Risiko als Element unternehmerischer Freiheit vor dem Hintergrund aktueller Compliance-Erwartungen und Corporate-Governance-Vorschriften

RAin Dr. Stephanie Troßbach
Catus Law + Compliance
trossbach@catuslaw.com

Stud. iur. Bero Gebhard
Johann Wolfgang Goethe-Universität
gebhard@catuslaw.com

*Dieser Beitrag geht auf einen Vortrag bei der Liberalen Rechtstagung 2020 zurück, der im Tagungsband „Rechtsfragen zum gesellschaftlichen und wirtschaftlichen Wandel im Jahr 2020“, Mirko Bange (Hg.), Göttingen 2020, dokumentiert ist.

Abstract

Risiko ist conditio-sine-qua-non jeder unternehmerischen Tätigkeit. Verlustgefahr und Gewinnchancen sind zwei Seiten derselben Medaille. Sowohl Überbetonung als auch Marginalisierung von Risiken kann zu Wertverlust führen und den Eigentümern von Unternehmen erheblich schaden. Nötig ist ein ausgewogenes Risikomanagement. Dieses ist ein zentraler Bereich unternehmerischer Entscheidung und Freiheit. Doch der Druck wächst: Compliance-Anforderungen steigen seit Jahren immer weiter. Für die europäische und deutsche Gesetzgebung ist hierbei vor allem der Trend zu beobachten, dass der Gesetzgeber zunehmend komplexe Vorgaben zu Prozessen für die Risikobewältigung macht und bei relativer Unbestimmtheit der Erwartungen einen sehr hohen Sanktionsrahmen definiert. Das bleibt nicht ohne Folgen. Unternehmen neigen dann zur ängstlichen oder sogar überängstlichen Risikoeinschätzung und erleiden dadurch spürbare Nachteile. Die Gesetzesprojekte binden dabei enorme Kapazitäten, da für jedes neue Gesetz eine Neubewertung der Risiken erfolgen muss. Viele der Vorhaben, etwa das Lieferkettengesetz und das Verbandssanktionengesetz („VerSanG“), zeigen zudem Merkmale symbolischen (Straf-)Rechts. Es bleibt unklar, auf den Schutz welcher konkreten Rechtsgüter sich der Gesetzgeber stützt, wenn er die Entscheidungsspielräume von Unternehmen einengt. Dabei kann es der Gesetz-

geber nicht besser als der Markt. Eigentümer bzw. Aktionäre sind sehr wohl imstande, ihr Unternehmen nach ihren Vorstellungen ausrichten, auch in Compliance-Fragen. Der Druck von Themen aus den Bereichen Environment, Social, Governance („ESG“) durch die Marktteilnehmer ist groß, auch ohne Intervention des Staates. In jedem Fall erfordert die verantwortliche Übernahme von Risiken einen bewussten Umgang mit diesen. Ein risiko- und wertebasiertes Compliance Management System („CMS“), dem jeweiligen Unternehmen individuell angepasst, ist dafür eine wichtige Grundlage. Ob Unternehmen über den eigentlichen Unternehmenszweck hinaus „sinnstiftende“ Maßnahmen ergreifen sollten, ist zweifelhaft: „The business of business is business“.[1]

„A ship is safe in harbor, but that's not what ships are for.“ (*John A. Shedd*)

I. Was ist Risiko?

Auch wenn die Herkunft des Wortes nicht mehr vollständig nachvollziehbar ist, wurde das Wort „Risiko“ oder „risk“ vermutlich im 16. Jahrhundert als kaufmännischer Terminus aus dem italienischen *risico* (Wagnis, Gefahr) entlehnt.[2] Auch das englische Wort „venture“ kann nicht nur „Unternehmen“ heißen, sondern auch Spekulation, Risiko, Wagnis oder Projekt. Wir bewegen uns bei der Betrachtung und Einschätzung von Risiko im Unternehmen also in einem grundsätzlichen Spannungsfeld zwischen Verlustgefahr und Gewinnchancen.[3]

Risiken für Unternehmen sind mannigfaltig. Nach dem Allianz Risk Barometer 2020 stehen nach den durchgeführten Befragungen Betriebsunterbrechungen (inkl. Lieferkettenunterbrechung), Cyber-Vorfälle (z.B. Cyberkriminalität, IT-Ausfall, Datenschutzverletzungen, Geldbußen und Strafen), sowie rechtliche Veränderungen (z.B. Wirtschaftssanktionen, Protektionismus, Brexit, Zerfall der Eurozone) auf den ersten drei Plätzen der genannten Geschäftsrisiken für Deutschland und global.[4]

---

[1] *Milton Friedman* zugeschrieben.
[2] *Duden*, Etymologie, „Risiko“.
[3] *Freidank*, Erfolgreiche Führung und Überwachung von Unternehmen, S. 223.
[4] *Allianz Global Corporate & Specialty (AGCS)*, Allianz Risk Barometer 2020, Top 10 Risiken Global, Top 10 Risiken Deutschland.

II. Compliance-Risiken

Compliance-Risiken stellen eine jedenfalls begrifflich noch relativ junge[5] Sonderform unternehmerischen Risikos dar. Zum einen reflektieren sie mit erheblichen Sanktions- und Schadensfolgen einhergehende handfeste rechtliche Risiken, wie Korruptionsrisiken (etwa Bestechung ausländischer Amtsträger oder privater Auftraggeber zur Realisierung von Geschäftschancen im Ausland), kartellrechtliche Risiken (z.B. Preisabsprachen mit Wettbewerbern) oder datenschutzrechtliche Risiken (wie durch unsachgemäße Behandlung personenbezogener Daten).[6] Zum anderen reichen Compliance-Risiken in weniger konkrete Bereiche teilweise reflexartig hinein, etwa bei der Sorge vor mit dem Eintritt großer Schadensereignisse verbundenen Reputationsverlusten. Diese benennen im Allianz Risk Barometer 2020 immerhin noch 14% der Befragten als wichtiges Geschäftsrisiko in Deutschland (Platz 9).[7]

Zum rechtlichen Aspekt der Compliance-Risiken gehören auch die deutlich gestiegenen internationalen Compliance-Erwartungen. Exemplarisch sind hier der U.S. Foreign Corrupt Practices Act (FCPA) von 1977 und der UK Bribery Act (UKBA) von 2010 zu nennen. Beide haben eine extraterritoriale Reichweite und können auf ausländische Unternehmen Anwendung finden, selbst wenn die Korruptionstaten nicht in den Vereinigten Staaten oder dem Vereinigten Königreich begangen wurden. Sie kennzeichnet nicht nur ein ausgesprochen hohes Sanktionspotential. Beide begnügen sich auch nicht mit der Konstatierung einer allgemeinen Legalitätspflicht. Sie machen konkrete Vorgaben für ein effektives Compliance-Programm, welche Unternehmen und deren Verantwortliche berücksichtigen müssen, wollen sie den Ausgang von Verfahren für sie günstig beeinflussen.

Das deutsche Recht ist hier – bislang – offener oder, je nach Lesart, unpräziser. Als Ausgangspunkt gilt jedenfalls die Legalitätspflicht, wie sie insbesondere in den §§ 76 Abs. 1 i.V.m. § 93 Abs. 1 Nr. 1 AktG Niederschlag gefunden hat. Danach ist

[5] Die Vereinigten Staaten gelten als das Ursprungsland von Compliance in der hier verwendeten Begrifflichkeit. Bei harschen Sanktionen ermöglichte der U.S.-Gesetzgeber im Gegenzug Sanktionsmilderung für Unternehmen, die ernsthafte Maßnahmen zur Sicherstellung von Regeltreue ergriffen hatten. In Deutschland erhielt das Thema Compliance durch den Siemens-Korruptionsskandal 2006-2008 Auftrieb.

[6] S. auch die Zusammenstellung in *DICO e. V.*, Risikokatalog.

[7] *Allianz Global Corporate & Specialty (AGCS)*, Allianz Risk Barometer 2020, Top 10 Risiken Global, Top 10 Risiken Deutschland.

der Vorstand verpflichtet, rechtswidriges Verhalten im Unternehmen zu verhindern. Hierzu gehört auch, gesetzeskonformes Verhalten der Gesellschaft und ihrer Mitarbeiter gegenüber Dritten sowie gegenüber der eigenen Belegschaft sicherzustellen.[8] Entsprechend heißt es im Deutschen Corporate Governance Kodex 2019 („DCGK"), A. I., „Empfehlung und Anregung" A.2: „Der Vorstand soll für ein an der Risikolage des Unternehmens ausgerichtetes Compliance Management System sorgen und dessen Grundzüge offenlegen."[9] Konkretisiert wurden die Erwartungen durch ein Urteil des Landgerichts München aus dem Jahr 2013, das als Siemens/Neubürger-Entscheidung Einfluss auf die Entwicklung von Compliance-Strukturen in Deutschland nahm. Das Gericht stellte eine Pflicht des Vorstandes einer Aktiengesellschaft zur Einrichtung eines Compliance Management Systems fest, um dessen Legalitätspflicht gerecht zu werden.[10] Wie ein solches Compliance Management System aussehen sollte, präzisierte das Landgericht München hierbei nicht.

III. Compliance-Risikomanagement

Verlustgefahr und Gewinnchancen sind eng miteinander verknüpfte Aspekte. Eine Marginalisierung von – insbesondere existenzbedrohenden – Gefahren kann fatale Folgen haben. Gleiches gilt für deren Überbetonung. Beides kann Eigentümern von Unternehmen erheblichen Schaden zufügen.

1. Compliance-Risikomanagement als Bestandteil des internen Kontrollsystems

Compliance-Risikomanagement steht dabei im Kontext des allgemeinen Risikomanagements in Unternehmen, das der Vorstand von Aktiengesellschaften nach § 91 Abs. 2 AktG einzurichten hat. Entsprechend heißt es auch im DCGK, A.I., Grundsatz 4: „Für einen verantwortungsvollen Umgang mit den Risiken der Geschäftstätigkeit bedarf es eines geeigneten und wirksamen internen Kontroll- und Risikomanagementsystems." Die aktienrechtliche Regelung hat Ausstrahlungswirkung auch auf andere Unternehmensformen.[11]

[8] *Spindler*, in: MüKo AktG, § 93 Rn. 87.

[9] Der DCGK ist ein rechtlich nicht verbindliches Werk einer Regierungskommission aus Fachexperten, die Empfehlungen für gute Unternehmensführung erarbeitet. Verpflichtend ist gemäß § 161 AktG allerdings die Abgabe einer sog. Entsprechenserklärung, ob die Empfehlungen befolgt werden, bzw. warum ggf. nicht.

[10] *LG München*, Urt. v. 10.12.2013, NZG 2014, 345 f.

[11] *Freidank*, Erfolgreiche Führung und Überwachung von Unternehmen, S. 220.

Risikomanagement bedarf immer eines individuellen Ansatzes. Jedes Unternehmen ist anders, kämpft mit unterschiedlichen Gegebenheiten, Herausforderungen und Prioritäten. Um das Unternehmen sicher zu steuern, sind passgenaue Entscheidungen und die Nutzung von Freiräumen fundamental. Je nach Art der Geschäftstätigkeit und ihrer konkreten Rahmenbedingungen werden auch immer Risiken verbleiben, die das beste Risikomanagement nicht aus der Welt schaffen kann.[12] Ziel sollte ein „entscheidungsorientiertes Risikomanagement" sein, das Ergebnisse der Risikoanalyse in die Entscheidungsvorbereitung entsprechend der *Business Judgement Rule* einbringt.[13] Risikomanagement ist damit ein bedeutender Bereich unternehmerischer Entscheidung und Freiheit.

Das heißt, dass Unternehmen durchaus hohe Risiken eingehen können. Zentral sind allerdings eine realistische Risikoeinschätzung und die Auswahl geeigneter Maßnahmen zur Kontrolle der Risiken. Oftmals finden sich Versäumnisse weniger in der Übernahme bestimmter Risiken an sich, sondern vielmehr im Risikomanagement: In der Folge der Finanzkrise stellte ein Untersuchungsausschuss des U.S.-Kongresses 2011 fest, dass zentraler Faktor der Entstehung der Krise die „leichtsinnige und exzessive Risikoübernahme"[14] war. Nicht die Risiken selbst waren also zu hoch. Vielmehr lag dem System der Ratingagenturen eine strukturelle Fehleinschätzung hinsichtlich der Ausfallrisiken der Kredite zugrunde.

2. Erwartungen an Compliance-Risikoanalysen

FCPA und UKBA betonen im Hinblick auf das Risikomanagement beide die Notwendigkeit, Compliance-Risikoanalysen durchzuführen.[15] FCPA hebt hier vor allem die Gefahren eines „one-size-fits-all" Compliance-Programms heraus. Auch UKBA bezieht sich auf die notwendige Individualisierung von Risikoanalysen und beschreibt sich gegenseitig beeinflussende externe und interne Faktoren, welche zum Risikoprofil beitragen.[16]

Geben diese Standards den Unternehmen also vor, wie sie Compliance-Risikomanagement konkret betreiben müssen? Ja und nein. Zwar beschreiben FCPA und UKBA konkrete Erwartungen, allerdings wird klar betont, dass Unternehmen

[12] *Gleißner*, GRC 2019, 148 (150).
[13] *Gleißner*, GRC 2019, 148.
[14] *The Financial Crisis Inquiry Commission*, The Financial Crisis Inquiry Report, S. 19.
[15] *FCPA Resource Guide*, S. 58; *UKBA Guidance*, Principle 3, S. 25. In diese Richtung gehen auch anerkannte Standards ohne Gesetzeskraft wie *ISO 37001* oder auch *DICO e. V.*, Standard S09 – Compliance Risikoanalyse (CRA).
[16] *FCPA Resource Guide*, S. 58; *UKBA Guidance*, S. 25.

bei der Durchführung von Risikoanalysen einen auf ihre Situation zugeschnittenen Weg beschreiten müssen.

IV. Steigende Compliance-Anforderungen

Die Compliance-Anforderungen steigen seit Jahren immer weiter und es zeichnet sich dabei sowohl eine größere Komplexität als auch eine zunehmende Detaillierung der Anforderungen ab. Hierzu gehört nicht nur die Hervorhebung des Elements persönlicher Haftung,[17] sondern auch das der angemessenen Ressourcen-Allokation. Unternehmen müssen zeigen, dass sowohl die personelle Ausstattung als auch finanzielle Mittel verfügbar gemacht werden, um Compliance-Risiken zu ermitteln und ihnen angemessen zu begegnen.[18] Dabei gehen die Vorgaben immer stärker in Details der Umsetzung hinein, etwa bei Themen wie Design eines CMS, Verständlichkeit des Programms, Kommunikation, Verankerung im operativen Geschäft und Einsatz von Kontrollmechanismen.[19]

Diese Entwicklung spiegelt sich auch in europäischen und nationalen Gesetzesvorhaben. Es lohnt sich, einige im genannten Kontext noch einmal genauer zu betrachten:

Die **EU-Datenschutzgrundverordnung** („DSGVO“) aus dem Jahr 2018 war ein Paukenschlag, der den Unternehmen viel abverlangt hat. Inhaltlich ging es gar nicht so sehr um eine Verschärfung des materiellen Datenschutzrechts. Entscheidend und für die Unternehmen sehr aufwändig waren vor allem die Vorgaben zur Einführung von Prozessen, also wie Unternehmen sich organisieren müssen, um die gesetzlichen Anforderungen zu erfüllen, und natürlich die immense Sanktionsdrohung von bis zu 10% des Jahresumsatzes.

Das neue **Geldwäschegesetz** 2020 verlangt von Unternehmen ausgiebige Kontrollen ihrer eigenen Kunden und Geschäftspartner bis hin zur verpflichtenden Meldung von Verdachtsfällen bei den Behörden, ebenfalls unter Androhung einer Sanktion von bis zu 10% des Jahresumsatzes. Auch hier liegt der Fokus auf der Organisation der Unternehmen zur Reduzierung von Geldwäscherisiken.

Das Europäische Parlament hat im April 2019 die **EU-Whistleblowing-Richtlinie** verabschiedet. Diese ist jetzt in nationales Recht umzusetzen und fordert von

[17] *U.S. DOJ*, „Yates Memo“, v. 09.09.2015.
[18] *U.S. DOJ*, Guidance 2020, S. 3, 12.
[19] *U.S. DOJ*, Guidance 2020, S. 2 ff.

Unternehmen ab 50 Mitarbeitern ebenfalls die Vorhaltung von Infrastruktur und Prozessen zur Bearbeitung von Meldungen und dem Schutz der Hinweisgeber.

Der Entwurf des geplanten **Lieferkettengesetzes** sieht vor, dass Unternehmen mit mehr als 500 Mitarbeitern in Zukunft prüfen sollen, ob sich ihre Aktivitäten nachteilig auf Menschenrechte auswirken und sie angemessene Maßnahmen zur Prävention und Abhilfe ergreifen. Unternehmen sollen einmal jährlich berichten, wie sie Menschenrechtsverletzungen unterbinden. Das zu entwickelnde Risikomanagement soll „verhältnismäßig und zumutbar“[20] sein. Gegen Unternehmen, die keine entsprechenden Maßnahmen vorweisen können, soll ein Bußgeld (Höhe noch unklar) und eine Ausschreibungssperre verhängt werden können, weitere Haftungsmöglichkeiten sind denkbar. Auch in diesem Entwurf finden sich wiederum Organisations- und Kontrollpflichten für Unternehmen, die eigenen Geschäftspartner und Zulieferer auf die Einhaltung der geforderten Standards zu prüfen.

Das prominenteste Beispiel für aktuelle gesetzgeberische Betätigung ist der Entwurf des VerSanG, auch genannt „Gesetz zur Stärkung der Integrität in der Wirtschaft“. Dieses soll Unternehmen, deren Mitarbeiter Straftaten begangen haben, mit Sanktionen bis zu 10% des Jahresumsatzes sowie einer öffentlichen Bekanntmachung drohen. Im Gegenzug könnten Unternehmen belohnt werden, die Compliance-Maßnahmen zur Prävention entwickelt haben oder durch interne Untersuchungen Straftaten selbst aufklären und dabei mit der Staatsanwaltschaft zusammenarbeiten. Aber: Die interne Untersuchung muss klar von der Unternehmensverteidigung getrennt werden und sowohl belastende als auch entlastende Erkenntnisse sammeln. Die interne Untersuchung erfolgt in enger Zusammenarbeit mit den Ermittlungsbehörden, während der Unternehmensverteidiger eigene Ermittlungen anstellen soll. Die Ermittlungen müssen wesentlich zur Aufklärung der Verbandsstraftat beitragen. Das Ergebnis der internen Ermittlung, die wesentlichen Dokumente und der Abschlussbericht werden den Verfolgungsbehörden offengelegt. Zu der Bewertung dieses gesetzgeberischen Vorhabens wurde in den letzten Monaten viel geschrieben.[21] An dieser Stelle soll vor allem

[20] Aus dem Eckpunktepapier für das Lieferkettengesetz, vgl. *Handelsblatt* v. 26.06.2020, Heil und Müller entschärfen die Haftungsregeln für Unternehmen, https://www.handelsblatt.com/politik/deutschland/lieferkettengesetz-heil-und-mueller-entschaerfen-die-haftungsregeln-fuer-unternehmen/25947310.html?ticket=ST-2259735-VTNtLgBrEaCu9IASGuhi-ap5 (Stand: 24.08.2020).

[21] Zusammenfassend zum Stand der Diskussion: *LTO* v. 12.06.2020, Gebündelte Kritik an BMJV-Plänen, https://www.lto.de/recht/nachrichten/n/verbandssanktionengesetz-unternehmen-wirtschaft-verbaende-kritik-bmjv-entwurf/ (Stand: 24.08.2020).

Folgendes herausgehoben werden: Auch mit den Plänen zum VerSanG wird ganz erheblich in die Art und Weise, wie Unternehmen risikobezogene Entscheidungen treffen, hineingewirkt. Zwar werden keine konkreten Erwartungen zur Ausgestaltung des CMS gestellt, es werden aber detaillierte Vorgaben für die Aufarbeitung von Compliance-Fällen gemacht. Unternehmen sollen vor allem die Behörden unterstützen und quasi strafverfolgend „als Hilfsbeamte" tätig werden. Damit werden die Entscheidungsspielräume bei Aufarbeitung und wirksamer Verteidigung erheblich eingeschränkt.

In den genannten Beispielen manifestiert sich ein **gemeinsamer Trend**: Zum einen wird ein gesteigerter Fokus darauf gelegt, welche Compliance-Risiken Unternehmen managen, wie sie im Eintrittsfall mit Schadensereignissen konkret umgehen sollen und welche Prozesse Unternehmen intern vorhalten müssen, wenn ihr Risikomanagement als ausreichend bewertet werden soll. Auch gibt es eine deutliche Entwicklung zu exorbitanten Sanktionsdrohungen für den Fall, dass Unternehmen diese Vorgaben nicht oder nicht ausreichend befolgen. Die Art und Weise, wie Unternehmen ihre Compliance-Risiken managen, wird durch diese Maßnahmen wesentlich geprägt.

V. Bewertung dieser Entwicklung

Wie sind diese Gesetzesvorhaben nun zu bewerten? Die steigende Regelungsdichte und konkrete Vorgaben muss man nicht grundsätzlich schlecht finden. Nicht selten begrüßen Compliance-Verantwortliche klare Gesetze. Denn diese tragen dazu bei, den Aufbau eines soliden CMS unternehmensintern besser zu begründen. Der Verweis auf das geltende Legalitätsprinzip hilft bei Einzelentscheidungen, reicht aber meistens nicht aus, um den notwendigen Aufbau von komplexen Strukturen und Prozessen im Unternehmen zur Reduzierung von Compliance-Risiken mit entsprechenden Budgetforderungen zu rechtfertigen. Zu abstrakt erscheint Unternehmensverantwortlichen zuweilen die Gefahr, dass sich Compliance-Risiken zu großen Schadensereignissen auswachsen. Oft wird ohne ausreichende Tatsachengrundlage und tendenziell „aus dem Bauch" heraus die Bedeutung von Compliance-Risiken (etwa das Risiko, dass eine anerkannte, erfahrene Führungskraft sich gegen Kick-Back-Zahlungen an Geldwäschehandlungen betätigt oder für bessere Verkaufszahlen Menschenrechtsverstöße in Kauf

nimmt) als „gering“ eingestuft.[22] Werden in Gesetzen konkrete Erwartungen niedergelegt, wissen Unternehmen jedenfalls genauer, „woran sie sind“ und welche Elemente ihr CMS abbilden soll. Dies gilt insbesondere in Unternehmen, auf welche FCPA und UKBA nicht direkt Anwendung finden und die sich mit einer Umsetzung des Legalitätsprinzips in ein konkretes CMS noch schwertun.

Allerdings gibt es auch eine Reihe nachteiliger Aspekte. Diese sind angelegt in den beschriebenen Vorgaben zum Risikomanagement, zu internen Prozessen, Verhaltensanweisungen und immensen Sanktionsrahmen. Rückblickend lässt sich die daraus resultierende Dynamik am Beispiel der DSGVO veranschaulichen. Am Anfang stand das Phänomen der ängstlichen oder sogar überängstlichen Risikoeinschätzung. In Anbetracht der sehr hohen Bußgeldandrohung hatten sich schon im Vorfeld der DSGVO viele Mutmaßungen dazu Bahn gebrochen, welche Szenarien zu erwarten seien, von welchen Aktivitäten Unternehmen nun unbedingt Abstand nehmen müssten und mit welchen Bußgeldern Unternehmen belegt werden könnten. Es war (und ist noch) zu beobachten, dass Unternehmen von zum Teil völlig problemlosen oder jedenfalls beherrschbaren Praktiken abrücken, obwohl diese für ihre Geschäftstätigkeit elementar sind. Eine solche Risikovermeidung ist nachvollziehbar: Wer bei gleichbleibender Eintrittswahrscheinlichkeit eines Szenarios mit einem Vielfachen der bisherigen Sanktion zu rechnen hat, der wird spürbare Nachteile in Kauf nehmen, um eine solche Sanktion unbedingt zu vermeiden. Dieser Gedanke lässt sich mit den Diskussionen rund um das 2017 erlassene Netzwerkdurchsetzungsgesetz[23] veranschaulichen: Wenn Unternehmen gezwungen sind, rechtliche Risiken unter hohem Druck zu eliminieren, ist es relativ wahrscheinlich, dass dies „im Zweifel“ zur übermäßigen Vermeidung

[22] „Risikoblindheit“ ist ein bekanntes Phänomen. *Taleb*, The Black Swan, S. XIII, beschreibt diese etwa als „(…) our blindness with respect to randomness, particularly the large deviations“ und nennt unvorhergesehene, sehr schadensträchtige Risiken „Black Swans“ und etwas weniger unwahrscheinliche Ereignisse „Mandelbrotian Grey Swans“, *Taleb*, The Black Swan, S. 37. In Anbetracht der Ubiquität von Kriminalität wird man das Auftreten strafrechtlich relevanter Vorgänge in Unternehmen allerdings eher als „White Swan“ zu bezeichnen haben. FCPA etikettiert die Risikoverdrängung als „willful blindness“ oder „deliberate ignorance“ und stellt klar, dass beides Unternehmen nicht entlasten kann, *FCPA Resource Guide*, S. 58.

[23] Wenn Unternehmen wie Facebook innerhalb von 24 Stunden entscheiden müssen, ob ein Tweet seinem Inhalt nach rechtlich zulässig ist, wird es sich angesichts der enormen Höhe des drohenden Bußgeldes im Zweifelsfall für eine Löschung entscheiden. Dies zeigt sich im Rahmen des sog. schematischen Overblockings, bei dem Posts mit bestimmten Stichwörtern automatisch gelöscht wurden, vgl. *SZ.de* v. 30.07.2018, Besser als nichts, https://www.sueddeutsche.de/digital/ein-jahr-netzdg-besser-als-nichts-1.4072485 (Stand: 24.08.2020).

von Risiken führt. Die Risikoscheu ist auch da besonders erwartbar und nachvollziehbar, wo die Folgen Unternehmensverantwortliche zunehmend nicht nur beruflich, sondern auch persönlich treffen.[24] Die Risikofreude fällt nicht überraschend umso gedämpfter aus, je unbestimmter die konkreten Erwartungen des Gesetzgebers bei gleichzeitig hoher Strafandrohung sind. Bei Einführung der DSGVO waren sowohl die Anforderungen an Risikomanagement, interne Prozesse und die Auslegung einer Vielzahl unbestimmter Vorgaben noch völlig unklar. Die Behörden wollten sich im Vorfeld auch nicht auf bestimmte Interpretationen festlegen lassen und Unternehmen waren ihrerseits nicht gerade erpicht darauf, Präzedenzfälle zu schaffen und aktiv an der allgemeinen Rechtsfortbildung mitzuwirken. Entsprechend defensiv gingen viele Unternehmen an die vermeintlich übergroßen Datenschutzrisiken heran.

Solche Gesetzesprojekte binden dabei enorme Kapazitäten, da Unternehmen sich detailliert mit den „neuen" Risiken beschäftigen müssen, ohne dass der Mehrwert für sie immer erkennbar ist. Denn für jedes Projekt des Gesetzgebers muss im Unternehmen eine Neubewertung der Risiken erfolgen und die Bereitstellung der geforderten Strukturen, Prozesse sowie Ressourcen mit erheblichem Aufwand geprüft und abgewogen werden. Hier ist auch zu beobachten, dass Unternehmen zu einem eher schematischen, nur scheinbar sicheren, Handeln neigen. Im schlechtesten Fall setzten Unternehmen verstärkt auf jedenfalls optisch zufriedenstellende Maßnahmen, damit sie sich nicht umgehend (womöglich unbegründeten) Vorwürfen ausgesetzt sehen. Eigenverantwortliches, unternehmerisches Handeln tritt dabei nicht selten in den Hintergrund. Strukturell haben wir es mit einer Verrechtlichung von Risiken zu tun, durch welche der Gesetzgeber den Unternehmen ureigene unternehmerische Entscheidungen de facto abnimmt.

Nun könnte man dies in Anbetracht der Wichtigkeit der Gesetzesinhalte bei Abwägung verschiedener Interessen für ein zumindest vertretbares Ergebnis halten. Gute Gesetze haben hoffentlich positive Folgen. Wenn diese eintreten, wird man gewisse „Nebenwirkungen", etwa gesteigerten Aufwand oder eine staatliche Einmischung in das Compliance-Risikomanagement, vielleicht akzeptieren können und müssen. Aber sind die genannten Gesetze „gute Gesetze" mit den

[24] So im bereits erwähnten „Yates-Memo" des *DOJ* v. 09.09.2015 sowie der „Siemens/Neubürger-Entscheidung", *LG München*, Urt. v. 10.12.2013, NZG 2014, 345 f.

genannten positiven Folgen oder handelt es sich vorrangig um symbolisch relevante Akte, welche die Unternehmen in Atem halten?

VI. Symbolisches Recht und symbolische Maßnahmen

Die Diskussion um den symbolischen Gehalt von (Straf-)Recht ist nicht neu. Der Symbolgehalt praktisch jeden Rechts ist evident und stellt eher den Normal- als den Ausnahmefall dar. Schon *Luhmann* hat dem Recht zugeschrieben, primär keine „Zwangsordnung, sondern eine Erwartungserleichterung" zu sein.[25] Es war auch *Hassemers* Ausgangspunkt, dass vor allem Strafgesetze auf symbolische Wirkungen ausgelegt sind. Dies sei eine „bare Selbstverständlichkeit".[26] Letztlich handele es sich auch nur um einen Steigerungsbegriff im Sinne eines „Mehr oder Weniger".[27] Die Kernfrage sei daher, „an welchem Punkt die Mischung symbolischer mit instrumentellen Bestandteilen des Strafrechts kritisch wird", und wie dies zu bestimmen sei.[28] Als problematisch hat *Hassemer* vor allem solche Bereiche gedeutet, in welchen begrenzter Rechtsgüterschutz im Kernbereich durch unbestimmte Universalrechtsgüter abgelöst werde: „Wirtschaft, Umwelt, Steuern, automatische Datenverarbeitung, Terrorismus, Drogen, Export gefährlicher Gegenstände. (…) Strafrechtsgüter, welche (…) in puncto Verallgemeinerung keine Wünsche offenlassen."[29] Das Strafrecht wachse dabei unter dem Gesichtspunkt der Risikobeherrschung zu einem „Steuerungsinstrument für gesellschaftliche oder staatliche Großstörungen".[30] Dieser Ansatz hat weiter an Bedeutung gewonnen.[31] So sind einige Strafvorschriften unserer Zeit nach *Jasch* „nicht mehr als ein Mittel der (Selbst-) Vergewisserung über normative Orientierungen der gesellschaftlichen Mehrheitsbevölkerung".[32]

Ja, es handelt sich bei dem Lieferkettengesetz und dem VerSanG natürlich um symbolisches (Straf-)Recht. Als „Schutzbereiche", die man kaum noch Rechtsgüter nennen kann, nennt der Gesetzgeber unbescheiden: Lauterkeit, Integrität, der Kampf gegen „schwerste Unternehmenskriminalität", die Ethik der Wirtschaft.

[25] *Luhmann*, Rechtssoziologie, S. 100.
[26] *Hassemer*, NStZ 1989, 553 (554); dazu auch *DIE ZEIT* v. 06.08.2020, Wer nicht hören will, S. 1.
[27] *Hassemer*, NStZ 1989, 553 (555 f.).
[28] *Hassemer*, NStZ 1989, 553 (556).
[29] *Hassemer*, NStZ 1989, 553 (557).
[30] *Hassemer*, NStZ 1989, 553 (558).
[31] *Günther*, WestEnd 2004, 117 (122); *Günther*, in: FS Lüderssen, 205 (206).
[32] *Jasch*, in: Interdisziplinäre Rechtsforschung, 82-99 (88).

Wie sehr die Bundesregierung „ein Zeichen setzen“ will, wird schon im Titel „Gesetz zur Stärkung der Integrität in der Wirtschaft“ deutlich.[33] Zur Vermeidung von Missverständnissen sei gesagt, dass „Symbolik“ nicht notwendigerweise „unsinnig“ heißt. Sicher kann man die genannten Ziele gutheißen. Sie sind ja auch sehr allgemein gefasst. Aber gerade das ist Teil des Problems. Denn ein „begrenzter Rechtsgüterschutz im Kernbereich“ ist mit Allgemeinplätzen eben nicht zu umreißen. Damit aber bleibt die Legitimität des einschränkenden staatlichen Handelns unklar. Bei den besprochenen Gesetzesvorhaben handelt es sich andererseits auch nicht um „harmloses“ (weil schlicht irrelevantes) symbolisches (Straf-) Recht. Denn wie oben beschrieben sind es nicht zuletzt die hohen Sanktionsandrohungen, welche Risikomanagement und Prozesse von Unternehmen erheblich beeinflussen, Ressourcen binden und zu ängstlichem Handeln verleiten. Der dadurch entstehende wirtschaftliche Schaden trifft die Unternehmen unter Umständen hart, nicht zuletzt vor dem Hintergrund der sich abzeichnenden Rezession durch die COVID-19-Pandemie.

Aber nicht nur die Gesetze selbst sind symbolisch aufgeladen. Auch die Maßnahmen, die zum Umgang mit Compliance-Risiken diskutiert und empfohlen werden, sind es. Das Compliance-Thema mag für eine gewisse Symbolik anfällig sein. Denn Compliance geht anerkanntermaßen über den reinen Buchstaben des Gesetzes hinaus.[34] Oft wird dann von einem „wertebasierten Ansatz“[35] gesprochen, was sich etwa in der Aussage wiederfindet, dass man nicht alles tun muss, was man tun darf, und ein CMS in den gelebten Werten eines Unternehmens sein Fundament finden muss. Dieser Ansatz ist auch richtig. Denn Mitarbeiter müssen befähigt werden, oft komplexe Entscheidungen über „Richtig und Falsch“ für das Unternehmen selbständig und eigenverantwortlich zu treffen. Dafür müssen sie verstehen, was anerkanntermaßen im Interesse des Unternehmens ist und welche dahinterstehenden Werte und Zielvorstellungen eine Rolle spielen. Unternehmen sollten hier – bei Beachtung des Legalitätsprinzips – frei entscheiden können, welche Werte und welches Maß für sie richtig ist. Unternehmen haben unterschiedliche Unternehmenskulturen und damit auch „ihre“ Kunden und Mitarbeiter. Ein Familienunternehmen ist kein Hedgefonds. Die jeweilige Corporate

[33] *Kämpfer* und *Nolte* haben in *FAZ.net* v. 29.04.2020, Skandale werden bald richtig teuer, https://zeitung.faz.net/faz/wirtschaft/2020-04-29/skandale-werden-bald-richtig-teuer/453927.html?GEPC=s5 (Stand: 24.08.2020), diesen Titel treffend mit dem „Gute-Kita-Gesetz“ verglichen.

[34] *Leyk*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, Handbuch der Haftungsvermeidung im Unternehmen, § 12 Rn. 1.

[35] *Geiß*, CB 2014, 45.

Identity kann dabei durchaus zur Marke und zum Erfolg beitragen. Es ist in diesem Zusammenhang nicht überraschend, dass auch das Risikomanagement in Unternehmen zunehmend als „strategisches Führungsinstrument verstanden [wird], das in Strategie- und Planungsprozesse integriert werden muss und Entscheidungsprozesse im Sinne eines wertorientierten Risikomanagements unterstützt".[36] Auch damit stellen sich Unternehmen dem Wettbewerb.

Problematisch wird dies, wenn die unternehmerische Tätigkeit weitere sinnstiftende Zwecke verfolgen soll.[37] Hierbei kommt es leicht zu unkonturierten Verschiebungen von rechtlichen Risiken oder wertebasierten Entscheidungen zu einem vermeintlich sinngebenden „Purpose".[38] Soll dies wirklich das Spielfeld von Unternehmen sein? *Friedman* schrieb einst: „[…] there is only one social responsibility of business – to use its resources and engage in activities designed to increase its profits so long as it stays within the rules of the game, which is to say, engage in open and free competition, without deception and fraud."[39] Das ist, wenn man so will, das „Legalitätsprinzip" in Reinform, ohne Anspruch auf Rettung der Welt und symbolhafte Übersprunghandlungen.

Indes: Menschen suchen Sinn in ihrem Tun. In der heutigen globalisierten Welt ist vielen Menschen mehr denn je unklar, welche Werte gelten und wie sich Sinn ableiten oder gar stiften lässt. Ideengeschichtlich haben wir uns von dem Verständnis eines aristotelischen „Telos" längst verabschiedet. Auch ein jüdisch-christliches Wertegerüst lässt sich nicht mehr ohne weiteres als konsensfähig voraussetzen. Entsprechend vage bleiben die Versuche, diese Lücke zu füllen. Unternehmensgetriebene Sinnstiftung gleicht eher einem Gefäß, das beliebig mit Inhalt gefüllt werden kann. Wahre Wertschöpfung ist hier nicht leicht und Sinnfindung scheint zudem eher ein individueller als ein kollektiver Prozess zu sein. Es wäre also klug, mit realistischen Erwartungen an diese Übung heranzugehen, denn Marketing-taugliche Allgemeinplätze können gewachsene, glaubwürdige Werte nicht ersetzen. Letztlich muss es aber auch hier Unternehmen freistehen, Ressourcen in die Entwicklung außerhalb der direkten Wertschöpfungskette stehender Sinnfindung zu investieren und im freien Markt ihr Glück zu suchen.

---

[36] *Gleißner/Hunzinger*, Expert Focus 2019, 745 (749).
[37] *FAS* v. 19.07.2020, Schuster, bleib bei deinen Leisten!, https://www.faz.net/aktuell/hanks-welt-schuster-bleib-bei-deinem-leisten-16866771.html (Stand: 24.08.2020).
[38] *FAS*, a.a.O.
[39] *Friedman*, Capitalism and Freedom, S. 133; auch referenziert von *FAS*, a.a.O.

Nur der Gesetzgeber sollte nicht ohne Not auf diesen Zug aufspringen und mit ebenfalls vagen Begrifflichkeiten und unklarer Legitimität außerhalb des Kernbereichs geschützter Rechtsgüter in immer stärkerem Umfang in unternehmerische Entscheidungen einwirken. Es geht nicht darum, „weniger Compliance" zu propagieren. Der Exzess besteht hier nicht in einem Exzess an Rechtstreue und wertebasiertem Handeln, sondern in einem Exzess an Unbestimmtheit sowie an potentieller Bevormundung. Der Staat weiß es hier auch nicht besser als der Markt: Stakeholder und Shareholder fordern von ihren Unternehmen verstärkt Nebenaspekte wirtschaftlichen Handels wie Nachhaltigkeit ein. *Larry Fink*, Gründer und Vorsitzender des weltgrößten Vermögensverwalters BlackRock – größter Einzelaktionär bei 30% aller DAX-Unternehmen, mit einem verwalteten Vermögen von 7,4 Bio. U.S.-Dollar – wandte sich im Januar 2020 mit einem Brief an die CEOs deutscher Konzerne und forderte eine stärkere Fokussierung auf sogenannte ESG-Themen. Auch solche Risiken seien Anlagerisiken, weshalb sein Unternehmen diese in Zukunft verstärkt in Anlageentscheidungen einbeziehen werde.[40] Diese Entwicklung zeigt wieder einmal eindrucksvoll, dass nicht der Gesetzgeber und sein Sanktionsrepertoire, sondern der Markt Treiber von Wandel sind.

VII. Vorschläge für ein „unternehmensfreundliches" Risikomanagement

Wir stellen fest: Risikomanagement im Compliance-Bereich ist kein einfaches Fahrwasser. Unternehmen müssen sich vor „zu viel" und „zu wenig" Risiko bzw. „zu viel" oder „zu wenig" Compliance-Maßnahmen in Acht nehmen und versuchen, das Schifft zwischen Skylla und Charybdis, in einem unruhigen Gewässer mit Stromschnellen gesetzgeberischer Hyperaktivität und Markterwartung, hindurch zu manövrieren.

Gleichwohl gibt es auf diesem Weg noch Handlungsspielräume, wobei folgende Aspekte besonders zu beherzigen sind: Effektives Management von Compliance-Risiken setzt voraus, diese wirklich zu kennen und realistisch einzuschätzen. Dieser Schritt wird in Unternehmen oft nicht hinreichend beachtet, denn gründliche Risikoanalysen sind mit Aufwand verknüpft. Aber nur ein Unternehmen, das seine Risiken genau kennt und sie nüchtern betrachtet, kann ein risiko-

[40] *Fink*, Brief an die CEOs v. 14.01.2020; vgl. auch *FAZ.net* v. 09.07.2020, Reiche wollen nachhaltiger anlegen, https://www.faz.net/aktuell/finanzen/wohlstand-reiche-wollen-nachhaltiger-anlegen-16852178.html (Stand: 24.08.2020); *Visual Capitalist* v. 11.08.2020, New Waves: The ESG Megatrend Meets Green Bonds, https://www.visualcapitalist.com/esg-megatrend-green-bonds/ (Stand: 24.08.2020).

spezifisches CMS entwickeln, das wirklich auf die Unternehmensrealität abgestimmt ist. Oft gleichen CMS in Unternehmen und dabei besonders das Risikomanagement dem „Bett des Prokrustes“. Dieser Riese aus der griechischen Mythologie bot Reisenden ein Bett an. Waren sie dafür zu groß, hackte er ihnen die Füße ab. Waren sie zu klein, streckte er ihnen die Gliedmaßen, bis sie für die Größe des Betts passend schienen.[41] Nicht überraschend sollten Unternehmen versuchen, sich besser eine ihnen angemessene Liegestatt auszusuchen. Wird dieser Schritt sorgfältig durchgeführt und erfolgt eine ehrliche und unvoreingenommene Auseinandersetzung mit den realen Risiken, lassen sich für die Unternehmen auch in Bezug auf die aktuellen Gesetzesvorhaben passende Maßnahmen entwickeln und in unternehmerischer Verantwortung umsetzen.

VIII. Fazit

Risikomanagement ist ein zentraler Bereich unternehmerischer Entscheidung und Freiheit. Solange sie die Spielregeln des Rechts und des fairen Wettbewerbs befolgen, sollten Unternehmen selbst bestimmen, wie sie mit ihren Risiken umgehen. Verantwortlich sind sie ihren Eigentümern. Wenn diese es wollen, können sich Unternehmen auch außerhalb der direkten Wertschöpfungskette engagieren. Der Gesetzgeber allerdings sollte Unternehmen nur mit Vorschriften im Kernbereich des Rechtsgüterschutzes belasten, insbesondere, wenn es gute Gründe für die Annahme gibt, dass der Markt im Wettbewerb das Notwendige regelt. Symbolische oder gar aktivistische Maßnahmen braucht es nicht. Mit Blick auf die aktuelle Gesetzgebung gilt wieder einmal, dass „gut gemeint“ nicht unbedingt „gut gemacht“ ist. *Friedman* spitzte dies wie folgt zu: „It is the internal threat coming from men of good intentions and good will who wish to reform us.”[42]

Literaturverzeichnis

Allianz Global Corporate & Specialty (AGCS), Risk Barometer 2020, 14.01.2020 (https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2020-de.html).

[41] Entnommen aus *Taleb*, The Bed of Procrustes, S. IX f.
[42] *Friedman*, Capitalism and Freedom, S. 201.

Deutsches Institut für Compliance (DICO e. V.), Risikokatalog, 17.12.2019 (https://www.dico-ev.de/2016/08/30/dico-risikokatalog).

Dass., Standard S09 – Compliance Risikoanalyse (CRA), Februar 2020 (Zugriff: 04.08.2020).

Dosdowski, Günther u.a. (Hrsg.), Duden, Band 7, Etymologie, 2. Aufl., Mannheim, Wien, Zürich 1989.

Fink, Larry, Brief an die CEOs: Eine grundlegende Umstellung der Finanzwelt, 14.01.2020 (https://www.blackrock.com/ch/privatanleger/de/larry-fink-ceo-letter).

Freidank, Carl-Christian, Erfolgreiche Führung und Überwachung von Unternehmen, Wiesbaden 2019.

Friedman, Milton, Capitalism and Freedom, 1962, 40th Anniversary Edition, Chicago 2002.

Geiß, Otto, Step-by-step: Einführung eines wertebasierten Compliance-Management-Systems, CB 2014, Aufsatz Nr. 45 (Heft 3).

Gleißner, Werner, Business Judgement Rule, GRC 2019, 148-153.

Ders./Hunzinger, Stefan, Mit Enterprise Risk Management die Entscheidungsqualität erhöhen, Expert Focus 2019, 745-749.

Günther, Klaus, Die symbolisch-expressive Bedeutung der Strafe, in: Festschrift für Klaus Lüderssen, Baden-Baden 2002, 205-219.

Günther, Klaus, Kritik der Strafe I+II, WestEnd – Neue Zeitschrift für Sozialforschung 2004, 117-131 sowie 2005, 131-141.

Hassemer, Winfried, Symbolisches Strafrecht und Rechtsgüterschutz, NStZ 1989, S. 553.

Hauschka, Christoph/Moosmayer, Klaus/Lösler, Thomas (Hrsg.), Corporate Compliance, Handbuch der Haftungsvermeidung im Unternehmen, 3. Aufl., München 2016.

Internationale Organisation für Normung (ISO), ISO 37001 Anti-bribery Management Systems - Requirements with guidance for use (ISO 37001:2016), Genf 2016.

Jasch, Michael, Das Strafrecht im Wohnzimmer: Zur Entwicklung symbolischer Strafgesetze, in: Interdisziplinäre Rechtsforschung zwischen Rechtswirklichkeit, Rechtsanalyse und Rechtsgestaltung, Bern 2009, 82-99.

Luhmann, Niklas, Rechtssoziologie, 3. Aufl., Opladen 1987.

Münchener Kommentar zum Aktiengesetz: AktG, Band 2: §§ 76-117, MitbestG, DrittelbG, Goette, Wulf/Habersack, Mathias/Kalss, Susanne (Hrsg.), 5. Aufl., München 2019.

Taleb, Nassim Nicholas, The Bed of Procrustes, London 2010.

Ders., The Black Swan, London 2007.

The Financial Crisis Inquiry Commission, The Financial Crisis Inquiry Report, Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States, Januar 2011 (https://fcic-static.law.stanford.edu/cdn_media/fcic-reports/fcic_final_report_full.pdf).

U.K. Ministry of Justice (MoJ), The Bribery Act 2010 Guidance, März 2011 (http://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf).

U.S. Department of Justice (DOJ), Evaluation of Corporate Compliance Programs, Juni 2019, aktualisiert Juni 2020 (https://www.justice.gov/criminal-fraud/page/file/937501/download).

U.S. Department of Justice (DOJ), *U.S. Securities and Exchange Commission (SEC),* FCPA Resource Guide, Second Edition, November 2012, aktualisiert Juli 2020 (https://www.justice.gov/criminal-fraud/file/1306671/download).

U.S. Department of Justice (DOJ), Memorandum on Individual Accountability for Corporate Wrongdoing („Yates Memo"), September 2015 (https://www.justice.gov/archives/dag/file/769036/download).