Kommunikation

Festschrift für Rolf H. Weber zum 60. Geburtstag

Herausgegeben von

Rolf Sethe
Andreas Heinemann
Reto M. Hilty
Peter Nobel
Roger Zäch

Sonderdruck

Stämpfli Verlag AG Bern · 2011

Compliance, Whistleblowing und Critical Incident Reporting

Verbesserung der unternehmensinternen Kommunikation

ROLF SETHE*

Inhaltsverzeichnis

* Für Diskussion und wertvolle Anregungen danke ich meinen Mitarbeitern FABIO ANDREOTTI und LORENA STUDER.

I. Einleitung

ROLF H. WEBER gehört zu den im In- und Ausland bekanntesten schweizerischen Wirtschaftsjuristen. Neben seinem breit gefächerten wissenschaftlichen Werk bestechen seine Innovationskraft und die Vielzahl der von ihm übernommenen verantwortungsvollen Aufgaben. Ich habe den Jubilar 1995 bei einem gemeinsamen Seminar zum Bank-, Börsen-, Gesellschafts- und Kapitalmarktrecht kennengelernt. Eines der Themen war die Compliance im Bankwesen. Seinerzeit steckte das Thema noch in den Kinderschuhen und die Diskussion drehte sich daher um die sehr grundsätzliche Frage, warum man überhaupt Unternehmen dazu anhalten müsse, die Gesetze einzuhalten, wo doch jedermann zu deren Einhaltung verpflichtet und dies daher eine Selbstverständlichkeit sei.

Wir wissen heute, dass eine solche Grundhaltung in komplexen Organisationen gerade nicht mehr ohne weiteres vorausgesetzt werden kann, was nicht zuletzt die Skandale von Enron (Bilanzfälschung), Siemens (Korruption) und der UBS (Beihilfe zu Steuerhinterziehung) gezeigt haben. Aus diesem Grund hat das Thema Compliance in den letzten 15 Jahren einen grossen Aufschwung erlebt. Heute müssen Unternehmensleiter – schon um Verantwortlichkeitsansprüchen vorzubeugen – ein Interesse daran haben, frühzeitig über Fehlentwicklungen innerhalb ihres Unternehmens informiert zu werden; sie müssen Strukturen schaffen, die dies ermöglichen. Einige Rechtsordnungen bzw. Organisationen schreiben die Errichtung von Whistleblowing-Systemen gesetzlich vor (so die USA mit dem Sarbanes-Oxley-Act für börsenkotierte Unternehmen im Hinblick auf Bilanzverstösse,[1] dem Dodd-Frank-Act in Bezug auf Compliance-Verstösse[2] und dem False Claim Act[3] oder die IOSCO für Kreditrating-

[1] Corporate and Auditing Accountability, Responsibility, and Transparency Act of 2002, (Sarbanes-Oxley Act), Pub. L. No. 107-204, 116 Stat. 745, dazu etwa DANIELA WEBER-REY, Whistleblowing zwischen Corporate Governance und Better Regulation, AG 2006, 406; THOMAS BERNDT/IVO HOPPLER, Whistleblowing – ein integraler Bestandteil effektiver Corporate Governance, BB 2005, 2623, 2625; CHRISTIAN REITER, Der Schutz der Whistleblowers nach dem Sarbanes-Oxley Act im Rechtsvergleich und im internationalen Arbeitsrecht, RIW 2005, 168 ff; GEORG VON ZIMMERMANN, „Whistleblowing" – Anforderungen des Sarbanes-Oxley Acts, WM 2007, 1060 ff. Sec. 301 (4) schreibt die Einrichtung von internen Whistleblowing-Systeme zur Meldung von Bilanzverstössen vor. Sec. 806 enthält die Vorgabe, wonach Meldende sanktionsfrei bleiben, wobei die Effektivität dieser gesetzlichen Bestimmung zweifelhaft ist, vgl. TERRY MOREHEAD DWORKIN, SOX and Whistleblowing, Michigan Law Review 105 (2007), 1757 ff. Generell zum Thema ROBERTA ANN JOHNSON, Whistleblowing: When It Works – And Why, Boulder, London 2003.

[2] Sec. 922 – 924 des Dodd-Frank Wall Street Reform And Consumer Protection Act 2010, Pub. L. No. 111-203, 124 Stat. 1376, sehen eine finanzielle Belohnung im Umfang von 10-30% der vom Staat verhängten Geldbusse oder des eingezogenen Geldes an den Whistleblower vor, dazu ROLF HÜNERMANN/TOBIAS DIETRICH, Aktuelle Rechtsentwicklungen in den USA – Einflussnahme auf europäische Unternehmen, Corporate Finance Law 2010, 357 ff.; CURTIS C. VERSCHOOR, Increased Motivation for Whistleblowing, Strategic Finance, Nov. 2010, 18.

[3] 31 U.S.C. §§ 3729–3733. Setzt ein Privater eine Qui tam-Klage durch, stehen ihm 15-25% des verhängten Strafbetrags zu, vgl. 31 U.S.C. § 3730(d). Zu Einzelheiten RALF KÖBEL, Zur wirtschaftsstrafrechtlichen Institutionalisierung des Whistleblowing, JZ 2008, 1134 ff.

agenturen[4] und der Europarat in Bezug auf Korruption[5]), andere kennen einen gesetzlichen Schutz von Whistleblowern (wie Grossbritannien mit dem PIDA,[6] Frankreich mit Art. L. 1161-1 Code du Travail und die USA im Bereich des Sarbanes-Oxley-Act, im Verbraucherschutz[7] und auf Ebene der einzelnen US-Bundesstaaten[8]) und wieder andere (wie die Schweiz[9] und Deutschland[10]) diskutierten eine solche gesetzliche Regelung[11] oder empfehlen sie (EU[12] oder ICC[13]). Im Folgenden soll daher untersucht werden, ob und unter welchen Bedingungen durch Whistleblowing eine Verbesserung der unternehmensinternen Kommunikation erreicht und damit ein wirksamer Beitrag zur Compliance geleistet werden kann.[14] Ich hoffe, dass dieses Thema, das eng mit den Forschungsinteressen von ROLF H. WEBER zusammenhängt,[15] sein Interesse findet.

---

4 Ziff. 1.16 des Code of Conduct Fundamentals for credit Rating agencies der IOSCO vom Dezember 2004, http://www.iosco.org/library/pubdocs/pdf/IOSCOPD180.pdf.

5 Art. 9 des Zivilrechtsübereinkommens über Korruption vom 4.11.1999.

6 Public Interest Disclosure Act 1998, Chapter 23. Die Bestimmungen wurden als Part IV A in den Employment Rights Act 1996 eingefügt, http://www.legislation.gov.uk/ukpga/1998/23/introduction/enacted.

7 Consumer Product Safety Improvement Act of 2008, Pub. L. No. 110-314, 122 Stat. 3016, 15 U.S.C. 2051.

8 ELLETTA SANGREY CALLAHAN/TERRY MOREHEAD DWORKIN, The State of State Whistleblower Protection, Am. Bus. L.J. 38 (2000), 99 ff.

9 S.u. III. 2. sowie statt vieler WOLFGANG PORTMANN, Gesetzliche Regelung des Whistleblowing in der Schweiz - überflüssig, nützlich oder notwendig?, AJP/PJA 2010, 987 ff.

10 Antrag der Fraktion der GRÜNEN, BT-Drucks. 16/4459; Vorschlag für eine gesetzliche Verankerung des Informantenschutzes für Arbeitnehmer im Bürgerlichen Gesetzbuch, in: Deutscher Bundestag, Ausschuss für Ernährung, Landwirtschaft und Verbraucherschutz, Ausschussdrucksache 16(10)849 vom Juni 2008, der allerdings am Widerstand der CDU/CSU scheiterte. Zu diesem Entwurf etwa MICHAEL KORT, Individualarbeitsrechtliche Fragen des Whistleblowing, in: Günther Hönn/Hartmut Oetker/Thomas Raab (Hrsg.), Festschrift für Kreutz, Köln 2010, 247, 251 ff.; ARND KOCH, Korruptionsbekämpfung durch Geheimnisverrat? Strafrechtliche Aspekte des Whistleblowing, ZIS 2008, 500, 503 ff. Vgl. auch § 32l Abs. 4 des Entwurfs zum Beschäftigtendatenschutz, BT-Drucks. 17/4230.

11 Whistleblowing ist keine Erfindung unseres Zeitalters. So gab es in Venedig an vielen Stellen sog. Bocca di Leone (Löwenmäuler), in die man anonym Anzeigen und Beschwerden einwerfen konnte, http://de.wikipedia.org/wiki/Bocca_di_Leone.

12 Mitteilung der Kommission an den Rat, das Europäische Parlament und den Europäischen Wirtschafts- und Sozialausschuss, Eine umfassende EU-Politik zur Bekämpfung der Korruption vom 28.5.2003, KOM(2003) 317 endgültig, 20.

13 Richtlinien der Internationalen Handelskammer zum Whistleblowing, http://iccwbo.org/uploadedfiles/ICC/policy/anticorruption/Statements/ICC%20Guidelines%20Whistleblowing%20%20as%20adopted%20204_08%282%29.pdf.pdf?terms=whistleblowing+guidelines.

14 Aus juristischer Sicht zum Thema Whistleblowing und Compliance ISABELLE AUGSBURGER-BUCHELI/BERTRAND PERRIN, Le Whistleblowing et la lutte contre la corruption, L'expert-Comptable Suisse 2009, 627 ff.; MARKUS BERNI/ANDREAS KELLERHALS, Internationales Handelsrecht III: Compliance Management als juristische Kernfunktion im Unternehmen, Zürich 2009; PETER BÖCKLI, Audit Committee, Zürich 2005; ZORA LEDERGERBER, Whistleblowing unter dem Aspekt der Korruptionsbekämpfung, Bern 2005; DIETER PFAFF/FLEMMING RUUD, Schweizer Leitfaden zum Internen Kontrollsytem, 5. Aufl., Zürich 2011, 55; DOMINIQUE PORTMANN/HERBERT WOHLMANN, Whistleblowing, SJZ 103 (2007), 179 ff.; PORTMANN (Fn. 9), 987 ff.; OTTMAR STRASSER, Whistleblowing als Element guter Corporate Governance, in: Rechtliche Rahmenbedingungen des Wirtschaftsstandortes Schweiz, Festschrift 25 Jahre Juristische Abschlüsse an der Universität St. Gallen, Zürich

II. Verrechtlichung von Organisationsanforderungen am Beispiel des Bankenrechts

Analysiert man, in welchen Fällen gesetzliche oder berufliche Pflichten verletzt wurden und in denen die Beherrschung schadensanfälliger Prozesse misslang, entpuppen sich vor allem die zunehmende Komplexität von Unternehmensabläufen sowie undurchlässige hierarchische Strukturen als Ursachen. In Einzelfällen spielen auch bewusste, mitunter kriminelle Verstösse eine Rolle, mit denen man sich (vermeintliche oder tatsächliche) Wettbewerbsvorteile verschaffen möchte (insbesondere Kartellabreden und Korruption).

Auf diese Entwicklung reagiert die Rechtsordnung zunehmend mit dem Erlass und weiteren Ausbau von Organisationspflichten. Betrachtet man das – aufgrund der Finanzkrise gerade im Brennpunkt stehende – Beispiel der Banken, sind vor allem folgende Schutzmechanismen zu nennen: (1) Die Aufnahme des Betriebes und das Betreiben von Banken unterliegt der staatlichen Beaufsichtigung und bedarf der Bewilligung (Art. 3 ff. BankG). (2) Die mit der Verwaltung und Geschäftsführung der Bank betrauten Personen müssen einen guten Ruf geniessen und Gewähr für eine einwandfreie Geschäftstätigkeit bieten (Art. 3 Abs. 2 lit. c BankG). (3) Die Banken unterliegen gesteigerten Organisationspflichten, da sie gemäss Art. 3 Abs. 2 lit. a BankG über eine ihrer Geschäftstätigkeit entsprechende Verwaltungsorganisation verfügen müssen; dabei ist insbesondere eine funktionelle und personelle Trennung der Geschäftsführung vom Organ für Oberleitung, Aufsicht und Kontrolle vorge-

2007, 485 ff.; ADRIAN VON KAENEL, Whistleblowing, SJZ 103 (2007), 309 ff. Aus dem deutschen Schrifttum GREGOR BACHMANN, Compliance – Rechtsgrundlagen und offene Fragen, sowie CHRISTOPH E. HAUSCHKA, Compliance – Praktische Erfahrungen und Thesen, beide in: Gesellschaftsrechtliche Vereinigung (Hrsg.), Gesellschaftsrecht in der Diskussion 2007, Köln 2008, 51 ff. bzw. 65 ff.; BERNDT/HOPPLER (Fn. 1), 2623 ff.; TORSTEN BRIEGEL, Einrichtung und Ausgestaltung unternehmensinterner Whistleblowing-Systeme, Wiesbaden 2009; JENS DÜSEL, Gespaltene Loyalität, Baden-Baden 2009; DIETER EISELE, in: Herbert Schimansky/Hermann-Josef Bunte/Hans Jürgen Lwowski (Hrsg.), Bankrechts-Handbuch, 3. Aufl., München 2007, § 109 N 1 ff.; HANS-JÜRGEN FRITZ, Whistleblowing – Denunziation oder Wettbewerbsvorteil, in: Frank Maschmann (Hrsg.), Corporate Compliance und Arbeitrecht, Baden-Baden 2009, 111 ff.; THOMAS KLEBE/ANDREJ WROBLEWSKI, Verbotene Liebe? Zur rechtlichen Zulässigkeit von Ethikrichtlinien, insbesondere von internen »Whistleblowing«-Systemen, in: Gedächtnisschrift Zachert, Baden-Baden 2010, 313 ff.; KATHRIN KORTE, Die Information des Aufsichtsrats durch die Mitarbeiter, Frankfurt/M. 2009, 119 ff.; JÜRGEN PAUTHNER-SEIDEL/HANS-JÜRGEN STEPHAN, in: Christoph E. Hauschka (Hrsg.), Corporate Compliance, 2. Aufl., München 2010, § 27 N 111 ff.; CHARLOTTE RAU, Compliance und Unternehmensverantwortlichkeit, Frankfurt/M. 2010, 41 ff.; ROLF SETHE, Erweiterung der bank- und kapitalmarktrechtlichen Organisationspflichten um Reporting-Systeme, ZBB 2007, 421 ff.; RAINER SIEG, Arbeitnehmer im Banne von Compliance-Programmen - zwischen Zivilcourage und Denunziantentum, in: Festschrift für Buchner, München 2009, 859, 865 ff.

15 Zuletzt ROLF H. WEBER/SALIM RIZVI, Compliance − Trojanisches Pferd vor den Toren der Wettbewerbsbehörden?, Zur Berücksichtigung von Compliance-Programmen in kartellrechtlichen Sanktionsverfahren, SJZ 106 (2010), 501, 505; ROLF H. WEBER, Prüfungsgegenstand und -umfang beim internen Kontrollsystem, SZW 2007, 472 ff.

schrieben (Art. 8 Abs. 2 BankV). (4) Die Bank muss die Grundzüge des Risikomanagements sowie die Zuständigkeit und das Verfahren für die Bewilligung von risikobehafteten Geschäften in einem Reglement oder in internen Richtlinien festlegen (Art. 9 Abs. 2 BankV). (5) Die interne Dokumentation der Bank über die Beschlussfassung und Überwachung der mit Risiko verbundenen Geschäfte ist so auszugestalten, dass sie der Prüfgesellschaft erlaubt, sich ein zuverlässiges Urteil über die Geschäftstätigkeit zu bilden (Art. 9 Abs. 3 BankV). (6) Die Bank muss für ein wirksames internes Kontrollsystem sorgen. Sie bestellt insbesondere eine von der Geschäftsführung unabhängige interne Revision (Inspektorat) (Art. 9 Abs. 4 BankV). Detailregelungen zu diesen Vorgaben finden sich im FINMA-RS 2008/24.[16]

Ist die Bank in der Rechtsform einer Kapitalgesellschaft verfasst, kommen (neben der allgemeinen Sorgfaltspflicht aus Art. 717 Abs. 1 OR) die entsprechenden gesellschaftsrechtlichen Organisationspflichten hinzu. (7) In Bezug auf das Interne Kontrollsystem und das Risikomanagement finden sich hierzu Vorgaben in Art. 728a Abs. 1 Ziff. 3, 728b Abs. 1, 663b Ziff. 12 OR. (8) Der Swiss Code of Best Practice for Corporate Governance enthält in seiner Ziff. 19 die Verpflichtung an den Verwaltungsrat, für ein dem Unternehmen angepasstes internes Kontrollsystem und Risikomanagement zu sorgen. (9) Die Corporate Governance-Richtlinie (RLCG) der Schweizer Börse von 2002 verpflichtet in Ziff. 3.6. die Unternehmen, Angaben zur Ausgestaltung der Informations- und Kontrollinstrumente des Verwaltungsrats gegenüber der Geschäftsleitung des Emittenten zu machen, wie z.B. interne Revision, Risikomanagement-System oder Management Information System (MIS).

Diese Entwicklung einer ständigen Ausweitung der Organisationspflichten ist keine nationale Besonderheit der Schweiz.[17] In der Europäischen Union wird der Ausbau der Organisationspflichten besonders augenfällig am Beispiel der MiFID[18] und ihrer Durchführungsrichtlinie.[19] Sie weiten die organi-

---

16 FINMA-RS 2008/24 „Überwachung und interne Kontrolle bei Banken“ vom 20.11.2008, mit dem das entsprechende RS 06/6 der EBK vom 27.9.2006 ersetzt wurde.

17 Zum europäischen und zum deutschen Recht vgl. etwa BOSCH, Organisationsverschulden in Unternehmen, Baden-Baden 2002; NATASCHA FISCHBACH, Organisationspflichten von Wertpapierdienstleistungsunternehmen nach § 33 Abs. 1 Nr. 1 WpHG, Hamburg 2000; ANNEMARIE MATUSCHE-BECKMANN, Das Organisationsverschulden, Tübingen 2001; GERALD SPINDLER, Unternehmensorganisationspflichten, Köln 2001.

18 Richtlinie 2004/39/EG über Märkte für Finanzinstrumente […], ABl. EU Nr. L 145 vom 30.4.2004, 1, berichtigt ABl. EU Nr. L 45 vom 16.2.2005, 18, vgl. hierzu PETER BALZER, Der Vorschlag der EG-Kommission für eine neue Wertpapierdienstleistungsrichtlinie, ZBB 2003, 177 ff.; HOLGER FLEISCHER, Die Richtlinie über Märkte für Finanzinstrumente und das Finanzmarkt-Richtlinie-Umsetzungsgesetz - Entstehung, Grundkonzeption, Regelungsschwerpunkte, BKR 2006, 389 ff.; ROLF SETHE, Anlegerschutz im Recht der Vermögensverwaltung, Köln 2005, 477 ff.; JULIANE THIEME, Wertpapierdienstleistungen im Binnenmarkt, Baden-Baden 2008; SIMONE WASSERER, Die Neuordnung des kapitalmarktrechtlichen Wohlverhaltens durch die MiFID, Innsbruck 2008.

19 Richtlinie 2006/73/EG zur Durchführung der Richtlinie 2004/39/EG, ABl. EU Nr. L 241 v. 2.9.2006, 26.

satorischen Vorgaben im Bereich der Wertpapierdienstleistungen stark aus. Deutschland geht sogar noch über diese Vorgaben hinaus und unterwirft die Compliance-Beauftragten nun einer besonderen Aufsicht.[20]

Es wird daher von einer zunehmenden „Verrechtlichung von Organisationsanforderungen" gesprochen.[21] Diese bergen die Gefahr einer Bürokratisierung. Zudem belegen die Erfahrungen, dass das Aufstellen gesetzlicher Organisationspflichten allein[22] nicht ausreicht, um Schädigungen von Kunden und Zusammenbrüche von Instituten völlig auszuschliessen. Sie müssen in der Praxis auch „gelebt" werden, denn gerade in komplexen Organisationsstrukturen lässt sich Fehlverhalten gut verbergen. An dieser Stelle zeigt sich die Bedeutung von Compliance.

III. Möglichkeiten zur Verhinderung von Fehlverhalten

1. Ausreichende Information und Kommunikation als Voraussetzung wirksamer Compliance

Die Compliance-Funktion umfasst insbesondere die Überwachung der Einhaltung gesetzlicher und unternehmensinterner Regeln (Prävention), die Aufdeckung von regelwidrigem Verhalten sowie das Management von Interessenkonflikten. Dass zu den Aufgaben des Verwaltungsrats auch die Compliance gehört, ergibt sich aus Art. 716a Abs. 1 Ziff. 1 und 5 OR. Die eigentliche Aufsicht (nicht Oberaufsicht) wird regelmässig an ein Audit Committee, einen Compliance Officer etc. übertragen. Der Verwaltungsrat hat Compliance lediglich sicherzustellen.[23]

Ihre Aufgaben kann die Compliance-Stelle nur wahrnehmen, wenn sie über ausreichende Informationen verfügt. Hier bieten sich verschiedene Wege an: (1) Sie kann diese Informationen aus einem Beschwerdewesen erlangen. Dieses wird – dies zeigt die praktische Erfahrung – aber oft nur bemüht, wenn ein Schaden bereits eingetreten ist; es ist daher zur Prävention von Fehlverhalten nur bedingt geeignet. (2) Die Compliance-Stelle kann auf die Ergeb-

[20] Vgl. Art. 1 Ziff. 8 des Entwurfs eines Gesetzes zur Stärkung des Anlegerschutzes und Verbesserung der Funktionsfähigkeit des Kapitalmarkts, BR-Drucks. 584/10, vgl. zu dieser Reform ROLF SETHE, Verbesserung des Anlegerschutzes?, ZBB 2010, 265 ff.

[21] SPINDLER (Fn. 17), 186 ff.; GERALD SPINDLER/ROMAN A. KASTEN, Organisationspflichten nach der MiFID und ihre Umsetzung, AG 2006, 785; SETHE, Reporting-Systeme (Fn. 14), 422.

[22] Neben den Organisationsvorgaben entfaltet auch das Haftungsrecht mit seiner präventiven Steuerungsfunktion eine wichtige Rolle. Es wirkt jedoch nur mittelbar, zumal Verantwortlichkeitsansprüche in der Praxis häufig nur im Konkursfall geltend gemacht werden, ROLF SETHE, in: Rolf Watter (Hrsg.), Die «grosse» Schweizer Aktienrechtsrevision, SSHW Band 300, Zürich 2010, 299, 306 f.

[23] Dazu HERBERT G. BUFF, Compliance. Führungskontrolle durch den Verwaltungsrat, Zürich 2000, N 116 ff.; BÖCKLI, Schweizer Aktienrecht, Zürich, Basel, Genf, 4. Aufl. 2009, § 13 N 378 ff.

nisse des Internen Kontrollsystems zurückgreifen. (3) Möglich ist auch der Weg, Meldepflichten aufzustellen. Wer jedoch gegen betriebsinterne Regeln verstösst, wird u.U. auch solche Meldepflichten ignorieren. Hinzu kommt, dass der Informationsfluss von der Mitarbeiterebene hin zur Compliance-Stelle häufig durch eine hierarchische Struktur im Unternehmen blockiert oder zumindest ausgedünnt wird. Die Compliance-Stelle ist daher darauf angewiesen, authentische Meldungen der unmittelbar Betroffenen zu erhalten. (4) In diesem Zusammenhang wird das sog. Whistleblowing als ein denkbares[24] Mittel zur Informationsbeschaffung genannt.

Unter Whistleblowing versteht man das Melden eines illegalen oder unethischen Verhaltens an Dritte mit dem Ziel, dass der Regelverstoss untersucht und abgestellt wird.[25] Der Meldende ist regelmässig Mitarbeiter des betroffenen Unternehmens; das Whistleblowing ist jedoch hierauf nicht beschränkt, sondern erfasst auch sonstige Personen, die Kenntnis von Missständen in einem Unternehmen erlangen (z.B. Beauftragte des Unternehmens, Geschäftspartner oder Nachbarn). Beim sog. internen Whistleblowing geht die Meldung an Personen, die innerhalb des Unternehmens beschäftigt sind oder die als Dienstleister für das Unternehmen solche Meldungen intern entgegennehmen (z.B. Rechtsanwälte). Beim – für das Unternehmen wesentlich gravierenderen – externen Whistleblowing werden Personen informiert, die ausserhalb des Unternehmens angesiedelt sind, wie z.B. Strafverfolgungsbehörden, Verbände, Medien.

2. Die Diskussion um das Whistleblowing

Aufgrund spektakulärer Einzelfälle tauchte das Thema Whistleblowing immer mal wieder kurzzeitig in der öffentlichen Diskussion auf.[26] Im juristischen Schrifttum erfährt es hierzulande[27] eine grössere Aufmerksamkeit seit

[24] Eine Verpflichtung zur Errichtung von Whistleblowing-Systemen besteht bislang weder aus Gesetz noch Selbstregulierung. Das Vorhaben der Eidgenössischen Bankenkommission, im Rundschreiben betreffend Überwachung und interne Kontrolle solche Systeme (s.o. Fn. 16) vorzuschreiben, wurde fallen gelassen, s. VON KAENEL (Fn. 14), 314; STRASSER (Fn. 14), 490 f. Auch im deutschen Recht besteht noch keine Verpflichtung zur Errichtung solcher Systeme, s. UWE H. SCHNEIDER/CLAUDIA NOWAK, Sind die Einrichtung einer Whistleblowing-Stelle und der Schutz des Whistleblowers Teil guter Corporate Governance?, in: Günther Hönn/Hartmut Oetker/Thomas Raab (Hrsg.), Festschrift für Kreutz, Köln 2010, 855, 864 f.; VON ZIMMERMANN (Fn. 1), 1061.

[25] Hierzu und zum Folgenden LEDERGERBER (Fn. 14), N 9; VON KAENEL (Fn. 14), 309; SILVIA HUNZIKER, Whistleblowing, in: Festschrift von der Crone, Zürich 2007, 164 f.

[26] Vgl. die Aufstellung im Erläuternden Bericht zum Vorentwurf, 3 Fn. 4, http://www.ejpd.admin.ch/ejpd/de/home/themen/wirtschaft/ref_gesetzgebung/ref_whistleblowing.html.

[27] Zur relativ jungen Geschichte des Whistleblowings LEDERGERBER (Fn. 14), N 159 ff. In den USA findet sich die erste umfassendere Veröffentlichung zum Thema bereits 1972, vgl. RALPH NADER/PETER BETKAS/KATE BLACKWELL, Whistle-Blowing, The Report on a Conference on Professional Responsibility, New York 1972.

den beiden 2003 eingebrachten Motionen von REMO GYSIN[28] und DICK MARTY,[29] die auf den Schutz des Whistleblowers vor Diskriminierung und Kündigung abzielten.[30] Diese mündeten 2008 in einen Vorentwurf.[31] Die Vernehmlassung offenbarte sehr gegensätzliche Standpunkte. Einem Teil der Vernehmlassungsteilnehmer genügte das geltende Recht. Genauso fanden sich aber auch Äusserungen für eine Revision oder gar weitergehende Standpunkte, die die vorgeschlagenen Änderungen für zu wenig streng hielten, da sie nicht ausreichten, um einen Missstände meldenden Arbeitnehmer wirkungsvoll zu schützen. Besonders hervorgehoben wurde dabei die fehlende Strenge der Sanktion im Fall einer Rachekündigung. Der Bundesrat entschloss sich zu einer zweiten Vernehmlassung, bei der die Wirksamkeit der Sanktionen gegen eine ungerechtfertigte Kündigung im Mittelpunkt stand und die bis zum 14.1.2011 lief.

Das Thema hat für Schweizer Unternehmen aus zwei Gründen eine grosse Bedeutung. (1) Unternehmen erleiden durch deliktische Handlungen enorme Schäden; man schätzt diese für das Jahr 2003 auf 8,7 bis 17,4 Mrd. CHF.[32] (2) Im Jahre 2005 nutzten bereits 42% der Unternehmen die Möglichkeit, eine unabhängige Instanz innerhalb oder ausserhalb des Unternehmens zu schaffen, die Meldungen entgegennimmt. Bei grossen Unternehmen waren es 45%, bei SOX-Gesellschaften gar 71%.[33] Inzwischen haben sich Firmen etabliert, die solche Whistleblowing-Systeme für private Unternehmen und Behörden vertreiben, nämlich die schweizer Firma *Integrity Line GmbH*,[34] die US-amerikanischen Firmen EthicsPoint, Inc.[35] und Global Compliance[36] und die deutsche *Business Keeper AG*.[37]

Dass Whistleblower Mobbing oder Kündigungen ausgesetzt sind, beruht auf dem Umstand, dass viele Chefs und Mitarbeiter in jemandem, der auf unternehmensinterne Missstände hinweist, einen Verräter sehen.[38] Es herrscht

---

28 Motion vom 7.5.2003, NR 03.3212.

29 Motion vom 19.6.2003, SR 03.3344.

30 Hierzu und zum Folgenden Erläuternder Bericht zum Vorentwurf, http://www.ejpd.admin.ch/ejpd/de/home/themen/wirtschaft/ref_gesetzgebung/ref_whistleblowing.html. Der Bericht enthält auf S. 3 Fn. 4 auch zahlreiche Beispiele für Fälle, in denen Arbeitnehmer Repressalien erlitten, nachdem sie kriminelles Verhalten in Unternehmen oder Behörden aufdeckten.

31 Vorentwurf zur Teilrevision des Obligationenrechtes (Schutz bei Meldung von Missständen am Arbeitsplatz) vom 5. Dezember 2008.

32 BERNDT/HOPPLER (Fn. 1), 2626.

33 KPMG UND INSTITUT FÜR RECHNUNGSWESEN UND CONTROLLING DER UNIVERSITÄT ZÜRICH, Interne Kontrolle in der Schweizer Praxis – Eine aktuelle Standortbestimmung, 2005, 55, http://www.irc.uzh.ch/fileadmin/downloads/forschung/studien/meyer/KPMG_Studie_397869.pdf.

34 http://www.integrityline.org.

35 http://www.ethicspoint.com.

36 https://www.compliance-helpline.com und http://www.globalcompliance.com.

37 http://www.business-keeper.com.

38 Dazu BRIEGEL (Fn. 14), 3 f. mit umfassenden Nachweisen. Auch in den USA, die eine längere Whistleblowing-Tradition haben, ist dieses Phänomen zu beobachten, vgl. ALEXAN-

ein Korpsgeist innerhalb von Unternehmen und Behörden, frei nach dem Satz von AUGUST HEINRICH HOFFMANN VON FALLERSLEBEN (1798-1874): „Der grösste Lump im ganzen Land, das ist und bleibt der Denunziant". In Deutschland sieht man dieses Thema nach zwei Diktaturen, deren Machterhalt ganz wesentlich auf Denunziationen beruhte, nochmals sensibler als hierzulande.[39] Der Begriff der Denunziation hat eine negative Konnotation und wird vor allem in repressiven politischen Systemen verwendet, wenn Bürger bei staatlichen Vollzugsbehörden angezeigt werden, obwohl dem Anzeigenden klar sein muss, dass er sie damit der Gefahr der politisch motivierten Verfolgung aussetzt. Dem Begriff nach liegt dagegen keine Denunziation vor, wenn die Anzeige gesellschaftlich akzeptiert ist, wie etwa bei Straftaten gegen Leib und Leben. Entscheidende Unterschiede sind also die innere Motivation des Anzeigenden,[40] das mit der Anzeige verfolgte Ziel sowie die gesellschaftliche Akzeptanz einer Anzeige. Neben diesen ist zu berücksichtigen, ob es sich um die Möglichkeit freiwilliger Meldungen handelt oder nicht. Wird eine Pflicht zu Meldungen aufgestellt, ist dies problematisch, da ein Eingriff in das Persönlichkeitsrecht des Arbeitnehmers erfolgt.[41]

Diese Kriterien lassen sich auch auf das Whistleblowing übertragen. Beim Korpsgeist handelt es sich, sofern fremde Rechtsgüter *erheblich* gefährdet sind, um falsch verstandene Solidarität, denn die Schäden, die durch Nichtmeldung von Fehlverhalten entstehen können, sind beträchtlich. Oft sind zudem keine ausreichenden Strukturen für den angemessenen Umgang mit unternehmensinternen Meldungen vorhanden und es fehlt an einer Unternehmenskultur, die hausinterne Meldungen schätzt. Wie fatal dies sein kann, zeigt der Fall von ROGER BOISJOLY, der vor der Challenger-Katastrophe eindringlich auf die undichten Dichtungsringe hinwies, aber nicht ernst genommen wurde. Funktionierendes Whistleblowing kann also u.U. Menschenleben retten.

Zu berücksichtigen ist noch ein weiterer Aspekt. Die negativen Auswirkungen von Whistleblowing auf Unternehmen sind dann besonders gross, wenn es sich um externes Whistleblowing handelt, die Informationen also an die Staatsanwaltschaft oder die Presse gelangen. Schafft man dagegen unternehmensintern ein Forum, in dem Meldungen erstattet werden können, tritt in den allermeisten Fällen gerade kein Reputationsverlust ein, sondern das Unternehmen kann Missstände rechtzeitig selbst abstellen. Dies allerdings setzt

---

DER DYCK/ADAIR MORSE/LUIGI ZINGALES, Who Blows the Whistle on Corporate Fraud?, http://ssrn.com/abstract=891482, 34 f. und Table 8.

39 REGINA OGOREK, Whistleblowing – oder vom Verpfeifen im Arbeitsrecht und anderswo, in: Liber amicorum M. Weiss, Berlin 2005, 539, 540; KLEBE/WROBLEWSKI (Fn. 14), 318 ff.

40 Eine völlig neue Motivation haben die USA geschaffen, indem man dem Whistleblower erhebliche finanzielle Anreize bietet, vgl. oben Fn. 2 und 3.

41 Dazu ausführlich KLEBE/WROBLEWSKI (Fn. 14), 317; ANJA MENGEL, in: Hauschka (Fn. 14), § 12 N 38.

voraus, dass solche Meldungen auch ernst genommen werden, man also eine entsprechende Unternehmens- und Fehlerkultur entwickelt hat. Diejenigen Unternehmensleiter, die *externe* Whistleblower in Bausch und Bogen verdammen, müssen sich also die Gegenfrage gefallen lassen, warum sie kein Forum für *betriebsinterne* Meldungen geschaffen haben, bzw. warum sie eine Meldung nicht ernst genommen haben, als diese zunächst *betriebsintern* erfolgte. Wer bei berechtigter Kritik bewusst wegschaut und dadurch Rechtsgüter anderer oder Arbeitsplätze gefährdet, hat seinerseits kein Recht, jemanden als Verräter oder Denunzianten zu brandmarken.[42] Eine davon zu trennende Frage ist diejenige des Mobbing durch Whistleblowing, auf die ebenfalls noch zurückzukommen sein wird (siehe unten IV. 4 a). Wie erfolgreich ein internes Whistleblowing sein kann, soll im Folgenden anhand der Erfahrungen in der Flugindustrie und der Medizin aufgezeigt werden.[43] [44]

IV. Critical Incident Reporting-Systeme als besondere Form des Whistleblowing

1. Die Entwicklung von Reporting-Systemen im Bereich der Luftfahrt

a) Technisches und menschliches Versagen

Aufgrund der Gefahrenträchtigkeit und des enormen Schadenspotentials hat die Flugindustrie frühzeitig begonnen, Vorsorge gegen Schadensfälle zu treffen und verfügt deshalb über eine reichhaltige Erfahrung (Einführung und Verbesserung von Sicherheitsstandards, Schulungen, technische Verbesserungen, wie Flight- und Voice-Recorder). Dennoch kam es immer wieder zu Unfällen oder Beinahkatastrophen aufgrund von menschlichem Versagen. Mit der Einführung des Computers verband man die Erwartung, man könne nun endlich den menschlichen Faktor ausschalten. Heute wissen wir, dass die Hoffnung nicht erfüllt wurde; zwar wurde die relative Anzahl der Zwischen-

[42] Ebenso PORTMANN (Fn. 9), 994.

[43] Dazu bereits SETHE, Reporting-Systeme (Fn. 14), 433 ff.

[44] Nicht eingegangen werden kann auf arbeits- und datenschutzrechtliche Fragen, dazu HUNZIKER (Fn. 25), 163 ff.; PORTMANN (Fn. 9), 987 ff; PORTMANN/WOHLMANN (Fn. 14), 179 ff.; STRASSER (Fn. 14), 493 ff.; VON KAENEL (Fn. 14), 314 ff. jeweils m.w.N.; zum deutschen Recht BVerfG, NJW 2001, 3474; BAG, NJW 2004, 1547; LAG Düsseldorf, ZIP 2006, 436 – Wal-Mart; BARTHEL/HUPPERTZ, Arbeitsrecht und Datenschutz bei "Whistleblower-Klauseln", AuA 2006, 204 ff.; DÜSEL (Fn. 14), 40 ff.; STEPHAN R. M. FAHRIG, Verhaltenskodex und Whistleblowing im Arbeitsrecht, NJOZ 2010, 975 ff.; ANJA MENGEL, MICHAEL SCHMIDL und LUTZ NEUNDORF, in: Hauschka (Fn. 14), § 12 N 89 ff., § 29 N 276 ff., § 30 N 27 ff.; MICHAEL MÜLLER, Whistleblowing – Ein Kündigungsgrund?, NZA 2002, 424 ff.; GERLIN WISSKIRCHEN/ANKE KÖRBER/ALEXANDER BISSELS, 'Whistleblowing' und 'Ethikhotlines', Probleme des deutschen Arbeits- und Datenschutzrechts, BB 2006, 1567 ff.; GEORG VON ZIMMERMANN, Whistleblowing und Datenschutz, RDV 2006, 242 ff.

fälle reduziert, aber immer noch beruhen 75% aller Schadensfälle auf menschlichem Versagen[45] bzw. auf einer Kombination von technischem Versagen gefolgt von menschlichem Fehlverhalten (z.B. Arbeitsbelastung, Kommunikationsfehler, Ausbildungs- und Überwachungsprobleme, ungenügende Ressourcen oder ungenügende Teamarbeit).[46] Eine Analyse zeigt rasch, dass der Computer nur so gut ist, wie der ihn programmierende Mensch oder sein Benutzer. Die von Menschen entworfenen Sicherheitsvorkehrungen sind daher nie vollkommen und weisen unerkannte Sicherheitslücken auf. Eine erhebliche Schwachstelle ist auch der User. In unglücklichen Konstellationen kann es nun zu einer Kumulation von Fehlern und damit dem Versagen der Sicherheitsbarrieren kommen.[47] Diese Feststellungen sollen jedoch nicht den Blick darauf verstellen, dass sich die Anstrengungen der Luftfahrtindustrie auszahlen, da die Zahl der Flugkatastrophen in Relation zur gestiegenen Kilometerleistung und Passagierzahl gesunken und im Ergebnis sehr gering ist. Erheblicher ist dagegen die Zahl der Beinahkatastrophen. Unbekannt ist die Anzahl von Zwischenfällen, die verheimlicht werden und die ein enormes Potential als Erkenntnisquelle für Verbesserungen aufweisen, wie im Folgenden zu zeigen ist.

b) Umgang mit Fehlern

Das Verheimlichen eigener Fehler liegt in der menschlichen Natur und beruht vor allem auf der Angst vor Sanktionen. Dem entspricht spiegelbildlich die Reaktion des Vorgesetzten, wenn ihm Fehlverhalten zu Ohren kommt. Er lobt nicht das Zugeben des Fehlers und allfällige Verbesserungsvorschläge, sondern konzentriert sich auf das Fehlverhalten und spricht Sanktionen aus. Es ist nur allzu menschlich, wenn der Chef „Dampf ablässt" und den „Schuldigen" massregelt.[48] Gerade die Angst des Mitarbeiters vor Zurechtweisung oder Sanktionen verhindert damit eine Auswertung des Fehlers. Der aus Angst ausgelöste Drang zur Verheimlichung von Fehlern steigt, wenn sich ein Zwischenfall wiederholt. Das erneute Auftreten eines Fehlverhaltens müsste an sich Anlass dafür sein, die internen Abläufe grundlegend zu verbessern;

---

45 MANFRED MÜLLER, Safety lessons taken from the airlines, British Journal of Surgery 91 (2004), 393.

46 M. KAUFMANN/S. STAENDER/G. VON BELOW/H. H. BRUNNER/L. PORTENIER/D. SCHNEIDEGGER, Computerbasiertes anonymes Critical Incident Reporting: ein Beitrag zur Patientensicherheit, Schweizerische Ärztezeitung 2002, 2554 m.w.N.

47 Erinnert sei nur an das letzte grosse Flugunglück der Schweiz, den Zusammenstoss zweier Maschinen über dem Bodensee am 1.7.2002, das ausweislich des Untersuchungsberichts auf einer Verkettung von verschiedenen, jeweils für sich nicht ausschlaggebenden Ursachen beruhte, http://www.bfu-web.de/nn_41544/DE/Publikationen/Untersuchungsberichte/2002/Bericht__02__AX001-1-2,templateId=raw,property=publicationFile.pdf/Bericht_02_AX001-1-2.pdf, 109 ff.

48 JAMES REASON, Human error: models and management, British Medical Journal 320 (2000), 768.

dennoch wird kein vernünftig denkender Mitarbeiter zu seinem Vorgesetzten gehen und die Wiederholung des Fehlers melden. Macht ein Kollege einen Fehler, wird dieser regelmässig aus Gründen des Korpsgeistes (s.o.) verschwiegen.

Ein Unternehmen, in dem solche Anreizstrukturen und Verhaltensweisen vorherrschen, verfügt nicht über eine ausreichende „Fehlerkultur".[49] Wenn die Geschäftsführung von Zwischenfällen im Unternehmen nichts erfährt, kann sie diese auch nicht auswerten und aus ihnen nichts lernen. Das Sprichwort „Aus Schaden wird man klug" gilt für Individuen, die aus Erfahrungen lernen. Arbeitsteilige Organisationen können aus Fehlern nur lernen, wenn sie nicht auf individueller Ebene verbleiben, sondern in das Bewusstsein der Organisation gehoben werden.[50] Während Katastrophen und Beinahkatastrophen aufgrund des Grades der Aufmerksamkeit, den sie erhalten, regelmässig von der ganzen Organisation zur Kenntnis genommen werden, gilt dies naturgemäss nicht für verheimlichte Zwischenfälle. Bildlich gesprochen haben wir es hier mit einem Eisberg zu tun. Oberhalb der Wasseroberfläche findet sich das eine Siebtel, in dem Schadensfälle und Beinahkatastrophen erkannt und gemeldet werden. Unter der Wasseroberfläche schlummern sechs Siebtel an Zwischenfällen, die wir bislang nicht kennen und die wir nutzen könnten, um effektive Gegenmassnahmen zu ergreifen.

c) Reaktion der Flugindustrie

Dies hat die Flugindustrie sehr früh erkannt und daher Fehleranalysen und Reporting-Systeme eingeführt.[51] Um Sicherheitsprobleme aufzudecken, wurde 1975 in den USA schliesslich das *Aviation Safety Reporting System* (ASRS) eingeführt.[52] Es handelt sich um ein anonymes, sanktionsfreies Reporting-System, in das unerwünschte Zwischenfälle eingegeben werden können. Die Daten werden systematisch ausgewertet und tragen erheblich zur Verbesserung der Flugsicherheit bei. Grossbritannien folgte diesem Modell mit dem *Confidential Human Factors Incident Reporting Programme*.[53]

Welch positive Erfahrungen mit einem solchen Reporting-System gemacht werden können, wurde von einem mit Luftsicherheit befassten Redner auf einer Tagung anhand des folgenden, recht skurrilen Beispiels aufge-

[49] Grundlegend dazu REASON (Fn. 48), 768 ff.; s.a. CHRISTIAN THOMECZEK/JULIA ROHE/GÜNTER OLLENSCHLÄGER, Incident Reporting Systeme – in jedem Zwischenfall ein Fehler?, in: Burkhard Madea/Reinhard Dettmeyer (Hrsg.), Medizinschadensfälle und Patientensicherheit, Köln 2007, 169.

[50] SETHE, Reporting-Systeme (Fn. 14), 433.

[51] Zu Einzelheiten SETHE, Reporting-Systeme (Fn. 14), 433 f.

[52] http://asrs.arc.nasa.gov/main.htm.

[53] http://www.chirp.co.uk.

zeigt:[54] Ein Kampfjetpilot flog mit einer Beobachtungsmission bei Nacht über die Nordsee. Da die Mission langweilig und der Pilot neugierig war, vertrieb er sich die Zeit damit, herauszufinden, wie eines seiner Instrumente funktioniert. Zu diesem Zwecke hat er das Cockpit aufgeschraubt, um dieses Instrument auszubauen. Dies verursachte in der Bordelektronik einen Kurzschluss. Sein gesamtes Instrumentenbrett wurde schlagartig dunkel und der Pilot war bei Überschallgeschwindigkeit ohne Orientierung. Seine einzige Rettung bestand im Einschalten der Notstromversorgung durch Druck auf den entsprechenden Schalter, der links vom Pilotensitz angebracht war. Fatalerweise befand sich auch der Auslöser für den Schleudersitz links am Sitz. Die Chancen des Piloten, den richtigen Schalter zu drücken, lagen also bei 50:50. Zum Glück hat er den richtigen Knopf getroffen und konnte mittels Notstromsystem sicher zurückkehren. Dieser Zwischenfall war so karriereschädlich, dass er um jeden Preis verheimlicht werden musste. Dass wir heute von ihm wissen, verdanken wir einem Reporting-System, in das der Pilot anonym den Vorfall eingeben konnte. Seitdem sind die Schalter für Notstrom und Schleudersitz auf verschiedenen Seiten des Sitzes angebracht. Ohne ein solches System hätte es erst eines Unfalls bedurft, um diesen Fehler aufzudecken (sofern der Pilot diesen überlebt und noch auf das Problem hätte aufmerksam machen können).

2. Die Entwicklung von Reporting-Systemen im Bereich der Medizin

a) Entwicklung von CIRS

In Spitälern ereignen sich täglich patientengefährdende oder gar patientenschädigende Zwischenfälle. Betroffen sind etwa 10% aller stationären Aufenthalte. Rund 50% der Ereignisse wären vermeidbar.[55] In dem Bestreben, Kunstfehler zu vermeiden, hat die Medizin Anleihen bei der Flugindustrie genommen. Neben den klassischen Möglichkeiten zur Fehlerauswertung und -vermeidung,[56] also der Analyse von Schadensfällen „oberhalb der Wasserlinie", ist man bestrebt, neue Wege zu gehen und die „verborgenen Bereiche unterhalb der Wasseroberfläche" für die Prävention zu nutzen: Am Universitätsspital Basel wird seit langem erfolgreich mit einem *Critical Incident Re-*

[54] MANFRED MÜLLER, Sicherheitskultur im Gesundheitswesen - Können wir von der Luftfahrt lernen?, Vortrag auf dem Fachworkshop "Fehlervermeidung und Sicherheitskultur im Gesundheitswesen" der Ärztekammer Berlin und des AOK-Bundesverbandes, 28.4.2004.

[55] NORBERT ROSE/URS HESS, Melden von Near Misses im Krankenhaus, Der Onkologe 2008, 1.

[56] Beispiele bei KAUFMANN/STAENDER/VON BELOW/BRUNNER/PORTENIER/SCHNEIDEGGER (Fn. 46), 2555; URSINA PALLY, Arzthaftung mit den Schwerpunkten Schwangerschaftsbetreuung und Geburtshilfe, Zürich 2007, 340 ff.

porting System (CIRS) gearbeitet.[57] Das System wurde 1995 auf Anregung von ROBERT HELMREICH, Department of Psychology der Universität Texas in Austin, USA, entwickelt, der seinerzeit Gastprofessor in Basel war. 1996 wurde die erste Version von CIRS im Intranet des Departments freigeschaltet. Im Jahre 1998 wurde CIRS dann zu einem nationalen Projekt der Schweizer Gesellschaft für Anästhesiologie und Reanimation (SGAR). Soweit ersichtlich, war es damit neben einem australischen System[58] das erste nationale Reporting-System im Bereich der Medizin. Seit 2001 ist CIRS bei der im selben Jahr gegründeten Stiftung für Patientensicherheit in der Anästhesie angesiedelt. Im April 2001 hat eine internationale Expertenkommission auf Einladung des Bundesamtes für Sozialversicherung in Luzern eine Empfehlung zum nationalen Risk-Management in der Schweiz erarbeitet. Diese Arbeitsgruppe empfiehlt ausdrücklich auch „Incident Reporting" als eine notwendige Massnahme.[59] Um das Ziel eines einheitlichen Reportings von kritischen Ereignissen im gesamten schweizerischen Gesundheitswesen zu verwirklichen, gründeten die Verbindung der Schweizer Ärztinnen und Ärzte (FMH), die Gesellschaft schweizerischer Amts- und Spitalapotheker und der schweizerische Berufsverband für Krankenpflege im Jahre 2002 CIRSmedical, die nun ein fächerübergreifendes Reporting-System betreibt.[60]

b) Funktionsweise des Systems

Bei CIRS kann jeder Klinikmitarbeiter anonym in einer den Bediensteten der angeschlossenen Kliniken offenstehenden Internetmaske kritische Zwischenfälle eingeben.[61] Der Meldende gibt an, in welcher Funktion er tätig war, ob er das kritische Ereignis verursacht oder nur beobachtet hat, ob der Patient geschädigt wurde und wie sich der Zwischenfall im Detail ereignete. Das Reporting-System wird von weisungsunabhängigen Mitarbeitern verwaltet, die dafür sorgen, dass die Meldungen anonym bleiben (z.B. durch Löschen der IP-Adresse des Rechners, von dem aus gemeldet wurde etc.).

---

57 Zum Folgenden http://www.cirs.ch/history.pdf; siehe auch S. STAENDER/J. DAVIES/B. HELMREICH/B. SEXTON/M. KAUFMANN, The anaesthesia critical incident reporting system: an experience based database, International Journal of Medical Informatics 47 (1997), 87 ff.

58 R.K. WEBB/M. CURRIE/C. A. MORGAN ET AL., The Australian Incident Monitoring Study: An Analysis of 2000 Incident Reports. Anaesth.Intensive.Care 21 (1993), 520 ff.

59 H. H. BRUNNER/D. CONEN/P. GÜNTER/M. VON GUNTEN ET. AL., Task Force Towards a safe Healthcare System, Proposal for a National Programme on Patient Safety Improvement for Switzerland, Luzern 4/2001, 16 f., http://www.swiss-q.org/pdf/Final_ReportE.pdf.

60 http://www.cirsmedical.org.

61 Hierzu und zum Folgenden M. KAUFMANN/D. SCHEIDEGGER, Anonymes Critical Incident Reporting: Ein Beitrag zur Patientensicherheit (Lernen aus Fehlern), Synapse, März 2004, 1 ff.; MARTINA MERTEN, Fehlermeldesysteme - Schweiz als Vorreiter, Deutsches Ärzteblatt 101 (2004), A 162.

c) Beispiele für Erfolge

Auswertungen zeigen, dass CIRS zu einer deutlichen Verbesserung der Sicherheit in der Medizin beiträgt.[62] Folgende Elemente haben sich als wesentlich für den Erfolg eines CIRS herauskristallisiert:[63]

sanktionsfrei	Berichterstatter müssen keine Sanktionen gegen sich oder andere befürchten.
streng vertraulich	Die Identität von Berichterstatter, Patient und Einrichtung bleibt verborgen.
unabhängig	Das Berichtssystem ist unabhängig von Behörden oder Organisationen und Sanktionsgewalt gegenüber Berichterstattern oder Einrichtungen.
Analyse durch Experten	Die Berichte werden durch Experten ausgewertet, die klinische Umstände verstehen und Fachwissen im Hinblick auf das Erkennen von zugrunde liegenden Systemursachen haben.
zeitnahe Rückmeldung	Berichte werden rasch analysiert und die abgeleiteten Empfehlungen – insbesondere beim Erkennen grosser Risiken – schnell an die Verantwortlichen vor Ort weitergeleitet.
systemorientiert	Empfehlungen richten sich auf Systemänderungen, Prozesse oder Produkte und zielen nicht auf individuelle Performanz.
gut reagierend	Die Träger des Berichtssystems sind zur Dissemination von Empfehlungen in der Lage. Teilnehmende oder angeschlossene Organisationen verpflichten sich, wo immer möglich die Empfehlungen zur Sicherheitsverbesserung umzusetzen.

Meldungen in einem CIRS bringen oft aussergewöhnliche Zwischenfälle ans Licht.[64] Ein bekanntes Beispiel betrifft die Verwechslung von Arzneimitteln. Früher hatten Medikamente *desselben* Herstellers höchst unterschiedliche Verpackungen, deren Gestaltung zufällig gewachsen war. Diese Optik war teilweise über Jahrzehnte gleich und damit unverwechselbar. In den 90er Jahren begann die Werbeindustrie, im Bereich der Pharmazie eine Corporate Identity durchzusetzen. Dies hatte zur Folge, dass plötzlich Arzneimittelpackungen eines Herstellers gleich aussahen und sich nur noch in der Beschrif-

62 ROSE/HESS (Fn. 55), 1.

63 Tabelle nach LUCIAN L. LEAPE, Reporting of adverse events, N Engl J Med 347 (2002), 1633, table 2; ebenso in deutscher Übersetzung JÖRG LAUTERBERG, in: Dieter Hart/Heiko Mattern/Monika Trent/Jörg Lauterberg (Hrsg)., Risiken verringern, Sicherheit steigern, Köln 2009, 27.

64 Umfangreiche Beispiele bei AKTIONSBÜNDNIS PATIENTENSICHERHEIT, Empfehlungen zur Einführung von Critical Incident Reporting Systemen (CIRS), 21 ff., http://www.german-coalition-for-patient-safety.org/apsside/07-11-27_CIRS_Brosch__re.pdf.

tung unterschieden. Die Zahl unterschiedlicher Packungsarten und -farben ging stark zurück und alle Produkte eines Herstellers sahen sich sehr ähnlich. Hierdurch wurde eine Vielzahl von Verwechslungen bei Medikamenten verursacht. Diese Fehlerquelle wurde allein durch CIRS aufgedeckt, denn welcher Arzt oder Pfleger würde zugeben, durch eine Medikamentenverwechslung den Tod eines Patienten verursacht zu haben. Heute wird das Design von Arzneimittelpackungen wieder unterschiedlich gestaltet, um die Warnfunktion zu erhöhen, oder Medikamente werden in den Spitälern umverpackt.

d) Weitere Verbreitung

Aufgrund der positiven Erfahrungen in der Schweiz und in Australien haben auch andere Länder (z.B. USA,[65] Grossbritannien[66] und Deutschland[67]) mit der Erprobung von Reporting-Systemen begonnen.

3. Die Vor- und Nachteile von Reporting-Systemen

Critical Incident Reporting-Systeme gewährleisten die Authentizität von Meldungen, da diese von Personen stammen, die an dem Vorfall beteiligt waren. Ist das System im Unternehmen akzeptiert, erlaubt die Vielzahl von Meldungen eine systematische Auswertung, was die Erfahrungen im Bereich der Medizin belegen. Erfasst werden auch seltene, atypische Zwischenfälle. Treten solche mehrfach auf, ist dies ein Anzeichen für einen Organisations- oder Prozessfehler. Schwachstellen werden sehr viel früher erkannt. Durch die Anonymität der Reporting-Systeme wird die Bereitschaft der Beteiligten erzeugt und erhöht, sich zu beteiligen. Dies allein ist jedoch nicht ausreichend. Wie bereits dargelegt, gilt es auch, das Vorurteil des Denunziantentums zu überwinden, so dass der Erfolg eines Reporting-Systems ganz massgeblich davon abhängt, welchen Stellenwert ihm das Unternehmen einräumt. Letztlich geht es also um die Unternehmenskultur und -ethik.[68]

Das Recht konzentriert sich in Haftungsfällen bisher auf den Ausgleich schon eingetretener Schäden, auf Strafverfolgung und Entlassung der Schadensverursacher. Gerade durch die drohenden Sanktionen wird der Anreiz gesetzt, Schadensfälle zu verheimlichen. Dies wiederum trägt dazu bei, dass sich kritische Zwischenfälle wiederholen können. Diesen Kreislauf gilt es zu

---

65 Positiv ist etwa der Bericht über das Medical Error Tracking System (METS), https://www.doctorquality.com/www/news/news_070001.htm. Siehe zur Manufacturer and User Facility Device Experience Database - (MAUDE), http://www.fda.gov/cdrh/maude.html.

66 Dazu JOHN AMOORE/PAULA INGRAM, Learning from adverse incidents involving medical devices, British Medical Journal (BMJ) 325 (2002), 272.

67 MERTEN (Fn. 61), A 162 sowie www.jeder-fehler-zaehlt.de und http://www.cirs-notfallmedizin.de.

68 Zu den Unterschieden zwischen der US-amerikanischen und der europäischen Unternehmenskultur vgl. PORTMANN/WOHLMANN (Fn. 14), 179.

durchbrechen. Erforderlich ist daher auch ein Umdenken für Juristen. Reporting-Systeme bieten hierzu die Möglichkeit. Gerade wenn man die Erfolge im Bereich der Medizin betrachtet, wird dies offensichtlich. Angesichts der erheblichen Schäden, die durch Behandlungsfehler drohen, ist hier interessanterweise auch der Vorwurf des Denunziantentums viel seltener zu hören, da den Mitarbeitern der Sinn dieser Systeme sofort einleuchtet.[69] Im Bereich der Korruptionsbekämpfung oder anderer Missstände in Unternehmen ist dagegen die Bereitschaft zu Meldungen oft geringer. Offenbar rechtfertigt unternehmerischer Erfolg in vielen Unternehmen immer noch jedes Mittel, doch haben Fälle, wie sie eingangs erwähnt wurden (Siemens, UBS etc.), deutlich gezeigt, dass gerade diese Einstellung die Existenz eines Unternehmens gefährden kann und ein Umdenken angezeigt ist.[70] Eine Unternehmensleitung, die illegale Aktivitäten des Unternehmens kennt und nicht abstellt, darf sich im Übrigen auch nicht wundern, wenn es die eigenen Mitarbeiter nicht mehr ganz so genau mit der Ehrlichkeit gegenüber ihrem Arbeitgeber nehmen oder wenn sich die Ehrlichen an die Öffentlichkeit wenden und den Skandal publik machen.[71]

Führt man ein anonymes, sanktionsfreies Reporting-System ein, hat dieses den Vorteil, dass auch Zwischenfälle unterhalb der Schwelle von Haftungsfällen eingegeben werden können, was die Möglichkeiten zur Fehlerauswertung und -vermeidung enorm steigert. Zudem erleichtert ein permanent zur Verfügung stehendes System die Meldung, da die Arbeitnehmer des Unternehmens wissen, wo sie ihre Meldungen „loswerden" können. Interne Systeme sind also geeignet, den sofortigen Gang von Mitarbeitern zur Presse oder zu Behörden zu verhüten. Das Schrifttum befürwortet daher zunehmend die Einführung solcher Systeme.[72]

Reporting-Systeme unterscheiden sich auch von herkömmlichen Qualitätssicherungsprogrammen. Diese haben sich oft als wenig geeignet erwiesen, individuelles Fehlverhalten aufzudecken.[73] Zudem gibt es häufig Vorfälle, bei denen eine Vielzahl von Ursachen massgebend war. Der einzelne Mitarbeiter kennt nur einen Ausschnitt des Gesamtbildes. Erfolgen nun verschiedene

---

69 Reporting-Systeme tragen auch dazu bei, den Korpsgeist im Gesundheitswesen, also die Kultur von Geheimhaltung und Protektionismus zu durchbrechen, KIERAN WALSHE/STEPHEN M. SHORTELL, When Things Go Wrong: How Health Care Organizations Deal With Major Failures, Health Affairs, 23 (2004), Nr. 3, 103, 107.

70 STRASSER (Fn. 14), 488.

71 BÖCKLI (Fn. 14), N 144. Das Bundesgericht hat entschieden, dass zur Wahrung der Verhältnismässigkeit zunächst der unternehmensinterne Instanzenzug zu erschöpfen sei, BGE 127 III 310, E.5a; ebenso BUFF (Fn. 23), N 624, 626, 629.

72 BÖCKLI, Schweizer Aktienrecht (Fn. 23), § 13 N 380a; PORTMANN (Fn. 9), 996; STEFAN RIEDER, Schutz für Whistleblower – Kommentar zum Gesetzentwurf, Jusletter 20. April 2009, 3; PASCAL DE PREUX, Entreprise et corruption: risques et responsabilité pénale, AJP/PJA 2010, 1092 ff.

73 WALSHE/SHORTELL (Fn. 69), 105.

Meldungen in einem Reporting-System, kann sich bei der Auswertung eine umfassendere Sichtweise ergeben.[74]

Zu den *Nachteilen* der Reporting-Systeme gehört der Umstand, dass es sich um ein freiwilliges System handelt,[75] so dass seine Funktionsfähigkeit von der Bereitschaft zur Eingabe abhängt. Diese ist umso grösser, je mehr Vertrauen die Meldenden in die Vertraulichkeit des Systems haben. Das System ist zudem auf ein wahrheitsgemässes und detailliertes Reporting angewiesen. Damit kommt der Sorgfalt der Meldenden eine Schlüsselrolle zu. Sie werden nur Ereignisse eingeben, die sie selbst als berichtswürdig einstufen, so dass oft kleinere Zwischenfälle als zu harmlos angesehen und nicht gemeldet werden.[76] Hier gilt es durch Schulungen zu verdeutlichen, dass gerade die Summierung vieler kleiner Missstände die grosse Katastrophe auslösen kann.

Ein den Reporting-Systemen immanenter Nachteil besteht darin, dass sie auch dazu dienen, nicht regelgerechtes Verhalten von Mitarbeitern zu erfassen. Eine Meldung von Verstössen gegen Verhaltenspflichten bedeutet in der Sache damit die Erhebung, Übermittlung und Speicherung von personenbezogenen Daten, so dass sich datenschutzrechtliche Fragen stellen.[77] Insbesondere besteht die Gefahr, dass im Wege anonymer Meldungen Mobbing betrieben wird.

Das System funktioniert nur, wenn Meldungen auf ihre Wahrhaftigkeit überprüft werden und man dem Vorfall auch nachgeht. Ein weiterer Nachteil sind schliesslich die Kosten eines solchen Systems, die aber oft geringer ausfallen als ein grosser Haftungsfall oder Reputationsschaden.

4. Ungelöste juristische Aspekte von Reporting-Systemen

Zu den Nachteilen der Reporting-Systeme gehört sicherlich auch ihr rechtlich ungesicherter Status. Ein solches System funktioniert nur, wenn es vertraulich und sanktionsfrei betrieben werden kann. Um dies zu gewährleisten, müssen bestimmte rechtliche Rahmenbedingungen geschaffen werden, auf die nachfolgend einzugehen ist.

---

74 WALSHE/SHORTELL (Fn. 69), 107.

75 Zur Diskussion über die flächendeckende und verpflichtende Einführung solcher Systeme LEAPE (Fn. 63), 1633 ff.

76 Wenn man an das Beispiel der Flugzeugkatastrophe vom Bodensee (s. Fn. 47) denkt, erscheint es äusserst fraglich, ob jemand als Meldung eingegeben hätte, die Telefonleitung sei besetzt gewesen. Dass eine solche Kleinigkeit gefährlich sein kann, bedenkt man im Vorhinein oft nicht.

77 Einzelheiten bei STRASSER (Fn. 14), 496 f.; s.a. zum deutschen Recht MARIE-THERES TINNEFELD, Whistleblowing: heikle Konfliktfelder, DIGMA 2009, 68 ff. Siehe auch die Stellungnahme 1/2006 der Article 29 Data Protection Working Party, http://ec.europa.eu/justice /policies/privacy/docs/wpdo cs/2006/wp117_de.pdf.

a) Anonymität versus Vertraulichkeit

Um Mitarbeitern die Angst vor Sanktionen zu nehmen, ist die Zusicherung völliger Anonymität sicherlich sehr effektiv. Allerdings birgt sie auch erhebliche Nachteile. Zum einen hindert sie andere nicht daran, (ggf. mit Erfolg) zu (er)raten, wer die Meldung erstattete. Zum anderen – und dies ist viel erheblicher – kann der Meldung nicht nachgegangen werden, wenn Unklarheiten bestehen oder Rückfragen nötig sind. Meldungen werden u.U. weniger ernst genommen, wenn und weil sie anonym vorgebracht wurden. Auch besteht die Gefahr, dass im Unternehmen eine Kultur anonymer böswilliger Meldungen entsteht und sich dadurch das Betriebsklima verschlechtert. Schliesslich bestehen gegen ein System, das völlig anonyme Meldungen über Personen zulässt, datenschutzrechtliche Bedenken.[78]

Aus diesem Grund ist es sinnvoller, wenn man nicht völlige Anonymität zusichert, sondern stattdessen ein System vorsieht, bei dem eine Person für das Meldesystem verantwortlich ist, diese aber zur absoluten Vertraulichkeit verpflichtet ist.[79] Diesem „Systembetreuer" steht dann die Möglichkeit offen, bei dem Meldenden rückzufragen, wenn Unklarheiten in Bezug auf die Meldung bestehen. Dies wiederum erhöht die Wirksamkeit des Reporting-Systems erheblich. Des Weiteren kann der Systembetreuer ein Mobbing verhindern, indem er erkennbar böswillige und ungerechtfertigte Meldungen nicht weiterleitet. Ein auf Vertraulichkeit basierendes System ist damit einem solchen, das auf völliger Anonymität beruht, deutlich überlegen. Voraussetzung dafür ist allerdings, dass der Systembetreuer über genügend Sachverstand und Unternehmenskenntnisse verfügt, um die notwendigen Sachfragen auch beurteilen zu können.[80]

Will man die Gefahr des Mobbing oder Missbrauchs des Systems verhindern, ist zudem darauf zu achten, dass das System nicht jedermann offen steht, sondern nur Personen Eingaben vornehmen können, die tatsächlich auch im Unternehmen oder für dieses tätig sind. Eine noch weitergehende Einschränkung, etwa auf bestimmte Abteilungen (z.B. im Anwendungsbereich des Sarbanes-Oxley-Act auf die Mitarbeiter der Buchführung) ist dagegen kontraproduktiv, denn oft kommen die Meldungen von aussenstehenden Mitarbeitern, die Missstände in einer anderen Abteilung des Unternehmens entdeckt haben.[81] Um der Gefahr des Missbrauchs vorzubeugen, ist aber darauf zu achten, dass alle Personen, denen die Möglichkeit zur Meldung offensteht, den Sinn des Systems verdeutlicht bekommen; sie sind entsprechend zu schulen.

---

78 PORTMANN (Fn. 9), 993; siehe auch TINNEFELD (Fn. 77), 68 ff.

79 STRASSER (Fn. 14), 494 f.; PORTMANN (Fn. 9), 993.

80 In diese Richtung zielen – allerdings aus datenschutzrechtlichen Gründen – auch die Vorschläge der Art. 29 Datenschutzgruppe (Fn. 77), 11 f.

81 So auch VON ZIMMERMANN (Fn. 1), 1064 f.

b) Schutz der Vertraulichkeit

aa) Unabhängigkeit der Systembetreuer

Vertraulichkeit ist nur gewährleistet, wenn – neben den notwendigen technischen Vorkehrungen gegen Zugriffe von aussen – die Personen, die das Reporting-System betreuen, Unabhängigkeit gegenüber Arbeitgebern, Staatsanwälten und Aufsichtsbehörden geniessen. Würde es etwa der Geschäftsführung des Unternehmens erlaubt, in das System hineinzuschauen, um den Namen des Meldenden oder des Verursachers eines Zwischenfalls zu erfahren, wäre das System wertlos. Kein weiterer Mitarbeiter wird mehr freiwillig eine Meldung über eigene oder fremde Fehler verfassen.

Bei der seit 2003 geführten politischen Diskussion über eine Änderung des Arbeitsrechts, um Whistleblower künftig vor Repressalien zu schützen, hat man das Naheliegendste vergessen, nämlich zu gewährleisten, dass die Person des Meldenden von vornherein unerkannt bleibt.[82] In diesem Fall ist ein Schutz vor Ausgrenzungen oder Sanktionen nämlich unnötig. Bei der anstehenden Einführung einer Whistleblowing-Regelung sollte der Gesetzgeber daher eine zweite Regelungsebene in Betracht ziehen: Systembetreuern sollte das Recht zustehen, Arbeitgebern, Staatsanwaltschaften und Aufsichtsbehörden jegliche Einsicht in das System zu verwehren und Auskunft über Einzelheiten zu verweigern. Zwar könnte man eine solche Privilegierung faktisch auch schon dadurch verwirklichen, dass man das Reporting-System an eine unabhängige und neutrale Instanz, z.B. einen Berufsverband, anbindet. In diesem Fall hat der Arbeitgeber keinerlei Zugriff auf Daten. Dies schützt allerdings nicht vor dem Zugriff von Staatsanwaltschaften und Aufsichtsbehörden. Letztlich hilft daher nur eine gesetzliche Privilegierung.

bb) Verwertungsverbot der Daten

Will man die Vertraulichkeit und Sanktionsfreiheit des Systems sicherstellen, gilt es zu verhindern, dass die eingegebenen Informationen Gegenstand eines Straf- oder eines Gerichtsverfahrens (z.B. wegen Kündigung oder Haftung) werden. Derzeit können die in einem Reporting-System gespeicherten Daten im Strafverfahren oder in Arbeits- oder Zivilstreitigkeiten als Beweismittel verwendet werden. Wurde die Meldung von den Systembetreuern rechtzeitig anonymisiert, kann sie keiner Einzelperson mehr zugeordnet werden und diese ist damit vor einer Sanktionierung sicher. Wurde die Information jedoch vorher beschlagnahmt, ist sie verwertbar. Um dies zu verhindern und die Funktionsfähigkeit des Reporting-Systems zu gewährleisten, bedarf es der Einführung eines gesetzlichen Verwertungsverbots.

[82] Dieser Gedanke klingt im juristischen Schrifttum an bei PORTMANN/WOHLMANN (Fn. 14), 181, sowie bei den in Fn. 72 Genannten.

Zu bedenken ist weiterhin, dass nicht nur der Arbeitnehmer, sondern auch der Arbeitgeber ein Interesse an einem Verwertungsverbot haben kann. Die Daten im System, selbst wenn sie anonymisiert wurden, können immer noch dazu dienen, dem Unternehmen ein Organisationsverschulden nachzuweisen. Unternehmen werden daher nur dann ein solches System einrichten, wenn sie sicher sind, dass sich dieses nicht für sie als Eigentor erweist.

cc) Zeugnisverweigerungsrechte

Allein die Einführung eines Verwertungsverbots für die Daten erscheint nicht ausreichend, denn einem potentiellen Kläger steht als Beweis immer noch die Zeugenaussage der Betreuer der Datenbank zur Verfügung. Für sie muss daher ein Zeugnisverweigerungsrecht („Beichtgeheimnis“) eingeführt und deshalb die Art. 171 Abs. 1 StPO, 166 Abs. 1 lit. b und d ZPO geändert werden. Nur so lässt sich verhindern, dass die Systembetreuer als Zeugen dafür benannt werden, von welchem PC die Meldung einging und ob in der Meldung Anhaltspunkte für eine Identifikation des Meldenden zu finden waren. Aus den gleichen Gründen müssen auch die in das System eingebenden Personen Zeugnisverweigerungsrechte erhalten.

Als vorübergehende Lösung bietet es sich im Moment an, das Reporting-System bei einer der Vertraulichkeit unterliegenden Anwaltskanzlei anzusiedeln. Dies ist jedoch keine dauerhafte Lösung, denn es benachteiligt Nichtanwälte als Anbieter von Reporting-Systemen und verzerrt damit den Wettbewerb. Zudem stellt es einen unnützen Umweg dar, denn der Systembetreuer sollte gerade ein Fachmann in der jeweiligen Branche des Unternehmens sein und beurteilen können, welche Meldungen Anlass zum Einschreiten geben. Rechtsanwälte aber sind für solche Aufgaben nicht unbedingt geeignet, da sie beispielsweise medizinische Sachfragen nicht beurteilen können. Auch der Ausweg, den fachmännisch ausgebildeten Systembetreuer in der Anwaltskanzlei anzustellen, ist letztlich ein Umweg.

dd) Schutz von beschuldigten Personen

Reporting-Systeme können nicht nur zur Aufdeckung von technischen oder organisatorischen Fehlern führen, sondern auch Fehlverhalten von Mitarbeitern aufdecken. Juristisch noch ungelöst ist der Schutz der Personen, denen im Wege des Whistleblowing ein Vorwurf gemacht wird.[83] Sinnvoll wäre eine Regelung des Spannungsverhältnisses zwischen Sicherung der Vertraulichkeit des Systems einerseits und den Möglichkeiten des Beschuldigten andererseits, zu Vorwürfen Stellung zu nehmen, deren Ursprung er nicht kennt.

[83] Einzig STRASSER (Fn. 14), 496 f., spricht diese Frage an.

c) Verhältnis zum Haftungs- und zum Strafrecht

Ohne die vorgeschlagenen Gesetzesänderungen besteht die Möglichkeit der prozessualen Verwertung der eingegebenen Informationen. Aus diesem Grunde warnten und warnen die vorhandenen Reporting-Systeme in den USA[84] und in der Schweiz[85] die eingebenden Personen, keine bereits eingetretenen Schadensfälle zu melden. Dies reduziert natürlich den Wert der Reporting-Systeme, da die meldenden Personen in Zweifelsfällen Abstand von einer Eingabe in das System machen. Deshalb wird nun in zahlreichen Staaten eine entsprechende gesetzliche Privilegierung gefordert.[86] Australien[87] hat bereits ein entsprechendes Gesetz für den Bereich des Gesundheitswesens erlassen, das komplette Sanktionsfreiheit garantiert. Die USA haben 2005 den Patient Safety and Quality Improvement Act[88] erlassen, mit dem Title IX des Public Health Service Act geändert wurde. Die neu eingefügte Sec. 922 sieht die Vertraulichkeit der eingegebenen Informationen und Verwertungsverbote vor. Allerdings kann gemäss Sec. 922 lit. (c) (1) im Strafverfahren auf die Informationen zugegriffen werden, wenn Beweismittel auf andere Weise nicht zu erlangen sind.

Offenbar sieht der Staat es in diesem Fall als gerechtfertigt an, in Strafverfahren das in Reporting-Systemen enthaltene Wissen verwerten zu dürfen. Auch wenn diese Ausnahme auf Fälle begrenzt ist, in denen das Beweismittel auf andere Weise nicht zu erreichen ist, schüttet man das Kind mit dem Bade aus. Die Strafverfolgungsbehörden gewinnen nur einen sehr kurzzeitigen Vorteil. Nur im ersten Strafverfahren, in dem Beweise anderweitig nicht erlangt werden können, führt der Zugriff auf das Reporting-System zu einem Vorteil. Anschliessend werden Mitarbeiter aus Furcht vor Strafverfolgung dort keine eigenen Fehler mehr eingegeben und damit versiegt diese so wertvolle Quelle für die Verhütung von medizinischen Zwischenfällen. Die Ausnahmeklausel verschafft dem Staat also einen Pyrrhussieg. Der Staat sollte bedenken, dass er die Information, die er aus dem Reporting-System erhält, andernfalls nie erhalten hätte. Warum soll er nun einmalig besser gestellt werden um den Preis, dass das ganze System wertlos wird? Der Schweizer

84 Rechtsvergleichend dazu HANSPETER KUHN, «Congress should pass legislation to extend protections …», «Critical Incident Reporting» und Recht, Schweizerische Ärztezeitung 2001, 1394 ff.

85 HANSPETER KUHN/GEORG VON BELOW, «Melden Sie keine Flugzeugunfälle auf diesem Formular!» - CIRSmedical - Massnahmen für den Vertraulichkeitsschutz, Schweizerische Ärztezeitung 2003, 1399 ff.

86 Beispielhaft KUHN/VON BELOW (Fn. 85), 1399 ff. (für die Schweiz) sowie die Nachweise bei KUHN/VON BELOW aaO. in Fn. 49 für die Niederlande und Dänemark.

87 WILLIAM B. RUNCIMAN, Lessons from the Australien Patient Safety Foundation: Setting up a national patient safety surveillance system - is this the right model?, Quality & Safety in Health (QSHC) 11 (2002), 246, 250.

88 Pub L. No. 109-41, 119 STAT. 424, http://www.gpo.gov/fdsys/pkg/PLAW-109publ41/pdf/LAW-109publ41.pdf.

Gesetzgeber sollte bei einer gesetzlichen Privilegierung also der Versuchung widerstehen, Sec. 922 lit. (c) (1) zu kopieren. Wenn man eine gesetzliche Privilegierung der Reporting-Systeme als besondere Form des internen Whistleblowing einführt, sollte man sich konsequent den Sinn und Zweck dieser Meldungen vor Augen halten und sich hüten, diesen mit dem der Strafverfolgung zu vermischen. Wer den Strafverfolgungsbehörden neue Beweise zugänglich machen will, muss dies über Kronzeugenregelungen tun.

5. Unternehmens- und branchenspezifische Lösungen

Da es sich bei den Reporting-Systemen um ein Mittel zum internen Whistleblowing handelt und es nicht um Meldungen an Behörden oder andere Externe geht, stellen sie ein Instrument zur Verhütung von fehlerhaftem, unethischem oder illegalem Verhalten dar. In der Praxis zeigt sich, dass ein dezentraler, unternehmens- oder branchenspezifischer Ansatz vorzugswürdig ist.[89] Grössere Unternehmen sind in der Lage, ein betriebsinternes Reporting-System zu errichten. Sie haben die Wahl zwischen einem IT-gestützten System oder einem solchen mit einer Vertrauensperson. Das System kann im IKS,[90] in der Compliance-Abteilung,[91] im Audit Committee[92] oder bei einem Ombudsmann[93] angesiedelt werden. Demgegenüber werden kleinere Unternehmen sich eher einer Verbandslösung oder Selbstregulierungsorganisationen anschliessen, die ein solches System für mehrere Unternehmen als internes Whistleblowing organisiert.[94]

V. Ergebnisse

- Auf komplexe und schadensanfällige Vorgänge reagiert die Rechtsordnung mit dem Erlass von Organisationspflichten. Diese bergen jedoch die Gefahr eines Aufblähens der Bürokratie. Ihr Einsatz will daher wohl überlegt sein.
- Die überwiegende Zahl der Schadensfälle beruht auf menschlichem Versagen oder auf einer Kombination von menschlichem und technischem Versagen. Zu deren Verhütung tragen Organisationspflichten nur bedingt bei.

---

89 Im Ergebnis auch WEBER-REY (Fn. 1), 409, die für eine Selbstregulierung eintritt.
90 So PFAFF/RUUD (Fn. 14), 55.
91 THOMAS LAMPERT, in: Hauschka (Fn. 14), § 9 N 35.
92 So BÖCKLI (Fn. 14), N 139 ff.; BERNDT/HOPPLER (Fn. 1), 2628; ROLF NONNENMACHER/KLAUS POHLE/AXEL VON WERDER, Aktuelle Anforderungen an Prüfungsausschüsse, DB 2009, 1447, 1451 f.
93 THOMAS LAMPERT/PHILIP MATTHEY, in: Hauschka (Fn. 14), § 26 N 85.
94 BERNDT/HOPPLER (Fn. 1), 2627 und 2629.

- Menschliches Fehlverhalten wird nur selten zugegeben, da sich Ehrlichkeit kaum karrierefördernd auswirkt. Eine Vielzahl von Zwischenfällen bleibt daher unentdeckt.
- Das Recht konzentriert sich in Haftungsfällen bisher auf den Ausgleich schon eingetretener Schäden, auf Strafverfolgung und Entlassung der Schadensverursacher. Gerade durch die drohenden Sanktionen wird der Anreiz gesetzt, Schadensfälle zu verheimlichen. Dies wiederum trägt dazu bei, dass es zu Wiederholungen von kritischen Zwischenfällen kommen kann.
- Der alte Satz „Aus Schaden wird man klug", gilt vor allem für das Individuum, das aus seinen Erfahrungen lernt. Arbeitsteilige Organisationen können aus Fehlern nur lernen, wenn diese nicht auf individueller Ebene verbleiben, sondern gleichsam in das Bewusstsein der Organisation gehoben werden.
- Critical Incident Reporting-Systeme, also auf Vertraulichkeit basierende sanktionsfreie Meldesysteme, wie sie in der Luftfahrt und Medizin seit Langem zum Einsatz kommen, haben sich als besonders geeignet erwiesen, um organisatorische oder verhaltensbedingte Risiken in Unternehmen aufzudecken. Solche Systeme gewährleisten den Schutz des Meldenden vor Repressalien und geben gleichzeitig dem Unternehmen die Möglichkeit, fehlerhaftes, unethisches oder kriminelles Verhalten abzustellen. Insbesondere können Personen, die selbst einen Fehler begangen haben, diesen melden, ohne Repressalien fürchten zu müssen. Dies führt zu einer wesentlich früheren Aufdeckung von Schwachstellen in einem Unternehmen als wenn man erst einen „richtigen" Schadensfall abwarten müsste.
- Um die Anonymität und Sanktionsfreiheit des Reporting-Systems zu gewährleisten, ist es notwendig, jeden Zugriff auf eingegebene Informationen durch Aufsichtsbehörden, Polizei, Strafverfolgung und Gerichte auszuschliessen. Die persönliche Unabhängigkeit des bedienenden Personals vom Arbeitgeber ist sicherzustellen. Personen, die in das System eingeben, dieses verwalten oder Informationen empfangen, müssen ein Zeugnisverweigerungsrecht erhalten.
- Die derzeit geführte Diskussion wird vor allem durch Fälle geprägt, bei denen ein Arbeitnehmer als externer Whistleblower aufgetreten ist und sich an Behörden, die Presse oder das Fernsehen gewandt hat. Durch die geplante Einführung eines Art. 321^{bis} E-OR will man den Grundsatz festschreiben, dass ein externes Whistleblowing erst zulässig ist, nachdem ein internes Whistleblowing erfolgte. Der gesetzgeberische Ansatz konzentriert sich allein auf die Rechtsfolgen von (unberechtigten) Kündigungen nach (berechtigtem) Whistleblowing. Sowohl Arbeitgeber als auch Arbeitnehmer haben aber ein Interesse daran, dass es gar nicht erst zu einem externen Whistleblowing kommt. Viel wirksamer wäre es daher, die Reform zur Stärkung des internen Whistleblowing zu nutzen und es sowohl

für Unternehmen als auch für Arbeitnehmer so attraktiv auszugestalten,[95] dass es Teil guter Unternehmenskultur wird. Dazu bedarf es der geschilderten Ergänzungen des Prozessrechts, damit vertrauliche Reporting-Systeme auch vertraulich bleiben.

[95] Vgl. dazu auch die Vorschläg von PORTMANN (Fn. 9), 998. Demgegenüber scheinen die USA vor allem auf externes Whistleblowing zu setzen, wenn dieses sogar finanziell belohnt wird, s.o. Fn. 2 und 3.