E-Compliance

Konzept, Merkmale, Aufgaben und organisatorische Auswirkungen

URS GASSER / DANIEL MARKUS HÄUSERMANN*

Inhaltsverzeichnis

E-Compliance **71**

1. Einleitung **72**

2. Von Compliance zu E-Compliance **73**

3. Kernthemen der E-Compliance **74**
3.1 Übersicht 74
3.2 Schutz- und Risikobereiche 75
3.3 Anwendungsfälle – fiktiv, aber mit realem Hintergrund 78

4. Merkmale von E-Compliance **81**
4.1 Thesen im Überblick 81
4.2 Verzahnung von Recht und Technologie 82
4.3 Innovation und Dynamisierung des Rechts 84
4.4 Internationalität von Rechtsproblemen 86
4.5 Bedeutungszuwachs von Soft Law 88

5. Aufgaben und Herausforderungen der E-Compliance: Risikomanagement **90**

6. Auswirkungen auf die Unternehmensorganisation **92**
6.1 Zusammenspiel von IT und Recht meistern 93
6.2 Veränderungen rechtzeitig erkennen 93
6.3 Globalen Blickwinkel einnehmen 94
6.4 Unternehmensübergreifende Zusammenarbeit verstärken 95

7. Schluss **96**

Literaturverzeichnis **98**

* Stand des Manuskripts: 10. April 2007.

1. Einleitung

Während der Geschäftsverkehr im Internet weiterhin wächst[1], hat sich innerhalb des Rechtssystems – von prominenten Ausnahmen abgesehen[2] – gleichsam alltägliche Professionalität breit gemacht, was den Umgang mit den rechtlichen Aspekten des E-Commerce betrifft. In der Tat scheint das Recht die ersten Schockwellen der Digitaltechnologien aufgefangen zu haben[3], sei es durch Subsumtion neuer oder nicht so neuer Probleme unter alte Regeln, sei es durch Innovationsleistungen des Rechtssystems selbst[4]. Systemisch betrachtet, hat das Rechtssystem die rasante Innovation in den Informations- und Kommunikationstechnologien und die Geschäftsmodelle des E-Business durch eine beachtliche Bewältigungsleistung[5] eingefangen. Die entsprechenden Veränderungs- und Rückkoppelungsprozesse der letzten zehn Jahre sind freilich nicht ohne Friktionen abgelaufen. Besonders deutlich haben sich diese Schwierigkeiten im Umgang mit einem dergestalt *dynamisierten Informationsrecht* in jenem *Schnittstellenbereich* der Unternehmenspraxis abgezeichnet, der sich mit dem *Management der Einhaltung* der teils neu geschaffenen, teils vertrauten, aber neu interpretierten Spielregeln befasst.

Damit ist der thematische Rahmen des vorliegenden Beitrags abgesteckt: Der Essay befasst sich unter dem Titel „E-Compliance“[6] mit der

---

1 Umfangreiches Datenmaterial findet sich dazu bei TNS INFRATEST, Monitoring Informationswirtschaft, 9. Faktenbericht 2006: E-Commerce, April 2006, abrufbar unter http://www.tns-infratest.com/06_BI/bmwi/Faktenbericht_9/pdf/FB9_EK_E-Commerce.pdf. (Die in diesem Text angegebenen URLs wurden am 3.1.2007 zuletzt besucht.)

2 Zum Beispiel *Metro-Goldwyn-Mayer Studios Inc., et al. v. Grokster, Ltd. et al.,* 125 S.Ct. 2764 (2005); *Copiepresse c. Google Inc.*, Tribunal de première instance de Bruxelles vom 5.9.2006, N°. 2006/9099/A, abrufbar unter http://www.chillingeffects.org/international/notice.cgi?action=image_7796; *Rolex v. Ricardo*, OLG Köln vom 18.3.2005, Aktenzeichen 6 U 12/01, abrufbar unter http://www.justiz.nrw.de/ses/nrwesearch.php.

3 Vgl. BURKERT, Internetrecht, 693-714.

4 Zu den möglichen Reaktionsweisen des Rechts hinten, Abschnitt 4.3.

5 Für eine Beurteilung siehe BURKERT, Internetrecht, 695 ff.

6 Im englischsprachigen Raum wird der gemeinfreie Begriff „e-compliance“ öfters im Zusammenhang mit oder zur Bezeichnung von Software verwendet, die im Bereich der Compliance (im herkömmlichen Sinn wie E-Compliance) eingesetzt wird: vgl. zum Beispiel ROSSI; PR NEWSWIRE: Made2Manage, Powerway and 4-Front Technologies Form an E-compliance 'Supply Chain' in the European Manufacturing Software Market, 6. September 2000 (erhältlich über factiva.com). Mitunter bezeichnet der Begriff „e-compliance“ auch die Gesetzeskonformität von Webseiten: vgl. PR NEWSWIRE: e-

Frage, welche strukturellen Auswirkungen die Digitalisierung der Kommunikation, genauer: der Einsatz digitaler Kommunikationsmittel im Unternehmen[7], auf die unternehmensinterne Compliance hat. E-Compliance kann somit im Sinne einer Arbeitsdefinition umschrieben werden als das Management der Risiken an der Schnittstelle von Recht, Technologie und Markt, welche durch und in Reaktion auf die Computerisierung und digitale Vernetzung entstanden sind. Damit wird vorweg klar, dass die hier behandelte Fragestellung über den Bereich des E-Commerce hinausgeht, diesen aber umschliesst.

2. Von Compliance zu E-Compliance

Compliance – ein Begriff, der ursprünglich aus der US-amerikanischen Bankenwelt stammt[8] – ist inzwischen im schweizerischen Wirtschaftsleben etabliert und bezeichnet allgemein die Einhaltung verhaltenslenkender Normen durch eine Unternehmung[9]. Nach dem Verständnis vieler Autoren, dem sich die Schreibenden anschliessen, bedeutet Compliance nicht nur die Einhaltung von Gesetzgebung, Branchenstandards, Statuten, Weisungen usw., sondern auch ethisches Verhalten der Unternehmung[10] im Sinne der *corporate citizenship*[11]. Compliance hat überdies eine *organisatorische* Dimension und bezeichnet in diesem Sinne die Gesamtheit aller von einer Unternehmung getroffenen Massnahmen, die darauf abzielen, Regelverstösse durch die Unternehmung, ihre Organe und Mitarbeiter zu verhindern[12]. Die Organisation der Compliance obliegt als Teil der Oberaufsicht (Art. 716a Abs. 1 Ziff. 5 OR) dem Verwaltungsrat[13], die Umset-

---

Compliance Concerns to be Addressed at the Market Conduct Exchange, 9 October 2001 (erhältlich über factiva.com).

7 Im Blickfeld liegt somit die digitale Kommunikation innerhalb einer Unternehmung, zwischen Unternehmungen (Business-to-Business) und zwischen Unternehmungen und Privatpersonen (Business-to-Consumer).

8 Vgl. BUFF, N 4; STRASSER, 539.

9 Vgl. BUFF, N 2; STRASSER, 539; BÜHLER, 211 f. Letzterer Autor beklagt freilich, dass Compliance zu einem Modewort geworden ist.

10 BUFF, N 2 und 16; BÜHLER, 211 f.; SUHR BRUNNER/PORTMANN, 1038; STRASSER, 539. Letzterer weist darauf hin (539, Fn. 5), dass Ethikbestimmungen oft als Regeln kodifiziert sind, weshalb unethisches Verhalten oft einen konkreten Regelverstoss bedeutet.

11 BUFF, N 204 f., m.w.H.

12 STRASSER, 539, m.w.H.

13 Statt aller BÖCKLI, Aktienrecht, § 13 N 378. Art. 716a Abs. 1 Ziff. 5 OR wird von Ziff. 20 und 24 2. Spiegelstrich des Swiss Code of Best Practice for Corporate Governance

zung dem operativen Management (Delegation im Sinne von Art. 716b OR).

Thematisch hat sich das Verständnis von Compliance in den letzten Jahren verändert. Aufgrund ihres Ursprungs im Bankenbereich ist Compliance traditionell auf die branchenspezifischen Schutz- und Risikobereiche wie die Dienstleistungs- und Finanzmarktaufsicht, Insiderdelikte, Geldwäscherei und dergleichen fokussiert gewesen. Mit der branchenmässigen Ausweitung – Kunden und Aktionäre eines jeden Unternehmens sind an der Aufdeckung von Fehlverhalten interessiert[14] – hat sich Compliance indes von einer punktuellen Betrachtung bestimmter Rechts- oder Tätigkeitsgebiete hin zu einer umfassenden Sichtweise entwickelt[15], welche heute auch die Einhaltung kartell-, wettbewerbs-, arbeits-, immaterialgüter-, steuer- und umweltrechtlicher Regeln umfasst, um nur einige Beispiele zu nennen[16]. Im Zuge namentlich des „Dot-com"-Booms Ende der 90er-Jahre hat sich unter der Überschrift „elektronische Kommunikation"[17] ein neuer Compliance-Bereich hinzugesellt, der die Anlage zu dem, was wir E-Compliance nennen, in sich trägt.

3. Kernthemen der E-Compliance

3.1 Übersicht

Wie angetönt, geht es bei der E-Compliance um die Bewältigung der durch die Digitalisierung verursachten Veränderungen im Rechtssystem durch die einzelne Unternehmung. Diese Veränderungen können – und müssen! – unter dem Gesichtspunkt des auf digitale Sachverhalte anwendbaren positiven Rechts analysiert werden, was traditionellerweise durch die Identifikation von Schutz- und Risikobereichen oder die Schaffung ei-

vom 25. März 2002 konkretisiert (STRASSER, 538). Dazu BÖCKLI, Swiss Code of Best Practice, 989 f., und zu möglichen Ausgestaltungen BUFF, N 14.

Mit der aus der Strafbarkeit des Unternehmens nach Art. 100^{quater} Abs. 1 und 2 StGB resultierenden Organisationspflicht hat der Gesetzgeber indirekt auch einen strafrechtlichen Mindeststandard für die Organisation der Compliance geschaffen. Dazu RYSER/KUCHOWSKY, insbes. 586 f., m.w.H.

Zu den speziell für Banken geltenden Rechtsquellen vgl. STRASSER, 540 f.; SUHR BRUNNER/PORTMANN, 1035 f. und 1039 f.

14 Vgl. zur Ausweitung über den Bankensektor hinaus BUFF, N 23-25.

15 STRASSER, 540.

16 Vgl. BUFF, N 292 ff., passim.

17 Als Schutz- und Risikobereich ausdrücklich erwähnt von BUFF, § 31.

nes neuen Risikobereichs der „elektronischen Kommunikation“ erreicht wird. Zugleich weisen aber die besagten Veränderungen im Rechtssystem selber gewisse, die Schutz- und Risikobereiche überlagernde – und teilweise von ihnen verdeckte – Strukturen auf, die grosse Auswirkungen auf die unternehmensinterne Ausgestaltung der (E-)Compliance haben und zu einem späteren Zeitpunkt (ab Abschnitt 4) vertieft erörtert werden.

Vor diesem Hintergrund skizziert Abschnitt 3.2 die wichtigsten Schutz- und Risikobereiche, mit denen sich E-Compliance zu befassen hat. Abschnitt 3.3 formuliert sodann drei Fallbeispiele als Scharniere zwischen den soeben identifizierten Schutz- und Risikobereichen und dem zweiten Teil dieses Artikels, der sich systematisch mit den Charakteristika von E-Compliance auseinandersetzt und aus diesen Merkmalen schliesslich Leitprinzipien für die Unternehmensorganisation zu gewinnen versucht.

3.2 Schutz- und Risikobereiche

Ein Blick in die Literatur sowie die Erfahrungen aus der Praxis verdeutlicht, dass E-Compliance durch *thematische Vielfalt* geprägt ist und eine eigentliche *Querschnittsaufgabe* darstellt. Im Wesentlichen können fünf zentrale Schutz- und Risikobereiche identifiziert werden, die gewöhnlich im Visier von E-Compliance liegen, wobei deren genaue Bedeutung für das einzelne Unternehmen von der jeweiligen Branche, der Grösse des Unternehmens, dem Geschäftsmodell etc. abhängig ist. Allgemein festhalten lässt sich indessen, dass die Mehrheit der nachstehenden Bereiche nicht nur für Unternehmungen wie zum Beispiel eBay oder Google relevant ist, welche E-Businesss betreiben, sondern (zunehmend) auch für traditionelle Unternehmungen, soweit intern und/oder im Aussenverhältnis über elektronische Kanäle bzw. Medien kommuniziert wird.

- *Sicherheit*: Die Gewährleistung von IT- und Informationssicherheit gehört fraglos zum Kernbereich von E-Compliance[18]. Sicherheitsfragen reichen dabei von Bedrohungen durch Viren, Würmern, Spyware und dergleichen bis hin zu Hacking, Datendiebstahl oder dem Entwenden von Hardware wie zum Beispiel Laptops[19]. Die Sicherung von Infor-

[18] Grundlegend WEBER/WILLI, passim.

[19] Gemäss einer Umfrage haben 72 % der befragten Schweizer Unternehmungen im Jahr 2005 mindestens einen Vorfall in der Informationssicherheit festgestellt. Grossfirmen sowie Unternehmen, die E-Commerce-Dienstleistungen anbieten, sind sehr viel häufi-

mationen und Informationssystemen verlangt vielgestaltige technische, administrative und personelle Massnahmen, die ihrerseits mit rechtlichen Anforderungen sowie selbstregulatorischen Initiativen, „Codes of Best Practice" von Branchen, Verbänden, usw. abzustimmen sind[20].

- *Datenschutz*: Mit dem Schutz- bzw. Risikobereich Sicherheit eng verwandt ist die Einhaltung des Datenschutzrechts bei der Bearbeitung von Kundendaten wie Mitarbeiterdaten. In vielen mittleren und grossen Unternehmungen sind derzeit datenschutz- und arbeitsrechtliche Fragen besonders aktuell, welche sich aus der Nutzung des Internets am Arbeitsplatz im Allgemeinen und von E-Mail im Besonderen ergeben[21]. So stellt sich etwa die Frage, inwiefern bzw. unter welchen Voraussetzungen die Einhaltung interner Richtlinien – speziell des Verbots privater E-Mail-Nutzung – überwacht werden darf. Die Frage des Schutzes von Kundendaten hat in jüngster Vergangenheit namentlich in den USA an Bedeutung gewonnen, so etwa im Kontext der personalisierten Online-Werbung[22], der Weitergabe von Suchmaschinen-Suchbegriffen an Strafverfolgungsbehörden[23] oder an Private[24], oder auch von „Social Networking Sites"[25].

---

ger von solchen Vorfällen betroffen. CENTER FOR SECURITY STUDIES: Informationssicherheit in Schweizer Unternehmen, Eine Umfragestudie über Bedrohungen, Risikomanagement und Kooperationsformen, August 2006, abrufbar unter http://www.melani.admin.ch/berichte/studien/index.html?lang=de&download=00049.

20 Ausführlich WEBER/WILLI, 37-81.

21 Vgl. zum Beispiel GASSER/HÄUSERMANN/MÜLLER, B 4.

22 Zum Beispiel hat Googles E-Mail-Service, Gmail, der dem Nutzer auf den Inhalt der abgerufenen E-Mails abgestimmte Werbung anzeigt, zu Beginn heftige Proteste von Datenschützern ausgelöst (BBC NEWS, 5.4.2004, http://news.bbc.co.uk/2/hi/business/3602745.stm, und 13.4.2004, http://news.bbc.co.uk/1/hi/business/3621169.stm), die sich dann allerdings rasch beruhigt haben, als Google die Funktionsweise des Dienstes erklärte und versicherte, die Privatsphäre der Nutzer zu respektieren (vgl. das Communiqué von Google, 15.6.2004, http://mail.google.com/mail/help/more.html).

23 Der bisher prominenteste Fall ist *Gonzales v. Google*, in dem das U.S. Department of Justice von Google die Edition von einer Million URLs aus dem Such-Index sowie sämtlicher Suchbegriffe, die von den Nutzern innerhalb von einer Woche eingegeben worden sind, verlangt hat. Schliesslich musste Google 50'000 URLs übergeben, nicht aber die Suchbegriffe: *Gonzales v. Google Inc.*, 234 F.R.D. 674, N.D.Cal., March 17, 2006 (No. CV06-8006MISCJW), abrufbar unter http://www.google.com/press/images/ruling_20060317.pdf.

24 Anfang August 2006 veröffentlichte der US-amerikanische Internet-Provider AOL zu Forschungszwecken 19 Millionen Suchanfragen seiner Nutzer, darunter viele Informationen, die auf die Identität der Nutzer rückschliessen liessen (BBC NEWS, 8.8.2006, http://news.bbc.co.uk/1/hi/technology/5255732.stm). Der Chief Technology Officer

- *Konsumentenschutz:* Mit den vorgenannten Schutz- bzw. Risikobereichen ebenfalls in Beziehung steht der Konsumentenschutz als ein weiterer wichtiger Betrachtungsgegenstand von E-Compliance. Konsumentenschutz spielt offenkundig im Bereich des E-Commerce eine bedeutsame Rolle, etwa hinsichtlich der Zulässigkeit von Gerichtsstandsvereinbarungen und Rechtswahl, der Vertragsanbahnung und des Vertragsschlusses, der inhaltlichen Gültigkeit sowie der Durchführung und Beendigung von Konsumentenverträgen[26]. Die Herstellung von E-Compliance wird dabei namentlich im grenzüberschreitenden Verkehr angesichts der noch immer heterogenen Konsumentenschutzvorschriften erschwert[27].
- *Immaterialgüter-, insbesondere Urheberrecht*: Im Online-Bereich mit Fug als traditionell zu bezeichnen ist der Compliance-Bereich des Immaterialgüterrechts, insbesondere des Urheberrechts. Dem allgemeinen Trend zu einer „participatory culture" folgend[28], werden Geschäftsmodelle des Online-Business zunehmend auf die Partizipation der Nutzer ausgerichtet (Web 2.0). Als Konsequenz nehmen die Verantwortlichkeitsrisiken von Online-Intermediären aus Urheberrecht stark zu[29], und dies vor allem für Verletzungen, welche durch ihre Kunden begangen worden sind. Dieser Trend ist sowohl in den USA wie auch diesseits des Atlantiks zu beobachten[30]. Besonders komplexe Fragen, die über

---

von AOL musste daraufhin zurücktreten (BBC NEWS, 21.8.2006, http://news.bbc.co.uk/1/hi/business/5272974.stm).

25 Dienste wie MySpace sehen sich unter anderem mit dem Problem konfrontiert, dass minderjährige Nutzerinnen und Nutzer sich durch die Veröffentlichung persönlicher Informationen gefährden können, insbesondere weil damit Pädophile angelockt werden können und worden sind (BBC NEWS, 11.4.2006, http://news.bbc.co.uk/1/hi/technology/4898526.stm).

26 Vgl. im Überblick zum Beispiel BALSCHEIT, passim.

27 Zu den Harmonisierungsbestrebungen stellvertretend BALSCHEIT, 88-101.

28 Vgl. etwa GASSER/ERNST, passim.

29 Jüngstes Beispiel ist die Klage des US-Medienkonzerns Viacom – der Eigentümerin zahlreicher Fernsehsender wie MTV und Comedy Central sowie des Filmkonzerns Paramount – gegen den von Google aufgekauften Video-Hosting-Service YouTube: Die Klägerin begehrt Feststellung und Unterlassung verschiedener Arten der Urheberrechtsverletzung, sowie Schadenersatz von mindestens USD 1 Mrd. Vgl. die Klageschrift in *Viacom International Inc., et al. v. YouTube Inc., Google Inc. et al., S.D.N.Y.*, March 13, 2007, abrufbar unter http://online.wsj.com/public/resources/documents/Viacom031207.pdf. Zuvor hatte Viacom angekündigt, seine Inhalte gratis via den Peer-to-Peer-Internet-TV-Anbieter Joost (http://www.joost.com) zu verbreiten, vgl. Medienmitteilung von Viacom vom 20. Februar 2007, abrufbar unter http://www.viacom.com/view_release.jhtml?inID=10000040&inReleaseID=227591.

30 Siehe die Beispiele in Fn. 31 und 32.

den Bereich der E-Compliance hinausgehen, betreffen derzeit vor allem grossangelegte Digitalisierungsprojekte[31] und Informations-Aggregationsdienste[32].

- *„Content Governance"*: Die Compliance-Abteilungen vor allem von Internet-Providern stehen vor der Herausforderung, eine Vielzahl unterschiedlicher nationaler Rechtsvorschriften zu befolgen, welche die Zulässigkeit der von ihnen global transportierten, zugänglich gemachten oder selbst angebotenen Online-Inhalte regeln. Die zivil- und strafrechtliche Verantwortlichkeit namentlich für Inhalte Dritter ist dabei vor allem in der Schweiz weitgehend ungeklärt. In den USA und in Europa scheint nach anfänglicher Privilegierung gewisser Kategorien von Internet-Providern gegen Ende der 90er-Jahre das Pendel zurückzuschlagen[33]. Daneben spielen in diesem Bereich ethische Normen eine zunehmend wichtige Rolle, wie etwa das Beispiel der US-Internet-Unternehmungen belegt, welche Dienstleistungen auf dem chinesischen Markt anbieten[34].

3.3 Anwendungsfälle – fiktiv, aber mit realem Hintergrund

Die im vorangehenden Abschnitt identifizierten Schutz- und Risikobereiche der E-Compliance sind nicht mehr als idealtypische Kategorien. Die folgenden drei Beispiele, welche die Autoren – leicht verändert – ihrer Beratungspraxis entnehmen, sind Momentaufnahmen des Prozesses der

---

31 Ein Beispiel ist Google Book Search (http://books.google.com): Google digitalisiert zurzeit in Zusammenarbeit mit fünf renommierten US-Universitätsbibliotheken 18 Millionen Bücher. Werke, die nicht mehr urheberrechtlich geschützt sind, sind im Volltext zugänglich, während geschützte Bücher zwar ebenfalls im Volltext durchsuchbar sind, aber nur Textausschnitte rund um den Suchbegriff herum sichtbar gemacht werden. Obschon Google den Rechtsinhabern die Möglichkeit eingeräumt hat zu verlangen, dass deren Werke aus der Datenbank entfernt werden, haben die US-amerikanische Authors' Guild und einige grosse Verlagshäuser gegen Google aus Urheberrecht geklagt. Siehe dazu LESSIG, Public Domain, 68 ff.; PROSKINE, passim; LUNDEEN, passim.

32 Davon handelt der in Fn. 2 erwähnte Fall *Copiepresse c. Google Inc.* in Belgien: Nach dem (nicht rechtskräftigen) Urteil vom 5.9.2006 verletze das „Caching" von Artikeln und Bildern aus den Online-Ausgaben der belgischen Tagespresse sowie deren Zugänglichmachen als Textausschnitte über Google News das Urheberrecht der betreffenden Medienunternehmen.

33 Siehe hinten, Abschnitt 4.3.

34 Siehe hinten, Abschnitt 4.4 am Ende. Vgl. auch GASSER, Search Engines, 146.

unternehmensinternen *Ausgestaltung* von E-Compliance. Sie verdeutlichen, dass ein und derselbe Sachverhalt regelmässig *Bezüge zu mehreren Teilbereichen* der E-Compliance aufweist und sollen zudem die Herausarbeitung der gemeinsamen Merkmale von E-Compliance vorbereiten.

(a) Kuckstdu.indie.roehre.net

Eine Gruppe von Wirtschaftsstudentinnen und Informatikstudenten plant, ein Unternehmen zu gründen, welches die Website www.kuckstdu.indie.roehre.net betreibt, wo die Benutzer gratis Videoclips ansehen und hochladen können. Die Betriebskosten für die Website und den Speicherplatz möchten sie über Werbung finanzieren. Falls die deutschsprachige Version reüssiert, ist eine Expansion in andere Sprachregionen geplant.

Ein Risikokapitalgeber ist grundsätzlich bereit, das Projekt zu finanzieren, verlangt jedoch von den Initianten ein detailliertes Compliance-Konzept, das unter anderem folgende Fragen beantwortet: Inwiefern haftet die Unternehmung für Urheberrechtsverletzungen der Nutzer, beispielsweise wenn diese kommerzielle Musikvideos hochladen? Welche Rechtspflichten hat die Unternehmung, um die Publikation rechtswidriger Videos (zum Beispiel Neonazi-Propaganda, gewisse Formen der Pornographie) zu unterbinden, und unterscheiden sich diese Pflichten je nach Land, in denen der Service auftritt? Kann die Unternehmung belangt werden, wenn ein Nutzer Videos hochlädt, welche die Intimsphäre einer anderen Person betreffen? Wie gedenkt die Unternehmung zu reagieren, falls auf der Website islamistische Videos auftauchen? Wie können die Kosten der Ermittlung der Urheber solcher Inhalte tief gehalten werden? Wie sind die AGB, wie sind die Datenschutzrichtlinien des Services auszugestalten, dass sie mit dem auf eine Kundenbeziehung anwendbaren Recht im Einklang sind?

(b) Brilliant Chemicals

Die in der Schweiz ansässige, weltweit tätige Brilliant Chemicals AG möchte ihr „Corporate Records & Information Management“ vereinheitlichen und vereinfachen, um ihre Geschäftsprozesse effizienter zu gestalten und um Kosten zu senken. Unter anderem sollen sämtliche Geschäftsunterlagen nicht länger als gesetzlich vorgeschrieben und ausschliesslich elektronisch aufbewahrt werden. Auch ein Outsourcing der Dokumenten-

verwaltungs-Infrastruktur in ein Schwellenland werde in Betracht gezogen.

Die zur Konsultation herbeigezogene Abteilung „Legal & Compliance“ weist auf Folgendes hin: (1) Die Aufbewahrung der Daten an einem einzigen Ort ist ausgeschlossen, weil zahlreiche Länder verlangen, dass vor allem steuerrelevante Unterlagen im Inland aufbewahrt werden. (2) Jedes Land, in dem Brilliant Chemicals tätig ist, kennt andere Vorschriften über den Umfang der kaufmännischen Aufbewahrungspflicht und das zu gewährleistende Niveau an Informationssicherheit. Dazu kommen spezifische und oft jahrzehntelange Aufbewahrungspflichten für Unterlagen über die Entwicklung und Zulassung von Chemikalien. (3) Die Rechtslage zur Beweiszulassung und Beweiskraft eingescannter Dokumente ist in vielen Ländern unklar, und die Prozessrisiken sind erheblich, wenn die Unternehmung keine Originale mehr vorlegen kann. (4) Das zu beschaffende „Enterprise Content Management System“ muss in der Lage sein, die regelmässige Löschung von Daten zu stoppen, wenn ein amerikanisches Gericht einen „litigation hold“ verfügt. Was das Outsourcing in ein Schwellenland betreffe, bestünden nicht nur datenschutzrechtliche Bedenken, sondern auch gewissen Risiken einer Preisgabe von Geschäftsgeheimnissen, weil die dortigen Gerichte einheimischen Konkurrenten prinzipiell Zugang zu den Unterlagen verschaffen könnten.

(c) E-Mail für Bankier Nötzli

Die Bank Nötzli AG ist eine im Bereich der Vermögensverwaltung und im Investment Banking tätige Schweizer Privatbank mit Tochtergesellschaften in mehreren EU-Ländern sowie in den USA. Bisher hat jede Konzerngesellschaft ihre eigene E-Mail-Aufbewahrungsrichtlinie: Die US-Filiale beispielsweise erlaubt ihren Mitarbeitern, auf Anfragen potenzieller Kunden per E-Mail zu antworten, überwacht den E-Mail-Verkehr der Angestellten systematisch und bewahrt alle E-Mails während zehn Jahren auf Magnetbändern auf. Die schweizerische Konzernmutter hingegen verbietet den E-Mail-Verkehr mit Kunden generell, überlässt es den Mitarbeitern, wichtige E-Mails abzuspeichern, und löscht alle anderen Nachrichten nach sechzig Tagen. Der Patron und Hauptaktionär der Bank Nötzli, Herr Dr. Nötzli, ist mit dieser Situation unzufrieden und beauftragt die Abteilung „Legal & Compliance“ mit der Ausarbeitung einer konzernweiten E-Mail-Aufbewahrungsrichtlinie.

In einem (per E-Mail versendeten) Zwischenbericht an Herrn Dr. Nötzli berichtet der General Counsel unter anderem von folgenden Problemen: Das amerikanische Back-up-System mit Magnetbändern könne aus technischen und organisatorischen Gründen keine lückenlose Aufbewahrung der E-Mails garantieren, und das Wiederauffinden von E-Mails im Rahmen eines Discovery-Verfahrens könne schnell Kosten in sechsstelliger Höhe verursachen[35]. Nicht alle Schweizer Mitarbeiter der Bank verfügten über genügend handelsrechtliche Kenntnisse, um zu entscheiden, welche E-Mails sie aufbewahren müssen und welche nicht. Ausserdem weist er auf viele datenschutzrechtliche Probleme im E-Mail-Verkehr in und zwischen den Ländergesellschaften hin, insbesondere betreffend das Weiterleiten von E-Mails und das Senden von Blindkopien. Durch einen Fall von Whistleblowing gerät der Bericht in die Hände der Securities and Exchange Commission (SEC), die die Bank daraufhin wegen mangelnder E-Mail-Aufbewahrung büsst.

4. Merkmale von E-Compliance

4.1 Thesen im Überblick

Welches sind – vor dem Hintergrund der in Abschnitt 3 skizzierten Risiko- und Schutzbereiche der E-Compliance und der gemachten Beispiele – die wichtigsten *Merkmale* von E-Compliance, worin sich diese mindestens teilweise von herkömmlicher Compliance unterscheidet?

Nach der hier vertretenen Auffassung sind es die folgenden vier Charakteristika:

1. Recht und Digitaltechnologie sind untrennbar miteinander verzahnt.
2. Im legislatorisch betrachtet jungen und dynamischen Umfeld des Internet- und IT-Rechts bedeutet E-Compliance das Management von Schnittstellen-Risiken unter Unsicherheitsbedingungen betreffend die gegenwärtige und zukünftige Rechtslage.

---

35 *Zubulake v. UBS Warburg LLC, et al.*, No. 02 Civ. 1243 (S.D.N.Y.), Zusammenfassung bei O'MELVENY & MYERS, 1. In dem Fall stellte die zuständige Richterin fest, dass auch „inaccessible data", d.h. Daten, die nicht mehr aktiv online verfügbar, sondern nur noch auf Back-up-Magnetbändern vorhanden sind, im Rahmen der Discovery beigebracht werden müssen, sofern diese für den Fall relevant sind. Im vorliegenden Fall wurde die Beklagte aufgrund der Umstände verpflichtet, den Löwenanteil der Kosten (ca. USD 450'000) selber zu tragen.

3. Die Digitalisierung, insbesondere die Verbreitung des Internets, hat zu einer starken Internationalisierung alter und neuer Rechtsprobleme geführt.
4. Die Dynamik der Digitalisierung und die damit einhergehende Rechtsunsicherheit hat die Schaffung internationaler Standards, Verhaltenskodizes und sogenannter „Best Practice Models" begünstigt und die Bedeutung von „Soft Law" gesteigert.

Die Thesen werden im Folgenden erläutert und illustriert.

4.2 Verzahnung von Recht und Technologie

Informations- und Kommunikationstechnologie und Recht sind in der Unternehmenspraxis eng miteinander verzahnt. Ein wichtiger Aspekt dieses Zusammenspiels ist in Art. 716a Abs. 1 Ziff. 1 und 5 OR enthalten, wonach der Verwaltungsrat nebst vielem anderem für eine angemessene IT-Governance zu sorgen hat[36]. Ihm obliegt es, zweckmässige elektronische Führungsinstrumente einrichten zu lassen und die Grundsätze der Informationsbewirtschaftung festzulegen. Die Geschäftsleitung hat schliesslich die Aufgabe, ein IT-Konzept auszuarbeiten und umzusetzen, wozu insbesondere die bereits erwähnte Sicherstellung der Informationssicherheit gehört[37]. Letztere hängt neben ihrer – ebenfalls wichtigen – organisatorischen Komponente[38] ganz wesentlich von der verfügbaren und eingesetzten Technologie ab. Der Einsatz von IT nach den Regeln der Kunst und dem Stand der Technik wird damit zur Rechtspflicht[39].

Aus Sicht der E-Compliance ist diesem Einsatz von Informations- und Kommunikationstechnologie zunächst ein Schutz- bzw. *Risikobereich* mit ausgeprägtem Querschnittsbezug zugeordnet. Dabei ergeben sich die Probleme und Fragen, die im Rahmen des Risikobereichs gelöst werden sol-

36 Dazu und zum Folgenden WEBER, Risikomanagement, 182.

37 Das Gesetz formuliert an verschiedenen Orten (mehr oder weniger detaillierte) Anforderungen an die Informationssicherheit: Art. 5 und 8 der Geschäftsbücherverordnung (GeBüV, SR 221.431); Art. 4 der Verordnung des EFD über elektronisch übermittelte Daten und Informationen [sc. im Bereich der Mehrwertsteuer] (ElDI-V, SR 641.201.1); Art. 8-12 der Verordnung zum Datenschutzgesetz (VDSG, SR 235.11). Zum Verhältnis zwischen ElDI-V und GeBüV siehe WEBER, Kompatibilität, passim, und STEINEGGER, 94 ff.

38 Dazu WEBER/WILLI, 176 ff.

39 Betreffend Auftragsrecht vgl. WEBER, Risikomanagement, 190, aber genauso gültig mit Bezug auf die vom Arbeits- und Gesellschaftsrecht geforderte Sorgfalt (Art. 321a Abs. 1 und 717 Abs. 1 OR).

len, überhaupt erst durch den (zunehmend globalen) Einsatz von IT im Unternehmen. Der mit dem Beispiel von Bankier Nötzli illustrierte Problembereich des E-Mail-Managements und der E-Mail-Aufbewahrung zeugt hiervon ebenso wie das Projekt kuckstdu.indie.roehre.net, welches durch die technische Entwicklung der letzten Jahre – namentlich durch die Verbreitung von Breitbandanschlüssen – erst möglich geworden ist.

Informationstechnologien bieten indes auch neue Ansätze zur Erfüllung (vorerst) technologieunabhängiger Rechtspflichten und sind damit ein *Instrument* der E-Compliance[40]. Erfahrungsgemäss spielt Software, die Compliance-Aufgaben unterstützt und teilweise automatisiert, in grossen und international tätigen Unternehmungen eine wichtige Rolle. Vorab Unternehmungen mit ausgeprägtem amerikanischem Bezug richten ihr Augenmerk dabei zunehmend auf Softwareprodukte, welche ein zentralisiertes und workflow-basiertes Informations- und Records-Management erlauben und beispielsweise die automatische Löschung von Daten im Falle eines „litigation hold" stoppen können.

Über diese zwar hochkomplexen, aber in ihrer Struktur konventionellen Softwareprodukte hinaus werden Rechtsnormen in gewissen Bereichen zunehmend formallogisch modelliert und ausgedrückt, was eine anschliessende Umsetzung in Softwareapplikationen ermöglicht[41]. Solche Anwendungen stehen beispielsweise im Bereich der Geldwäscherei-Bekämpfung im Einsatz[42] oder befinden sich im Blick auf die Durchsetzung von Urheberrechten im Internet in Entwicklung[43]. LAWRENCE LESSIGS berühmter, im Zusammenhang mit der Architektur des Cyberspace formulierter Satz „Code is law"[44] muss deshalb um die Komponente der *automatisierten Durchsetzung* von Recht durch Code erweitert werden[45]. Diese Entwicklung steht aber noch am Anfang und die Zuverlässigkeit solcher Systeme wird im Einzelfall zu prüfen sein.

E-Compliance ist also mindestens so sehr – und in Zukunft wohl noch mehr – eine *informationstechnische* wie juristische Aufgabe.

---

40 Dieses einzusetzen, schlägt WEBER, E-Governance, 364, als Konkretisierung von Ziff. 20 des Swiss Code of Best Practice vor.

41 Vgl. MÜLLER/PFITZMANN, 36 ff., und GIBLIN et al., passim.

42 Ein solches Produkt ist beispielsweise der KYC Spider (http://www.kyc.ch).

43 Vgl. DELANEY, 1.

44 LESSIG, Code, 6.

45 Vgl. zu diesen Fragen im Detail GRIMMELMANN, passim.

4.3 Innovation und Dynamisierung des Rechts

Die im vorangehenden Abschnitt aus der Unternehmensoptik skizzierte Verzahnung von IT und Recht spiegelt sich auch auf der systemischen Ebene wider. Besonders augenfällig wird diese Interdependenz anlässlich der Einführung eines Produkts, das auf einer informationstechnischen Innovation aufsetzt: Typischerweise durchlaufen technische Innovationen im hier interessierenden Kontext eine Reihe von Phasen[46], während derer es – aufgrund der „disruptive effects“ [47] der neuen Technologie – zu Konflikten kommt, die unter anderem auch in rechtlichen Arenen (Gerichte, Gesetzgebung) ausgetragen werden. Es lassen sich dabei idealtypisch drei Reaktionsweisen des Rechts unterscheiden[48]: erstens die Subsumtion neuer Phänomene unter bestehende Rechtsnormen[49]; zweitens die Schaffung neuer Rechtsnormen[50]; drittens eine subtilere Form rechtlicher Erneuerung, die sich beispielsweise dadurch bemerkbar macht, dass sie bestehende Strukturen des Rechts erschüttert[51] und sich oft in Reformbedarf äussert[52]. Alle diese Reaktionsweisen bewirken begriffsnotwenig eine *Dynamisierung des Rechts*[53], wobei die exakte Stossrichtung dieser Reaktionsweisen – analog zur „disruptive innovation“ – auch für Experten schwer

46 Grundlegend für den Bereich Informations- und Kommunikationstechnologie SPAR, insbes. 11-22, die zwischen vier Phasen unterscheidet: Innovation, Kommerzialisierung, Kreative Anarchie („creative anarchy“), sowie Regulierung („rules“).

47 Zur Theorie der „disruptive technology“ siehe CHRISTENSEN, passim. Manche „disruptive technologies“ – und allen voran die digitale Informationstechnologie im Vergleich zur analogen – führen zunächst oft zu Verwerfungen bei den Geschäftsmodellen, aber in einigen Fällen auch in der Rechtsordnung, indem sie beispielsweise bestehende rechtliche Institutionen obsolet machen. Dass diese Verwerfungen ihrerseits rechtliche Innovationen auslösen, ist wahrscheinlich, aber kein Automatismus, weil es dafür der Handlungen des Justizpersonals (Gerichte, Gesetzgeber, Akademie) bedarf.

48 GASSER, E-Commerce, 387 f. und 389 ff.

49 Für den Bereich des E-Commerce vgl. etwa WEBER, E-Commerce, passim.

50 Ein berühmtes Beispiel ist das Datenschutzrecht: siehe BasK-DSG-SEETHALER, N 3 und 9 zu Entstehungsgeschichte DSG.

51 Beispiele: Einerseits die Differenzierung zwischen dem Vertragsschluss unter Anwesenden (Art. 4 OR) und unter Abwesenden (Art. 5 OR), die im Zuge der technischen Entwicklung vordergründig aufrechterhalten bleibt, aber medienbedingt eine neue Struktur erhalten hat (GASSER, E-Commerce, 389 f.); andererseits die Unterscheidung zwischen „Führung“ und „Aufbewahrung“ von Geschäftsunterlagen (bzw. zwischen „Original“ und „Aufzeichnung“ eines Dokuments) in Art. 962 Abs. 2 aOR, die in der Revision von 2002 als technisch obsolet gestrichen wurde (BBl 1999 5152).

52 GASSER, E-Commerce, 390 f.

53 Illustrativ etwa das im Entstehen begriffene Recht der Suchmaschinen, vgl. GASSER, Search Engines, insbes. 131-143.

vorhersehbar sein kann. Dadurch kann beträchtliche, für die Unternehmen ausgesprochen unangenehme Rechtsunsicherheit entstehen. Beispiele hierfür sind das Grokster-Urteil des U.S. Supreme Court vom Sommer 2005[54] und jüngst die Klage von Viacom gegen YouTube[55] – Fälle, die für neuartige Dienstleister wie kuckstdu.indie.roehre.net unabsehbare Folgen haben bzw. haben können –, aber auch die vom Rechtsdienst der Brilliant Chemicals angesprochenen Unsicherheiten bei der Beweisführung mit Scans[56].

Auch in Gebieten, wo die Gesetzgeber relativ rasch auf das Phänomen der Digitalisierung und die Verbreitung des Internets reagiert haben, kann mitunter Rechtsunsicherheit herrschen – nicht nur betreffend die Anwendung der neuen Normen, sondern auch in Bezug auf die *zukünftige Rechtsentwicklung*, welche durchaus gegenläufig zur Entwicklung in der Vergangenheit sein kann: So wurden beispielsweise beidseits des Atlantiks in den späten 90er-Jahren und noch um die Jahrtausendwende Vorschriften erlassen, welche Online-Intermediäre aller Art von der Haftung für Inhalte Dritter ausnahmen, um die Entwicklung des E-Commerce zu fördern[57]. Seit der Jahrtausendwende hat dazu weltweit eine Gegenbewegung eingesetzt, die dazu tendiert, Online-Intermediäre für die Einhaltung des Rechts durch ihre Nutzer verantwortlich zu machen[58]. Anders ausgedrückt: Um selber *compliant* zu sein, müssen Online-Intermediäre ver-

---

54 *Metro-Goldwyn-Mayer Studios Inc., et al. v. Grokster, Ltd. et al.*, 125 S.Ct. 2764 (2005). Aufgrund der Urteile der Vorinstanzen sowie der gesamten Vorgeschichte wurde allgemein erwartet, der Supreme Court würde seine im Sony-Betamax-Urteil entwickelte Rechtsprechung zu sogenannten „dual-use"-Technologien, die sowohl für legale wie illegale Zwecke benutzt werden können, präzisieren und auf die Anwendbarkeit der sogenannten „Sony-Doktrin" in digitalen Netzwerken eingehen. Das Gericht liess indessen just diese Fragen offen und führte stattdessen eine neue, aus dem Patentrecht stammende, dogmatische Figur ins Urheberrecht ein, welche namentlich für Technologieentwickler unabsehbare Folgen hat. Vgl. dazu GASSER/PALFREY, passim.

55 Vgl. vorne Fn 29.

56 Zur aktuellen Situation in der Schweiz vgl. GASSER/HÄUSERMANN, 309 ff. Auch die zukünftige schweizerische ZPO wird die derzeitige Rechtsunsicherheit nicht gänzlich beseitigen können, obschon sie die Problematik berücksichtigt: HÄUSERMANN/GASSER, Rz. 12.

57 Dazu PALFREY/ROGOYSKI, 20. Beispiele sind Section 230 des U.S. Communications Decency Act, 47 U.S.C. § 230 (1996, zuletzt geändert 1998), und Section 512 Digital Millennium Copyright Act, 17 U.S.C. § 512 (1998, zuletzt geändert 1999), sowie die Beschränkung der Haftung von Intermediären in Art. 12-15 der E-Commerce-Richtlinie (2000/31/EG vom 8. Juni 2000).

58 PALFREY/ROGOYSKI, 20 ff.

mehrt auch die Einhaltung des Rechts durch ihre Nutzer sicherstellen. Die im Beispiel von kuckstdu.indie.roehre.net vom Risikokapitalgeber formulierten Fragen sind somit brandaktuell, und die Initianten tun vor diesem Erfahrungshintergrund gut daran, Massnahmen zur Früherkennung zukünftiger Rechtsentwicklungen in ihr Compliance-Konzept aufzunehmen.

Zusammenfassend lässt sich festhalten, dass E-Compliance im legislatorisch betrachtet jungen und dynamischen Umfeld des Internet- und IT-Rechts das Management von Schnittstellen-Risiken[59] unter Ungewissheitsbedingungen betreffend die gegenwärtige und zukünftige Rechtslage bedeutet.

4.4 Internationalität von Rechtsproblemen

Die Digitalisierung und insbesondere die Verbreitung des Internets hat alten und neuen Rechtsproblemen zusätzlich eine gewichtige internationale Dimension aufgesetzt. Die globale Reichweite des Internets (aber etwa auch der Intranets) und der damit zumindest potenziell[60] hergestellte Bezug zu einer Vielzahl nationaler Rechtsordnungen wird namentlich für Unternehmungen mit internationalem Tätigkeitsfeld zur grossen Herausforderung. Kollisionsrechtliche Fragen des E-Business sind dabei nur die Spitze des Eisbergs. Wesentlich anspruchsvoller ist die Sicherstellung der Einhaltung der – trotz bereichsweiser Harmonisierung im Detail regelmässig *unterschiedlichen – Rechtsnormen* bei gleichzeitiger und vielerorts schon weit fortgeschrittener Zentralisierung der IT-Infrastruktur und der Forderung des Managements nach einheitlichen Richtlinien für das Informationsmanagement (zum Beispiel Document Retention Policy) und die elektronische Kommunikation (zum Beispiel E-Mail-Policy)[61].

Die auch aus IT-Sicht anforderungsreiche Compliance-Aufgabe wird zusätzlich in jenen Fällen erschwert, in denen die Regelungsmodelle,

---

59 Dazu mehr hinten, Abschnitt 5.

60 Namentlich in Australien und in Kanada sind in jüngerer Vergangenheit im Bereich des E-Business interessante Urteile zu den Minimalanforderungen an die gerichtliche Zuständigkeit ergangen. Vgl. *Dow Jones & Company Inc. v. Gutnick*, High Court of Australia, [2002] HCA 56, 10.12.2002, abrufbar unter http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html und *Bangoura v. The Washington Post et al.*, Court of Appeal for Ontario, 16.9.2005, No. C41379, abrufbar unter http://www.ontariocourts.on.ca/decisions/2005/september/C41379.htm.

61 Allgemein zum informationsrechtlichen Spannungsverhältnis zwischen Internationalisierung des Informationsrechts und informationellen Orts- und Kontextbindungen GASSER, Delokalisierung, passim.

Rechtsauffassungen und Rechtsnormen nicht nur divergieren, sondern sich gar *widersprechen*. Ein aktuelles Beispiel, welches derzeit vor allem den Finanzsektor beschäftigt, betrifft die elektronische Beweisbeschaffung in Zivilprozessen dies- und jenseits des Atlantiks[62]. Nach verbreiteter amerikanischer Auffassung erstreckt sich eine sogenannte E-Discovery auf sämtliche (relevanten) elektronischen Unterlagen, auf welche die beklagte Partei (zum Beispiel die US-Tochter einer Schweizer Bank) Zugriff hat – unabhängig vom Ort der Datenspeicherung bzw. dem physischen Serverstandort. Diese Praxis steht nach dominierender europäischer Auffassung im Widerspruch zu den Prinzipien der internationalen Rechtshilfe[63] und kann die verantwortlichen Personen allenfalls gar mit dem schweizerischen Strafrecht in Konflikt bringen (Art. 271 und 273 StGB)[64].

Hinzu kommt, dass die Vernetzung der Welt über das Internet der *extraterritorialen Anwendung* nationalen Rechts nochmals einen Schub gegeben hat: Der vielzitierte Sarbanes-Oxley Act[65] beispielsweise gilt nicht nur für nicht-amerikanische, in den USA zweitkotierte Gesellschaften[66], sondern unter Umständen auch für ausländische Unternehmungen, die mehr als 300 US-amerikanische Aktionäre haben[67]. Auch die EU-Datenschutzrichtlinie[68] hat indirekt extraterritoriale Geltung, weil der Transfer von Personendaten in Drittländer ohne angemessenes Datenschutzniveau nur unter sehr restriktiven Voraussetzungen zulässig ist (Art. 25 Abs. 1 und 26 Abs. 1 Datenschutzrichtlinie). Dies hat die USA bekanntlich veranlasst, in Zusammenarbeit mit der Europäischen Kommission ein Selbstzertifizierungsprogramm für US-Unternehmen (den sogenannten „Safe Harbor") zu entwickeln[69]. Grosse Schweizer Unternehmungen wie die Brilliant Chemicals AG aus unserem Beispiel können sich diesen Rechtsakten realistischerweise nicht entziehen.

---

62 Vgl. GASSER/HÄUSERMANN/MÜLLER, B 4.

63 Etwa dem Haager Übereinkommen über die Beweisaufnahme im Ausland in Zivil- oder Handelssachen (HBÜ) vom 8. März 1970, SR 0.274.132. Zum Problemkreis Discovery und Haager Beweisübereinkommen MEIER, passim.

64 Dazu und zur E-Discovery allgemein GASSER/THURMAN (in Vorbereitung). Im Bankenbereich wird darüber hinaus die Frage des Verhältnisses von E-Discovery und Bankgeheimnis (Art. 47 BankG) diskutiert.

65 Zum Beispiel VON DER CRONE/ROTH, 131 ff.; BERTSCHINGER/SCHAAD, 883 ff.

66 VON DER CRONE/ROTH, 136 m.H.

67 Die betreffenden Rules der Securities Exchange Commission (SEC) werden zurzeit freilich überarbeitet (vgl. SEC Release No. 34-55005 (2006), abrufbar unter http://www.sec.gov/rules/proposed/2006/34-55005.pdf, Abschnitt II.A.).

68 Richtlinie 95/46/EG vom 24. Oktober 1995.

69 Vgl. ANTOKOL, 31, insbes. Fn. 10 und 11.

E-Compliance muss indes nicht nur die Nutzung eines globalen Mediums mit lokalen Gesetzen synchronisieren, sondern auch unter Umständen stark divergierende *soziale Normen*[70] sowie *ethische Grundsätze* berücksichtigen, ganz im Sinne des eingangs erwähnten breiten Verständnisses von „Compliance“[71]. Ein besonders eindrucksvolles Beispiel dieser (oft vernachlässigten) Dimension von E-Compliance bietet der Fall der amerikanischen Internet-Intermediäre, die aufgrund ihrer Geschäftstätigkeit in China und der „Compliance“ mit chinesischem „Recht“ in ihrem Heimatland ins Kreuzfeuer der Kritik geraten sind[72]. Als Folge öffentlichen Drucks wurden im Kongress Hearings veranstaltet und ein Gesetzesentwurf eingebracht, der sicherstellen will, dass amerikanische Internet-Unternehmen, welche in Ländern mit repressiven Regimes arbeiten, nicht gegen die rechtlichen und ethischen Grundsätze der USA betreffend freie Meinungsäusserung und Privatsphärenschutz verstossen[73]. Die betroffenen Unternehmungen sind nun daran, das an den Hearings abgegebene Versprechen einzulösen, einen „Code of Ethics“ auszuarbeiten, und werden dabei durch eine Gruppe von universitären Forschungszentren[74] unterstützt. Damit möchten sie der – nach Meinung von Beobachtern – ungünstigen Gesetzgebung zuvorkommen. Dies leitet über zum nächsten Charakteristikum von E-Compliance: der gesteigerten Bedeutung von „Soft Law“.

4.5 Bedeutungszuwachs von Soft Law

Die mit der Dynamisierung des Rechts einhergehende Rechtsunsicherheit, die besonders ausgeprägte Internationalität der Rechtsprobleme digitaler Kommunikation sowie die bereichsweise hohe Technizität der Regelungsmaterie haben dazu beigetragen, dass das sogenannte „Soft Law“, also zum Beispiel internationale Standards, Verhaltenskodizes und „Best Prac-

70 Schon im Vergleich Europa-USA bestehen bedeutende Mentalitätsunterschiede: Beispielsweise sind die Anforderungen an „political correctness“ hierzulande deutlich lockerer als in den USA.

71 Siehe vorne bei Fn. 10 f.

72 Vgl. stellvertretend THOMPSON, 1. Auf globale Auswirkungen primär lokaler Handlungen weist auch BUFF, N 39, hin.

73 Vgl. Global Online Freedom Act of 2006, H.R. 4780, abrufbar unter http://www.govtrack.us/congress/billtext.xpd?bill=h109-4780.

74 Darunter die Forschungsstelle für Informationsrecht an der Universität St. Gallen (FIR-HSG, http://www.fir.unisg.ch), an welcher die Autoren dieses Beitrags tätig sind. Vgl. PALFREY, Testimony.

tice Models“[75], einen wesentlichen Anteil an der Gesamtheit der Normen ausmacht, die im Rahmen der E-Compliance zu berücksichtigen sind[76]. Diese ausser- oder vorrechtlichen Normen betreffen unterschiedlichste Materien und alle Ebenen der elektronischen Kommunikation, einschliesslich der physischen und logischen Infrastruktur sowie der Inhalte („content“). Die folgende Auswahl an Beispielen mag die thematische Vielfalt verdeutlichen:

- IT-Sicherheit: die Standards BS 7799/ISO 17799 und Cobit[77] sowie die OECD Guidelines for the Security of Information Systems and Networks[78] und die OECD Guidelines for Cryptography Policy[79];
- Datenschutz: das „Web Privacy Seal“ von TRUSTe[80] sowie die OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[81];
- Freiwillige Inhaltskontrolle der Online-Intermediäre: die Verhaltenskodizes von Verbänden der Access-Provider, Hosting Services und Suchmaschinen in Deutschland, Frankreich und dem Vereinigten Königreich[82];
- Records Management: der Standard ISO 15489-1 (bzw. eCH-0002) sowie zu dessen Konkretisierung und Umsetzung eCH-0026 und eCH-0038[83].

Die Relevanz dieser heterogenen Normbestände variiert naturgemäss mit dem Geschäftsmodell, dem geografischen Tätigkeitsbereich, der Produkte- und Servicepalette etc. des jeweiligen Unternehmens. Bereits aus diesen wenigen Beispielen wird aber ersichtlich, dass „Soft Law“ nicht nur für Unternehmungen der „Dot-com“-Branche eine Rolle spielt: Während für kuckstdu.indie.roehre.net die soeben erwähnten Kodizes der On-

75 Begriffliche Klärungen bei SCHREIBER, 53-65.
76 Vgl. BUFF, N 600.
77 Dazu WEBER/WILLI, 67-70.
78 Abrufbar unter http://www.oecd.org/dataoecd/16/22/15582260.pdf.
79 Abrufbar unter http://www.oecd.org/document/11/0,2340,en_2649_34255_1814731_1_1_1_1,00.html.
80 Dazu WEBER, Regulatory Models, 167-169.
81 Abrufbar unter http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.
82 Deutschland: Verein Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V. (http://www.fsm.de); Frankreich: Association des Fournisseurs d'Accès et de Services Internet (http://www.afa-france.com); UK: Internet Watch Foundation (http://www.iwf.org.uk). Zu den Vor- und Nachteilen solcher Ansätze WEBER, Regulatory Models, 195-202.
83 Alle abrufbar unter http://www.ech.ch.

line-Intermediäre und Datenschutznormen zentral sein werden[84], wird sich die „traditionelle" Industrieunternehmung Brilliant Chemicals – neben den Datenschutznormen – in erster Linie für Records Management- und IT-Sicherheitsstandards interessieren.

5. Aufgaben und Herausforderungen der E-Compliance: Risikomanagement

Aus den bisherigen Ausführungen geht hervor, dass sich E-Compliance insbesondere (aber längst nicht nur) mit der *Prüfung der Einhaltung* von Rechts- und anderen verhaltenslenkenden Normen befasst. Als *weitere Funktionen* fallen hier wie bei der herkömmlichen Compliance auch folgende Aufgaben in Betracht: das aktive Verfolgen der rechtlichen, regulatorischen, technischen und marktlichen Entwicklungen; die Unterstützung beim Erlass interner Richtlinien und Weisungen (zum Beispiel E-Mail-Policy); das Mitwirken bei der Entwicklung von Branchenstandards und Best Practices; die Information und Ausbildung von Mitarbeitern; das Ausarbeiten von Vorschlägen von organisatorischen Massnahmen; die Beratungstätigkeit im Falle konkreter Anfragen usw.[85]

Der Akzent bei der Erfüllung dieser Aufgaben liegt dabei bei der E-Compliance, wie bereits erwähnt, auf dem *Management der Risiken an der Schnittstelle von Recht, Technologie und Markt.* Dieser Fokus auf Risikomanagement ist nicht neu, denn verschiedene Faktoren haben dazu geführt, dass Compliance heute allgemein als Element des Risikomanagements verstanden wird[86]. Zu den „Motoren" dieser Entwicklung gehören namentlich die Mindestkapitalanforderungen des Basler Komitees für Bankenaufsicht (Basel II), welche auch operationelle Risiken umfassen, darunter insbesondere rechtliche Risiken[87]. Basel II richtet sich naturgemäss an die Banken, doch dürften die Richtlinien auch die Kreditvergabe-

84 Siehe vor Fn. 82.

85 Zu den Aufgaben und Funktionen der Compliance allgemein SUHR BRUNNER/PORTMANN, 1036.

86 So BÖCKLI, Swiss Code of Best Practice, 990; ähnlich HELBLING, 684. Zu den Pflichten des Verwaltungsrats in diesem Bereich siehe BUFF, N 293 ff.

87 WEBER, Risikomanagement, 186; PFENNINGER/BÜRGI, 290, beide m.w.H. Welche Arten rechtlicher Risiken Basel II genau abdeckt, ist freilich umstritten. Ein wichtiger Diskussionspunkt ist dabei deren Quantifizierbarkeit. Ferner zählen nach einer Lehrmeinung Risiken im Zusammenhang mit E-Commerce unter den Begriff der operationellen Risiken. Vgl. zum Ganzen PFENNINGER/BÜRGI, 292.

politik der Banken beeinflussen, indem sie die Kreditwürdigkeit von Unternehmen, welche ungenügende Massnahmen zum Management operationeller Risiken getroffen haben, geringer einstufen[88]. Weiter hat sich die Erkenntnis durchgesetzt, dass sich rechtliche Probleme bis hin zu Rechtsverstössen nie ganz verhindern lassen, diese mithin zum allgemeinen Geschäftsrisiko gehören, und dass ein rationaler Umgang mit diesen Risiken Bestandteil einer „Good Corporate Governance" ist[89].

Was beinhaltet ein rationaler Umgang mit Risiken im Einzelnen? Beim Risikomanagement sind in einem ersten Schritt die relevanten Risiken zu identifizieren und, wenn möglich quantitativ, zu bewerten[90]. Zu diesem Zweck müssen die Bedingungen, unter denen ein Risiko entsteht und sich realisieren kann, analysiert und deren Eintrittswahrscheinlichkeit wie auch das Schadenspotenzial abgeschätzt werden. In der Folge lassen sich Massnahmen, die auf Risikominimierung abzielen, entwerfen, priorisieren und schliesslich umsetzen[91].

Werden nun Compliance-Fragen (mindestens teilweise) als rechtliche Risiken interpretiert und mit der Methodik des Risikomanagements zu bewältigen versucht, eröffnen sich freilich – wie die Praxis lehrt – zwei bedeutende Problemkreise: Erstens beim Personal, das heisst bei (unternehmensinternen oder externen) Juristen, die fast zwangsläufig dazu berufen sind, rechtliche Risiken zu identifizieren und zu bewerten[92], weil dafür theoretische und praktische Rechtskenntnisse notwendig sind. Diesen fehlt jedoch in der Regel das Handwerkszeug dazu, insbesondere die Beherrschung quantitativer Methoden[93]. Zudem ist die Inkaufnahme von Risiken dem auf Absicherung gerichteten juristischen Denken fremd, woraus eine Risikoaversion entstehen kann, die sich zumindest in Unverständnis gegenüber einem Risikomanagement-Ansatz äussern kann. Der zweite Problemkreis liegt bei den Informationen, genauer bei den quantitativen Da-

88 Vgl. WEBER, Risikomanagement, 186.

89 So implizit BUFF, N 293. In diese Richtung geht die Aktienrechtsreform 2007, welche für Gesellschaften, die der ordentlichen Revision unterstehen, ein internes Kontrollsystem vorschreibt (Art. 728a Abs. 1 Ziff. 3), das auch das „Legal Risk Management" zum Gegenstand haben soll. Dazu WYSS, passim.

90 Statt aller: BUFF, N 293.

91 Vgl. etwa das Risk Management Framework, das WEBER, Risk Management, 472, skizziert. Siehe auch WYSS, 36 f.

92 So implizit PFENNINGER/BÜRGI, 294 (mit Bezug auf den Bankensektor).

93 Daneben kann auch der Wechsel von überwiegend reaktiver Juristentätigkeit zum vorausschauenden Risikomanagement (vgl. PFENNINGER/BÜRGI, 294) Schwierigkeiten bereiten.

ten, die für eine verlässliche Risikoabschätzung unabdingbar sind[94]: Gerichtsfälle, die einen bestimmten Typ von Compliance-Risiken vertreten, sind rar und meist sehr schlecht miteinander vergleichbar.

Diese allgemeinen Schwierigkeiten im Umgang mit Risiken werden durch einige *Besonderheiten* des Betrachtungsgegenstands der E-Compliance akzentuiert. Auf rechtstatsächlicher Ebene ist auf den in Abschnitt 4.3 angesprochenen raschen technologischen Wandel hinzuweisen, der zu einer Dynamisierung des Rechts und insbesondere zur verminderten Vorhersehbarkeit zukünftiger Rechtsentwicklungen führt. Damit wird es noch schwieriger bis unmöglich, rechtliche Risiken zu quantifizieren: Während die Unternehmen in „traditionellen" Risikobereichen der Compliance in der Regel auf einen reichen Erfahrungsschatz zurückgreifen können, um rechtliche Risiken abzuschätzen[95], ist genau dies mit Blick auf jene Schnittstellenrisiken, mit welchen sich E-Compliance beschäftigen muss[96], nicht möglich. Diese Besonderheiten gilt es auf organisatorischer Ebene zu berücksichtigen, wie der nächste Abschnitt argumentiert.

6. Auswirkungen auf die Unternehmensorganisation

Wie bereits erwähnt, ist der Verwaltungsrat für die Festlegung der Unternehmensorganisation und damit auch für die Festlegung und „Einbettung"

94 Vgl. auch PFENNINGER/BÜRGI, 292.

95 In der Finanzbranche beispielsweise besteht zumindest die Chance, dass das vorhandene Datenmaterial quantitative Aussagen darüber zulässt, in welchen Fällen die Vermögensverwalterin von einem Kunden verklagt wird oder wie häufig Finanzprodukte aus vertragsrechtlichen Gründen Verluste generieren, vgl. PFENNINGER/BÜRGI, 292. Ähnliches gilt für Risiken, die im Rahmen eines staatlichen Aufsichtsverhältnisses bestehen, zum Beispiel in der Finanz-, Pharma- oder Luftfahrtbranche.

96 Beispiel 1: Bevor Papierdokumente eingescannt und die Originale vernichtet werden, sind unter anderem die Risiken der Beweislosigkeit in einem zukünftigen Prozess abzuschätzen (etwa weil sich die Echtheit einer Unterschrift nicht nachweisen lässt). Hierzu existiert nicht nur keine Praxis, sondern es ist auch aus theoretischen Gründen äusserst schwierig, das Verhalten der Gerichte vorherzusagen, nicht zuletzt weil die Einstellung der Richter gegenüber neuen Technologien unberechenbar ist (siehe GASSER/HÄUSERMANN, 311).
Beispiel 2: Ob und inwiefern sich der Online-Intermediär der Verantwortlichkeit für Urheberrechtsverletzungen seiner Nutzer aussetzt, ist sogar in den USA, wo die Gerichtspraxis zum Urheberrecht vergleichsweise reichhaltig ist, höchst ungewiss (vgl. PALFREY, Making a Market, abrufbar unter http://blogs.law.harvard.edu/palfrey/2006/10/11/).

der Compliance-Organisation verantwortlich[97]. Die Anforderungen und Aufgaben sowie die organisatorische Ausgestaltung müssen dabei selbstverständlich den sich *verändernden Rahmenbedingungen angepasst* werden, auch mit Blick auf den paradigmatischen Wandel von einem papierbasierten zu einem digital vernetzten informationellen Ökosystem der Unternehmensinformation. Die folgenden Überlegungen mögen dazu einige Hinweise bieten.

6.1 Zusammenspiel von IT und Recht meistern

Wie dargelegt, ist E-Compliance ebenso sehr eine technische wie juristische Aufgabe[98]. Erfolgreiche E-Compliance setzt deshalb viel Schnittstellenwissen zwischen IT und Recht voraus. Dementsprechend gehört eine institutionalisierte und enge Zusammenarbeit zwischen Compliance- und IT-Abteilungen zu einer guten Unternehmensorganisation[99]. Die Kommunikation zwischen Informatikern und Juristen ist angesichts der verschiedenen Denkweisen und Arbeitsmethoden der beteiligten Personen indes erfahrungsgemäss nicht immer einfach, aber sowohl bei der Identifikation als auch der Bewertung von Risiken an der Schnittstelle von Recht und Technologie unentbehrlich.

6.2 Veränderungen rechtzeitig erkennen

E-Compliance ist, so das vorn entwickelte Argument, in hohem Masse durch technologischen Fortschritt gekennzeichnet, welcher seinerseits rechtlichen Anpassungsbedarf erzeugt[100]. Im Ergebnis entwickelt sich so das rechtliche Umfeld der Informationstechnologien ähnlich dynamisch wie die Technologien selber. Unternehmen, welche die rechtlichen Entwicklungen nicht vorhersehen, riskieren im Extremfall den Totalverlust

---

97 Siehe vorne vor Fn. 13.

98 Siehe vorne, Abschnitt 4.2 am Ende.

99 Daneben ist die Trennung zwischen Rechtsdienst und Compliance-Abteilung zu überdenken (PFENNINGER/BÜRGI, 294), es sei denn, der Rechtsdienst sei ausschliesslich für die Prozessführung zuständig. Doch selbst in diesem Szenario ist der stete Kontakt zwischen Rechtsdienst und Compliance-Abteilung unentbehrlich, alleine schon, damit Letztere mit Datenmaterial zur Risikoabschätzung versorgt wird.

100 Siehe vorne, Abschnitt 4.3.

ihres Geschäftsmodells, wie das Beispiel von Grokster zeigt[101]. In gewissen Konstellationen – auch der fiktive Anwendungsfall kuckstdu.indie.roehre.net gehört dazu – kann es mit anderen Worten überlebenswichtig sein, das Politik- und Rechtssystem kontinuierlich und systematisch im Sinne einer „Rechts-Früherkennung" auf Signale hin abzufragen, die mögliche Veränderungen ankündigen[102]. Dies kann beispielsweise durch Gründung eines oder Zusammenarbeit mit einem interdisziplinären[103] Think Tank geschehen. Ein solches Frühwarnsystem drängt sich bei „Dotcom"-Unternehmungen geradezu auf, wiewohl es auch für Firmen in traditionellen Branchen wie dem Finanzsektor von strategischer Bedeutung sein kann, rechtliche Entwicklungen zu antizipieren.

6.3 Globalen Blickwinkel einnehmen

Aus dem diskutierten Merkmal der Internationalität des Gegenstands von E-Compliance[104] ergibt sich die Notwendigkeit, im Rahmen der Ausgestaltung der Unternehmensorganisation jene Voraussetzungen zu schaffen, die es erlauben, dass diese aus einer *globalen Optik* erfolgen kann. Internationalität von E-Compliance bedeutet dabei zunächst, dass (hier wie bei der traditionellen Compliance) fundierte Kenntnisse über jene betroffenen Rechtsordnungen aufgebaut werden können, zu denen Anknüpfungspunk-

101 Siehe vorne, Fn. 54.

102 Die aus dem strategischen Management stammende Lehre von der Technologie-Früherkennung liefert nützliche Hinweise, wie sich eine „Rechts-Früherkennung" bewerkstelligen lässt: Die Literatur versteht unter Technologie-Früherkennung „das systematische Beobachten und das Erkennen neuer Technologien …, die sich häufig in Form ‚schwacher Signale' ankündigen" (REGER, 304, m.H.). Es geht dabei also nicht um Prognosen, sondern um Vorausschau. In der Praxis wird Technologie-Früherkennung dabei grossteils auf Konzern-Ebene, als Teil des strategischen Forschungs- und Entwicklungsmanagements, betrieben. Die Organisationsformen sind vielfältig; in einigen Fällen ist die Technologie-Früherkennung als Stabsstelle organisiert und mit einem internen Netz von bis zu hundert „Informanten" aller Hierarchiestufen verbunden. Nicht selten werden auch Netzwerke mit Forschungsinstitutionen, Berufsverbänden, Standardisierungskomitees und dergleichen gebildet. Vgl. zum ganzen Themenkomplex ausführlich REGER, 304 ff.

103 Der Ansatz leitet sich direkt von der St. Galler informationsrechtlichen Betrachtungsweise (Englisch: Information Law Approach) ab, d.h. der Betrachtung informationeller Phänomene durch eine Folie, die sich aus der Schnittmenge von Recht, Technik, Wirtschaft und Politik zusammensetzt: BURKERT, Aufgaben, 156; GASSER, Information Law, 12 ff.; BURKERT, Information Law Approach, 76 ff.

104 Siehe vorne, Abschnitt 4.4.

te bestehen. Damit lassen sich auch mögliche Konfliktzonen identifizieren und aktiv bearbeiten, die das Spannungsverhältnis zwischen globaler Infrastruktur und lokalem Recht[105] hervorruft. Zur hier geforderten globalen Optik zählt aber auch der Aufbau von „weichem" Wissen, da kulturspezifische soziale Normen bei der E-Compliance ebenfalls zu berücksichtigen sind[106]. Organisatorisch bedeutet dies konkret, dass zwischen den geografisch oft getrennten Compliance-Abteilungen eines Grossunternehmens ein kontinuierlicher Informationsfluss sichergestellt werden muss. In der Praxis wird entsprechendes Wissen überdies oft durch den Beizug externer Berater oder die Bildung von sogenannten Advisory Boards bereitgestellt.

6.4 Unternehmensübergreifende Zusammenarbeit verstärken

Im Bereich der E-Compliance erscheint eine vermehrte unternehmensübergreifende Zusammenarbeit geboten. Zum einen empfehlen sich Kooperationen im Sinne der Bildung von „communities of knowledge", um die hohe Komplexität der Problemstellungen im Bereich E-Compliance, die teils branchenspezifisch[107], teils branchenübergreifend[108], aber kaum je unternehmensspezifisch sind, überhaupt angemessen bewältigen zu können. Zum anderen – möglicherweise noch wichtiger – erfordert der Bedeutungszuwachs von „Soft Law"[109], welches regelmässig dem Zusammenwirken verschiedener Akteure innerhalb einer Branche entspringt, na-

105 Siehe vorne vor Fn. 61.

106 Siehe vorne vor Fn. 70.

107 Neue branchen*spezifische* Problemstellungen ergeben sich, wo sektorspezifische Spezialgesetzgebung auf „E-Sachverhalte" anwendbar ist: zum Beispiel gilt das Bankgeheimnis (Art. 47 BankG) auch für den E-Mail-Verkehr, doch ist dieser Bereich besonders anfällig für Verletzungen: Eine von einem US-Gericht angeordnete E-Discovery kann sich durchaus auf E-Mails oder andere elektronische Informationen beziehen, die in der Schweiz aufbewahrt werden und dem Bankgeheimnis unterstehen. Allgemein lässt sich vermuten, dass die meisten neuen Rechtsfragen in stark regulierten Branchen (wie zum Beispiel Finanzdienstleistungen, Pharma) auftauchen. Immerhin existiert dort meistens eine Regulierungsbehörde, die Probleme und Unsicherheiten idealerweise rasch erkennt und sie rechtssicher entscheidet.

108 Die wichtigsten branchen*übergreifenden* Fragestellungen betreffen die Aufbewahrung elektronischer Daten, Fragen des internationalen Datenschutzes, E-Mail-Aufbewahrung, Konsumentenschutz im E-Commerce u.a.m., vgl. BUFF, N 598.

109 Siehe vorne, Abschnitt 4.5.

türlich die Bereitschaft der Branchenmitglieder, an dessen Ausarbeitung auch mitzuwirken. Hier mündet die unternehmensübergreifende Zusammenarbeit zumindest teilweise auch in neue Formen der „Public-Private-Partnership“[110].

Neben diesen Formen der institutionalisierten Zusammenarbeit ist auch der *informelle Erfahrungsaustausch* über die Unternehmensgrenzen hinweg nicht zu vernachlässigen: Gerade weil Fragen der E-Compliance in der Regel neu und mit beträchtlicher Rechtsunsicherheit behaftet sind, ist jeder einzelne Praxisfall ein „reality check“ für Massnahmen, deren Tauglichkeit im Zeitpunkt, als sie getroffen wurden, in der Regel nur aufgrund theoretischer Überlegungen beurteilt werden konnte.

7. Schluss

Das Rechtssystem hat die Veränderungen in der Informations- und Kommunikationstechnologie im Unternehmensalltag – und damit an der Schnittstelle von Markt, Technologie und Recht – durch bedeutende Anpassungsleistungen bewältigt. Eine Unternehmung muss ihrerseits eine Anpassungsleistung erbringen, um die Effekte der Anpassungsleistungen des Rechtssystems zu bewältigen. Dass dies eine grössere Herausforderung darstellt, als das Absenken der kurzfristig gestiegenen Entropie um Begriffe wie „E-Commerce-Recht“ oder „Cyberlaw“ suggerieren würde, war die Beobachtung der Autoren, die diesem Essay vorausging. Eine erste Annäherung an Konzept, Merkmale, Aufgaben und organisatorische Leitprinzipien von E-Compliance bestätigt diesen Befund.

E-Compliance sieht sich dabei, wie in diesem Beitrag diskutiert, mit den Phänomenen einer engen Verzahnung von Recht und Technologie, einer ausgeprägten Dynamisierung des Rechts, einer massiven Internationalisierung von Sachfragen und Rechtsproblemen sowie einer stark erhöhten Bedeutung von „Soft Law“ konfrontiert. Diese Merkmale, die teilweise auch auf vertraute Bereiche der Compliance wie beispielsweise Finanzmarktrecht zutreffen mögen, erfordern in ihrem Zusammenspiel eine Weiterentwicklung bestehender Compliance-Konzepte und eine Anpassung der entsprechenden Organisation. Die wechselseitigen Bezüge zwischen „klassischer“ Compliance und E-Compliance werden sich dabei mit der immer noch zunehmenden Verquickung von organisatorischem Nexus

[110] Vgl. etwa WEBER, Risk Management, 476, für das Risikomanagement im Bereich Informationsinfrastrukturen.

und Informations- und Kommunikationstechnologie verstärken. Die Ansicht, E-Compliance sei bloss einer von vielen „Schutz- bzw. Risikobereichen" der Compliance[111], erscheint uns deshalb überholt: E-Compliance ist eine eigentliche Querschnittsaufgabe, wiewohl es natürlich Rechtsgebiete gibt, die von der Digitalisierung tatsächlich besonders betroffen sind (oder auch: von denen die Digitalisierung besonders betroffen ist)[112] und deshalb im Rahmen der E-Compliance besonderes Gewicht haben.

Damit ist abschliessend auch verdeutlicht, dass die Autoren keineswegs „E-Sonderrechte" oder einen „E-Sonderbereich" inner- oder ausserhalb bestehender Compliance-Instanzen fordern. Vielmehr plädieren wir für ein *integriertes und umfassendes Compliance-Konzept*, das – im Gleichschritt mit der Digitalisierung – den in diesem Beitrag skizzierten strukturellen Besonderheiten von E-Compliance angemessen Rechnung trägt.

[111] Siehe vorne bei Fn. 17.
[112] Siehe vorne, Abschnitt 3.2.

Literaturverzeichnis

ANTOKOL, JOAN: Complying with Data Privacy Requirements. A Look at Challenges Faced by Multinational Companies, digma 2005, 30.

BALSCHEIT, PHILIPP: Konsumvertragsrecht und E-Commerce, Eine Übersicht, Bern 2005.

BERTSCHINGER, PETER/SCHAAD, MARTIN: Der amerikanische Sarbanes-Oxley Act of 2002 – Mögliche Auswirkungen auf die amerikanische und internationale Wirtschaftsprüfung und Corporate Governance, ST 2002, 883.

BÖCKLI, PETER (Swiss Code of Best Practice): Harte Stellen im Soft Law – Zum Swiss Code of Best Practice for Corporate Governance, ST 2002, 981.

BÖCKLI, PETER (Aktienrecht): Schweizer Aktienrecht, Zürich 2004.

BUFF, HERBERT: Compliance, Diss., Zürich 2000.

BÜHLER, THEODOR: Corporate Governance und Compliance: Modewörter oder Bedürfnis im schweizerischen Aktienrecht, in: VON DER CRONE, HANS CASPAR/WEBER, ROLF H./ZÄCH, ROGER/ZOBL, DIETER (Hrsg.): Neuere Tendenzen im Gesellschaftsrecht: Festschrift für Peter Forstmoser zum 60. Geburtstag, Zürich 2003, 211.

BURKERT, HERBERT (Aufgaben): Von künftigen Aufgaben des Informationsrechts, in: MEIER-SCHATZ, CHRISTIAN J./SCHWEIZER, RAINER J. (Hrsg.): Recht und Internationalisierung, Zürich 2000, 155.

BURKERT, HERBERT (Internetrecht): Internetrecht – Informationsrecht, Vom zwar Nützlichen aber eher Zufälligen zurück zum möglicherweise Wesentlichen?, in: SCHWEIZER, RAINER J./BURKERT, HERBERT/GASSER, URS (Hrsg.): Festschrift für Jean Nicolas Druey, Zürich 2002, 693.

BURKERT, HERBERT (Information Law Approach): The Information Law Approach: An Exemplification, in: GASSER, URS (Hrsg.): Information Quality Regulation: Foundations, Perspectives, and Applications, Baden-Baden 2004, 75.

CHRISTENSEN, CLAYTON M.: The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail, Boston 2003.

VON DER CRONE, HANS CASPAR/ROTH, KATJA: Der Sarbanes-Oxley Act und seine extraterritoriale Bedeutung, AJP 2003, 131.

DELANEY, KEVIN J.: Copyright Tool Will Scan Web For Violations, The Wall Street Journal Online, December 18, 2006, abrufbar unter http://tinyurl.com/sjmp6.

GASSER, URS (Delokalisierung): Delokalisierung des Wissens – Internationalisierung des Informationsrechts?, in: MEIER-SCHATZ, CHRISTIAN J./SCHWEIZER, RAINER J. (Hrsg.): Recht und Internationalisierung, Zürich 2000, 175.

GASSER, URS (E-Commerce): E-Commerce: Innovation im (Vertrags-)Recht?, SJZ 2001, 386.

GASSER, URS (Information Law): What is Information Law – and what could it be?, in: GASSER, URS (Hrsg.): Informationsrecht in „e"-Umgebungen – Information Law in eEnvironments, Baden-Baden 2004, 7.

GASSER, URS (Search Engines): Regulation of Search Engines: Taking Stock and Looking Ahead, 9 Yale Journal of Law & Technology 124 (2006).

GASSER, URS/ERNST, SILKE: From Shakespeare to DJ Danger Mouse: A Quick Look at Copyright and User Creativity in the Digital Age, Berkman Center Research Publication No. 2006-05, abrufbar unter http://ssrn.com/abstract=909223.

GASSER, URS/HÄUSERMANN, DANIEL MARKUS: Beweisrechtliche Hindernisse bei der Digitalisierung von Unternehmensinformationen, AJP 2006, 305.

GASSER, URS/HÄUSERMANN, DANIEL M./MÜLLER, MICHAEL: E-Mail im Wechselspiel von IT und Recht, NZZ vom 16. Mai 2006, B 4.

GASSER, URS/PALFREY, JOHN G.: Catch-as-Catch-Can: A Case Note On Grokster, abrufbar unter http://ssrn.com/abstract=869030 (Kurzfassung unter demselben Titel in SZW 2006, 119).

GASSER, URS/THURMAN, JAMES M.: E-Discovery: Neuerungen im amerikanischen Prozessrecht – Konsequenzen für die Schweiz? (zur Publikation vorgesehen in ZZZ 2007).

GIBLIN, CHRISTOPHER/LIU, ALICE Y./MÜLLER, SAMUEL/PFITZMANN, BIRGIT/ZHOU, XIN: Regulations Expressed As Logical Models (REALM), in: MOENS, M.-F./SPYNS, P. (Hrsg.): Proceedings of the 18th Annual Conference on Legal Knowledge and Information Systems (JURIX 2005), Amsterdam 2005, 37, abrufbar unter http://www.zurich.ibm.com/security/publications/2005/GiLiMuPfZh05aREALM-JURIX.pdf.

GRIMMELMANN, JAMES: Regulation by Software, 114 Yale Law Journal 1719 (2005).

HÄUSERMANN, DANIEL MARKUS/GASSER, URS: Beweisführung mit Scans im Entwurf zur schweizerischen ZPO: Bundesrat schafft mehr Rechtssicherheit, in: Jusletter vom 17. Juli 2006, abrufbar unter http://www.weblaw.ch/jusletter/Artikel.asp?ArticleNr=4895.

HELBLING, CARL: Risk & Management Control – Überwachung der Risiken als Teil der Corporate Governance, ST 2003, 681.

LESSIG, LAWRENCE (Code): Code and Other Laws of Cyberspace, New York 1999.

LESSIG, LAWRENCE (Public Domain): Re-Crafting a Public Domain, 18 Yale Journal of Law and the Humanities 56 (2006).

LUNDEEN, KYLE: Searching for a Defense: The Google Library Litigation and the Fair Use Doctrine, 75 University of Missouri–Kansas City Law Review 265 (2006).

MAURER-LAMBROU, URS/VOGT, NEDIM PETER (Hrsg.) (BasK-DSG-BEARBEITER): Basler Kommentar zum Datenschutzgesetz, Basel/Genf/München 2006.

MEIER, ANDREAS L.: Die Anwendung des Haager Beweisübereinkommens in der Schweiz, Basel et al. 1999.

O'MELVENY & MYERS LLP: Shifting the Costs of Restoring and Producing Electronic Data to Plaintiffs May Be More Difficult After Judge Scheindlin's Zubulake Decisions, 29 July 2003, abrufbar unter http://www.omm.com/webdata/content/publications/client_alert_securities_litigation_2003_07_30.htm.

MÜLLER, SAMUEL/PFITZMANN, BIRGIT: Effektives Compliance Management, digma 2006, 36.

PALFREY, JOHN G. (Testimony): Testimony to the U.S. House of Representatives Committee on International Relations, February 15, 2006, abrufbar unter http://blogs.law.harvard.edu/palfrey/testimony-to-the-us-house-of-representatives-committee-on-international-relations/.

PALFREY, JOHN G. (Making a Market): Making a Market Emerge out of Digital Copyright Uncertainty, abrufbar unter http://blogs.law.harvard.edu/palfrey/2006/10/11).

PALFREY, JOHN G., JR./ROGOYSKI, ROBERT: The Move to the Middle: The Enduring Threat of "Harmful" Speech to Network Neutrality, Berkman Center Research Publication No. 2006-08, abrufbar unter http://ssrn.com/abstract=916748.

PFENNINGER, MARKUS D./BÜRGI, JOHANNES A.: Legal Risk unter Basel II – Vermehrte Ausgliederung rechtlicher Risiken?, ST 2004, 290.

PROSKINE, EMILY ANNE: Google's Technicolor Dreamcoat: A Copyright Analysis of the Google Book Search Library Project, 21 Berkeley Technology Law Journal 213 (2006).

REGER, GUIDO: Technologie-Früherkennung: Organisation und Prozess, in: GASSMANN, OLIVER/KOBE, CARMEN (Hrsg.): Management von Innovation und Risiko, Berlin et al. 2006.

ROSSI, SANDRA: Insurers sign mega-dollar e-compliance deal, IDG Data, 11 December 2003 (erhältlich über factiva.com).

RYSER, ROLAND M./KUCHOWSKY, NATALIE: Die Strafbarkeit des Unternehmens – Organisationspflichten und Strafrecht, ST 2005, 583.

SCHREIBER, VERA: International Standards – Neues Recht für die Weltmärkte?, Bern et al. 2005.

SPAR, DEBORA L.: Ruling the Waves, From the Compass to the Internet, a History of Business and Politics along the Technological Frontier, New York et al. 2001.

STEINEGGER, MARC: Elektronische Rechnungen – Grundlagen des Handelsrechts und der MWST, Änderungen der ElDI-V, ST 2006, 94.

STRASSER, OTHMAR: Aspekte von Compliance als Teil von Corporate Governance aus Sicht einer Bank, in: VON DER CRONE, HANS CASPAR/FORSTMOSER, PETER/WEBER, ROLF H./ZÄCH, ROGER (Hrsg.): Aktuelle Fragen des Bank- und Finanzmarktrechts: Festschrift für Dieter Zobl zum 60. Geburtstag, Zürich 2004, 537.

SUHR BRUNNER, CHRISTIANA/PORTMANN, PASCAL: Compliance bei Banken – Vertrauenswürdigkeit als entscheidender Faktor, ST 2005, 1035.

THOMPSON, CLIVE: Google's China Problem (and China's Google Problem), The New York Times, April 23, 2006, abrufbar unter http://www.nytimes.com/2006/04/23/magazine/23google.html?ei=5090&en=972002761056363f&ex=1303444800.

WEBER, ROLF H. (E-Commerce): E-Commerce und Recht, Zürich 2001.

WEBER, ROLF H. (Regulatory Models): Regulatory Models for the Online World, Zurich et al. 2002.

WEBER, ROLF H. (E-Governance): E-Governance im Unternehmen, in: VON DER CRONE, HANS CASPAR/WEBER, ROLF H./ZÄCH, ROGER/ZOBL, DIETER (Hrsg.): Neuere Tendenzen im Gesellschaftsrecht: Festschrift für Peter Forstmoser zum 60. Geburtstag, Zürich 2003, 347.

WEBER, ROLF H. (Kompatibilität): Kompatibilität von Handels- und Steuerrecht bei der elektronischen Belegsverwahrung?, Jusletter 3. März 2003.

WEBER, ROLF H. (Risikomanagement): Risikomanagement durch Einhaltung von IT-Sicherheitsstandards – Rechtliche Aspekte der Inkorporierung privater Normenkomplexe in unternehmerische Abläufe, sic! 2004, 181.

WEBER, ROLF H. (Risk Management): Legal Framework for Risk Management in Information Infrastructures, in: KIERKEGAARD, SYLVIA MERCADO (Hrsg.): Business, Law & Technology: Present and Emerging Trends, Volume 1, Copenhagen 2006, 470.

WEBER, ROLF H./WILLI, ANNETTE: IT-Sicherheit und Recht, Grundlagen eines integrativen Konzepts, Zürich 2006.

WYSS, LUKAS: Das IKS und die Bedeutung des (Legal) Risk Management für VR und Geschäftsleitung im Lichte der Aktienrechtsreform 2007, SZW 2007, 27.