JURISTISCHE FAKULTÄT

UNIVERSITÄT HEIDELBERG
ZUKUNFT SEIT 1386

Zusammenfassung der Dissertation mit dem Titel

„Industrie- und Wirtschaftsspionage in Deutschland Phänomenologie – materielles Recht – prozessuale Durchsetzung: Bestandsaufnahme und Perspektiven“

Dissertation vorgelegt von Jonathan Drescher

Erstgutachter: Prof. Dr. Dieter Dölling
Zweitgutachter: Prof. Dr. Gerhard Dannecker

Institut für Kriminologie

Einleitung

Spionage wird von vielen als das „zweitälteste Gewerbe der Welt“ bezeichnet.[1] Während mit diesem Begriff in der öffentlichen Wahrnehmung lange Zeit vor allem militärische und politische Spionage verbunden wurde (man denke nur an James Bond, Lawrence von Arabien oder die Affäre um Günther Guillaume), steht in der heutigen Zeit mehr denn je die Beschaffung wirtschaftlicher Informationen im Fokus staatlicher Nachrichtendienste. Und Geheimdienste sind nicht die einzigen Akteure, die es auf geheimes Firmen-Know-how abgesehen haben – auch Unternehmen müssen sich häufig an der Konkurrenz und deren Produkten „orientieren“, um wettbewerbsfähig zu bleiben. Dass es häufig nicht bei der bloßen Orientierung im Sinne des sog. „Competitive Intelligence Gathering“[2] bleibt, sondern zuweilen die Grenzen zur strafbaren Konkurrenzausspähung überschritten werden, kann angesichts des steigenden Wettbewerbsdrucks, der fortschreitenden globalen Vernetzung und immer günstigeren digitalen Spähwerkzeugen kaum verwundern.

I. Untersuchungsgegenstand

Erstaunlich ist indes, dass es bislang keine Arbeit gibt, die sich dem Phänomen der Industrie- und Wirtschaftsspionage in all seinen Facetten widmet – und dies obwohl der deutschen Wirtschaft hierdurch je nach Studie pro Jahr ein Schaden von 12 bis 50 Mrd. Euro entsteht. So wurde in den letzten Jahren zwar eine Vielzahl an Arbeiten über das oder mit Bezug zu dem Thema „Wirtschafts- und Industriespionage“ bzw. „Know-how-/Geheimnisschutz“ verfasst, diese beschränken sich aber in aller Regel auf einzelne (Teil-) Aspekte dieses Themengebiets und beleuchten es allein aus betriebswirtschaftlicher[3] oder rechtlicher Sicht[4], fokussieren sich auf datenschutz- oder prozessrechtliche Problemstellungen oder widmen sich ausschließlich der Erarbeitung von Know-how-Schutzkonzepten.[5]

Gerade die Erarbeitung wirksamer Präventionskonzepte kann aber nur durch eine ganzheitliche Betrachtung gelingen. Essenziell ist zunächst die empirische Seite: Nur wenn bekannt ist, wie hoch die tatsächliche Bedrohung durch Ausforschung ist, wer daran beteiligt ist, auf welche Art und Weise Industriespione typischerweise vorgehen und welche Tatmotivation vorliegt, lassen sich Know-how-Abflüsse wirksam verhindern. Daneben ist auch die rechtliche Seite von einiger Bedeutung: Zum einen, um etwaige Schutzlücken im gesetzlichen Geheimnisschutz über vertragliche Regelungen schließen zu können, zum anderen, um Gesetzesverstöße zeitnah als solche zu erkennen und gerichtlich zu verfolgen. Da sich bislang niemand dem Phänomen Wirtschafts- und Industriespionage in seiner Gesamtheit gewidmet hat, war es an der Zeit für eine ganzheitliche Arbeit, die all diese Erkenntnisse zusammenführt und systematisiert.[6]

---

[1] *Cilluffo/Cardash,* Economic Espionage: A Case for Why the U.S. Needs to Push Back, The Wall Street Journal Online, 17.08.2015; *Jakob,* Nachrichtendienste, S. 13; *Röper,* Trade secret theft, S. 35.

[2] Übersetzt so viel wie „Konkurrenz- oder Wettbewerbsanalyse“, *Hummelt,* Wirtschaftsspionage, S. 21; vgl. insoweit den Vgl. insoweit den „Code of Ethics“ der Strategic and Competitive Intelligence Professionals (SCIP), abrufbar unter http://www.scip.org/?page=CodeofEthics.

[3] *Glitz/Meyersson,* Industrial Espionage and Productivity; *Hofer/Weiß,* Wirtschaftsspionage; *Stauf,* IP Management, Ganzheitliches Intellectual Property Management im Unternehmen.

[4] In der Übersicht *Ann,* GRUR 2007, 39 ff.; *McGuire,* GRUR 2015, 424 ff.; *Ohly,* GRUR 2014, 1 ff.

[5] So etwa *Bierekoven,* ITRB 2012, 106; *Börger/Rein,* CB 2017, 118 ff.; *Diringshofen,* GRUR-Prax 2013, 397 ff.; *Karden/Freiberg,* Praxishandbuch Unternehmenssicherheit; *Lindemann/Meiwald/Petermann u. a.,* Know-how-Schutz; *Lotrointe,* N.C. J. Int'l L. & Com. Reg., 2014, 443; *Meiwald,* Konzepte zum Schutz vor Produktpiraterie, S. 81 ff.; *Weber/Buschermöhle,* CB 2016, 339 ff.; *Wurzer,* CCZ 2009, 49 ff.; vertragsrechtlich *Kurz,* Vertraulichkeitsvereinbarungen; *Schöwerling,* GRUR-Prax 2015, 52 ff.; in der Übersicht *Initiative Wirtschaftsschutz,* Leitfaden Wirtschaftsschutz.

[6] Einen interdisziplinären Ansatz verfolgt lediglich *Fleischer,* Wirtschaftsspionage. Dort fehlt allerdings eine Darstellung der (zahlreichen) prozessrechtlichen Problemstellungen.

II. Gang der Untersuchung

Die Arbeit umfasst sechs Kapitel:

Das erste Kapitel enthält einen Abriss der Geschichte der Industrie- und Wirtschaftsspionage und der bedeutsamsten Entwicklungen in der Rechtsprechung und von Seiten des Gesetzgebers.

Ausgehend von diesem historischen Hintergrund gibt das zweite Kapitel einen Überblick über die Bedrohungslage für deutsche Unternehmen: Wer sind die Täter und Opfer von Wirtschaftsausspähung? Welche Angriffsmethoden und Vorgehensweisen werden zur Ausspähung vorwiegend eingesetzt? Gibt es besonders häufig betroffene Branchen oder Unternehmensgrößen? Auf welche Daten und Geheimnisse haben es die Täter abgesehen? Welche Schäden werden verursacht? Welche Erkenntnisse gibt es zu Tatmotivation und Täterprofilen? Was kann Prävention leisten und wie ist es um den Schutz deutscher Unternehmen bestellt? Wie ist die Bedrohung durch fremde Nachrichtendienste einzuschätzen?

Das dritte Kapitel beleuchtet die dogmatischen Grundlagen des rechtlichen Geheimnisschutzes und geht der Frage nach, ob und warum es überhaupt eines gesetzlichen Schutzes von geheimem Know-how bedarf und in welcher Form dieser ausgestaltet sein muss.

Hierauf aufbauend wird im vierten und fünften Kapitel en détail die juristische Seite des Phänomens Wirtschaftsausspähung untersucht: Während sich das vierte Kapitel mit den straf-, arbeits- und zivilrechtlichen Folgen von Wirtschafts-, Industrie- und Cyberspionage für den einzelnen Täter befasst, behandelt das fünfte Kapitel die Frage, wie sich derartige Taten den eigentlichen Profiteuren – den dahinterstehenden Unternehmen und deren Leitungspersonen – zurechnen lassen.

Nach Abschluss der materiell-rechtlichen Ausführungen beschäftigt sich der letzte Teil der Arbeit in Kapitel sechs mit dem derzeit wohl größten Hindernis für eine wirksame (repressive) Spionagebekämpfung: dem Prozessrecht. Denn sowohl der strafrechtlichen Verurteilung von Wirtschaftsspionen als auch der Durchsetzung zivilrechtlicher Ansprüche des Geschädigten steht eine Vielzahl zivil- und strafprozessualer Problemstellungen im Wege – von der Täterermittlung über die Beweisbeschaffung bis hin zum Geheimnisschutz im Prozess selbst – , was dazu führt, dass der rechtliche Schutz oft nur auf dem Papier besteht.

III. Zusammenfassung der wesentlichen Ergebnisse

1. Status quo der empirischen Forschung in Deutschland

Im Rahmen einer Metaanalyse aktueller Studien zum Thema Industrie- und Wirtschaftsspionage[7] wurde deutlich, dass es sehr schwierig ist, ein realitätsgetreues Bild von Spionageangriffen gegen deutsche Unternehmen zu erhalten. Dies hängt damit zusammen, dass es bislang an einer klaren, allgemeingültigen Definition des Untersuchungsgegenstands „Industrie- und Wirtschaftsspionage“ fehlt, sodass jede Studie eine eigene Bewertung vornehmen muss, welche Vorgehensweisen sie hierunter fasst. Dementsprechend ist in einer Vielzahl empirischer Untersuchungen zu diesem Thema nicht ersichtlich, ob es sich bei den angegebenen Ausspähungsvorfällen tatsächlich um illegale (oder zumindest moralisch fragwürdige) Verhaltensweisen handelt. Gerade die Auflistung von OSINT (Open Source Intelligence = Informationsgewinnung aus öffentlich zugänglichen Quellen) legt den Verdacht nahe, dass in manchen Studien jeglicher Know-how-Abfluss wie etwa die Verletzung

[7] Im Einzelnen wurden untersucht: *Bitkom,* Studie Wirtschaftsschutz 2016; *BMWi,* Studie IT-Sicherheitsniveau in KMU 2012; *Bollhöfer/Jäger*, WISKOS-Studie Wirtschaftsspionage 2018; *CT,* Studie Industriespionage 2014; *Ernst & Young,* Studie Datenklau 2017; *kes,* Sicherheitsstudie 2016; *KPMG,* Studie Wirtschaftskriminalität 2016; *KPMG,* Studie e-Crime 2017; *PwC,* Studie Wirtschaftskriminalität 2016; *SiFo,* Studie Know-how-Schutz in Baden-Württemberg 2009/2010; *WIK/ASW,* Sicherheits-Enquête 2014/2015.

gewerblicher Schutzrechte als Ausspähung aufgefasst wurde. Letztere können indes aufgrund der mit ihrer Anmeldung einhergehenden Offenlegung per se keine Geheimnisse sein. Darüber hinaus unterscheiden sich die Befunde der untersuchten Studien aufgrund ihrer verschiedenen Studiendesigns und -schwerpunkte nicht nur untereinander, sondern zum Teil weichen selbst die Angaben in der jeweiligen Nachfolgestudie deutlich von ihrer Vorgängerstudie ab. Insbesondere zu den Fragen nach der Betroffenheit deutscher Unternehmen durch Ausforschung, den hierdurch verursachten Schäden sowie den Tatmitteln ließen sich studienübergreifend kaum belastbare Ergebnisse, sondern allenfalls einige Anhaltspunkte bzw. Tendenzen finden. Im Einzelnen konnte festgestellt werden:

- Etwa 30 bis 50 Prozent der mittelständischen und Großunternehmen in Deutschland waren in den letzten zwei bis drei Jahren von einem Ausforschungsfall betroffen,[8] wobei die Betroffenheitsrate seit 2010 kontinuierlich (wenn auch nur leicht) abnimmt.[9]

- Das wirtschaftliche Schadenspotential von Spionage für die Bundesrepublik dürfte in einer Größenordnung von etwa 12 Mrd. Euro jährlich liegen.[10]

- Demgegenüber lassen sich nicht einmal Tendenzen festmachen, welche Unternehmensgrößen, Branchen oder Industriezweige besonders betroffen sind.[11]

- Ein Großteil der Ausforschung entfällt auf elektronische Angriffe und den Verrat durch Mitarbeiter.[12] Weitgehend ungeklärt ist indes, welche Schäden rein elektronische Ausspähung letztlich zu verursachen in der Lage ist, wenn keine Innentäter beteiligt sind, die die abgeschöpften Informationen in den richtigen Kontext setzen können.

- Die meisten Angriffe zielen nicht auf technisches Know-how ab, sondern vor allem Kunden- und Geschäftsdaten befinden sich im Visier der Datenspione.[13]

- Das Gefahrenbewusstsein für das Risiko von Spionage (die „Awareness“) ist bei den Befragten zwar durchgehend hoch und nahezu alle befragten Unternehmen gehen von einer Zunahme der Bedrohungslage aus,[14] gleichwohl existiert in mittelständischen Unternehmen Informationssicherheit häufig nur auf dem Papier.

2. Unzureichende Präventionsmaßnahmen

Im Hinblick auf die Erarbeitung von Präventionskonzepten konnte festgestellt werden, dass die Motive der Täter sowie die maßgeblichen kriminogenen Faktoren weitgehend bekannt sind und sich auch Theorien zur Erklärung wirtschaftskriminellen Handelns auf Industrie- und Wirtschaftsspionage übertragen lassen.[15] Somit lassen sich Präventionskonzepte erarbeiten, die einen wirksamen und ganzheitlichen Know-how-Schutz ermöglichen. Bei Betrachtung der Studien ist allerdings zu konstatieren, dass insbesondere in kleinen und mittleren Unternehmen häufig keine ganzheitliche Sicherheits-Strategie implementiert ist, sondern das Thema Informationsschutz allein als Aufgabe der IT angesehen wird[16] – und selbst dort unterbleiben notwendige Sicherheitsvorkehrungen häufig aus Kostengründen oder Bequemlichkeit. Dies hat zur Folge, dass mittelständische Unternehmen zwar dem Grunde nach keiner höheren

[8] *Drescher*, Industrie- und Wirtschaftsspionage, 1. Aufl., Münster 2019, Kap. 2 § 2 B. I. 1.
[9] *Drescher* (Fn. 8), Kap. 2 § 2 B. I. 2.
[10] *Drescher* (Fn. 8), Kap. 2 § 2 B. III. 3.
[11] *Drescher* (Fn. 8), Kap. 2 § 2 B. II.
[12] *Drescher* (Fn. 8), Kap. 2 § 3.
[13] *Drescher* (Fn. 8), Kap. 2 § 2 B. II. 3.
[14] *Drescher* (Fn. 8), Kap. 2 § 2 B. I. und § 6 A. VI.
[15] *Drescher* (Fn. 8), Kap. 2 § 4 C. V.
[16] *Drescher* (Fn. 8), Kap. 2 § 6 A. I. und VI.

Gefährdung als Großunternehmen ausgesetzt sind,[17] wenn sie aber Ziel von Ausforschung werden, sich dieser schlechter erwehren können.

3. Geringes Entdeckungs- und Verfolgungsrisiko: Das „Kardinalproblem“

Neben Defiziten in der Prävention erweist sich vor allem das äußerst geringe Risiko einer Entdeckung und Strafverfolgung als „Hemmschuh“ einer effektiven Spionageabwehr. Insbesondere das bereits von vielen Seiten bemängelte Problem einer sehr zurückhaltenden Anzeigebereitschaft von Spionageopfern wurde auch in den hier untersuchten Studien deutlich: In lediglich 10 bis 20 Prozent aller Ausforschungsfälle wandten sich betroffene Unternehmen an die Strafverfolgungsbehörden.[18] Mögen auch die Gründe, aus denen Unternehmen erfolgreiche Angriffe auf ihr Know-how nicht publik machen wollen (insbesondere die Angst vor Reputationsverlust oder das Scheuen des Aufwands eines Strafverfahrens), durchaus nachvollziehbar sein, nimmt dieses Vorgehen nicht nur dem Strafrecht einen Großteil seiner Abschreckungswirkung und trägt dazu bei, dass Industriespione ohne größere Sorge vor negativen Konsequenzen ihrem Werk nachgehen und unter Umständen weitere Unternehmen schädigen können. Die mangelnde Anzeigebereitschaft hat auch zur Folge, dass die Strafverfolgungsbehörden nicht in ausreichendem Maß relevante Erkenntnisse zur Phänomenentwicklung von Industrie- und Wirtschaftsspionage erhalten.

4. Bedrohung durch Geheimdienste

Im Hinblick auf die Bedrohungslage der deutschen Wirtschaft durch fremde Geheimdienste ergibt sich ein ambivalentes Bild. Einerseits scheint der Anteil nachrichtendienstlicher Spionageangriffe gegen deutsche Unternehmen nach den Ergebnissen der vorgestellten Studien relativ gering zu sein[19] und zumindest von Seiten westlicher Dienste auch keine Gefahr eines Know-how-Diebstahls zugunsten einzelner Unternehmen zu drohen. Denn soweit deutsche Unternehmen Aufklärungsziel von NSA und anderen westlichen Nachrichtendiensten sind, ist davon auszugehen, dass dort abgeschöpfte Informationen aus rein praktischen sowie kartellrechtlichen Erwägungen nicht zur Erzielung von Wettbewerbsvorteilen für die heimische Wirtschaft eingesetzt werden.[20]

Andererseits kann auch die Ausspähung der Wirtschaft allein zu (wirtschafts-) politischen Zwecken nachteilige Auswirkungen auf die Volkswirtschaft des Ziellands entfalten (etwa bei der Nutzung besagter Informationen zur Durchsetzung nationaler Interessen im Rahmen von Wirtschaftsgipfeln oder der Verhandlung von Handelsabkommen) und damit mittelbar zulasten des ausgespähten Unternehmens gehen. Daneben besteht bei Wirtschaftsspionage durch Staaten ohne eine vergleichbar offene Wettbewerbsgesellschaft (insbesondere China und Russland) durchaus ein reales Risiko, dass abgeschöpftes Know-how unmittelbar zur Stärkung einzelner (Staats-) Unternehmen eingesetzt wird.[21] Da in beiden Fällen ein Abschluss entsprechender „No-Spy-Abkommen“ wohl illusorisch ist,[22] muss die Spionageabwehr insbesondere durch technische Sicherheitsmaßnahmen gewährleistet werden. Hierzu ist ein Ausbau der Kapazitäten der staatlichen Sicherheits- und Spionageabwehrbehörden unumgänglich. Denn bei einem Vergleich der Kapazitäten westlicher, chinesischer und russischer Geheimdienste mit der Ausstattung der deutschen Dienste wurde deutlich, dass Deutschland hier sowohl technisch als auch personell einen deutlichen Rückstand aufweist.

---

[17] *Drescher* (Fn. 8), Kap. 2 § 2 B. II. 1.
[18] *Drescher* (Fn. 8), Kap. 2 § 6 B. III.
[19] *Drescher* (Fn. 8), Kap. 2 § 4 A.
[20] *Drescher* (Fn. 8), Kap. 2 § 5 B. VI. 2.
[21] *Drescher* (Fn. 8), Kap. 2 § 5 C. III.
[22] Vgl. *Goetz/Mascolo/Obermayer,* Geschichte eines Täuschungsmanövers, Süddeutsche Online, 27.05.2015.

5. Spionageschutz nach deutschem Recht

Der materiell-rechtliche Schutz vor Wirtschafts- und Industriespionage ist in Deutschland insgesamt recht gut ausgeprägt. Dabei richtet sich die Reichweite des Schutzes maßgeblich danach, ob der Geheimnisinhaber zum Täter in einer vertraglichen Sonderverbindung steht. Ist dies der Fall, wird dem Verletzten durch § 4 Abs. 2 Nr. 2 und Nr. 3 GeschGehG ein umfassender Schutz vor Geheimnisverrat gewährt – der Vertragspartner darf das Geheimnis nicht Nutzen oder Offenlegen. Demgegenüber existiert außerhalb vertraglicher Sonderbeziehungen kein vergleichbar absoluter Schutz für geheimes Know-how. Denn § 4 Abs. 1 und Abs. 2 Nr. 1 GeschGehG verbietet als maßgebliche Geheimnisschutznorm gegenüber jedermann nicht die Nutzung einer Information an sich, sondern pönalisiert nur die Überwindung faktischer Schutzvorrichtungen, die ihr Inhaber gewährleisten muss.[23] Es wird also zum einen nur *geheimes* Know-how geschützt und zum anderen besteht auch dieser Schutz nur „*als Reflex des Zugangsschutzes, der primär gewährleistet wird. Know-how-Schutz besteht, anders gewendet, nur gegen die unlautere Offenbarung von Know-how.* […] *Wird Know-how durch Nachlässigkeit beim Geheimschutz bekannt, geht sein Schutz verloren*“.[24] Der Geheimnisschutz im deutschen Recht ist damit – im Gegensatz zu Immaterialgüterrechten, denen als positive Schutzformen auch gegenüber Dritten eine absolute Ausschlussfunktion zukommt – als reines Abwehrrecht ausgestaltet.[25]

Gleichwohl vermag im Bezug auf Industrie- und Wirtschaftsspionage auch dieser bloß „abgestufte Schutz“ im Ergebnis alle denkbaren Spionageangriffe auf geheimes Unternehmenswissen adäquat zu erfassen – so lange der Geheimnisinhaber nur für ein Mindestmaß an faktischen Sicherheitsvorkehrungen sorgt (vgl. § 2 Nr. 1 GeschGehG). Zudem existiert seit dem Inkrafttreten des GeschGehG erstmals ein ausdifferenziertes und flexibles Rechtsfolgensystem. So hat der Verletzte nun insbesondere die Möglichkeit, mit Hilfe von Vernichtungs- und Rückrufansprüche wirksam den Vertrieb von Produkten zu unterbinden, die in irgendeiner Form auf der Wirtschaftsausspähung beruhen, und sich so seine verlorene Marktposition zurückzuerobern.[26]

Demgegenüber weist der strafrechtliche Know-how-Schutz einigen Raum zur Verbesserung auf. Zwar lässt sich der „Kernbereich“ solcher Tathandlungen, die im allgemeinen Sprachgebrauch als „Wirtschafts- und Industriespionage“ verstanden werden (insbesondere die Ausforschung mittels technischer Spähwerkzeuge oder durch das Anwerben/Ausfragen von Mitarbeitern) über § 23 GeschGehG sowie §§ 202a ff. und 99 StGB strafrechtlich erfassen. Allerdings ist gerade der „zentrale Antispionagetatbestand“ § 23 GeschGehG an Unübersichtlichkeit kaum zu überbieten und weist überdies einige Schutzlücken auf. Dies liegt darin begründet, dass der Gesetzgeber bei der Schaffung des GeschGehG den strafrechtlichen Schutz einerseits zivilrechtsakzessorisch ausgestalten, andererseits aber keine rechtlichen Änderungen gegenüber der früheren Rechtslage herbeiführen wollte.[27] Herausgekommen ist ein hybrides Schutzregime, das sich zunächst über die zivilrechtlichen Verbotsnormen stülpt, um sodann durch (unnötige) Einschränkungen auf Tatbestandsebene schon geschlossene Strafbarkeitslücken wieder aufzureißen. Dies zeigt sich exemplarisch an § 23 Abs. 3 GeschGehG, der die abredewidrige Verwendung im geschäftlichen Verkehr anvertrauter Informationen unter Strafe stellt, und der den – im GeschGehG sonst überall verwendeten – Schutzgegenstand des Geschäftsgeheimnisses eigens auf technisches Know-how beschränkt,

---

[23] *Ann,* GRUR 2007, 39, 40 f.; *McGuire,* GRUR 2015, 424, 426.
[24] *Ann,* GRUR 2007, 39, 40 f.; ähnlich *McGuire,* GRUR 2015, 424, 426.
[25] Im US-amerikanischen Recht wird dagegen auch nicht offenbartes Know-how als positive Schutzform des Immaterialgüterrechts begriffen, *Sander,* GRUR-Int. 2013, 217, 219.
[26] *Drescher* (Fn. 8), Kap. 4 § 4 B. I. 2. b) und Kap. 4 § 4 B. II. 3.
[27] *Drescher* (Fn. 8), Kap. 4 § 2 A. IV.

um der mangelhaften alten Rechtslage zu entsprechen.[28] Hier hätte mit etwas mehr Mut zur Reform ein deutlich stimmigeres strafrechtliches Gesamtbild geschaffen werden können.

6. Höhe der Sanktionen und Erfassbarkeit von Unternehmen

Zudem mag das Strafrecht in seiner jetzigen Ausgestaltung zwar in der Lage sein, die gefährlichsten Formen von Wirtschafts- und Industriespionage zu erfassen, die Strafrahmen spiegeln indes kaum wider, dass durch Spionage dem Geschädigten häufig „*das gebündelte Extrakt jahre- oder jahrzehntelanger, mit immensen Investitionen betriebener Forschung entzogen wird*".[29] Dies wird besonders im Vergleich mit den Strafrahmen der klassischen Vermögensdelikte (z.B. Diebstahl oder Betrug) deutlich, die für vergleichbare Schadenshöhen doppelt so hohe Mindest- und Höchststrafen vorsehen.[30] Leider hat der Gesetzgeber die Umsetzung der Geheimnisschutz-RL[31] nicht zum Anlass genommen, die Strafrahmen der §§ 17 ff. UWG a.F. entsprechend umzuformen, sondern hat diese unverändert in § 23 GeschGehG übernommen. Auch nach der Reform spiegelt sich das hohe Gefährdungspotential von Wirtschafts- und Industriespionage mithin nicht in einem entsprechenden Strafmaß wider.

Ähnliches gilt im Hinblick auf die Sanktionierung der „delinquenten" Unternehmen. Hier stellt sich das Problem, dass das deutsche Ordnungswidrigkeitenrecht mit § 30 OWiG zwar dem Grunde nach die Möglichkeit bietet, das Unternehmen selbst mit einer Geldbuße zu belegen. Da die durch Spionage erlangten Vorteile aber häufig nur mittelbarer Art sind (etwa eine Verbesserung der Marktposition oder die teilweise oder vollständige Verdrängung der Konkurrenz vom Markt) und sich kaum beziffern oder abschöpfen lassen, kann selbst nach Verhängung einer Geldbuße die Geheimnisverletzung im Ergebnis vorteilhaft gewesen sein. Gleiches gilt für die Einziehung. Gerade im Hinblick auf die Verhinderung von Spionage durch „altruistisch" motivierte Täter, die aus falsch verstandenem Loyalitätsgefühl zu ihrem Arbeitgeber Konkurrenten ausforschen, ist die Höhe der drohenden Sanktionen ein wichtiger Aspekt der Abschreckung.[32] Hier wäre die Schaffung eines „echten" Unternehmensstrafrechts die konsequenteste Lösung.[33] Zumindest aber sollte in Anlehnung an die Datenschutz-Grundverordnung über eine Verhängung von am Jahres-Konzernumsatz orientierten Geldbußen,[34] ein Importverbot rechtsverletzender Waren[35] oder – ähnlich wie bei kartellrechtswidrigen Absprachen, Korruption oder Verstößen gegen das Schwarzarbeitsgesetz – über einen Ausschluss von öffentlichen Aufträgen[36] nachgedacht werden.

Eine Verschärfung der drohenden Sanktionen könnte auch im Hinblick auf Compliance positive Effekte erzielen. Denn wie sich bei einer Untersuchung der verwirklichten Compliance-Maßnahmen zeigt, sind diese oftmals nur auf die Einhaltung solcher Normen ausgerichtet, deren Verletzung massive Bußgelder nach sich zieht – und damit sparen sie die Verhinderung von Spionage aus.[37] Dabei wäre gerade in diesem Zusammenhang eine Sensibilisierung der

---

[28] *Drescher* (Fn. 8), Kap. 4 § 2 A. I. 6. e).
[29] *Kragler,* wistra 1983, 2.
[30] *Drescher* (Fn. 8), Kap. 4 § 2 D. III. 2.
[31] Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung.
[32] *Schünemann,* Unternehmenskriminalität, S. 158.
[33] *Drescher* (Fn. 8), Kap. 5 § 1 C. I. 3.
[34] Nach Art. 83 Abs. 4 DSGVO können gegen Unternehmen Geldbußen in Höhe von bis zu 4 % des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden.
[35] So besteht nach US-amerikanischem Recht die Möglichkeit, bei der International Trade Secret Commission Beschwerde einzulegen und so den Import von Waren zu verhindern, die auf Basis eines unbefugt erlangten Geheimnisses hergestellt wurden, vgl. *McGuire*, GRUR 2016, Fn. 47.
[36] Vgl. zu den bestehenden Regelungen *Greeve,* in: Ignor/Mosbacher, HB Arbeitsstrafrecht, § 17 Rn. 10 ff.
[37] *Drescher* (Fn. 8), Kap. 2 § 6 C.

Mitarbeiter besonders wichtig, da bei einigen Formen von Geheimnisverletzungen (speziell bei der Abwerbung von Mitarbeitern sowie der Nutzung mitgenommener Unterlagen vom früheren Arbeitgeber) die Rechtswidrigkeit der Handlung nicht immer ins Auge sticht. Hier kann und muss Compliance einen wichtigen Beitrag zur Prävention leisten.

7. Der Nachweis von Industrie- und Wirtschaftsspionage

Die dringlicheren Probleme bei der rechtlichen Behandlung von Wirtschafts- und Industriespionage finden sich allerdings auf der prozessualen Ebene. Denn das beste materielle Schutzregime ist „zahnlos", wenn strafrechtliche Ermittlungsverfahren wegen fehlender Anhaltspunkte zur Identität des Täters im Sande verlaufen und der Geschädigte aufgrund mangelnder Möglichkeiten zur Beweisbeschaffung seine Ansprüche nicht vor Gericht durchsetzen kann – und genau dies ist bei Geheimnisverletzungen häufig der Fall. Bis zu einem gewissen Maß liegt diese Problematik in der Natur der Sache. Spionage ist ihrem Wesen nach ein heimliches Delikt, welches gerade nicht entdeckt werden soll. Technische Maßnahmen wie Intrusion-Detection-Systeme und eine regelmäßige Auswertung der Logfiles können zwar im Einzelfall dazu beitragen, den Tätern auf die Spur zu kommen.[38] Im Übrigen ist aber gerade bei Spionage über das Internet eine Identifizierung der Täter kaum möglich, wenn diese die sich bietenden Möglichkeiten zur Anonymisierung nutzen.

In der Praxis werden Geschädigte daher häufig erst durch das Auftauchen von Konkurrenzprodukten oder eine Niederlage in einem Bieterwettstreit auf einen Informationsabfluss aufmerksam.[39] An dieser Stelle sind die im deutschen Zivilrecht vorgesehenen Möglichkeiten zur Beweisbeschaffung dem Geschädigten aber häufig keine Hilfestellung, da diese, um auf Ausforschung gerichteten Anträgen Einhalt zu gebieten, ihrerseits bereits hinreichende Nachweise für eine unerlaubte Wirtschaftsausspähung voraussetzen[40] – Nachweise, die der Geschädigte meist nicht erbringen kann. Auch Vermutungen und Beweiserleichterungen sind wegen der drohenden Gefahr eines Missbrauchs zur Ausforschung der Gegenseite kein adäquates Mittel, um dieser Problematik beizukommen.[41] Allenfalls durch ein dem US-amerikanischen „pretrial discovery" Verfahren nachgebildetes Konstrukt ließe sich dieses Spannungsfeld auflösen – wobei dieses mit dem deutschen Zivilprozessrecht in seiner jetzigen Form kaum vereinbar wäre.[42]

Im Ergebnis ist der Geschädigte daher häufig auf die weitergehenden Befugnisse der Staatsanwaltschaft angewiesen, um an die erforderlichen Beweismittel zu gelangen. Die Hinzuziehung staatlicher Ermittlungsbehörden birgt indes das latente Risiko einer Vertiefung der Geheimnisverletzung. Zum einen sieht die StPO keine wirksamen Regelungen des Geheimnisschutzes gegenüber dem Beschuldigten vor, zum anderen steht dem Geschädigten kein Antragsrecht für einen Ausschluss der Öffentlichkeit im Rahmen der Hauptverhandlung zu. Aus diesen Gründen verzichten viele Betroffene auf eine Einschaltung der Staatsanwaltschaft und sehen auch von einer Geltendmachung ihrer zivilrechtlichen Ansprüche ab. Eine Besserung der Beweissituation für Spionageopfer lässt sich daher nur durch einen effektiven Geheimnisschutz im Prozess erreichen.

8. Der Geheimnisschutz in Zivil- und Strafprozess

Im Hinblick auf die Möglichkeiten eines effektiven Geheimnisschutzes stellt der Zivilprozess das weniger große Problem dar. Zum einen bestimmen hier die Parteien den Gegenstand des

---

[38] Vgl. *BKA,* Studie Wirtschaftsspionage 2014, S. 71.
[39] Zur Entdeckung *Drescher* (Fn. 8), Kap. 2 § 6 B. I.
[40] *Drescher* (Fn. 8), Kap. 6 § 1 B. VIII.
[41] *Föbus,* Insuffizienz des § 17 UWG, S. 279. Gleiches gilt auch für den Strafprozess, wo der Grundsatz „in dubio pro reo" einer Beweislastumkehr von Grund auf entgegensteht.
[42] Vgl. *Schönknecht,* GRUR-Int. 2011, 1000.

Verfahrens und den Umfang, in dem dieser mündlich verhandelt wird, sodass der Inhalt des ausgespähten Geheimnisses nicht in der Hauptverhandlung selbst thematisiert werden muss.[43] Zum anderen sehen die §§ 16, 19 GeschGehG die Möglichkeit eines bindenden Antragsrechts der Parteien für den Ausschluss der Öffentlichkeit vor und ermöglichen es, der Gegenpartei ein strafbewehrtes Nutzungs- und Offenbarungsverbot bzgl. aller im Rahmen des Prozesses eingebrachten Geschäftsgeheimnisse aufzuerlegen. Im Zivilprozess mag daher lediglich der Umstand, dass gegenüber dem Beklagten kein faktischer Ausschluss von den streitgegenständlichen Geheimnissen möglich ist, den einen oder anderen Verletzten von einem Prozess zurückschrecken lassen. Hieran ist indes nichts zu ändern. Eine Geheimhaltung streitentscheidender Tatsachen gegenüber der anderen Partei im Sinne eines „in-camera-Verfahrens" ist mit den Grundsätzen eines *Erkenntnis*verfahrens nicht vereinbar,[44] sodass an dieser Stelle dem Risiko weiterer wirtschaftlicher Schäden nur durch die Auferlegung von Nutzungs- und Mitteilungsverboten entgegengetreten werden kann.

Im Strafverfahren ist das Risiko, dass die Verletzung des Spionageopfers durch eine Offenbarung des Geheimnisses im Rahmen der Hauptverhandlung noch vertieft wird, hingegen ungleich höher, da die Hoheit über das Verfahren nicht beim Geheimnisinhaber liegt, sondern Staatsanwaltschaft und Gericht die Entscheidungen treffen, in welchem Umfang Geschäftsgeheimnisse in die Hauptverhandlung eingeführt werden. Ein bindendes Antragsrecht des Geschädigten über den Ausschluss der Öffentlichkeit wäre daher an dieser Stelle umso wichtiger, um seinen Geheimhaltungsinteressen hinreichend Rechnung zu tragen. Dass der Gesetzgeber geichwohl bei der Umsetzung der Geheimnisschutz-RL ein solches Antragsrecht allein für den Zivilprozess implementiert hat, ist bedauerlich, zumal die übrigen Regelungen über die Öffentlichkeit und ihre Einschränkungsmöglichkeiten ebenfalls für beide Verfahrensarten einheitlich im GVG geregelt sind.

---

[43] *Drescher* (Fn. 8), Kap. 6 § 1 C. I.

[44] *Föbus,* Insuffizienz des § 17 UWG, S. 279; *Stadler,* NJW 1989, 1202, 1203. Im Strafprozess ist ein Ausschluss des Angeklagten von der Beweisaufnahme freilich aufgrund von Art. 103 Abs. 1 GG von vornherein nicht zulässig, *BVerfGE* 57, 250, 288; *BVerfG,* NStZ-RR 2008, 16; *BGH,* NJW 2000, 1661, 1662; *Ann,* in: Ann/Loschelder/Grosch, Kap. 7 Rn. 78; *Dorner,* Know-how-Schutz, S. 86; *Stadler,* ZZP 2010, 261 Fn. 69.