Teil 1

Das neue, europarechtlich geprägte Geschäftsgeheimnisstrafrecht

Kapitel 1

Einleitung – Bedeutung des strafrechtlichen Geschäftsgeheimnisschutzes

Das Inkrafttreten des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) am 26. 04. 2019[1] mit seinem nunmehr umfassend ausgestalteten Regelungskonzept, sowohl in materiell-rechtlicher als auch prozessrechtlicher Art und Weise, bietet den Anlass, auch den strafrechtlichen Schutz von Geschäftsgeheimnissen einmal genauer unter die Lupe zu nehmen. Nachdem nämlich das frühere Geschäftsgeheimnisstrafrecht, schwerpunktmäßig verortet in den §§ 17 – 19 UWG, über das Eingangstor des § 823 Abs. 2 BGB auf Grund der primär strafrechtlichen Ausgestaltung auch im Zivilrecht von großer Bedeutung war, ist zu befürchten, dass dem nun zivilrechtsakzessorischen Strafrecht[2] in Zukunft ein gewisses Schattendasein droht.

Umso mehr gilt es festzustellen, ob das Strafrecht durch die Umsetzung der Richtlinie 2016/943 des Europäischen Parlaments und des Rates vom 08. 06. 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, kurz Geschäftsgeheimnis-RL, Neuerungen erfahren hat. Dabei wird zu ermitteln sein, ob sich aus der zivilrechtsakzessorischen Ausgestaltung systematische Spannungen ergeben, bestehende Probleme gelöst beziehungsweise neue Baustellen eröffnet wurden. Mithin ist also zu klären, ob es sich beim neuen Geschäftsgeheimnisstrafrecht um ein gelungenes materiell-rechtliches Regelungskonzept handelt. Dazu sind Umfang und Grenzen des Geschäftsgeheim-

---

[1] Beim 26.04. handelt es sich um den Welttag des Geistigen Eigentums. Auch wenn dieser Tag womöglich recht gezielt gewählt wurde, wird diesem Umstand jedoch keine eigenständige Bedeutung zugemessen werden können, mithin spricht etwa *Reinfeld* von einem guten Omen, vgl. GeschGehG, Vorwort.

[2] Zur zivilrechtsakzessorischen Ausgestaltung vgl. etwa *Hohmann*, in: MüKo-StGB, § 23 GeschGehG Rn. 3; *Hiéramente*, in: BeckOK GeschGehG, § 23 Rn. 3; *Alexander*, in: Köhler/Bornkamm/Feddersen, UWG, 40. Aufl., § 23 GeschGehG Rn. 10, 19 f.

nisschutzes durch das Strafrecht in seiner Gesamtheit – über den Tellerrand des GeschGehG hinaus – auf den Prüfstand zu stellen. Nachdem der Gesetzgebungsvorgang als *„Sternstunde des Parlaments"*[3] bezeichnet wurde, liegt die Messlatte hierfür jedenfalls sehr hoch.

Abseits des Zivilrechts ist die enorme praktische Bedeutung des Schutzes von Geschäftsgeheimnissen durch das Strafrecht nicht von der Hand zu weisen. Denn gerade beim Verlust besonders werthaltiger Geschäftsgeheimnisse besteht die Gefahr, dass etwaige Schadensersatzansprüche mangels ausreichender Solvenz des Schuldners weder im Vorfeld noch im Nachhinein abschreckende Wirkung entfalten können.[4] Um dies zu unterstreichen, genügt es, einige der diesbezüglichen Schätzungen zu Rate zu ziehen. So geht etwa der Verein Deutscher Ingenieure (VDI) davon aus, dass durch Wirtschaftsspionage jährlich Schäden in Höhe von 100 Milliarden Euro entstehen.[5] Der Bundesverband der Deutschen Industrie (BDI) schätzt die Schadenssumme unter Einschluss von Datendiebstahl, Industriespionage und sonstiger Sabotage vergleichbar ein.[6] Andere Quellen gehen immerhin von Schadenssummen im Bereich von 50 Milliarden Euro aus.[7] Mithin richten sich diese Angriffe unternehmensübergreifend gegen ganze Bereiche der Wirtschaft, wie etwa die stark technisch geprägte Automobilindustrie, Maschinenbau- und Kommunikationsunternehmen, die Informationstechnik-, Biotechnologie- und Finanzbranche, aber auch – obgleich vielleicht weniger naheliegend – Kosmetikproduktehersteller.[8] Sie sind zudem nicht nur für das individuell betroffene Unternehmen von enormer Bedeutung, sondern können ein Risiko für die gesamte volkswirtschaftliche Entwicklung darstellen.[9]

---

[3] So etwa die Berichterstatterin *Nina Scheer* in der Sitzung des Bundestages vom 21.03.2019, vgl. Plenarprotokoll 19/89, 10655.

[4] Statt vieler *Nastelski*, GRUR 1957, 1, 2; *Harte-Bavendamm*, in: FS Köhler, S. 235, 236; *Föbus*, Insuffizienz des Geheimnisschutzes, S. 34; krit. hingegen *Aplin*, IPQ 2014, 257, 274.

[5] http://www.faz.net/aktuell/wirtschaft/wirtschaftspionage-ingenieursverband-100-milliarden-euro-schaden-12782369.html (zuletzt abgerufen am 27.10.2020).

[6] https://bdi.eu/artikel/news/wirtschaftsspionage-kriminalitaet-und-sabotage-die-unterschaetzte-gefahr/ (zuletzt abgerufen am 27.10.2020).

[7] *Föbus*, Insuffizienz des Geheimnisschutzes, S. 24 f. m. w. N.; *Bott*, in: FS Wessing, S. 311, 312 m. w. N.

[8] Dazu etwa *Wilke*, NZWiSt 2019, 168; *Bundesamt für Verfassungsschutz* Wirtschaftsspionage – Risiko für Unternehmen, Wissenschaft und Forschung, 2014, 6; *Drescher*, Industrie- und Wirtschaftsspionage, S. 79 ff.; zutreffend formuliert auch *Brammsen „Wird schließlich das sich neben den klassischen ‚Einsatzfeldern' Anlagen- und Betonbau, Auto-, Chemie-, Metall-, Pharma- und Rüstungsindustrie, Materialtechnik usw. immer mehr auf die Beschichtungs-, Bio-, Solar-, Windtechnologie, der Energiesektor, die Finanzbranche, die Computer- und Telekommunikationsindustrie, die Medizin-, Steuerungs- und Umwelttechnik, selbst die Fahrradproduktion einbeziehende ‚Spionagespektrum' einberechnet, bleibt nur die Schlussfolgerung: Geheimnisverrat und Wirtschaftsspionage haben weltweit längst beängstigend stabile und expansive Hochkonjunktur"*, vgl. Lauterkeitsstrafrecht, Vor § 17–19 Rn. 8.

[9] So bereits etwa *Schafheutle*, Wirtschaftsspionage, S. 2 und *Tuffner*, Wirtschaftsgeheimnisse, S. 2 f., 106.

All dies vorangestellt, wird im Rahmen dieser Untersuchung festzustellen sein, ob das GeschGehG in strafrechtlicher Hinsicht hinreichende materiell-rechtliche Mittel zur Verfügung stellt, um den – auch unter Zuhilfenahme der Literatur – herausgearbeiteten Risikoquellen für den Geheimnisschutz zu begegnen.[10] Dabei sind vor allem auch die aus dem zunehmenden Einsatz von Informationstechnologie erwachsenden Angriffsmöglichkeiten zu bedenken.[11] Es spielen nicht nur der Einsatz von Schadsoftware, sondern auch die Nutzung privater *Hardware* im betrieblichen Umfeld, etwa im *Home Office*, eine Rolle.[12] Zusätzlich stellen aus dem Transfer von Technologie erwachsende Risiken eine immer größere Herausforderung dar, welche jedoch im Hinblick auf die bezweckte Innovationsförderung praktisch unumgänglich erscheinen.[13]

Andererseits sind dem notwendigen strafrechtlichen Schutz von Geschäftsgeheimnissen Grenzen zu setzen, allein schon aus Gründen eines Angebots und Nachfrage vermittelnden Warenverkehrs und des daraus resultierenden Wettbewerbsumfelds. Neben wirtschaftlichen Erwägungen sind auch andere, für das gesellschaftliche Zusammenwirken unerlässliche Ausnahmen zu berücksichtigen. Besonders in dieser Hinsicht wurden bereits vielfach Bedenken wegen des neuen Gesetzes geäußert, deren Erörterung an geeigneter Stelle erfolgen wird.[14] Dabei gilt es vor allem auf die Arbeit von (investigativen) Journalisten als sogenannte „vierte Gewalt“ im Staat oder das Wirken von *Whistleblowern*, etwa im Bereich der Wirtschaftskriminalität, hinzuweisen. Gerade diese Form der Kriminalität – welche oft mit erheblichen Schäden für Rechtsgüter der Allgemeinheit einhergeht – kann häufig erst durch Hinweise Privater effektiv verfolgt werden.[15]

Um die aufgeworfenen Fragestellungen zu beantworten, ist zunächst einmal ein kursorischer Überblick über die Gesetzgebungshistorie des GeschGehG angezeigt, um sich dann dem Regelungskonzept in seinen materiell-rechtlichen Facetten zu nähern. Dafür ist die Auseinandersetzung mit dem nationalen Zivilrecht, aber auch dem europäischen Recht unerlässlich. Der sich anschließenden Untersuchung des tatbestandlichen Schutzumfangs folgt im nächsten Schritt eine Analyse der bestehenden rechtlichen Grenzen des Geschäftsgeheimnisschutzes. Abgerundet werden

---

[10] Siehe dazu etwa *Föbus*, Insuffizienz des Geheimnisschutzes, S. 27 f.; *McGuire*, GRUR 2016, 1000 ff.; *Reinfeld*, GeschGehG, § 1 Rn. 91 ff.; *Brammsen*, Lauterkeitsstrafrecht, Vor § 17 – 19 UWG Rn. 8; *Drescher*, Industrie- und Wirtschaftsspionage, S. 92 ff.

[11] Etwa *Brammsen*, Lauterkeitsstrafrecht, Vor § 17 – 19 UWG Rn. 8 m. w. N.; *Müller*, Cloud Computing, S. 26. f., 83 ff.

[12] Etwa *Brammsen*, Lauterkeitsstrafrecht, Vor § 17 – 19 UWG Rn. 8 m. w. N.

[13] Siehe dazu *Reinfeld*, GeschGehG, § 1 Rn. 94; dabei ist vom sogenannten *Knowledge-Protection-Sharing-Dilemma* die Rede, vgl. *Nienaber*, Geschäftsgeheimnisse, Rn. 203.

[14] So etwa bei *Alexander*, AfP 2019, 1, 3.

[15] So auch *Buchert/Buchert*, ZWH 2018, 309, 310; *Redder*, Whistleblowing, S. 183; ähnlich bei *Hopt*, der von einer wichtigen Informationsquelle spricht, vgl. ZGR 2020, 373, 381; kritisch *Hefendehl*, in: FS Amelung, S. 617, 622 f., 636, 641 f. jeweils m. w. N.