

Jonathan Drescher

Industrie- und Wirtschaftsspionage in Deutschland

Phänomenologie – materielles Recht –
prozessuale Durchsetzung:
Bestandsaufnahme und Perspektiven

LIT

Inhaltsverzeichnis

Vorwort	i
Inhaltsübersicht	iii
Abbildungsverzeichnis	xxix
Tabellenverzeichnis	xxx
Abkürzungsverzeichnis	xxxi
Einleitung	1
§ 1 Thematische Einführung	1
§ 2 Bestimmung des Untersuchungsgegenstands	6
A. Die Formen von Spionage: Begriffsbestimmungen	8
I. Wirtschaftsspionage	9
II. Industriespionage und Competitive Intelligence	10
III. Cyberspionage	12
IV. Wirtschaftssabotage	13
B. Das Zielobjekt: Know-how und Geschäftsgeheimnisse	13
I. Unterscheidung zwischen Know-how und Geschäftsgeheimnissen	14
1. (Betriebs- und) Geschäftsgeheimnisse	14
2. Know-how	15
II. Die Abgrenzung zu gewerblichen Schutzrechten	17
1. Das Ziel: Schaffung von Knappheit und Vermögenswert	18
2. Instrumente des Know-how-Schutzes	18
a) Konzeptionelle Unterschiede zwischen Geheimnisschutz und Schutzrechten	18
b) Exkurs: Entscheidungsparameter.	19
3. Gleiche Zielsetzung, unterschiedliche Ausgestaltung	21

§ 3	Gang der Untersuchung.	22
Erstes Kapitel: Die Geschichte der Wirtschafts- und Industriespionage		
§ 1	Von der Steinzeit zur Moderne	26
	A. Die Anfänge	26
	B. Die Wirtschaftsstruktur im Mittelalter	27
	I. Spionage innerhalb Europas	27
	II. Geheimnisschutz durch staatliche Vorschriften	29
	C. Die Industrialisierung und ihre Folgen	30
	D. Protektionismus in der Zeit vor dem ersten Weltkrieg.	32
§ 2	Spionage zwischen 1914 und 1945	33
§ 3	Spionage im Kalten Krieg	35
	A. Bedrohungslage im geteilten Deutschland	36
	B. Der Siegeszug elektronischer Datenverarbeitung	38
§ 4	Wirtschaftsausspähung im 21. Jahrhundert	41
	A. Know-how-Schutz im Zeitalter des Internets	42
	B. Die Globalisierung als Herausforderung für Unternehmen	43
	C. Geheimdienste auf Orientierungskurs.	45
§ 5	Die moralische Dimension von Wirtschaftsausspähung	46
Zweites Kapitel: Empirische Befunde.		
§ 1	Überblick.	50
	A. Grundsätzliche Problemstellungen und methodisches Vorgehen	50
	B. Abgrenzung von Industrie- zu Wirtschaftsspionage	52
§ 2	Umfang und Strukturen von Industrie- und Wirtschaftsspionage in Deutschland	54
	A. Hellfeldanalyse	55
	B. Systematische Analyse von Dunkelfeld-Studien	58
	I. Risikoeinschätzung deutscher Unternehmen.	63

II.	Betroffenheit deutscher Unternehmen	65
	1. Ausgangspunkt: Die Untersuchung des BKA (Stand 2014)	66
	2. Untersuchung im Längsschnitt	70
III.	Bedeutung von Unternehmensgröße und Branche	74
	1. Unternehmensgröße	74
	a) Ergebnisse der Studien	74
	b) Mittelstand im Fokus	76
	2. Sonstige Faktoren	77
	3. Gefährdete Branchen und Bereiche	79
IV.	Wirtschaftliches Schadenspotential	83
	1. Allgemeine Probleme bei der Schadensbestimmung	83
	2. Durchschnittlicher finanzieller Schaden pro Vorfall	85
	3. Umfragebasierte Hochrechnungen	87
	4. Stellungnahme	88
	a) Keine Berücksichtigung von Kleinstunternehmen	89
	b) Hochrechnung anhand der Fallzahlen der PKS	90
	C. Zwischenergebnis	91
§ 3	Methoden der Informationsbeschaffung	92
	A. Human Source Intelligence (HUMINT)	95
	I. Operativer Bereich	96
	II. Rezeptiver Bereich	98
	B. Technical Intelligence (TECHINT)	98
	I. Communication Intelligence (COMINT)	99
	1. Voraussetzungen und Grenzen der Spionage durch COMINT	101
	2. Risiken durch Auslagerung von Datenspeicherung und Dienstleistungen	102
	a) Outsourcing	102
	b) Risiken durch Cloud-Computing und Off-Premise-Diensten	102
	II. Cyberangriffe	105
	1. Bedrohungslage	106

	2. Schema eines Hacking-Angriffs	107
	3. Advanced Persistent Threats	110
	III. Risikofaktor „Smartphone“	111
	IV. IMINT und MASINT	113
	V. Grenzen der elektronischen Ausspähung	113
	C. Open Source Intelligence (OSINT)	114
	I. „Freiwillige“ Offenbarung von Know-how	115
	1. Öffentlichkeitsarbeit	115
	2. Anmeldung gewerblicher Schutzrechte.	116
	3. Sonderfall „Reverse Engineering“	116
	II. Normative Gefahrenquellen	117
	1. Gesetzliche Offenlegungspflichten gegenüber der öffentlichen Verwaltung	118
	2. Privatseitige Informationsrechte „erga omnes“	118
	3. Situationsabhängige Zugangsrechte	119
	III. „Neue“ Formen der Spionage: Intelligence Gathering	120
	D. Klassisch-kriminelle Informationsgewinnung	121
	E. Kombination der Angriffsmethoden	122
§ 4	Tatmotivation und Täterprofile	123
	A. Der Täterkreis	123
	B. Motivlage und kriminogene Strukturen	130
	I. Innentäter bzw. die „Quelle im Objekt“	130
	1. Die Motivlage von Innentätern	132
	2. Kriminogene Strukturen	134
	3. Fahrlässige Informationsweitergabe	136
	II. Spionage durch Konkurrenzunternehmen	137
	1. Industriespionage als lohnende Kriminalität für Unternehmen.	137
	a) Vorteile für das „delinquente“ Unternehmen	138
	b) Risiken und Kosten für das „delinquente“ Unternehmen.	140
	2. Industriespionage als lohnende Kriminalität für den handelnden Mitarbeiter	142
	a) Motivlage	142

b) Vorteile und Risiken für den Mitarbeiter	143
III. Tatmotivation und „Cybercrime“	144
IV. Spionage durch Nachrichtendienste: Der „Berufsspion“	145
V. Intelligence Trader	145
C. Kriminologische Erklärungsansätze	147
I. Industrie- und Wirtschaftsspionage als Teilbereich der Wirtschaftskriminalität	148
II. Corporate Deviance und Occupational Deviance	152
III. Industrie- und Wirtschaftsspionage aus der Perspektive allgemeiner Kriminalitätstheorien.	153
1. Theorie der differenziellen Kontakte	153
2. Anomietheorie	154
3. Subkulturtheorie	155
4. Kontroll- und Kontrollbalancetheorie	157
5. Routine-activity-Ansatz	158
6. Neutralisationstechniken	159
IV. Spezifische Erklärungsansätze für Wirtschaftskriminalität	160
1. Kriminalitätsökonomik.	162
2. Leipziger Verlaufsmo­dell wirtschaftskriminellen Handelns.	164
V. Fazit.	166
§ 5 Bedrohung durch nachrichtendienstliche Spionage	167
A. Untersuchung des Geheimen, oder: die Suche nach dem Leak	168
B. NSA und die UKUSA: Spionage durch westliche Dienste	169
I. Die UKUSA-Vereinbarung	170
II. Struktur und Kapazitäten der Nachrichtendienste	171
III. Methoden zur systematischen Überwachung des Fernmeldeverkehrs	173
1. Anzapfen von Glasfaserkabeln.	174
2. Kooperationen mit ausländischen Nachrichtendiensten	175

3.	Zugriff auf die Server großer Internetkonzerne (PRISM)	176
4.	Datensammlung und Auswertung: XKeyScore	178
IV.	Ziele und Grenzen der systematischen Überwachung	180
V.	Tailored Access Operations	181
1.	Die Programme „Quantumtheory“ und „Regin“	182
2.	Installation von Backdoor-Programmen	183
VI.	Zielsetzung und Profiteure der Spionage.	184
1.	Aufklärungsziel BRD: Ausspähung der Wirtschaft?	184
2.	Stärkung der nationalen Wirtschaftskraft	187
a)	Stellungnahme der US-Regierung	187
b)	Risikoeinschätzung	188
3.	Die „Kunden“ der NSA	191
a)	Nutzung zu (wirtschafts-) politischen Zwecken	191
b)	Konsequenzen und Nachteile für die ausgespähten Unternehmen durch Strafverfahren und Sanktionen	193
VII.	Zusammenfassung: Bedrohungslage für die deutsche Wirtschaft	194
C.	Aggressoren aus dem Osten: Spionage „feindlicher“ Nachrichtendienste	195
I.	Volksrepublik China.	196
1.	Volkswirtschaftlicher und soziokultureller Hintergrund	197
2.	Einbindung der Geheimdienste in die Modernisierung der Wirtschaft	198
a)	Nachrichtendienste	198
b)	China und die Cyberspionage	198
II.	Die russische Föderation	201
1.	Nachrichtendienste.	201
2.	Ziele und Methoden	202
III.	Gefährdungslage aus Sicht deutscher Unternehmen	202
D.	Fallzahlen.	203

E.	Die Rolle des deutschen Staates	204
I.	Ausstattung und Kapazitäten deutscher Geheimdienste	204
II.	Deutsche Spionage im Ausland	206
§ 6	Der Status quo der Bekämpfung von Wirtschaftsausspähung	207
A.	Verhinderung von Know-how-Abflüssen im Unternehmen	208
I.	Strukturelle und organisatorische Maßnahmen	211
II.	Personelle Maßnahmen	214
1.	Verhinderung von vorsätzlichen Know-how-Abflüssen	216
2.	Maßnahmen zur Schulung und Sensibilisierung	218
III.	Objektschutzvorkehrungen	220
IV.	IT-Sicherheitsmaßnahmen.	221
1.	Firewall, Virens Scanner und Passwortschutz als Standardmaßnahme	221
2.	Weitergehende Schutzmaßnahmen	222
3.	Mitarbeitersensibilisierung für Gefahren aus dem Cyberraum	224
4.	„Cyber Deception“: Der nächste Schritt der Spionageabwehr?	225
V.	Sicherheit im privaten Umfeld und auf Auslandsreisen	227
VI.	Überprüfung und Monitoring	228
VII.	Selbsteinschätzung der unternehmensinternen Schutzvorkehrungen	230
B.	Reaktion auf Ausforschungsangriffe in den Unternehmen	231
I.	Entdeckung von Spionageangriffen	232
II.	Operative Aufklärung: Innerbetriebliche Maßnahmen gehen vor	234
III.	Zusammenarbeit der Unternehmen mit Sicherheitsbehörden	236
1.	Angst vor Reputationsverlust.	237
2.	Vermeidung sonstiger negativer Folgen	238
3.	Notwendigkeit einer stärkeren Zusammenarbeit	239
IV.	Auswirkungen eines Spionagevorfalls auf künftige Prävention.	242

C. Unterhaltung geeigneter Compliance-Programme	243
D. Die Bekämpfung von Spionage von staatlicher Seite	244
I. Präventive Maßnahmen	245
1. Angebote der Aufklärung und Hilfestellung	245
2. Schutz gegen nachrichtendienstliche Überwachung des Fernmeldeverkehrs.	246
3. Normierung einzuhaltender Sicherheitsstandards.	247
II. Strafverfolgung und Sanktionierung.	247
1. Schwierigkeiten bei der Täterermittlung	249
2. Höhe der verhängten Sanktionen.	250

Drittes Kapitel: Dogmatische Grundlagen des gesetzlichen Know-how-Schutzes 251

§ 1 Innere Rechtfertigung eines gesetzlichen Schutzes von geheimem Know-how	253
A. Wirtschaftlicher Wert als Rechtfertigung	254
B. Vertrags- und Vertrauensschutz	255
C. Immaterialgüterrechtlicher Ansatz	256
I. Naturrechtlicher Begründungsansatz	257
II. Anreizfunktion zu Innovationstätigkeit	258
1. Notwendigkeit von Amortisierungsmöglichkeiten	259
2. Gesamtwirtschaftliche Nachteile der Geheimhaltung.	261
D. Ökonomische Überlegungen als Rechtfertigungsgründe	261
I. Theorie der Kostenreduktion	262
II. Effizientere Übertragung von Know-how / Innovationsförderung	263
III. Notwendigkeit einer geschützten Innensphäre.	264
§ 2 Ausgestaltung des rechtlichen Geheimnisschutzes	265
A. Internationale Vorgaben für rechtlichen Geheimnisschutz.	265
I. Völkerrechtliche Übereinkommen.	265
II. Europarechtliche Vorgaben	266
B. Ausschließlichs- vs. Zugangsschutz.	268
C. Notwendigkeit strafrechtlicher Sanktionierung	270

§ 3 Die Rechtsnatur geheimen Know-hows.	272
A. Know-how-Schutz als Teilbereich des geistigen Eigentums?	273
B. Verfassungsrechtliche Anknüpfungspunkte	275
I. Art. 14 Abs. 1 GG (Eigentumsfreiheit)	276
II. Art. 12 Abs. 1 GG (Berufsfreiheit)	278
§ 4 Schutzgut „Integrität elektronischer Daten und Systeme“.	279
Viertes Kapitel: Rechtliche Folgen für Tatbeteiligte	281
§ 1 Übersicht	281
A. Rechtslage vor Inkrafttreten des GeschGehG	281
B. Die Reform des gesetzlichen Geheimnisschutzes 2019	282
C. Sonstige Strafvorschriften mit Geheimnisbezug im Überblick	283
D. Hinweise zum methodischen Vorgehen und dem Aufbau des Kapitels.	284
§ 2 Strafrechtliche Konsequenzen	284
A. Strafrechtliche Erfassung der Konkurrenzausspähung.	285
I. Strafbarkeit gem. § 23 GeschGehG	285
1. Überblick	285
2. Übergreifende Punkte	287
a) Tatobjekt: Der Begriff des Geschäftsheimnisses.	287
aa) Keine allgemeine Bekanntheit, § 2 Nr. 1 lit. a) GeschGehG	288
bb) Vermögenswert der Information, § 2 Nr. 1 lit. a) GeschGehG	290
cc) Angemessene Geheimhaltungsmaßnahmen, § 2 Nr. 1 lit. b) GeschGehG.	294
dd) Berechtigtes Geheimhaltungsinteresse, § 2 Nr. 1 lit. c) GeschGehG	296
ee) Keine Voraussetzung: Geheimhaltungswille	298

b) Geschädigter: Inhaber des Geschäftsgeheimnisses, § 2 Nr. 2 GeschGehG	299
c) Subjektiver Tatbestand	301
3. Tatbestand des Geheimnisverrats, § 23 Abs. 1 Nr. 3 GeschGehG	302
a) Täterkreis	303
b) Tatgegenstand	304
c) Tathandlung	305
d) Schutzlücken des § 23 Abs. 1 Nr. 3 GeschGehG	306
aa) Nachvertragliche Mitteilungen	306
bb) Eigene Verwertung durch den Beschäftigten	307
4. Tatbestand der Betriebsspionage, § 23 Abs. 1 Nr. 1 GeschGehG	308
a) Tathandlung	308
b) Keine Beschränkung auf bestimmte Tatmittel	310
c) Unbefugt	312
5. Tatbestand der Geheimnishehlerei, § 23 Abs. 1 Nr. 2 und Abs. 2 GeschGehG.	313
a) Tathandlung	314
b) Geheimnishehlerei infolge drittseitig vermittelter Erlangung des Geheimnisses	315
aa) Vorsätzliche, rechtswidrige Vortat	315
bb) Subjektiver Tatbestand	316
c) Eigene Erlangung des Geheimnisses als Vortat.	317
aa) Eigene, eigengesteuerte Betriebsspionage als Vortat	317
bb) Keine vorsätzliche Vortat erforderlich	318
d) Grenzen des Schutzes nach § 23 Abs. 1 Nr. 2, Abs. 2 GeschGehG.	318
aa) Gutgläubigkeit und grobe Fahrlässigkeit nicht ausreichend	319
bb) Verstoß gegen § 23 Abs. 3 GeschGehG keine taugliche Vortat	319

cc) Schutzlücken in der nacharbeitsvertraglichen Phase	319
6. Tatbestand der Verwertung von Vorlagen, § 23 Abs. 3 GeschGehG	321
a) Täterkreis	322
b) Tathandlung	323
c) Tatobjekt	323
aa) Vorlagen oder Vorschriften technischer Art	324
bb) Anvertraut im geschäftlichen Verkehr	325
d) Subjektiver Tatbestand	325
e) Schutzlücken	326
7. Tatbestandsausnahmen, § 5 GeschGehG	326
8. Rechtswidrigkeit	330
9. Strafbarkeit von Vorbereitungs- und Versuchshandlungen	331
10. Strafrahmen und Qualifikationen, § 23 Abs. 4 GeschGehG	332
11. Verhältnis der Tatbestände zueinander	333
II. Geheimnisschützende Straftatbestände mit besonderen Anforderungen an das Täterprofil	334
1. Strukturelle Gemeinsamkeiten	334
a) Täterkreis	334
b) Tatgegenstand	335
c) Tathandlung	336
2. Verrat durch Organe juristischer Personen	337
3. Wirtschafts- und Abschlussprüfer	339
4. Regelungen im kollektiven Arbeitsrecht	340
5. Schutz von Berufs- und Amtsgeheimnissen	340
III. Sonstige relevante Straftatbestände ohne Geheimnisbezug	341
1. Diebstahl und Unterschlagung, §§ 242, 246 StGB	341
2. Vermögensschützende Straftatbestände	342
a) Anforderungen an die Tathandlung	342
b) Das Unmittelbarkeitserfordernis	344

c)	Eintritt einer schadensgleichen Vermögensgefährdung?	345
3.	Bestechung und Bestechlichkeit („Korruption“)	347
a)	Bestechung und Bestechlichkeit im Geschäftsverkehr, § 299 StGB	347
aa)	Wettbewerbsbezogene Bestechlichkeit, Abs. 1 Nr. 1	347
bb)	Geschäftsherrenmodell, Abs. 1 Nr. 2.	349
cc)	Ausschreibungsverfahren	350
b)	Bestechung und Bestechlichkeit im Amt, §§ 331 ff. StGB	351
4.	Hausfriedensbruch, § 123 StGB	351
IV.	Zwischenfazit	352
B.	Strafrechtliche Erfassung der Cyberspionage	354
I.	Übersicht zum IuK-Strafrecht	354
1.	„Unechte“ Computerdelikte	354
2.	„Echte“ Computerdelikte.	355
II.	Der Datenbegriff	356
1.	Gespeicherte Daten	356
2.	Datenübermittlung	357
3.	Qualität der Daten	357
III.	Der „zusammengesetzte Hackingparagraph“	358
1.	Ausspähen von Daten, § 202a StGB	358
a)	Zugangssicherung	359
b)	Tathandlung: Zugangsverschaffung	360
c)	Nicht für den Täter bestimmt.	361
d)	Subjektiver Tatbestand	362
2.	Abfangen von Daten, § 202b StGB.	363
a)	Nichtöffentliche Datenübermittlung	363
b)	„Abhören“ elektromagnetischer Abstrahlung	364
c)	Tathandlung und Subsidiarität	364
3.	Vorbereiten des Ausspähens und Abfangens von Daten, § 202c StGB	365
a)	Tatgegenstände.	365
b)	Tathandlung und subjektiver Tatbestand	367

4. Datenhehlerei, § 202d StGB	367
IV. Computerbezogene Sabotageakte	368
1. Datenveränderung, § 303a StGB	368
2. Computersabotage, § 303b StGB.	369
a) Tathandlung	369
b) Qualifikation	370
3. Versuch und Vorbereitungsstrafbarkeit	371
V. Sonstige Delikte im Zusammenhang mit Cyberspionage	371
1. Abhören von Kommunikationsvorgängen	371
2. Verstöße gegen das Datenschutzrecht, § 42 BDSG	372
3. Computerbetrug, § 263a StGB	373
VI. Zwischenfazit	374
C. Strafrechtliche Erfassung der Wirtschaftsspionage	374
I. Völkerrechtlicher Rahmen.	374
1. Die offizielle Nachrichtenbeschaffung	375
2. Informationsbeschaffung durch Nachrichtendienste	376
3. Besonderheiten des Diplomatenrechts	377
II. Vorschriften zum Schutz von Staatsgeheimnissen	378
1. Der Begriff des Staatsgeheimnisses, § 93 StGB	378
2. Weitere Tatbestandsvoraussetzungen der §§ 94 ff. StGB.	381
a) Landesverrat und landesverräterische Ausspähung, §§ 94, 96 StGB.	381
b) Landesverräterische Agententätigkeit, § 98 StGB.	382
3. Sondertatbestände	383
III. Nachrichtendienstliche Agententätigkeit, § 99 StGB.	383
1. Hintergrund und Entstehungsgeschichte	384
2. Objektiver Tatbestand	385
a) Geheimdienst einer fremden Macht	386
b) Tatobjekt	387
c) Ziel- und Zweckrichtung der Handlung	388
d) Ausüben bzw. Bereiterklären zu geheimdienstlicher Tätigkeit	389

e)	Erheblichkeitsschranke: Gegen die Bundesrepublik Deutschland	391
aa)	Wirtschaftsspionage zu (wirtschafts-)politischen Zwecken.	391
bb)	Wirtschaftsspionage zur Unterstützung heimischer Unternehmen	391
3.	Subjektiver Tatbestand und Rechtfertigungsgründe	393
IV.	Abhören von Kommunikationsvorgängen nach TKG	394
V.	Strafbarkeit des Begünstigten	394
VI.	Praktische Bedeutung	395
D.	Konkurrenzen und Sanktionierung	397
I.	„Übersetzung“ der Phänomenbereiche in Straftatbestände	397
II.	Konkurrenzen	398
1.	Abgrenzung von Gesetzeseinheit zu Idealkonkurrenz	399
a)	Das Verhältnis von § 23 GeschGehG zu § 99 StGB.	401
b)	Das Verhältnis von § 23 Abs. 1 Nr. 1 GeschGehG zu § 202a Abs. 1 StGB	401
2.	Realkonkurrenz (Tatmehrheit), § 53 StGB	403
a)	Wirtschaftsausspähung als Handlungseinheit oder -mehrheit	404
aa)	Enger räumlicher und zeitlicher Zusammenhang	404
bb)	Handlungsmehrheit bei unterbrochenem Geschehensablauf	405
cc)	Mitbestrafte Vor- oder Nachtat	406
b)	Die „Klammerwirkung“ des § 99 StGB	407
aa)	Voraussetzungen der „Verklammerung“	407
bb)	Die tatbestandliche Handlungseinheit bei § 99 StGB	408
III.	Vergleich der gesetzlichen Strafraumen	409
1.	Auslandsverwertung	411

2. Vergleichende Betrachtung mit den vermögensschützenden Straftatbeständen des Kernstrafrechts	411
E. Anwendbarkeit deutschen Strafrechts	413
F. Der strafrechtliche Schutz vor Spionage in der Gesamtschau .	414
I. Die Strafbarkeit im Vorbereitungsstadium	415
II. Fazit	417
§ 3 Strafrechtliche Nebenfolgen und außerstrafrechtliche Konsequenzen	418
A. Arbeitsrechtliche Folgen	419
B. Disziplinarrechtliche Folgen	420
C. Tätigkeits- und Berufsverbote	421
I. Tätigkeitsverbote gem. §§ 6 Abs. 2 GmbHG, 76 Abs. 3 S. 3 AktG	421
II. Berufsverbot gem. § 70 StGB	421
1. Voraussetzungen des Berufsverbots	422
2. Keine berufsspezifische Pflichtverletzung	423
§ 4 Zivilrechtliche Folgen	424
A. Zivilrechtlicher Geheimnisschutz vor Inkrafttreten des GeschGehG.	425
I. Ansprüche gegen Arbeitnehmer und Geschäftspartner. .	426
II. Ansprüche außerhalb vertraglicher Sonderbeziehungen .	427
1. Ansprüche im wettbewerblichen Kontext, §§ 8, 9 UWG	427
a) Wettbewerbsverhältnis	428
b) Lauterkeitsrechtliche Generalklausel, § 3 Abs. 1 UWG	429
aa) Geschäftliche Handlung	429
bb) Bestimmung unlauteren Handelns: Die Doppelfunktion des § 3 UWG	430
c) Rechtsbruchtatbestand, § 3a UWG	430
d) „Ergänzungsfunktion“	431
aa) Gezielte Behinderung und Produktnachahmung, § 4 UWG	431

bb)	Ausfüllen strafrechtlicher Schutzlücken . . .	432
2.	Ansprüche gegen jedermann	432
a)	Strafrechtsakzessorischer Ersatzanspruch: § 823 Abs. 2 BGB i.V.m. Schutzgesetzen	433
b)	Vorsätzliche, sittenwidrige Schädigung, § 826 BGB	434
3.	Rechtsfolgen einer Geheimnisverletzung	435
a)	Inhalt und Umfang der Schadensersatzansprüche	436
4.	Unterlassung und Beseitigung	436
III.	Gesamtbild und Schutzlücken des zivilrechtlichen Geheimnisschutzes vor der Reform	438
IV.	Exkurs: Anwendbarkeit zivilrechtsautonomer Ansprüche?	439
1.	Problemaufriss	440
2.	Diskussionsstand in Rechtsprechung und Literatur	442
3.	Verdichtung zu einer Position mit Zuweisungsgehalt?	444
4.	Wirtschaftsgeheimnisse als Ausprägung des Rechts am Gewerbebetrieb	446
5.	Bedeutung der Normen in der Praxis	447
B.	Rechtsslage nach Inkrafttreten des GeschGehG	450
I.	Erlaubte Verhaltensweisen und Handlungsverbote	450
1.	Erlaubte Handlungen, § 3 GeschGehG	450
2.	Handlungsverbote, § 4 GeschGehG	452
a)	Unbefugte Erlangung, § 4 Abs. 1 GeschGehG	453
b)	Unbefugte Nutzung oder Offenlegung, § 4 Abs. 2 GeschGehG	455
aa)	Geheimhaltung als vertragliche Nebenpflicht kraft Gesetzes	456
bb)	Umfang der Geheimhaltungspflicht nach § 241 Abs. 2 BGB	456
cc)	Zeitlicher Geltungsbereich der Schutzpflichten	457

dd) Ausdrückliche Geheimhaltungsvereinbarungen	461
c) Von Dritten erlangte Geheimnisse, § 4 Abs. 3 S. 1 GeschGehG	462
d) Mittelbare Geheimnisverletzungen, § 4 Abs. 3 S. 2 GeschGehG	464
3. Ausnahmen, § 5 GeschGehG.	466
II. Das Rechtsfolgenregime des GeschGehG	466
1. Unterlassungsanspruch, § 6 Alt. 2 GeschGehG.	466
a) Umfang und Grenzen des Unterlassungsanspruchs	467
b) Erstbegehungs- oder Wiederholungsfahr.	468
2. Beseitigungsanspruch, § 6 Alt. 1 GeschGehG	470
3. Anspruch auf Vernichtung, Herausgabe, Rückruf, Entfernung und Rücknahme vom Markt, § 7 GeschGehG	471
4. Auskunftsanspruch, § 8 GeschGehG	472
5. Korrektiv: Verhältnismäßigkeitsvorbehalt und Abfindung in Geld	472
a) Die Abwägungsgesichtspunkte.	473
aa) Das Verhalten des Rechtsverletzers (Nr. 3).	473
bb) Die getroffenen Geheimhaltungsmaßnahmen (Nr. 2).	474
cc) Die Auswirkungen bei Erfüllung der Ansprüche (Nr. 5)	475
dd) Sonstige Abwägungsgesichtspunkte.	475
b) Rechtsfolge der Unverhältnismäßigkeit	476
c) Abfindung in Geld, § 11 GeschGehG.	477
d) Verhältnis von § 9 zu § 11 GeschGehG.	478
6. Schadensersatzanspruch, § 10 GeschGehG.	479
a) Ersatz des tatsächlich eingetretenen Schadens, § 10 Abs. 1 GeschGehG	480

b)	Dreifache Schadensberechnung, § 10 Abs. 2 GeschGehG	480
aa)	Berechnung nach fiktiven Lizenzgebühren (Lizenzanalogie)	481
bb)	Herausgabe des Verletzergewinns	482
cc)	Das Verhältnis der drei Berechnungsarten zueinander.	484
c)	Ersatz von Nichtvermögensschäden, § 10 Abs. 3 GeschGehG	484
d)	Kein Verhältnismäßigkeitsvorbehalt	485
7.	Missbrauchsverbot, § 14 GeschGehG	485
III.	Ansprüche innerhalb vertraglicher Sonderverbindungen.	486
1.	Anspruchsvoraussetzungen.	487
2.	Umfang des Schadensersatzes	487
3.	Bedeutung vertraglicher Ansprüche unter Geltung des GeschGehG	488
IV.	Weitere Ansprüche nach dem BGB	489
1.	Strafrechtsakzessorische Ansprüche, § 823 Abs. 2 BGB	490
2.	Zivilrechtsautonome Ansprüche	491
V.	Anspruchsgrundlagen im „Umfeld“ von Wirtschaftsausspähung	492
1.	Gezielte Behinderung, § 4 Nr. 4 UWG	493
2.	Unlautere Produktnachahmung, § 4 Nr. 3 lit. c) UWG	494
3.	Verleitung zum Vertragsbruch	495
VI.	Urheberrechtliche Ansprüche, § 97 UrhG	497
VII.	Verjährung	497
C.	Anwendbarkeit deutschen Zivilrechts.	498
D.	Gesamtbild zivilrechtlicher Ansprüche	499
	Fünftes Kapitel: Unternehmens- und Staatshaftung	501
§ 1	Rechtliche Konsequenzen im „delinquenten Unternehmen“	501
A.	Überblick	502

B. Verantwortung. auf Führungsebene	504
I. Aktive Beteiligung an oder positive Kenntnis von der Geheimnisverletzung	504
II. Verletzung von Aufsichtspflichtverletzungen	507
1. Verhängung einer Geldbuße gem. § 130 OWiG.	507
2. Zivilrechtliche Haftung wegen Verstößen gegen § 831 BGB sowie aufgrund von Organisationsmängeln	508
3. Anforderungen an eine ordnungsgemäße Aufsicht	509
a) Einzelfallorientiertes Vorgehen der Rechtsprechung	510
b) Versuch einer Systematisierung in der Literatur	510
c) Rückgriff auf Compliance-Richtlinien	512
C. Verantwortung des „delinquenten Unternehmens“	515
I. Straf- und ordnungswidrigkeitenrechtliche Folgen.	515
1. Geldbuße, § 30 OWiG	515
2. Einziehung von Taterträgen, §§ 73 ff. StGB und § 29a OWiG	517
a) Adressatenkreis	518
b) Umfang der Abschöpfung: Die Wertberechnung	518
aa) Das Kriterium der Unmittelbarkeit	519
bb) Das Brutto-Prinzip	521
c) Kein Ausschluss der Einziehung wegen Ansprüchen des Verletzten	522
3. Grenzen der Ahndbarkeit: Notwendigkeit eines echten Unternehmensstrafrechts?	523
II. Zivilrechtliche Haftung	526
1. Zurechnung analog § 31 BGB	527
2. Haftung gem. § 831 Abs. 1 BGB	527
3. Haftung für Organisationsmängel gem. §§ 823 Abs. 1 BGB und 9 UWG i.V.m. § 31 BGB	528
4. Umfang des Schadensersatzes	530
D. Faktische Folgen	531

§ 2	Folgen für das geschädigte Unternehmen	532
A.	Ansprüche des geschädigten Unternehmens	532
I.	Ansprüche gegen Lieferanten und Sicherheitsdienstleister	533
II.	Ansprüche gegen eigene Arbeitnehmer	534
III.	Ansprüche gegen die Geschäftsführung	535
1.	Verstoß gegen gesetzliche Vorschriften.	535
2.	Verstoß gegen allgemeine Pflichten zur Risikovorsorge	536
B.	Haftung des geschädigten Unternehmens gegenüber Dritten	537
§ 3	Zurechenbarkeit der Spionage fremder Nachrichtendienste zum deutschen Staat	538
A.	Schutzpflichten bei Kenntnis konkret geplanter Operationen	538
B.	Generelle Schutzpflichten zur Abwehr von Spionageangriffen	540
I.	Schutzauftrag aufgrund des „status positivus“	540
II.	Begrenzungen der Schutzpflicht	541
Sechstes Kapitel: Prozessrechtliche Behandlung von Wirtschafts- und Industriespionage		543
§ 1	Zivilprozessuale Anspruchsdurchsetzung	544
A.	Verteilung der Darlegungs- und Beweislast	544
B.	Der Nachweis der Spionagehandlung	545
I.	Beweisnot im Geheimnisverletzungsverfahren	545
II.	Die vorprozessuale Informationsbeschaffung	547
1.	Auskunftspflichten des Anspruchsgegners	548
a)	Akzessorischer Auskunftsanspruch	549
b)	Anspruch auf Drittauskunft	552
c)	Praktische Bedeutung der Auskunftsansprüche.	552
2.	Besichtigungsanspruch gem. § 809 Alt. 2 BGB	553
a)	Anwendungsbereich und Voraussetzungen	554
b)	Die Geeignetheit des Besichtigungsanspruchs im Spionagekontext	555
c)	Grenzen des Besichtigungsanspruchs	557

3.	Die vorprozessuale Informationsbeschaffung nach dem Düsseldorfer Modell	559
a)	Hintergrund des Verfahrens: Die Unzulänglichkeit bestehender Möglichkeiten zur Beweisbeschaffung.	560
b)	Regelungsinhalt und Ablauf	561
aa)	Erste Stufe: Anordnung und Durchführung der Besichtigung	562
bb)	Zweite Stufe: Herausgabe des Gutachtens	563
c)	Die Grenzen des Verfahrens bei Spionage	564
III.	Mitwirkungspflichten des Anspruchsschuldners im Prozess	565
1.	Prozessuale Anträge auf Beweismittelvorlage	565
2.	Die Grundsätze der sekundären Darlegungslast	566
3.	Vorlageanordnungen von Amts wegen, §§ 142, 144 ZPO	567
4.	Rechtsfolge einer unberechtigten Verweigerung	569
IV.	Zwischenfazit	569
V.	Beweismittelbeschaffung ohne Mitwirkung des Anspruchsgegners	570
1.	Einsichtnahme in strafrechtliche Ermittlungsakten, § 406e StPO	570
2.	Zeugenbeweis und der Zeuge vom Hörensagen	572
a)	Die Problematik des Zeugenbeweises im Geheimnisverletzungsprozess	572
b)	Zulässigkeit des „Zeugen vom Hörensagen“	573
c)	Praktische Umsetzung	574
VI.	Beweisbeschaffung im Ausland	575
VII.	Beweisverwertungsverbote	576
VIII.	Indizienbeweise	577
1.	Beim Beklagten aufgefundene Geschäftsgeheimnisse des Klägers	577
2.	Verwertungshandlungen ohne aufgefundene Aufzeichnungen	578
3.	Indizien für eine drohende Geheimnisverletzung	578

IX. Fazit	578
C. Geheimnisschutz des Geschädigten im Zivilprozess	580
I. Problemaufriss	580
1. Geheimnisse als Fremdkörper im Erkenntnisverfahren	581
2. Abgrenzung zum Düsseldorfer Verfahren	581
II. Geheimnisschutz der beweisbelasteten Partei	582
1. Schutz gegenüber der Öffentlichkeit	582
a) Öffentlichkeitsgrundsatz und Dispositionsmaxime	582
b) Ausschluss der Öffentlichkeit, § 172 Nr. 2 GVG und § 19 GeschGehG	583
2. Geheimhaltung dem Prozessgegner gegenüber	585
a) Rechtslage vor Inkrafttreten des GeschGehG.	585
b) Ausweitung der Verschwiegenheitspflichten durch § 16 GeschGehG.	587
c) De lege ferenda: Notwendigkeit eines „in-camera-Verfahrens“?	588
III. Fazit	590
D. Gerichtliche Zuständigkeit	591
E. Streitwertbegünstigung	592
§ 2 Strafprozessuale Problemstellungen	593
A. Formelle Voraussetzungen der Strafverfolgung	594
I. Das Strafantragserfordernis	594
1. Antragsberechtigung	594
2. Strafverfolgung von Amts wegen	595
3. Entscheidung über die Erhebung der öffentlichen Klage	596
II. Problemstellungen bei Taten mit Auslandsbezug	598
1. Aufklärungshindernisse bei elektronischen Angriffen	599
2. Eingeschränkte Befugnisse der Staatsanwaltschaft	600
3. Opportunitätserwägungen bei der Strafverfolgung	600

4. Staatsschutz- vs. Wirtschaftsstrafverfahren: Die Zuständigkeitsverteilung zwischen Bund und Ländern	601
B. Stellung und Rechte des Verletzten im Strafprozess.	603
I. Akteneinsichtsrecht des Verletzten, § 406e StPO	603
1. Anforderungen an das berechnete Interesse.	605
2. Versagungsgründe gem. § 406e Abs. 2 StPO	605
II. Die Stellung als Privatkläger	608
III. Erweiterte Möglichkeiten als Nebenkläger	609
1. Die Rolle des Nebenklägers	609
2. Die Mitwirkungsrechte im Einzelnen	610
IV. Zusammenfassung.	612
C. Geheimnisschutz des Verletzten im Strafprozess	613
I. Unterschiedliche Grundkonzeption der Verfahrensarten	614
II. Risiken im Ermittlungsverfahren	615
1. Vernehmungssituationen	615
a) Geheimnissoffenbarungen durch den Vernommenen	615
b) Geheimnissoffenbarungen gegenüber dem Vernommenen	617
2. Durchsuchungen und Beschlagnahme	619
3. Einsichtnahme in die Ermittlungsakte	620
a) Akteneinsichtsrecht des Beschuldigten.	620
aa) Umfang des Akteneinsichtsrechts	621
bb) Beschränkung der Akteneinsicht des Verteidigers, § 147 Abs. 2 StPO	622
cc) Einschränkungen gem. Nr. 260b Abs. 1 RiStBV	622
dd) Einschränkungen gem. Nr. 260b Abs. 2 RiStBV	624
ee) Zwischenfazit	624
b) Akteneinsichtsrechte nicht verfahrensbeteiligter Dritter	625
aa) Berechnetes Interesse	625

bb) Versagungsgrund gem. § 475 Abs. 1 S. 2 StPO	€
III. Gefährdungslage in der Hauptverhandlung	€
1. Der Öffentlichkeitsgrundsatz im Strafverfahren	€
2. Gefahren der Offenbarung von Geheimnissen im Einzelnen	6
a) Verlesung der Anklageschrift	6
b) Aussagen des Angeklagten und von Zeugen	6
c) Erstattung von Sachverständigengutachten	6
d) Einführungen von Urkunden	6
e) Die Urteilsverkündung	6
3. Ausschluss der Öffentlichkeit, § 172 Nr. 2 GVG	6
a) Interessenabwägung	6
b) Einflussmöglichkeiten des Betroffenen.	6
IV. Der strafprozessuale Geheimnisschutz in der Gesamtschau	6
Siebentes Kapitel: Schlussbetrachtung	637
§ 1 Zusammenfassung der wesentlichen Erkenntnisse	637
A. „Orientierung“ an der Konkurrenz – ein ubiquitäres Verhalten	637
B. Status quo der empirischen Forschung in Deutschland	638
C. Unzureichende Präventionsmaßnahmen	641
D. Geringes Entdeckungs- und Verfolgungsrisiko: Das „Kardinalproblem“	642
E. Bedrohung durch Geheimdienste	644
F. Spionageschutz nach deutschem Recht	645
G. Höhe der Sanktionen und Erfassbarkeit von Unternehmen	647
H. Der Nachweis von Industrie- und Wirtschaftsspionage	649
I. Der Geheimnisschutz in Zivil- und Strafprozess	650
§ 2 Rückblick und Ausblick	652
Literaturverzeichnis	653