Herausforderungen bei der Bekämpfung von Wirtschaftskriminalität

Beim Thema Wirtschaftskriminalität hat sich in den letzten Jahrzehnten ein grundlegender Bewusstseins- und Bedeutungswandel vollzogen. Lange Zeit eher ignoriert und verharmlost, ist sie zu einem rechtspolitischen Kernthema geworden. Globalisierung und Digitalisierung eröffnen größere Spielräume für Wirtschaftsdelinquenz, die große Herausforderungen für die Bekämpfung für Strafverfolgungsbehörden und Unternehmen mit sich bringen.

Prof. Dr. Bernd Noll
ist Professor für Volkswirtschaftslehre und Wirtschaftsethik an der Hochschule Pforzheim. Bevorzugte Forschungsgebiete: Wirtschaftsethik, Wirtschaftsgeschichte, Institutionenökonomik.

Andreas Witt,
M.A., ist Kriminalbeamter beim Polizeipräsidium Pforzheim, Wirtschaftskriminalist und Lehrbeauftragter an der Hochschule Pforzheim. Bevorzugte Forschungsgebiete: Wirtschaftskriminalität, Wirtschaftsethik.

Stichwörter: Wirtschaftskriminalität, Digitalisierung, Globalisierung, Compliance

1. Vorbemerkungen

Beim Thema Wirtschaftskriminalität hat sich in den letzten Jahrzehnten ein grundlegender Bewusstseins- und Bedeutungswandel vollzogen. Lange Zeit wurden delinquente Verhaltensweisen im Wirtschaftsleben ignoriert oder verharmlost und blieben daher unterbelichtet. Augenzwinkernd sprach man von „Kavaliersdelikten", wenn es um Steuerhinterziehung, Subventionsbetrug oder Bestechung ausländischer Amtsträger ging. Der Ökonom *Adolf Zybon* schrieb 1972, dass den Wirtschaftsdelikten nicht nur die gesellschaftliche Ablehnung fehlt, „sondern allzu oft lösen sie sogar noch Bewunderung aus" (*ders.*, 1972, S. 47). Diese Sichtweise hat sich in den Folgejahrzehnten grundlegend geändert und zu einer fortschreitenden Neukriminalisierung delinquenter Sachverhalte geführt. Die zeitgleich einsetzenden Globalisierungs- und Digitalisierungsprozesse haben hierbei als Verstärker gewirkt. Sie haben eine grenzüberschreitende Ausdehnung des Aktionsradius' für wirtschaftskriminelles Verhalten mit unterschiedlichen normativen Standards gesorgt.

Mit der Informations- und Kommunikationstechnologie haben sich nicht nur effiziente, vielseitig nutzbare Tatwerkzeuge im virtuellen Raum für Betrug, Diebstahl oder Erpressung eröffnet. Hinzu kommt, dass sich Geschäftsabläufe der Unternehmen zunehmend ins Internet verlagern, so dass über Computerkriminalität interne Datennetze oder informationstechnische Systeme gestört, manipuliert oder zum Erliegen gebracht werden können. Für Wirtschaftskriminalität eröffnet sich mithin ein größeres Spektrum von Möglichkeiten, das neue Herausforderungen für deren Bekämpfung mit sich bringt. Die hieraus resultierenden Problemstellungen sollen im Folgenden paradigmatisch verdeutlicht werden, bevor auf die Schwierigkeiten von Strafverfolgungsbehörden und Unternehmen beim Umgang mit Wirtschaftskriminalität eingegangen wird.

2. Globalisierung und Digitalisierung

Am auffälligsten zeigt sich die Entwicklung hin zu einer globalen Ordnung beim Kampf gegen Korruption multinationaler Unternehmen; Korruption ist kein eigenständiger Straftatbestand, sondern ein unscharfer Begriff, mit dem viele Praktiken umschrieben werden. Wichtigste Variante ist, dass Funktionsträger (= Agenten) die ihnen von einem Geschäftsherren (= Prinzipal) anvertraute Macht miss-

bräuchlich nutzen, indem sie einem Anbieter (= Klient) nach einer Schmiergeldzahlung einen Auftrag oder andere Vorteile zukommen lassen. In Deutschland ist sie in den wichtigsten Formen von Bestechung/Bestechlichkeit oder Vorteilsgewährung/Vorteilsnahme schon lange strafrechtlich sanktioniert. Allerdings rechtfertigte der *BGH* noch im Jahre 1985 Auslandskorruption, als er formulierte, von „einem deutschen Unternehmer" könne nicht „erwartet werden", „dass es in den Ländern, in denen staatliche Aufträge nur durch Bestechung … zu erlangen sind, auf dieses Mittel völlig verzichtet" (zitiert nach *Berghoff*, 2016, S. 31). Im Ausland bezahlte Schmiergelder waren zudem steuerlich abzugsfähig, weil sie als „nützliche Aufwendungen galten. Doch ab 1999 kriminalisierte der deutsche Gesetzgeber auf Druck der *USA*, die mit dem *Foreign Corruption Practise Act* (*FCPA*) 1977 Vorreiter im Kampf von Auslandskorruption wurden, diese ebenfalls, und zwar die Bestechung ausländischer Amtsträger wie im geschäftlichen Verkehr.

Bei *Siemens* wurde die lange gelebte Praxis, im **Wettbewerb** auf **globalen Märkten** um Großprojekte mit Schmiergeldzahlungen nachzuhelfen, indes nicht aufgegeben. Dabei ignorierten ihre Manager, dass der *FCPA* extraterritoriale Wirkung entfaltet. Multinational agierende Unternehmen können danach von den US-Justizbehörden für Bestechungszahlungen in Drittländern belangt werden, wenn diese sich auf die US-Wirtschaft erheblich auswirken („substantial effect") können (vgl. *Tiedemann*, 2017, S. 187). Die beschuldigten Unternehmen müssen also keine delinquenten Handlungen in den USA vorgenommen haben, soweit sie nur auch in den USA Geschäfte tätigen.

Am 15.11.2006 durchsuchten Ermittler der Staatsanwaltschaft München 30 *Siemens*-Büros in Deutschland und Österreich nach Hinweisen auf Korruption bei Auslandsgeschäften. Mehrere Manager wurden verhaftet. *Siemens* praktizierte ein weltweites System schwarzer Kassen, aus denen rund 4300 illegal ausgeführte Zahlungen von rund 1,3 Milliarden € für eine Vielzahl von Projekten bezahlt worden sind, von Kraftwerken in Israel bis hin zu fälschungssicheren Ausweisen in Argentinien. Somit waren durch die globalen Aktivitäten Interessen von mehreren Jurisdiktionen betroffen. Neben Bußgeldzahlungen in Deutschland in Höhe von 395 Millionen Euro musste Siemens beachtliche Strafzahlungen leisten, unter anderem 450 Millionen Dollar an das US-amerikanische Justizministerium, und durch die US-Börsenaufsicht *SEC* erfolgte eine Gewinnabschöpfung in Höhe von 350 Millionen Dollar. Strafzahlungen, Bußgelder und Rechtskosten beliefen sich auf einen Gesamtbetrag von 2,5 Mrd. €.

Mit der Digitalisierung erweitert sich zum einen die Art, wirtschaftskriminelle Handlungen zu begehen: die Informationstechnologie als vielseitig einsetzbares **Tatwerkzeug**. Diebstahl vollzieht sich zunehmend als **Datendiebstahl**. Computergeschulte Kriminelle gelangen durch Ausnutzung von Sicherheitslücken in Unternehmensnetzwerke, um dort geistiges Eigentum oder vertrauliche Geschäftsinformationen bequem, anonym und transnational abzugreifen. Auch für Betrüger ergeben sich neue Handlungsspielräume im Internet, wie steigende Fallzahlen beim Kreditkartenbetrug und beim sog. CEO-Fraud zeigen. Der **Betrug** mit Kreditkarten profitiert von dem zunehmenden Online-Handel. Bei dem letztgenannten Delikttyp werden Unternehmen von den Tätern ausgespäht. Dabei nutzen sie die Möglichkeiten einer Open Source Intelligenz Recherche im Internet, klären Unternehmensstrukturen und sammeln alle verfügbaren Informationen. Sie geben sich dann als Geschäftsführer des Unternehmens aus und veranlassen führungsverantwortliche Mitarbeiter im Finanzwesen oder Geschäftsführer von Tochtergesellschaften, hohe Geldsummen auf ausländische Konten der Täter zu überweisen. Dabei soll strikte Vertraulichkeit gewahrt werden. Durch die missbräuchlich erlangten unternehmens- und personenbezogenen Daten wirken die Betrüger sehr glaubwürdig auf die Opfer, weshalb diese Betrugsmasche häufig erfolgreich ist (*Bundeskriminalamt*, 2016, S. 8 ff.). Beliebt ist bei Cyberkriminellen gegenwärtig eine Praxis, die Daten angegriffener Unternehmen mit Randomsoftware zu verschlüsseln und zu sperren, um Lösegeld zu fordern. Hier wird Computersabotage mit **Erpressung** verknüpft, die zur nächsten Fallvariante hinführt.

Die Verbreitung der Informationstechnologien eröffnet **neuen Delikten** Raum, die es so nicht offline gibt. Zu dieser Cyberkriminalität gehört z.B. das Hacking. Kriminelle gelangen in die internen Netzwerke und die informationstechnischen Systeme von Unternehmen, um Finanz- und Wirtschaftsdaten zu manipulieren und/oder betriebliche Prozesse zu sabotieren oder lahm zu legen. So hat *Thyssenkrupp* Ende 2016 den gravierendsten Cyberangriff in seiner Geschichte erfahren. Die Cyberwehr, das vom Unternehmen etablierte Notfallzentrum, benötigte 45 Tage, um den Angriff aufzudecken und abzustellen. Viren, Würmer oder Trojaner legen mittlerweile auch Ticket-Systeme von öffentlichen Verkehrsunternehmen lahm oder blockieren die IT-Netze von Krankenhäusern, so dass diese – wie kürzlich das Uniklinikum Düsseldorf – von der Notfallversorgung abgehängt werden.

Der von dem *DAX*-Unternehmen *Wirecard* im Jahre 2020 ausgelöste Finanzskandal kann sowohl unter Globalisierung wie Digitalisierung rubriziert werden. *Wirecard* war ein Global Player in einer digitalen Welt. Der Konzern steuert(e) das bargeldlose Bezahlen via Smartphone oder Kreditkarte und ist somit das Bindeglied zwischen Händler und Kunde. Der Schwerpunkt liegt im Onlinehandel, ein großer Teil der transnationalen Geschäftsabläufe erfolgt auf virtu-

eller Ebene. Um die Finanztransaktionen abzusichern, werden Zahlungen über Treuhandkonten abgewickelt. Im Juni 2020 musste der Konzern gegenüber der Öffentlichkeit eingestehen, dass bilanzierte Vermögenswerte von über 1,9 Milliarden Euro auf Treuhandkonten gebucht wurden, die nicht zu belegen sind und bei den genannten asiatischen Banken nicht existieren. In der Folge beantragte der Konzern im Juni 2020 die Eröffnung des Insolvenzverfahrens. Diese beispiellose **Bilanzmanipulation** wirft auch auf die Wirtschaftsprüfer und die Aufsichtsbehörde *BaFin (= Bundesanstalt für Finanzdienstleistungsaufsicht*) ein trübes Licht, ist es doch gerade ihre Kontrollaufgabe, Aktionäre und den Finanzplatz Deutschland vor solchen wirtschaftskriminellen Machenschaften zu schützen. Auffällig ist, dass hier wie bei anderen Skandalen (z.B. bei der Abgasmanipulation von *VW*) die entscheidenden Hinweise für die Delinquenz nicht von deutschen Behörden, sondern aus dem Ausland kommen.

3. Herausforderungen an die hoheitliche Strafverfolgung

Wirtschaftskriminalität, v.a. wenn sie sich im internationalen Kontexten abspielt, weist im Vergleich zur Bekämpfung anderer Formen von Kriminalität besondere Schwierigkeiten auf. Drei zentrale Aspekte sollen aufgezeigt werden:

Einer der bekanntesten Staatsanwälte für Wirtschaftsstrafsachen hat vor einigen Jahren auf eine erhebliche **Ressourcenungleichheit** zwischen den **Strafverfolgungsbehörden** und **Beschuldigten** hingewiesen. Staatsanwaltschaften kämpfen mit Nachwuchsproblemen, und Spezialistenwissen für komplexe Wirtschaftsstrafsachen ist häufig weder behördenintern vorhanden noch kann es ohne Weiteres über externe Gutachter hinzugekauft werden. Den Beschuldigten stehen demgegenüber ein „Heer hochqualifizierter, weil hochbezahlter und publizistisch sehr engagierter Anwälte gegenüber, die sich tief in die Materie eingearbeitet haben." (*Richter*, 2015, S. 4). Diese Rekrutierungsproblematik nimmt mit der „Digitalisierung der Wirtschaftskriminalität" weiter zu. Benötigt wird Personal, das sowohl über die erforderlichen rechtlichen als auch über die notwendigen IT-Kenntnisse verfügt. Hinzu kommt ihre Ausstattung mit moderner datentechnischer Infrastruktur, um die von Kriminellen genutzte Informationstechnologie effektiv bekämpfen zu können. Konsequenz dieser Asymmetrie ist der rechtsstaatlich heikle Befund, dass Wirtschaftsstrafverfahren übermäßig lange dauern, ein erheblicher Teil aus Mangel an Beweisen oder aus Opportunitätsgründen, meist nach Zahlung hoher Geldauflagen, eingestellt werden. Zur Anklage kommt es nur in jedem 20. Fall (vgl. *Meier,* 2016, S. 323 f.).

Bisher ist die Setzung von Strafnormen und ihre Durchsetzung grundsätzlich Aufgabe der Nationalstaaten. Dies ist Konsequenz des **völkerrechtlichen Nichteinmischungsprinzips**, wonach kein Staat in die Angelegenheiten eines anderen Staates eingreifen soll. Für die Zuständigkeit deutscher Behörden gilt demgemäß das **Tatortprinzip**, also der Ort, an dem die Tat begangen worden oder ihr Erfolg eingetreten ist. Die Ermittlungsmöglichkeiten sind also territorial begrenzt, auch wenn Kriminalität nationale Grenzen überschreitet. Das verlangt zwischenstaatliche Kooperation zur Aufklärung von Straftaten. Bei manchen Wirtschaftsdelikten wie Korruption oder jüngst bei der Steuerhinterziehung sind Fortschritte erkennbar. So haben *OECD* und *Europarat* eine Konvention zur gegenseitigen Amtshilfe verabschiedet, wonach sich inzwischen auch die Schweiz und Lichtenstein verpflichtet haben, von sich aus Amtshilfe zu leisten. Sie teilen danach z.B. der Bundesrepublik mit, wenn ein Ausländer, ein deutscher Bankkunde, in der Schweiz eine Steuerstraftat wie die Anlage von Schwarzgeld begeht (vgl. *Tiedemann*, 2017, S. 192). Andererseits gibt es Delikte wie Marken- oder Produktpiraterie, Industriespionage oder Cybercrime, bei denen eine stärkere Zusammenarbeit der involvierten Staaten kaum zu erwarten ist. Dafür sprechen ganz unterschiedliche Gründe: Niveaudiskrepanzen bei den Strafverfolgungsbehörden hinsichtlich ihrer kriminaltechnischen Expertise, unterschiedliche wirtschaftspolitische Interessenlagen oder eine divergierende Interpretation von Freiheits- und Eigentumsrechten in ihrer Rechtssphäre.

Innere Sicherheit kann im Zeitalter der Globalisierung und Digitalisierung nicht mehr primär aus nationaler Perspektive betrachtet werden. Allerdings gibt es bislang weder international verbindliche Strafvorschriften noch überstaatliche Strafverfolgungsbehörden (vgl. *Hecker*, 2015, S. 47).

- ***Europol***, eine Organisation der EU und 1998 gegründet, übernimmt keine operativen Ermittlungstätigkeiten, sondern hat koordinierende Aufgaben für die Mitgliedstaaten bei der Strafverfolgung. So wurden unter ihrer Leitung mittlerweile mehrere tausend Domains stillgelegt, auf denen gefälschte Produkte – Sportbekleidung, Elektronik, Toilettenartikel, Medikamente etc. – angeboten wurden, also dem Betreiben illegaler Geschäfte dienten. Erfolgreich war auch die gemeinsame Ermittlungsarbeit zwischen zwei oder auch mehreren EU-Nachbarländern bei der Bekämpfung der Mafia oder Darknet-Plattformen. Diese Kooperation ist indes noch nicht der Normalfall.
- ***OLAF*** (*Office Européen de Lutte Anti-Fraude*) ist im Jahre 2000 als ein Europäisches Amt für Betrugsbekämpfung etabliert worden. Das Amt soll wirtschaftskriminelles Verhalten, insbesondere Subventionsbetrug zum Nachteil der EU, angehen, indem es Untersuchungen vornimmt und nationalen Behörden Sanktionsempfehlungen gibt.
- Eine weltweite polizeiliche Zusammenarbeit zum Informations- und Datenaustausch ist über die internationale

kriminalpolizeiliche Organisation ***Interpol*** mit mittlerweile 194 Mitgliedstaaten möglich. Allerdings liegt die Art und Intensität der Beteiligung der Mitgliedstaaten im nationalen Ermessen. Zudem besteht der Vorbehalt, dass autoritäre Regime wie Russland oder die Türkei die Organisation in ihrem Kampf gegen Regimegegner nutzen.

Der Status quo zeigt also, dass der wirksamen Bekämpfung transnationaler Kriminalität durch die Territorialstaaten enge Grenzen gesetzt sind und die bisherigen Formen intergouvernementaler oder supranationaler Zusammenarbeit noch unzulänglich sind.

4. Kriminalprävention der Unternehmen

Lange Zeit haben Unternehmen das Thema Wirtschaftskriminalität wenig ernst genommen. Risiken wurden erkannt, aber v.a. bei anderen Unternehmen vermutet, mögliche Schäden wurden unterschätzt, so dass sich keine hinreichende Sensibilität für das Thema entwickelte. Diese Wahrnehmung und Einstellung hat sich grundlegend gewandelt: Die strafrechtliche Inanspruchnahme der Führungskräfte bei Verletzung von Aufsichtspflichten, empfindliche Strafen und Bußgelder für die Unternehmen bei Wirtschaftsdelinquenz und eine hohe Sensibilität wichtiger Stakeholder wie Kunden oder Zulieferer wie das emotionalisierende Engagement von NGOs gegenüber Unternehmenskriminalität haben dafür gesorgt, dass Unternehmen seit den 1990er Jahren zunehmend Compliance-Management-Systeme implementiert haben (vgl. *Noll*, 2020, S. 213 ff.). Ihr zentrales Anliegen soll es sein, Regeltreue sicherzustellen. **Diskretionäre Handlungsspielräume** der Mitarbeiter sollen **begrenzt** werden, um Tatgelegenheiten unattraktiver zu machen oder das Entdeckungsrisiko zu erhöhen (vgl. *Noll*, 2013, S. 185). Verbrechensbekämpfung wird so zu einer arbeitsteiligen Aufgabe von Unternehmen und Staat. Die aus den Unternehmen rührenden Aktivitäten sollen dazu dienen, den **staatlichen Rechtsrahmen präventiv zu stützen** und die Strafverfolgungsorgane zu entlasten. Ob Compliance diese Funktion tatsächlich erfüllt oder dem Top-Management eher als „Enthaftungsinstrument" dient und Mitarbeiter mit krimineller Energie veranlasst, intelligentere Wege zur Umgehung der Compliance-Regelungen ausfindig zu machen, darüber gibt es gegenwärtig eine intensive Debatte (vgl. *Noll*, 2020, S. 232 ff.).

Literatur

Berghoff, H., Von Watergate zur Compliance Revolution, in: *ders./C. Rauh/T. Welskopp* (Hrsg.), Tatort Unternehmen. Zur Geschichte der Wirtschaftskriminalität im 20. und 21. Jahrhundert, Berlin/Boston, 2016, S. 19 – 46.

Bundeskriminalamt, Wirtschaftskriminalität. Bundeslagebild 2016, Wiesbaden 2016.

Hecker, B., Europäisches Strafrecht, 5. Aufl., Berlin/Heidelberg 2015.

Horten, B./Gräber, M., Cyberkriminalität. Übersicht zu aktuellen und künftigen Erscheinungsformen, in: Forensische Psychiatrie, Psychologie Kriminologie, 14. Jg. (2020), S. 233–241.

Meier, B.-D., Kriminologie, 5. Aufl., München 2016.

Noll, B., Wirtschafts- und Unternehmensethik in der Marktwirtschaft, 2. Aufl., Stuttgart 2013.

Noll, B., Wirtschaftskriminalität: Eine wirtschaftsethische Perspektive, Stuttgart 2020.

Richter, H., Interview: Wir haben eine Zwei-Klassen-Täterschaft, in: Handelsblatt, Nr. 178 vom 16.09.2015, S. 4.

Tiedemann, K., Wirtschaftsstrafrecht, 5. Aufl., Köln/München 2017.

Zybon, A., Wirtschaftskriminalität als gesellschaftliches Problem, München 1972.