen berücksichtigt hat. In diesem Rahmen sind wegen ihrer mittelbaren Drittwirkung die Grundrechte der Arbeitnehmer besonders zu berücksichtigen.

---

<sup>11</sup> Maschmann, a.a.O

<sup>12</sup> BAG vom 29.10.1997 – 5 AZR 508/96 –, NZA 1998, S. 307.

Begrenzt wird das einseitige Bestimmungsrecht durch die Grundrechte der Arbeitnehmer und dem Umstand, dass außerdienstliches Verhalten grundsätzlich nicht dem Weisungsrecht des Arbeitgebers unterliegt.

Complianceregeln und Verhaltenskodices können auch durch einzelvertragliche Vereinbarungen verbindlich eingeführt werden. Das ist dann notwendig, wenn die eigentlichen Vertragspflichten erweitert werden sollen. Da sich Ethikregeln nicht auf die Arbeitsleistung an sich beziehen, sind sie grundsätzlich vom Weisungsrecht nicht erfasst.

Sind Complianceregeln standardisiert, unterliegen sie der allgemeinen Inhaltskontrolle der §§ 305 ff. BGB. Nach § 307 BGB dürfen solche Regeln die Arbeitnehmer nicht unangemessen benachteiligen, insbesondere dürfen sie nicht inhaltlich unangemessen und/oder intransparent sein. Im Rahmen des § 307 Abs. 1 BGB sind die Grundrechte der Arbeitsvertragsparteien gegeneinander abzuwägen. Der Rechtfertigungsdruck für den Arbeitgeber nimmt im Verhältnis zur Entfernung von der eigentlichen Arbeitspflicht immer mehr zu.

Ausufernde Compliance Kataloge oder schwer verständliche Insiderregeln scheitern an ihrer Intransparenz. Schließlich darf durch Complianceregeln nicht in Rechte Dritter (z. B. Familienangehörige) eingegriffen werden

Vertragliche vereinbarte Complianceregeln können nicht ohne weiteres abgeändert oder angepasst werden, insbesondere nicht durch Flexibilisierungsklauseln. Denn solche Klauseln sind in der Regel intransparent und damit nach § 307 Abs. 1 Satz 2 BGB unwirksam.

Für diesen Bereich bietet sich der Abschluss von Betriebsvereinbarungen an, wozu meine Kollegin umfassend berichten wird.

## **B. Compliance und Datenabgleiche.**

Beim sog. „Mitarbeiterscreening“ unterwirft der Unternehmer oder von ihm beauftragte Dritte bereits beim Arbeitgeber vorhandene oder zu Screening-Zwecken erhobene Mitarbeiterdaten mittels Datenverarbeitung Prüfrastern, um bei damit erzielte Trefferfälle dann zu „verwerten“.

Worum geht es?

Beim „Data Mining“, wird in Buchhaltungssystemen nach Manipulationsmustern gesucht. Verbreitet ist auch der systematische Abgleich von verschiedenen Datenbanken (Daten-Doubletten-Abgleich).

Eingesetzt werden hochintelligenten Screening-Tools wie IDEA, SAS, SiRON und FRAUD-SCAN, die wissenschaftlich fundierte Methoden wie z.B. die Benford-Analyse verwenden. Es müssen dabei möglichst viele Daten verglichen werden, damit man überhaupt systematisch und nicht nur zufällig auf auffällige Parallelen stößt. Das Mitarbeiterscreening wird in weiten Bereichen der deutschen Wirtschaft bei der präventiven Korruptionsbekämpfung standardmäßig eingesetzt.

Da dafür entweder Daten neu erhoben oder bereits gespeicherte Daten zum geänderten Zweck des Abgleichens genutzt und verarbeitet werden, bedarf das gem. § 4 Abs. 1 BDSG einer rechtlichen Grundlage. Dafür kommt entweder eine Einwilligung der Betroffenen oder eine

Erlaubnisvorschrift in Frage. In der Regel ist nicht davon auszugehen, dass mit der allgemeinen Einwilligung der Verarbeitung beschäftigungsrelevanter Arbeitnehmerdaten z. B. in Formulararbeitsverträgen die Beschäftigten nach § 4a BDSG auch in Datenabgleiche einwilligen. Außerdem muss in Frage gestellt werden, inwieweit Beschäftigte gegenüber dem Arbeitgeber überhaupt freiwillig handeln werden.<sup>13</sup>

Eine die Datenerhebung rechtfertigende Einwilligung muss den Anforderungen des § 4 a BDSG genügen, insbesondere muss sie freiwillig erfolgt sein. Die nicht hervorgehobene Erwähnung im Vertragstext reicht nicht aus. Denn bei einer Koppelung von Arbeitsvertrag und Einwilligung entsteht sofort der Anschein von Unfreiwilligkeit. Eine Einwilligung ist allerdings grundsätzlich möglich, auch kann sie in AGB vereinbart werden, dann greift jedoch die entsprechende Kontrolle. Dabei gilt nach der jüngsten Rechtsprechung des BAG, dass eine Einwilligungserklärung, die über die ohnehin gesetzlich normierten Erlaubnistatbestände des BDSG hinausgeht, dem Arbeitnehmer regelmäßig nicht ohne jegliche Gegenleistung abverlangt werden darf. Hierin liegt eine unangemessene Benachteiligung.

Ob Mitarbeiterscreenings zulässig waren, hing vor der Einführung des § 32 BDSG allein von § 28 Abs.1 Nr. 2 BDSG ab, weil sie wenn überhaupt mit der „Wahrung berechtigter Interessen der verantwortlichen Stelle“ gerechtfertigt wurden.

Die Unternehmen beriefen sich auf ihr Interesse an der Beachtung nebenvertraglicher Pflichten der Arbeitnehmer, nämlich der Pflicht zur Unterlassung von Schädigungen des Arbeitgebers oder Compliance-Verstößen und auf die unternehmerische Verpflichtung, Schaden durch Korruption oder Normverstöße zu verhindern. Allerdings war die einschränkende Rechtsprechung des BAG zu beachten, wonach das allgemeine Persönlichkeitsrecht eine lückenlose technische Überwachung am Arbeitsplatz z. B. durch verdeckte Videoaufnahmen ausschloss. Solche Eingriffe wurden nur dann für zulässig gehalten, wenn überragende berechnete Interessen des Arbeitgebers gefährdet waren.

§ 32 Abs. 1 BDSG nach der Novelle vom 1.9.2009 hilft auch nicht weiter. Für Maßnahmen, die (auch) zur Ermittlung von Straftaten Beschäftigter geeignet sind, gilt § 32 Abs. 1 S. 2 BDSG. Das „schutzwürdige Interesse der Beschäftigten“ darf hier nicht das Interesse des Arbeitgebers am Datenabgleich überwiegen. Diese Vorschrift lässt allenfalls bei Auftreten konkreter Verdachtsmomente einen Datenabgleich zu, zusätzlich müssen die Daten anonymisiert oder pseudonymisiert werden. Der Datenabgleich darf auch nur zur Aufdeckung schwerwiegender Pflichtverletzungen eingesetzt werden.

Denn nach den Grundsätzen der Videoentscheidung des BAG<sup>14</sup>, die auch auf Eingriffe in das allgemeine Persönlichkeitsrecht durch heimliche elektronische Datenabgleiche zu beachten sind, muss der Datenabgleich verhältnismäßig sein. Die Intensität des Eingriffs und das Gewicht und das Gewicht der ihn rechtfertigenden Gründe sind gegeneinander abzuwägen.<sup>15</sup> Für die Schwere des Eingriffs ist insbesondere von Bedeutung, wie viele Personen wie intensiv den Beeinträchtigungen ausgesetzt sind. Das Gewicht der Beeinträchtigung hängt ua. davon ab, ob die Betroffenen als Personen anonym bleiben, welche Umstände und Inhalte der Kommunikation erfasst werden und welche Nachteile den Grundrechtsträgern aus der Überwachungsmaßnahme drohen oder von ihnen nicht ohne Grund befürchtet werden.<sup>16</sup> Von

---

<sup>13</sup> Heinson, Compliance durch Datenabgleiche BB 2010, S. 3084

<sup>14</sup> BAG vom 26. 8. 2008 - 1 ABR 16/07 -, NZA 2008, 1187

<sup>15</sup> so auch BAG vom 29.6.2004 - 1 ABR 21/03 - BAGE 111, 173, zu B I 2 d cc der Gründe; BVerfG vom 11.3.2008 - 1 BvR 2074/05 - und - 1 BvR 1254/07 - Rn. 168, NJW 2008, 1505).

<sup>16</sup> BAG vom 26. 8. 2008 - 1 ABR 16/07 -, NZA 2008, 1187

ausschlaggebender Bedeutung ist, ob Betroffene einen ihnen zurechenbaren Anlass für die Datenerhebung geschaffen hat - etwa durch eine Rechtsverletzung - oder ob diese anlasslos erfolgt. Auch die "Persönlichkeitsrelevanz" der erfassten Informationen ist zu berücksichtigen. Die Heimlichkeit einer in Grundrechte eingreifenden Ermittlungsmaßnahme erhöht das Gewicht der Freiheitsbeeinträchtigung. Den Betroffenen wird nämlich vorbeugender Rechtsschutz faktisch verwehrt und nachträglicher Rechtsschutz erschwert.<sup>17</sup>

Datenabgleiche ähneln in ihren Auswirkungen der staatlichen Rasterfahndung. Sie sind eine Überwachungsmethode bei der ebenfalls Daten zum automatischen Abgleich verwendet werden, die vormals zu anderen Zwecken gespeichert wurden. Daten aus unterschiedlichen Quellen werden kombiniert und anhand vorher erstellter Muster ausgewertet. Es werden Daten einer großen Zahl von Unschuldigen mitverarbeitet. Aus Sicht der betroffenen besteht kein Unterschied, ob er sich privater oder staatlicher Rasterfahndung unterwerfen muss. Hinsichtlich der Rechtmäßigkeit der Ermittlungen müssen daher ähnliche Maßstäbe angelegt werden, als würden sie unmittelbar staatlich durchgeführt. Das folgt auch aus dem objektiven Gehalt der Grundrechte als Garanten der Selbstbestimmung. Sie schließen aus, dass Vertragsverhältnisse als Mittel der Fremdbestimmung erhalten. Das wäre im Beschäftigungsverhältnis der Fall, wenn sich die Arbeitnehmer den Ermittlungsmaßnahmen des Unternehmens bedingungslos unterwerfen müssten.<sup>18</sup>

Damit scheidet präventive nicht anonymisierte Datenabgleiche aus.

Mithilfe eines anonymisierten Screenings können allenfalls kritische Bereiche in Unternehmen dargestellt werden, in denen es mit erhöhter Wahrscheinlichkeit zu Compliance-Verstößen kommt. Datenschutzrechtlich zulässig bleibt, mit so gewonnenen Ergebnissen besondere Prüfaufgaben für Revisionen oder Audits zu benennen oder in solchen Bereichen durch die Einführung von Verfahrenssicherungen Compliance-Verstöße zukünftig auszuschließen. Datenschutzwidrig bleibt demgegenüber das standardmäßige Durchreichen von Screening-Treffern an die Revision zum Zwecke der Intervention/Sanktion.<sup>19</sup>

### **C. Auswertung von e-mail accounts**

Das Unternehmen ist geschäftsmäßiger Erbringer von Telekommunikationsdiensten, wenn es wie in § 3 Nr. 10 TKG definiert, ein „nachhaltiges Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht“ vorhält. Unschädlich ist, dass der Telekommunikationsdienst nur für eine geschlossene Benutzergruppe, erbracht werden soll. Räumt das Unternehmen seinen Arbeitnehmern ein, vom Arbeitsplatz auf das Internet zuzugreifen und über einen personalisierten EMail-Account des Arbeitsgebers nicht nur dienstlich, sondern auch für private Zwecke zu kommunizieren, ist der Arbeitnehmer Dritter, soweit er diesen Service privat nutzt.

Der Zugriff auf e-mail accounts privaten Inhalts in diesem Rahmen ist strafbar nach § 206 Abs. 1 StGB. Danach wird bestraft, wer einer anderen Person Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen. Andere Personen sind auch eigene Mitarbeiter (z.B. einer forensischen Abteilung), die im gewöhnlichen Geschäftsgang

---

<sup>17</sup> BVerfG 11.3.2008 - 1 BvR 2074/05 - und - 1 BvR 1254/07 - aaO, Rn. 77 - 79).

<sup>18</sup> Heinson a.a.O., 3086

<sup>19</sup> •Brink/Schmidt, Die rechtliche (Un-)Zulässigkeit von Mitarbeiterscreenings - Vom schmalen Pfad der Legalität. MMR 2010. 592 ff.. 595 f.

von den E-Mails keine Kenntnis erlangt hätten. Deshalb kann die Weitergabe einzelner belastender E-Mails an Vorgesetzte, die Compliance- oder Personalabteilung, Unternehmensanwälte, Strafverfolgungsbehörden etc. tatbestandsmäßig ein Fall von § 206 StGB sein.

Das Fernmeldegeheimnis umfasst gem. § 206 Abs. 5 S. 2 StGB den Inhalt der Telekommunikation und ihre näheren Umstände. Telekommunikation selbst ist gem. § 3 Nr. 22 TKG der technische Vorgang des Aussendens, Übermittels und Empfangens. Werden private E-Mails zu diesem Zeitpunkt abgefangen und kopiert, um sie nachträglich auszuwerten und weiterzuleiten, ist das Telekommunikationsgeheimnis auf jeden Fall betroffen. Z. B. ist das bei Sicherungskopien, die von vielen Unternehmen durch Backup-Systeme standardmäßig in der Übertragungsphase hergestellt werden, der Fall.

Was gilt aber, wenn die E-Mails im Zeitpunkt des ersten Zugriffs bereits auf dem Mailserver des Arbeitgebers „ruhen“, also ein Telekommunikationsvorgang in einem dynamischen Sinne gar nicht mehr stattfindet?

Hier ist auf eine Entscheidung des Hess. VGH hinzuweisen,<sup>20</sup> der über die Rechtmäßigkeit eines Auskunfts- und Vorlageersuchens der BaFin zu befinden hatte. Die BaFin hatte auf Ersuchen der amerikanischen Wertpapieraufsicht SEC den Arbeitgeber gem. § 4 Abs. 3 WpHG aufgefordert, sämtliche E-Mails namentlich bezeichneter Mitarbeiter, die bestimmte Namen und Stichworte enthielten, vorzulegen. Gegen diesen Bescheid hatte der Arbeitgeber mit Hinweis auf das Fernmeldegeheimnis Widerspruch eingelegt und geklagt, allerdings ohne Erfolg. Das Gericht meinte, Art. 10 GG und § 88 TKG seien nicht betroffen. Dabei berief sich das Gericht auf die Rechtsprechung des BVerfG bezüglich E-Mails, die der Nutzer auf die Festplatte seines PCs heruntergeladen hatte: Wenn nur auf den PC selbst zugegriffen wird, so ist das Fernmeldegeheimnis nicht betroffen – genauso wenig wie z. B. bei einem ausgedruckten Telefax oder den Aufzeichnungen eines häuslichen Anrufbeantworters.

Das Herunterladen von E-Mails auf dem Arbeits-PC („POP3“) ist in Unternehmen allerdings eher ungewöhnlich.

Das bloße Belassen auf dem E-Mail-Server („IMAP“) kann nicht mit dem Belassen auf dem Server gleichgesetzt werden. Das ergibt sich aus der Entscheidung des BVerfG vom 16. 6. 2009<sup>21</sup> zum Schutzbereich des Art. 10 GG: Solange die E-Mail auf dem Mailserver eines Providers verbleibt und nicht in den Herrschaftsbereich des Nutzers gelangt, kann der Nutzer die E-Mails zwar für sich auf einem Bildschirm lesbar machen. Er hat aber keine technische Möglichkeit, die Weitergabe der E-Mails durch den Provider zu verhindern. Dieser weiter bestehende, technisch bedingte Mangel an Beherrschbarkeit begründet die besondere Schutzbedürftigkeit durch das Fernmeldegeheimnis. Irrelevant ist demnach auch die Kenntnisnahme durch den Nutzer, solange die E-Mail auf dem Server verbleibt. § 206 Abs. 1 StGB steht deshalb der Weitergabe privater E-Mails bei erlaubter privater Nutzung grundsätzlich entgegen.

Mit einem ausdrücklichen Einverständnis des Arbeitnehmers zur Weitergabe des Inhalts seiner e-mails im Gegenzug zu der Gestattung gelegentlicher privater E-Mail-Nutzung zu verbinden, ist im Rahmen der Arbeitnehmerüberwachung auch nicht zu arbeiten, da Existenz, Anlass und Art der Untersuchung den Mitarbeitern zunächst verborgen bleiben müsste, um

---

<sup>20</sup> Hess. VGH vom 19.5.2009 – 6 A 2672/08.Z., NJW 2009, 2470

<sup>21</sup> - 2 BvR 902/06 -. NJW 2009, 2431

erschöpfend Beweismaterial sammeln zu können und Verdunklungshandlungen zu vermeiden.

Außerdem ist ein wirksamer Verzicht auf Wahrung des Fernmeldegeheimnisses nur dann möglich, wenn dadurch ausschließlich schützenswerte Belange der Mitarbeiter betroffen sind. Denn niemand kann ohne Ermächtigung über fremde Rechte verfügen. Dazu kann auf die Fangschaltungsentscheidung des BVerfG zurückgegriffen werden<sup>22</sup>. Danach bedarf die e-mail Überwachung nicht nur der Zustimmung des Empfängers, sondern auch des Absenders, insbesondere wegen § 101 TKG. Bei einer unternehmensspezifischen E-Mail-Adresse („mustermann@unternehmen.de“) muss der Absender zwar damit rechnen, dass auf diesen Account durchaus anderweitige Zugriffsrechte (z.B. des Sekretariats, der Urlaubs- oder Krankheitsvertretung) bestehen können. Er kann sich nicht einmal darauf verlassen, dass der Arbeitgeber überhaupt Telekommunikationsdienste erbringt, also die private E-Mail-Nutzung erlaubt hat. Diese Erwägungen ziehen aber nicht, weil auch der Briefabsender und der Teilnehmer beim Telefonieren immer damit rechnen müssen, dass unerlaubt und verbotenerweise „mitgelesen und mitgehört“ wird.

Allenfalls kommen für den Arbeitgeber besondere Rechtfertigungsgründe in Betracht. So bedarf die Weiterleitung von Kommunikationsinhalten an Strafverfolgungsbehörden eines wirksamen Beschlusses gem. §§ 100a, 100b StPO oder bei ruhenden E-Mails gem. §§ 94 ff., 102 ff. StPO.

Auf Rechtfertigungsgründe des TKG kann nicht zurückgegriffen werden. Denn § 88 Abs. 3 S. 4 TKG z.B. gilt nur für bevorstehende in § 138 StGB genannte Katalogtaten, die komplette Weitergabe bestimmter E-Mail-Bestände lässt sich damit nicht rechtfertigen.

§ 100 TKG dient der Störungssuche und Ermittlung von Leistungerschleichungen und betrifft ohnehin nur die Bestands- und Verkehrsdaten, nicht die Kommunikationsinhalte.

§ 88 Abs. 3 S. 3 TKG erlaubt eine Durchbrechung des Fernmeldegeheimnisses nur dann, wenn eine gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht.

§ 227 BGB scheidet, weil sich Notwehr nur gegen den Angreifer richten darf. Außerdem wird zum Zeitpunkt des Zugriffs gar kein gegenwärtiger, rechtswidriger Angriff mehr vorliegen.

Die Eingriffsnorm des § 32 BDSG setzt konkrete Verdachtsmomente und die Gefahr des Eintritts schwerwiegender Nachteile zu Lasten des Unternehmens voraus.

„Werden bei der E-Mail- und Internetkommunikation dienstliche mit privaten E-Mails durchmischt, führt dies zu einem umfassenden Einsichts- und Kontrollverbot auch der betrieblichen Korrespondenz. Eine unzulässige Kontrolle der E-Mail-Kommunikation am Arbeitsplatz kann für den Arbeitgeber empfindliche zivilrechtliche (Schadensersatzansprüche) und strafrechtliche (§ 201 StGB: Verletzung der Vertraulichkeit des Wortes; § 202 StGB: Verletzung des Briefgeheimnisses; § 202 a StGB: Ausspähen von Daten; § 206 StGB: Verletzung des Fernmeldegeheimnisses) Folgen haben.“<sup>23</sup>

---

<sup>22</sup> BVerfG vom 25.3.1992 - 1 BvR 1430/88 -, NJW 1992, 1875

<sup>23</sup> Heldmann, Betrugs- und Korruptionsbekämpfung zur Herstellung von Compliance aus arbeits- und datenschutzrechtlicher Sicht, Betrieb 2010, 1235

Ist dem Arbeitnehmer die E-Mail- und Internetnutzung nur zu dienstlichen Zwecken gestattet, ist der Arbeitgeber nicht Provider.

Die Zulässigkeit von Zugriffen im Rahmen von Compliance-Maßnahmen folgt dann aus § 32 BDSG. Dabei wird das Interesse des Arbeitgebers regelmäßig dahin gehen, Verkehrsdaten (Datum, Uhrzeit von Versand/Empfang der E-Mail sowie ggf. das übermittelte Datenvolumen) zu erfassen, zu speichern und zu nutzen. Diese auf § 32 BDSG gestützte Überwachung der dienstlichen Telekommunikation muss aber erforderlich und verhältnismäßig sein. Die Erfassung des Inhalts der Kommunikation als dauerhafte und schrankenlose „Totalüberwachung“ ist nicht zulässig.<sup>24</sup>

Hinzuweisen ist in diesem Zusammenhang die Entscheidung des OLG Karlsruhe vom 10.1.2005.<sup>25</sup> Danach ist das Herausfiltern von E-Mails immer dann strafbar, wenn ein Arbeitgeber die private Nutzung von Internet und E-Mail gestattet, die beteiligten Kommunikationspartner (also der Absender einer Nachricht ebenso wie ihr Empfänger im Unternehmen) nicht in die Kontrolle eingewilligt haben und kein Ausnahmetatbestand diese rechtfertigt.

Völlig unzulässig sind sog. Rasterfahndungen im Sinne einer sog. Online-Durchsuchung, wenn damit ermöglicht werden soll, die auf dem Computer einer überwachten Person gespeicherten Dateien (Dokumente, E-Mail-Korrespondenz, Bilder, etc.) einzusehen, ohne dass diese es bemerken. Bei Online-Durchsuchungen wird ein im Hintergrund laufendes Programm benötigt, weil ein unmittelbarer Zugriff (z. B. ein heimliches "Aufschalten") auf den Rechner einer Person, um "an der Quelle" Telekommunikationsinhalte zu überwachen oder Dateien einzusehen, nur mit Hilfe von auf diesem Rechner installierter Software möglich ist.

Nach der Entscheidung des des BVerfG zur sog. Online-Durchsuchung<sup>26</sup> steht fest, dass ein heimlicher Zugriff auf ein "informationstechnisches System" (z. B. PC, Notebook aber auch Smartphone) einen Eingriff in das allgemeine Persönlichkeitsrecht in seiner Ausformung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (kurz: IT-Grundrecht) darstellt. Das ist nur unter engen, durch Gesetz zu regelnden Voraussetzungen statthaft. Eine entsprechende formell-gesetzliche Befugnisnorm, die den heimlichen Zugriff auf informationstechnische Systeme rechtfertigen könnte, existiert weder in der Strafprozessordnung noch im BDSG.

**Eine Online-Durchsuchung zu Compliance-Zwecken ist deshalb unzulässig.**<sup>27</sup>

---

<sup>24</sup> Heldmann, a.a.O.

<sup>25</sup> Az: 1 Ws 152/04

<sup>26</sup> BVerfG vom 27.02.2008 - 1 BvR 370/07 -, BVerfGE 120, 274 = NJW 2008, 822

<sup>27</sup> Braun, Ozapftis - (Un)Zulässigkeit von "Staatstrojanern", JurPC Web-Dok. 167.2011, Abs. 1 - 35

## **D. Befragung von Mitarbeitern, Einschalten unternehmensfremder „Privatermittler“**

Bei der internen Ermittlung von Compliance-Verstößen – der „investigation“ – wird es früher oder später auch zu Befragungen von Arbeitnehmern kommen. Das kann entweder dann eintreten, wenn sie selbst verdächtig sind, sich an den Verstößen beteiligt zu haben, oder weil sie zu Wahrnehmungen befragt werden, die zur Aufklärung der Verstöße beitragen. Die Mitarbeiterbefragung (auch „Interview“ genannt) kann zu einer verhörsähnlichen Lage werden, in der sich der Arbeitnehmer auch externen Ermittlern, meist Rechtsanwälten, gegenüber sieht.

Dass der Arbeitnehmer an dem Interview teilnehmen muss, folgt aus dem Weisungsrecht des Arbeitgebers, § 106 GewO. Der Arbeitgeber kann die sich nur dem Rahmen nach aus dem Arbeitsvertrag ergebende Arbeitspflicht näher konkretisieren, auch bezüglich Ordnung und Verhalten im Betrieb und im Hinblick auf so genannte leistungssichernde Verhaltenspflichten. Deren Erfüllung ist unumgänglich, um einen sinnvollen Austausch der Hauptleistungspflichten zu ermöglichen. Sollen diesbezüglich Weisungen erteilt oder soll die Nichteinhaltung von Weisungen beanstandet werden, ist der Arbeitgeber berechtigt, den Arbeitnehmer zur Teilnahme an Gesprächen zu verpflichten.<sup>28</sup>

Soll das Interview ausnahmsweise mit der Anhörung für eine spätere Verdachtskündigung verbunden werden, sind die vom BAG<sup>29</sup> für diese Anhörung aufgestellten Anforderungen zu beachten. Dann hat das (nur noch vermeintliche) „Interview“ sich auf einen greifbaren Sachverhalt zu beziehen. Dem Arbeitnehmer ist dabei die Möglichkeit zu geben, bestimmte Tatsachen zu bestreiten oder Entlastendes zu bezeichnen.

Anerkannt ist zwar, dass der Arbeitnehmer nicht generell dem Arbeitgeber für Auskünfte zur Verfügung stehen muss. Der Arbeitgeber darf den Arbeitnehmer aber anweisen, wahrheitsgemäß und vollständig Auskunft zu erteilen über Art und Umfang der eigenen Leistung, über den eigenen Arbeitsbereich insgesamt sowie über Wahrnehmungen im Zusammenhang mit der Arbeitsleistung, soweit die Erteilung der Auskunft dem Arbeitnehmer nicht unzumutbar ist und ihn nicht übermäßig belastet.

Zur Offenbarung von Umständen, die kündigungrechtlich verwertet werden können, oder die ihn Schadensersatzansprüchen des Arbeitgebers aussetzen, ist der Arbeitnehmer aber, gleich ob auf Nachfrage oder ungefragt, nicht verpflichtet. Ihm ist hier ein Schweigerecht einzuräumen.

Wenn der im Raum stehende Verdacht eines Compliance-Verstoßes zugleich den Verdacht einer Straftat begründet, kann der Arbeitnehmer die Beschuldigtenrechte des Strafverfahrens in Anspruch nehmen, er kann also die Aussage verweigern.

Soll der Arbeitnehmer als „Zeuge“ interviewt werden, besteht ebenfalls eine arbeitsvertragliche Auskunftspflicht. Sie erstreckt sich vor allem auf objektive Umstände ohne Bezug zu bestimmten Personen. So wäre die Frage nach Fehlbeständen in der Kasse ebenso wahrheitsgemäß zu beantworten wie die nach Unregelmäßigkeiten bei Buchungen von Unternehmenskonten.

---

<sup>28</sup> Rudkowski: Die Aufklärung von Compliance-Verstößen durch „Interviews“ NZA 2011, 612

<sup>29</sup> BAG, NZA 2008, 809 (810).

Die Auskunftspflicht endet auch hier, wenn der Arbeitnehmer sich bei wahrheitsgemäßer Aussage selbst belasten müsste. Soweit es um die Selbstbezeichnung bei Straftaten oder Ordnungswidrigkeiten geht, folgt das aus einem allgemeinen Rechtsgedanken, der sich auch im Arbeitsgerichtsprozess findet, § 384 Nr. 2 ZPO i.V. mit § 46 II 1 ArbGG. Niemandem, auch nicht dem Zeugen-Arbeitnehmer, ist es zuzumuten, sich selbst zu schaden.<sup>30</sup>

Diese Grundsätze gelten unabhängig davon, wer auf der Arbeitgeberseite die Befragung durchführt – der Arbeitgeber selbst, der direkte Vorgesetzte des verdächtigen Arbeitnehmers, interne Ermittler etwa aus der Personal- oder Complianceabteilung oder vom Arbeitgeber beauftragte Rechtsanwälte.

Allerdings muss sich der Arbeitnehmer besonders schützen können, wenn ausländische Rechtsanwälte eingeschaltet werden, die nicht ausschließlich im Interesse des Arbeitgebers, sondern auch im Interesse von Aufsichtsbehörden tätig sind und Informationen an diese weiterleiten.<sup>31</sup> Das kann dann der Fall sein, wenn in Unternehmen ermittelt wird, die den US-amerikanischen Kapitalmarkt nutzen und deshalb mit der dortigen Aufsicht kooperieren müssen. Hier besteht das unabdingbare Recht zu schweigen und seinerseits einen Rechtsanwalt hinzuzuziehen.

Der Einsatz von Detektiven stellt einen Eingriff in das Persönlichkeitsrecht dar. Er ist nur bei konkretem Verdacht einer gegen den Arbeitgeber gerichteten Straftat oder einer schweren Arbeitspflichtverletzung zulässig, und auch nur dann, wenn er die einzig erfolgversprechende Möglichkeit bietet, den Verdacht zu klären.<sup>32</sup> Nach Auffassung des BAG können Detektive zur Überprüfung der ordnungsgemäßen Arbeitsleistung in Form einer Stichprobenkontrolle eingesetzt werden.<sup>33</sup> Erlaubt ist aber nur eine Überprüfung dienstlichen Verhaltens; eine Erfassung außerdienstlicher oder privater Aktivitäten ist immer eine nicht zu rechtfertigende Verletzung des allgemeinen Persönlichkeitsrechts des Arbeitnehmers.<sup>34</sup>

## **E. Exkurs Whistleblowing**

Element eines effizienten Compliance-Umfeldes ist ein funktionsfähiges Whistleblowing-System. Der Whistleblower kann als „ethischer Dissident“ bezeichnet werden: Es handelt sich um jemanden, der nicht bereit ist, Gesetzesverstöße mitzutragen, sondern Courage zeigt und auf diese Weise zur Aufdeckung von Straftaten und Ordnungswidrigkeiten beiträgt. Dies kann nicht nur für das Unternehmen, sondern auch für die Allgemeinheit von erheblichem Nutzen sein.

Allerdings gibt es in Deutschland keinen effektiven Schutz für Whistleblower, im Gegenteil!. Der Whistleblower begibt sich in Gefahr, des Verrats von Betriebs- und Geschäftsgeheimnissen (§ 17 UWG) bezichtigt zu werden, wenn er Rechtsverstöße eines Unternehmens bekannt macht. Meist droht nach der Rechtsprechung des BAG auch der Verlust seines Arbeitsplatzes.<sup>35</sup>

---

<sup>30</sup> Rudkowski a.a.O.

<sup>31</sup> a. M. Rudkowski a.a.O.

<sup>32</sup> Jousen, Mitarbeiterkontrolle: Was muss, was darf das Unternehmen wissen?, NZA-Beil. 2011, 35

<sup>33</sup> BAG NZA 2000, 1176

<sup>34</sup> Jousen, a.a.O.

<sup>35</sup> BAG vom 3.7.2003 - 2 AZR 235/02 -, NZA 2004, 427

Zwar hat der EGMR in Straßburg am 21.7.2011 mit Kammerurteil im Verfahren Heinisch gegen Deutschland (Beschwerdenummer 28274/08), einstimmig festgestellt, dass eine Verletzung von Artikel 10 (Freiheit der Meinungsäußerung) der Europäischen Menschenrechtskonvention (EMRK) vorlag. Der Fall betraf die fristlose Kündigung einer Altenpflegerin, nachdem sie Strafanzeige gegen ihren Arbeitgeber erstattet hatte, mit der Begründung, Pflegebedürftige und ihre Angehörigen erhielten wegen Personalmangels keine angemessene Gegenleistung für die von ihnen getragenen Kosten. Die Entscheidung ersetzt aber nicht eine gesetzliche Schutzvorschrift.

Das ist angesichts des Rufs nach funktionierenden Compliance-Systemen eigentlich nicht hinnehmbar. Eine „Whistleblowerinitiative der Großen Koalition ist gescheitert. Die jetzige Regierungskoalition sträubt sich gegen eine gesetzliche Absicherung des Whistleblowing, ungeachtet der Tatsache, dass bis Ende 2012 Deutschland nach der Vorgabe des G20 Gipfels in Seoul im November 2010 gesetzliche Regelungen zum Whistleblowerschutz einführen muss.

Das bestehende Maßregelverbot des § 612a BGB bietet keinen ausreichenden Schutz für Whistleblower.<sup>36</sup>

---

<sup>36</sup> Göpfert, Landauer „Arbeitsstrafrecht“ und die Bedeutung von Compliance-Systemen: Straftaten „für“ das Unternehmen, NZA-Beil. 2011, 16 ff., 21