

# GeschGehG

## Geschäftsgeheimnisgesetz

Herausgegeben von

**Dr. Joerg Brammsen**

Privatdozent  
an der Universität Bayreuth

und

**Dr. Simon Apel**

Rechtsanwalt, Mannheim, und Lehrbeauftragter  
an der Universität Mannheim

Bearbeitet von

Dr. Simon Apel; PD Dr. Joerg Brammsen; Serpil Dilbaz, LL.B.;  
Dr. Jonathan Drescher; Dr. Julia Exner-Kuhn; Prof. Dr. Kristian Fischer;  
Dr. Steffen Henn; Dr. Christian Peter Hille; Dr. Raphael Höll;  
Dr. Arnd-Christian Kulow; Dr. André Reinhard; Dr. Moritz Schroeder;  
Dr. Julian Slawik, LL.M. (Cambridge); Dr. Ben Steinbrück, MJur  
(Oxford); Alexander Stolz, LL.M. (Dresden/Exeter); Dr. Florian Winzer

Zitervorschlag: Brammsen/Apel/*Bearbeiter*, GeschGehG

**Bibliografische Information der Deutschen Nationalbibliothek**

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.de> abrufbar.

**I S B N 9 7 8 - 3 - 8 0 0 5 - 1 6 8 0 - 3**

**dfv'** Mediengruppe

© 2022 Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft,  
Frankfurt am Main

Der Verlag im Internet: [www.ruw.de](http://www.ruw.de)

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Druckvorstufe: Lichtsatz Michael Glaese GmbH, 69502 Hemsbach

Druck und Verarbeitung: Kösel GmbH & Co. KG, 87452 Altusried-Krugzell

Printed in Germany

# Einleitung A

## Geschäftsgeheimnisschutz – Daten und Fakten

**Schrifttum:** *Ambrosch*, Großbritannien, in: Oehler (Hrsg.), Der strafrechtliche Schutz des Geschäfts- und Betriebsgeheimnisses in den Ländern der Europäischen Gemeinschaft sowie in Österreich und der Schweiz, Bd. 2, 1978, S. 129; *Amstutz*, Dateneigentum, AcP 2018, 438; *Apel/Kaulartz*, Rechtlicher Schutz von Machine Learning-Modellen, RD 2020, 24; *Bakowitz*, Informationsherrschaft im Kartellrecht, 2018; *Bitkom* (Hrsg.), Spionage, Sabotage und Datendiebstahl: Wirtschaftsschutz in der Industrie, 2018 (<https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf>); *Boerger*, Zur Schutzfunktion des Wirtschaftsstrafrechts, 2018; *Borges/Meents*, Cloud Computing, 2016; *Bormann/Ludwig*, Geheimerschutz in der Wirtschaft, DÖV 2020, 1061; *Born*, Unternehmen am Pranger?! – Öffentliche Äußerungen von Datenschutzbehörden im Zusammenhang mit Bußgeldverfahren, K&R 2021, 13; *Bottke*, Strafrechtswissenschaftliche Methodik und Systematik bei der Lehre vom strafbefreienden und strafmildernden Täterverhalten, 1979; *Brammsen*, „Durchlöcherter“ Bestandsschutz – Wirtschaftsgeheimnisse im 21. Jahrhundert, ZIP 2016, 2193; *Breitenbach*, Steuer-CDs, 2017; *Büdenbender*, Die Veröffentlichung unternehmerischer regulatorischer Daten durch die Bundesnetzagentur im Energierecht, RdE 2020, 221; *Bundeskriminalamt* (BKA, Hrsg.), Wirtschaftsspionage und Konkurrenzausspähung: eine Analyse des aktuellen Forschungsstandes, Studie 2014; *Busching*, Der Schutz »privater« Informationen bei Cloud Computing, 2019; *Buxbaum/Cooter*, Keeping Secrets, in: FS Ch. Kirchner, 2014, S. 681; *Canaris*, Systemdenken und Systembegriff in der Jurisprudenz, 2. Aufl. 1983; *Conrad/Fechtner*, IT-Outsourcing durch Anwaltskanzleien nach der Inkasso-Entscheidung des EuGH und dem BGH, Urteil vom 7.2.2013, CR 2013, 137; *Cornelius*, Cloud Computing für Berufsgeheimnisträger, StV 2016, 380; *Corporate Trust* (Hrsg.), Studie: Industriespionage: Cybergeddon der deutschen Wirtschaft durch NSA & Co.?, 2014 ([https://www.corporate-trust.de/pdf/CT-Studie-2014\\_DE.pdf](https://www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf)); *ders.*, Future Report, 2019; *Daimagüler*, Nebenklage im Wirtschaftsstrafverfahren, wistra 2017, 180; *Drescher*, Industrie- und Wirtschaftsspionage in Deutschland, 2019; *Fleischer*, Wirtschaftsspionage: Phänomenologie – Erklärungsansätze – Handlungsoptionen, 2016; *Freund*, Zur Übermittlung von sich im Besitz der Kommission befindlichen Dokumenten an nationale Gerichte – Anmerkungen zum Mitteilungsentwurf über den Schutz vertraulicher Informationen, GRUR Int. 2019, 1161; *Friedlaender*, Der strafrechtliche Schutz des Geschäfts- und Betriebsgeheimnisses, 1903; *Grünwald*, Die (Re) Kommunalisierung in der Energieverteilung, 2016; *Haedicke*, Zweckbindung und Geheimnisschutz bei Auskunft- und Rechnungslegungsansprüchen, GRUR 2020, 785; *Hambach/Berberich*, Ausnutzen von Softwarefehler straffrei? – der Gesetzgeber ist gefragt! ZfWG 2017, 60; *Hauck*, Besichtigungsanspruch und Geheimnisschutz im Patentrecht und (Software-)Urheberrecht nach Inkrafttreten des GeschGehG, GRUR 2020, 817; *Heldmann*, Dienstliche Nutzung privater Endgeräte (BYOD) und privater Gebrauch betrieblicher Kommunikationsmittel, 2015; *Hennrich*, Cloud Computing, 2016; *Herm*, Die Phönizier, 1973; *Hillenbrand*, Der Begriff des Betriebs- und Geschäftsgeheimnisses, 2017; *Hof*, Wettbewerb im Zunftrecht, 1983; *Hofer/Weiß*, Wirtschafts- und Industriespionage, 2016; *Hornkohl/Melzer*, Prozessualer Geheimnisschutz im Kartellschadensersatzrecht nach der 10. GWB-Novelle – eine Novelle ohne Novellierung, NZKart 2021, 214; *Hruschka*, Verhaltensregeln und Zurechnungsregeln, Rechtstheorie 22 (1991), 449; *Janke*, Kompendium Wirtschaftskriminalität, 2008; *Johnson/Kierkus/Barton*, The Economic Espionage Act and Trade Secret Theft: The Insider Threat, I.P.Q. 2017, 152; *Kahler*, Outsourcing im öffentlichen Sektor und § 203 Abs. 2 StGB, CR 2015, 153; *Karikari*, Big Data in der Automobilindustrie, 2018; *Kerkmann/Proelß*, Der Schutz von

## Einl. A Geschäftsgeheimnisschutz – Daten und Fakten

Geschäftsgeheimnissen im Beihilferecht, *VerwArch* 2017, 52; *Kilchling*, Wirtschaftsspionage und Konkurrenzausspähung – Herausforderungen für Staat und Wirtschaft, *GSZ* 2020, 57; *Kluge*, Topf Secret – Zum (rechtlichen) Stand der Dinge, *ZLR* 2019, 518, 524 ff.; *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2015; *Kort*, Strafbarkeitsrisiken des Datenschutzbeauftragten nach § 203 StGB beim IT-Outsourcing, insbesondere in datenschutzrechtlich „sichere“ Drittstaaten, *NStZ* 2011, 193; *KPMG* (Hrsg.), Studie e-Crime: Computerkriminalität in der deutschen Wirtschaft, 2015, <https://home.kpmg.com/content/dam/kpmg/pdf/2015/03/e-crime-studie-2015.pdf>; *dies.*, Tatort Deutschland: Wirtschaftskriminalität in Deutschland 2016, 2016, <https://assets.kpmg.com/content/dam/kpmg/pdf/2016/07/wirtschaftskriminalitaet-2016-2-KPMG.pdf>; *dies.*, Wirtschaftskriminalität in Deutschland, 2020; *Kroker*, Wege zur Verbreitung technologischer Kenntnisse zwischen England und Deutschland in der zweiten Hälfte des 18. Jahrhunderts, 1971; *Lederer*, Open Data Informationsöffentlichkeit unter dem Grundgesetz, 2015; *Liebl*, Schaden – Eine ökonomische Analyse, in: *Tuck/Liebl* (Hrsg.), Industriespionage des Ostens, 1988, S. 103; *Lück/Penski*, Aus Anlass von „Topf Secret“: Antragsbezogener Informationszugang als staatliches Informationshandeln? *DÖV* 2020, 506; *Maier*, Der Schutz von Betriebs- und Geschäftsgeheimnissen im schwedischen, englischen und deutschen Recht, 1998; *McGuire*, Der Schutz von Know-how im System des Immaterialgüterrechts, *GRUR* 2016, 1000; *Melzer*, § 33g GWB: Offenlegung versus Geheimnisschutz, 2020; *Merk*, Der Gedanke des gemeinen Besten in der deutschen Staats- und Rechtsentwicklung, 1934; *Th. Meurer*, Die Zulässigkeit der Abwerbung von Mitarbeitern unter lauterkeits- und vertragsrechtlichen Gesichtspunkten, 2012; *Müller*, Cloud Computing, 2020; *ders.*, Cloud Computing, *DuD* 2017, 371; *Müllmann*, Auswirkungen der Industrie 4.0 auf den Schutz von Betriebs- und Geschäftsgeheimnissen, *WRP* 2018, 1177; *Nathusius*, Wirtschaftsspionage – Gefahren, Strukturen und Bekämpfung, 2001; *Nienaber*, Bedeutung und Schutz von Geschäftsgeheimnissen im Mittelstand, 2019; *Otto*, Methode und System in der Rechtswissenschaft, *ARSP* 55 (1969), 493; *PricewaterhouseCoopers* (Hrsg.), Wirtschaftskriminalität in der analogen und digitalen Wirtschaft, 2016 (<https://www.pwc.de/de/risiko-management/assets/studie-wirtschaftskriminalitaet-2016.pdf>); *dies.*, Wirtschaftskriminalität 2018 Mehrwert von Compliance – forensische Erfahrungen, 2018 (<https://www.pwc.de/de/risk/pwc-wikri-2018.pdf>); *Psaroudakis*, Trade Secrets in the Cloud, *E.I.P.R.* 2016, 344; *Reinholz/Kraushaar*, Geistiges Eigentum, Leistungsschutzrechte und Geheimnisschutz beim Building Information Modeling (BIM), *K&R* 2020, 788; *Rody*, Der Begriff und die Rechtsnatur von Geschäfts- und Betriebsgeheimnissen unter Berücksichtigung der Geheimnisschutz-Richtlinie, 2019; *Rombach*, Geheimniskartelle oder effektive Durchsetzung kartellrechtlicher Schadenserstattungsansprüche in camera? *GRUR* 2021, 334; *Roper*, Trade Secret Theft, Industrial Espionage, and the China Threat, 2014; *Schaaf*, Industriespionage, 2009; *Scheja*, Schutz von Algorithmen in Big Data Anwendungen, *CR* 2018, 485; *Scheuner*, Die Staatszwecke und die Entwicklung der Verwaltung im deutschen Staat des 18. Jahrhunderts, in: *GS Conrad*, 1979, S. 467; *P. Schmid*, Der gesetzliche Schutz der Fabrik- und Geschäftsgeheimnisse in Deutschland und im Ausland, 1907; *ders.*, Zur Geschichte des Musterschutzes, *ZfgewR* Bd. 2 (1893), 70; *Schwarz*, Industriespionage, 1937; *Schlupe*, Über das innere System des neuen schweizerischen Wettbewerbsrechts, in: *FS Giger*, 1989, S. 561; *Sendzik*, Der „Datendiebstahl“, 2014; *Slawik*, Die Entstehung des deutschen Modells zum Schutz von Unternehmensgeheimnissen, 2017; *Söbbing*, Fundamentale Rechtsfragen zur künstlichen Intelligenz (AI Law), 2019; *Söhmer*, Insiderhandel und Marktmanipulation durch Geheimdienste – Informationen in Zeiten von PRISM und ihre Nutzung, *KJ* 2015, 56; *Staffler*, Industrie 4.0 und wirtschaftlicher Geheimnisschutz, *NZWiSt* 2018, 269; *Stancke*, Grundlagen des Unternehmensdatenschutzrechts – gesetzlicher und vertraglicher Schutz unternehmensbezogener Daten im privaten Wirtschaftsverkehr, *BB* 2013, 1418; *Stender-Vorwachs/Steeger*, Wem gehören unsere Daten? *NJOZ* 2018, 1361; *Surblyté*, Data Mobility at the Intersection of Data, Trade Secret Protection and the Mobility of Employees in the Digital Economy, *GRUR Int.* 2016, 1121; *Taeger* (Hrsg.), *Big Data & Co*, 2014; *Ulfkotte*, Wirtschafts-

I. Daten und Fakten zur heutigen Lage **Einl. A**

spionage, 2001; *Voigt*, Weltweiter Datenzugriff durch US-Behörden, MMR 2014, 158; *Weber*, Industriespionage als technologischer Transfer in der Frühindustrialisierung Deutschlands, Technikgeschichte Bd. 42 (1975), S. 287; *Wicker*, Cloud Computing und staatlicher Strafanspruch, 2016; *Wiebe/Schur*, Ein Recht an industriellen Daten im verfassungsrechtlichen Spannungsverhältnis zwischen Eigentumsschutz, Wettbewerbs- und Informationsfreiheit, ZUM 2017, 461; *Zech*, „Industrie 4.0“ – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151; *Zimmermann*, Frühe Beispiele aus der Welt der gewerblichen Eigentumsrechte, GRUR 1967, 173.

**Übersicht**

	Rn.		Rn.
I. Daten und Fakten zur heutigen Lage	1	b) Aktuelle Angriffsweisen . . .	15
1. Historischer Exkurs . . . . .	1	aa) Faktische Zugriffs-	
2. Aktuelle Bedeutung . . . . .	7	methoden . . . . .	15
a) Gesamtvolkswirtschaft-		bb) Erlaubte Zugriffe . . . . .	16
liche Schäden . . . . .	8	c) Exemplifikationen . . . . .	20
b) Individuelles Schadens-		d) Ausblick . . . . .	21
spektrum . . . . .	10	II. Forschungsstand . . . . .	22
3. Aktuelle Gefahrensituation . . . . .	12	1. Rückblick . . . . .	22
a) Vielfalt der Angriffsziele . . . . .	13	2. Entwicklung . . . . .	23
		III. Resümee . . . . .	24

**I. Daten und Fakten zur heutigen Lage**

**1. Historischer Exkurs**

Geschäftsgeheimnisse, Betriebsspionage und Geheimnisverrat sind seit alters her **1** bekannte Phänomene, die über die Jahrtausende hinweg wellenmäßig mehr und mehr an Verbreitung und Verfeinerung gewonnen haben. Gleichwohl hat sich ihre praktische Bedeutung über die verschiedensten Epochen hinweg doch sehr lange in engen Grenzen gehalten, um dann in den letzten 150 Jahren im Zuge der rapide anwachsenden Industrialisierung sowie der sich immer mehr entfaltenden Globalisierung und Technisierung schließlich auch weltweit zu verbreiten. Waren es anfangs im **Altertum** nur wenige bekannte Fälle wie die der Phönizier oder der Japaner, die den Ägyptern das Verfahren der Glasherstellung und dem syrischen Ugarit das Geheimnis der Purpurherstellung<sup>1</sup> bzw. den Chinesen das Geheimnis der Seidengewinnung<sup>2</sup> entwendeten, so erlebte der Geheimnisschutz nach längerer Stagnation im Gefolge des Niedergangs des Römischen Reiches und der Völkerwanderungen mit dem heraufziehenden **Mittelalter** seine erste Expansionsphase.

<sup>1</sup> *Drescher*, S. 27; *Herm*, S. 114 f.

<sup>2</sup> *Capital* 12/1985, 116; *Spiegel* 12/1972, 48; *Drescher*, S. 26; *Janke*, S. 263. Die Angaben schwanken stark – zwischen 1500, 300 und 140 v. Chr.

## Einl. A Geschäftsgeheimnisschutz – Daten und Fakten

- 2 Kannten die vorherigen urbanen oder territorialen Herrschaftsgebilde (mit fragwürdiger Ausnahme der äußerst umstrittenen spätrömischen *actio servi corrupti*<sup>3</sup>) keine bislang bekanntgewordenen einschlägig bezogenen Umgangs- bzw. Zuordnungsregeln, so änderte sich im Gefolge der wachsenden mediävalen Verstädterung Mittel- und Nordeuropas die Situation grundlegend. Es waren die berufsständischen Vorgaben der **Zünfte und Gilden**, die mit Wander- und Auswanderverboten für bestimmte Handwerkszweige,<sup>4</sup> Abwerbeverboten<sup>5</sup> und Geboten, Arbeitsgeräte, Werkzeuge und Rohmaterialien nicht Orts- oder Zunftfremden zugänglich zu machen,<sup>6</sup> die seinerzeit dominierende vornehmlich regionale Versorgungswirtschaft abzusichern suchten. Dieser Trend fand mit dem Niedergang des spätmittelalterlichen Personenverbandsstaats und dem Verlust der politischen Macht der Zünfte seit dem 15. Jahrhundert sein langsames Ende: Zunehmend eingeengt durch kaiserliche Edikte, Reichsabschiede, Reichspolizeiverordnungen und das Privilegienwesen verloren ihre wettbewerbsregelnden Satzungen beständig an Wirkung und waren schließlich seit dem **dreißigjährigen Krieg** kaum noch von verhaltenssteuernder Kraft.<sup>7</sup>
- 3 Unter den desolaten Zuständen der damaligen Nachkriegswirtschaft konnte die längst überfällige Reformbewegung in den erstarkenden **Kleinstaaten** des zersplitterten Reiches einsetzen. Politisch geprägt vom **Absolutismus**, dem Kameralismus, dem Merkantilismus, zugleich materiell maßgeblich ausgerichtet auf den alleinigen Staatszweck „Gemeinwohl“<sup>8</sup> wurden im Gefolge von England<sup>9</sup> vornehmlich im deutschsprachigen Raum, aber auch in Frankreich<sup>10</sup> zwecks verstärkter Förderung von Industrie und (primär: Außen-)Handel erstmals strafrechtliche Normen zum

3 In dieser Korruptionklage wegen fremdtäterschaftlicher Wissensvermittlung durch fremde oder eigene Sklaven sieht A. Arthur Schiller, Columbia Law Review 1930 (30. Band), S. 837 ff., 843 einen Beweis römischrechtlichen Geheimnisschutzes; dezidiert ablehnend Kamperman Sanders, The ‚Actio Servi Corrupti‘ from the Roman Empire to the Globalised Economy, in: Health/Kamperman Sanders (Hrsg.), Employees, Trade Secrets and restrictive Covenants, 2017, S. 3, 4; s. auch Drescher, S. 26.

4 Als spätes Beispiel das Auswanderverbot der Lübecker Paternostermacher (Bernsteindreher) von 1385: „So we van der paternostermaker ampte ut desser stad wandert undre in andren landen edder steden dat ampte ovet, den schal men na der tet hir nicht steden to des amptes werke“; Schwarz, S. 5 ff. mw. Bsp.

5 Zum damaligen „Abmieten, Abspenstigmachen, Entspannen oder Entfremden“ Schwarz, S. 10 ff.; Ziekow, Freiheit und Bindung des Gewerbes, 1992, S. 149 ff. Spektakulärstes neuzeitliches Beispiel: Der Wechsel des Einkaufs- und Produktionsvorstands Ignacio Lopez von General Motors zu VW (WiWo 15/1993, S. 124 f.); s. auch OLG Hamburg, GRUR-RR 2020, 18 ff. Aktuelle Risikoschätzungen: PWC, Studie 2016, S. 35 ff.

6 Beispielhaft das Verbot der Berliner Wollenweber von 1295: „Pretera statuimus quod nullus alius extra fraternitatem videlicet monialibus aut aliunde venientibus sua instrumenta concedat“; Schwarz, S. 7 f.

7 Komprimiert dazu Hof, S. 249 ff.

8 Zu den Entwicklungsstadien Scheuner, GS Conrad, S. 467 ff., und Merk, S. 54 ff.

9 England hatte bereits ab dem 14., vermehrt aber erst ab Mitte des 17. Jahrhunderts strafbewehrte Geheimnisschutznormen etabliert; Nachweise zu einschlägigen Gesetzen bei Ambrosch, S. 129 ff.

10 Zusammenstellungen bei Friedlaender, S. 30 f.; Kroker, S. 91 ff.; Th. Meurer, S. 37 ff.; Schmid, ZfgewR Bd. 2 (1893), 70 ff.; Schwarz, S. 19 f.

Schutz von Geschäftsgeheimnissen erlassen. Zumeist an bestimmte Gewerbe-  
zweige gerichtet, enthielten die einschlägigen Reskripte und Verordnungen dem Zunft-  
recht vielfach nachempfundene Auswanderungs-, Export-, Gebrauchs-, Kooperati-  
ons-, Mitteilungs- und Verleitungsverbote,<sup>11</sup> die neben einer ungebrochenen Fort-  
setzung in der Erstreckung der Strafbarkeit auf den Auslandsverrat und fremde  
Auslandsspionage in § 148 Teil II Titel 20 ALR 1794 ihren vorläufig **ersten Höhe-**  
**punkt** erlebten.<sup>12</sup> Konträr dazu hatte sich die eigene Auslandsspionage zur wohl  
wichtigsten Wirtschaftsförderungsmaßnahme entwickelt, die viele Kleinstaaten  
nach Kräften zu forcieren suchten.<sup>13</sup> Als prägnantes Beispiel wird hier nur auf die  
(1787 gescheiterten) Spionageversuche des *Frhr. vom Stein* in England verwiesen<sup>14</sup>  
– ein Land, das auch in späteren Jahrzehnten das bevorzugte Ziel insbesondere  
deutscher (Stahl-)Industriespionage sein sollte.<sup>15</sup>

Waren die bisherigen Normen mehr auf die Abwehr der Auslandsspionage gerich- **4**  
tet,<sup>16</sup> so erlebte der bisherige primär kollektivistisch fundierte Geheimnisschutz mit  
dem Durchbruch der **Gewerbefreiheit** im Gefolge der französischen Revolution  
eine schrittweise Umkehrung hin zum Schutz vor vornehmlich inländisch-privater  
Ausspähung und Kenntnisverbreitung in Gestalt von Individualschutzdelikten.<sup>17</sup>  
Anknüpfend an das als Vermögensdelikt eingeordnete<sup>18</sup> Verratsdelikt des Art. 418  
code pénal 1810 eröffnete das Königreich **Bayern** bereits **1813** die nunmehrige part-  
ikulargesetzliche „Normierungswelle“ mit der Etablierung gleich zweier Schutz-  
normen gegen Ausspähung und Entwendung (Art. 396 f. StGB).<sup>19</sup> Ähnliche **Straf-**  
**vorschriften**, die sich zumeist nur geringfügig in Anwendungsbereich und Täter-  
kreis voneinander unterschieden, entstanden in den Folgejahrzehnten in einer  
ganzen Reihe von **Partikularstaaten** in deutschen Ländern,<sup>20</sup> aber nicht überall.<sup>21</sup>  
Sie eröffneten den Geheimnisinhabern den Weg zu einem eigenständigen Ge-  
schäftsgeheimnisschutz, der allerdings in den nachfolgenden Jahrzehnten in allen  
Partikularstaaten keine sehr große Resonanz fand – ganz im Gegensatz wiederum

11 Zusammenstellungen bei *Kroker*, S. 99 ff.; *Schmid*, ZfgewR Bd. 2 (1893), 144; *Schwarz*, S. 16 ff.;  
*Zimmermann*, GRUR 1967, 173, 177.

12 Aktuelle Staatsschutznormen sind ua. Art. 411, 5–8 code pénal, § 124 öst. StGB, Art. 273  
schweiz. StGB, § 1839 Abs. 3 US-EEA 1996.

13 Eingehender *Kroker*, S. 128 ff.; *Weber*, Technikgeschichte 42 (1975), 287 ff.; *Johnson/Kierkus/  
Barton*, I.P.Q. 2017, 152 ff.

14 Näher dazu *Weber*, Technikgeschichte 42 (1975), 301 f.

15 Vgl. *Drescher*, S. 31 f. sowie *Schaaf*, S. 14 f. zum Vorgehen der späteren „Stahlbarone“ *Hoesch*  
und *Krupp*.

16 Resultat ihrer merkantilistischen Ausrichtung; statt vieler *Slawik*, S. 133 ff., 148 f. mwN.

17 Zu dieser Neuausrichtung zuletzt *Slawik*, S. 150 ff.

18 Im III. Buch 2. Titel 2. Kap. (Gegen das Eigentum) 2. Abschnitt: Betrügereien. Einschlägige  
Einordnungen in den Partikularstrafgesetzen benennt *Slawik*, S. 77.

19 Eingehender zu ihnen *P. Schmid*, S. 39 ff.; *Schwarz*, S. 23 ff.; *Slawik*, S. 56 ff., 78 ff.

20 Ausführlichere Darstellungen bei *Finger*, Der Geheimnisbruch, in: Birkmeyer/van Calker/Mayer  
(Hrsg.), Vergleichende Darstellung des deutschen und ausländischen Strafrechts BT Bd. 8, 1906,  
S. 293, 308 ff.; *Schwarz*, S. 25 ff. und *Slawik*, S. 62 ff.

21 Ohne strafrechtlichen Geheimnisschutz blieben Bremen, Hessen, Lübeck, Mecklenburg, Olden-  
burg, Preußen, Schaumburg-Lippe und Waldeck.

## Einl. A Geschäftsgeheimnisschutz – Daten und Fakten

zu **England**, das nahezu zeitgleich unter dem Einfluss des Liberalismus statt auf Strafrechts- auf **Zivilrechtsschutz** „umgestiegen“ war.<sup>22</sup>

- 5 Die strafrechtliche Bestandssicherung unternehmensbezogener Geheimheit sollte sich bis über die dritte **Millenniumswende** hinaus als verlässliches „Minimalrefugium“ eines Geschäftsgeheimnisschutzes erweisen. Zwar wurde er von einem anfänglich ebenso zersplitterten wie umstrittenen Patentschutz und einem den Freihandel präferierenden Preußen unterbrochen, deren diesbezüglich lückenhafte Ausgestaltung erst für 20 Jahre das heimische Strafgesetz, sodann für weitere 25 Jahre auch das spätere Reichsstrafrecht von 1871 „negativ“ prägte.<sup>23</sup> Noch während seiner Hochphase erlebte der Trend zur gesetzlichen „Freigabe“ der Geheimnisse im Gefolge der Gründerkrise, der reichseinheitlich strafgeschützten Etablierung gewerblicher Schutzrechte, dem politischen Kurswandel zum Wirtschaftsinterventionismus uam. eine wirkmächtige Rückkehr zur Tradition der vorunitarischen Zeit<sup>24</sup> – in Gestalt der Strafnormen der **§§ 9 f. UWG 1896** bzw. der §§ 17 ff. UWG 1909.<sup>25</sup> Die folgenden Weimarer, nationalsozialistischen und bundesrepublikanischen Jahrzehnte kulminierten dann, abgesehen von zahlreichen spektakulären Fällen wie jenen der „I. G. Farben“, der „Surete“, „Opel/VW (Lopez)“, „Enercon“, „Kirch/Breuer“ oder „Heraeus“<sup>26</sup> und einem beständigen **Ausbau** weiterer nebenstrafrechtlicher Schutznormen,<sup>27</sup> in einer breiten nationalstaatlichen Verbreitung, die den strafrechtszentrierten Geschäftsgeheimnisschutz bis zur Jahrtausendwende nahezu weltweit etablierten.<sup>28</sup>
- 6 Dergestalt etabliert, entwickelten sich unter seiner Ägide auf inter- wie auf supranationaler Ebene zunehmend zivilistisch inspirierte Unitarisierungsbestrebungen,

22 Zahlreiche Belege zum seinerzeitigen „Schwenk“ zum *breach of confidence*-Ansatz bei *Hillenbrand*, S. 85 ff.

23 Das preußische StGB von 1851, Vorbild des StGB für den Norddeutschen Bund 1870 und über dieses auch für das RStGB 1871, enthielt wie seine Nachfolger keine geschäftsgeheimnisschützenden Strafvorschriften; zu den vielfältigen Hintergründen dieser „Regelungslücke“ *Slawik*, S. 158 ff., 203 ff.

24 Zur (Re-)Implementierung des Geschäftsgeheimnisstrafrechts im UWG eingehend *Slawik*, S. 226–429, 494 ff.

25 Bemerkenswert ist, dass in etwa zeitgleich England zu einem (nunmehr verstärkenden) Strafrechtsschutz zurückkehrte; vgl. *Ambrosch*, S. 134 f., 173 f., 179.

26 Nachweise zu diesen und anderen bedeutsamen Fällen bei *Brammsen*, ZIP 2016, 2193, 2195, 2198; *Janke*, S. 266 ff.; *Nathusius*, S. 4 ff., 11 ff. Zum Ausmaß ausländischer Wirtschaftsspionage im Gefolge des ersten Weltkriegs *W. Fischer*, Die feindliche Handels- und Industriespionage und der wirtschaftliche Landesverrat, 1922, S. 66 ff.; *Schwarz*, S. 46 ff.; *Stranders*, Die Wirtschaftsspionage der Entente, 1929, S. 66 ff.

27 Aktuell ua. die §§ 404 AktG, 120 BetrVG, 22a BStatG, 43 f. EBRG, 95b EnWG, 14 EWIV-AG, 151 GenG, 85 GmbHG, 5 GrenzkraftwerkeG, 333 HGB (auch iVm. §§ 335b, 340m, 341 HGB und § 47 DMBilG), 55a und b KWG, 34 MgVG, 19 PublG, 47 SCEBG, 45 SEBG, 237a und b SGB IX, 35 SprAuG, 315 UmwG, 17 ff. UWG, 138 VAG, 133b und c WPO; s. auch § 85a SGB X iVm. § 35 Abs. 4 SGB I sowie *Stancke*, BB 2013, 1418, 1420 ff.

28 *Anderson/Turner*, Report on Trade Secrets for the European Commission, in: Hogan Lovells International LLP (Hrsg.), Study on Trade Secrets and Parasitic Copying (Look-alikes) MARKT/2010/20/D, abgeschlossen am 23.9.2011 und veröffentlicht am 13.1.2012 unter: [ec.europa.eu/internal\\_market/iprenforcement/docs/trade/201201-study\\_en.pdf](http://ec.europa.eu/internal_market/iprenforcement/docs/trade/201201-study_en.pdf) (Stand: 31.8.2012).

die den arg rudimentären Rechtsgüterschutz der Geschäftsgeheimnisse nach dem Vorbild des Immaterialgüterrechts umfassender auszugestalten trachteten.<sup>29</sup> Der vorläufige Abschluss dieser Entwicklung erfolgte in drei Schritten: (1) Der Umwandlung des früheren „Billigkeitsaspekts“ der Geheimhaltungsmaßnahmen einer „obligation of confidence“<sup>30</sup> in ein neues inhaltskonformes Güterkonstituens sowie (2) im Anschluss an die einflussreiche Einstufung als strafrechtlich geschütztes „gegenstandsähnliches“ *property-Vermögensgut* im Fall Carpenter/United States.<sup>31</sup> Die Vollendung vollzog sodann (3) die primär vom TRIPS-Abkommen (von anderen Modellvorhaben<sup>32</sup> weniger) nachhaltig vorangetriebene Entwicklung mit der detailliert ausgeformten **Know-how-RL 2016/943/EU**,<sup>33</sup> deren zivilistisch geprägter Rechtsrahmen das GeschGehG mit leichten Modifizierungen in das bundesdeutsche Recht überführte.<sup>34</sup> Dergestalt vornehmlich auf überindividuelle Interessen (Binnenmarktangleichung, Art. 114 AEUV)<sup>35</sup> gegründet und „anharmomisiert“<sup>36</sup> steht zu erwarten, dass die gem. Art. 18 der Richtlinie RL 2016/943/EU anstehenden Berichte die praktische Bedeutung des rechtlichen Geschäftsgeheimnisschutzes auch zahlenmäßig deutlich transparenter werden lassen.

## 2. Aktuelle Bedeutung

Welche tatsächlichen Ausmaße Wirtschaftsspionage und Geheimnisverrat in den modernen wettbewerbsorientierten Industrieländern angenommen haben, ist für Deutschland, ebenso aber auch für viele andere (außer-)europäische Staaten nicht konkret zu ermitteln. Es **fehlt** nicht nur **an** abgestimmt gebietsübergreifend erstellten nationalen wie internationalen **Statistiken**, selbst beschränkt allein auf das Strafrecht lässt sich das einschlägige Tataufkommen mangels einheitlicher Datenerfassung, ungeklärter Dunkelziffer und geringer Aufklärungsquoten nicht mit hinreichender Genauigkeit angeben.<sup>37</sup> Wie schon zu Beginn des vergangenen Jahr-

29 Erste Ansätze bereits in der Pariser Verbandsübereinkunft zum Schutze des gewerblichen Eigentums von 1883; vgl. *Brammsen*, Lauterkeitsstrafrecht, Vor §§ 17–19 Rn. 9 mwN.

30 Prägnant dargestellt von *Hillenbrand*, S. 125 ff., 140 ff., 188 ff.

31 488 U.S. 19 (1987). Dazu und zur US-property-Konzeption, die vermögensstrafrechtlichen Geschäftsgeheimnisschutz als „gegenstandsähnliche“ Verkörperung dem Vorbild des Sacheigentums entlehnt, prägnant *Boerger*, S. 259 ff.

32 Zum TRIPS-Abkommen, den WIPO Model Provisions und dem Modellgesetz des Europarates zum Schutz von Fabrikations- und Handelsgeheimnissen komprimiert *Brammsen*, Lauterkeitsstrafrecht, Vor §§ 17–19 Rn. 10–13 mwN.

33 Richtlinie 2016/943 EU vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl. EG 2016 Nr. L 157, 1 ff.

34 Vgl. GeschGehG vom 18.4.2019, BGBl. I, 466 ff.

35 Know-how-RL 2016/943/EU, Erwgrd. 22, 36.

36 Mindestharmonisierung steht außer Streit; vgl. Art. 1 UAbs. 2 RL 2016/943/EU.

37 Näher zu den verschiedenen Angaben *Drescher*, S. 54 ff.; *Maier*, S. 31 ff.; s. auch Antwort der Bundesregierung auf eine Große Anfrage der SPD-Fraktion zur Wirtschaftsspionage, BT-Drs. 13/8368, S. 3 f. und *Kilchling*, GSZ 2020, 57, 58 f.

## Einl. A Geschäftsgeheimnisschutz – Daten und Fakten

hunderts<sup>38</sup> so vermitteln die Fallzahlen der bundesdeutschen polizeilichen Kriminalstatistik auch heutzutage kaum einen gesicherten Überblick über den Umfang der tatsächlichen Bedrohung bzw. Schädigung der Unternehmen: Sie stagnieren seit Jahrzehnten konstant im mittleren bzw. unteren **dreistelligen** Bereich.<sup>39</sup> Ähnliches scheint für die Schweiz zu gelten, die für die Jahre 2000–2005 lediglich 364 Verratsfälle benennt.<sup>40</sup> Und auch neue Unternehmensstudien berichten über auffallend konstante bzw. sogar sinkende Schadens- und Verdachtsquoten sowohl privaten wie staatlichen Geheimnisbruchs.<sup>41</sup>

### a) Gesamtvolkswirtschaftliche Schäden

- 8 Schon seit Längerem werden die jährlichen Schäden, die der bundesdeutschen Wirtschaft durch staatlich betriebene Industriespionage entstehen, konstant hoch eingeschätzt,<sup>42</sup> was zahlreiche Beispiele nachrichtendienstlich gesteuerter Wirtschaftsspionage während der früheren deutschen Doppelstaatlichkeit<sup>43</sup> als auch seitens befreundeter Staaten bis heute zu bestätigen scheinen.<sup>44</sup> Größenmäßig exakter erfassbar wird das aktuelle Bedrohungsszenario erst, wenn einmal die allein für **Deutschland** insgesamt geschätzten jährlichen **Schadenssummen** in den Blick genommen werden: Sie bewegen sich mehrheitlich in einer Spanne von 5–25 Mrd. EUR,<sup>45</sup> nach neueren Schätzungen (mit Dunkelziffer) sogar bis hin zu 55 Mrd. EUR.<sup>46</sup> Für die **USA** wurde eine ähnliche Schadenssumme (über 45 Mrd. Dollar) bereits um die Jahrtausendwende errechnet und inzwischen auf 250 Mrd. Dollar er-

38 In den beiden Jahrzehnten vor und nach dem ersten Weltkrieg bewegten sie sich um die 80–90 bzw. zwischen 24 und 101 Fällen; vgl. *Eb. Schmidt*, Bedarf des Betriebsgeheimnis eines verstärkten Schutzes? in: Verhandlungen des 36. Deutschen Juristentages (DJT), Bd. 1, Gutachten, 1930, S. 101, 112 ff., 117.

39 In den Jahren 2009–2019 betrug die Straftaten nach § 17 UWG 646, 500, 525, 425, 397, 394, 397, 322, 297 und 285 Fälle; Bundeskriminalamt Polizeiliche Kriminalstatistik 2010–2019 (Sach-Schlüsselnummer 715300 und 715400) <https://www.bka.de/Publikationen>; s. auch *Drescher*, S. 54 und MK-StGB/*Hohmann*, § 23 GeschGehG Rn. 4. Ältere Zahlen (seit 1994) bei *Fleischer*, S. 11 ff.; *W/J/S/Möhrenschlager*, Kap. 16 Rn. 5.

40 Vgl. *Ackermann/Heine/Schwarz*, § 19 Rn. 9.

41 Vgl. *KPMG*, 2020, S. 11, 15 ff.; *PWC*, Studie 2018, S. 16 ff.; *Corporate Trust*, 2019, S. 21, 69; 2014, S. 13 ff., 67 ff.; s. auch *Drescher*, S. 55 f.

42 Hbl. v. 16./17./18.11.2018, Nr. 222, 25; 21.7.2014, Nr. 137, 22; *WiWo* 6/2017, S. 30; 45/2013, S. 18; *Nathusius*, S. 20 ff., 37 ff.; (aus den USA) *Roper*, S. 87 f., 245 ff., 261 ff.; *Corporate Trust*, 2014, S. 11, 13, 67 ff.; zurückhaltender *BKA*, S. 57 ff.; *Drescher*, S. 90 f.; *Ernst&Young*, Datenklau, 2018, S. 10 f.

43 Prägnant *Nehring*, Gerbergasse 18, 3/2017, Heft 84, S. 8 ff.

44 Neuere Beispiele: *WiWo* 42/2018, S. 80 ff.; 28/2013, S. 58 ff.; Hbl. v. 15.3.2019, Nr. 12, 32 ff.; 9.3.2017, Nr. 49, 11; 17.8.2015, Nr. 156, 48; 28.1.2015, Nr. 19, 26 f.; 1.12.2014, Nr. 231, 8; 14.4.2014, Nr. 73, 17; s. auch BVerfG, *NVwZ* 2014, 1652 Rn. 181 ff.; <https://www.pwc.com/gsis> 2015, S. 2; *Drescher*, S. 46 ff., 167 ff.; *Kochheim*, Rn. 223 ff.

45 *BKA*, S. 6, 89 (einstelliger Mrd.-Betrag); *Corporate Trust*, 2014, S. 8, 23, 73 (11,8 Mrd. EUR); *ABZ* 2/2015, 17; Hbl. v. 21.7.2014, Nr. 137, 22; *WiWo* 45/2013, S. 18; *Bitkom*, S. 25; *Brammsen ZIP* 2016, 2193, 2194 f.; *Drescher*, S. 91; *Tiedemann*, *WiStR*, Rn. 876.

46 Hbl. v. 26.4.2016, Nr. 80, 6; *WiWo* 23/2018, S. 44; 52/2017, S. 16; *BKA*, S. 50 ff.; *Bitkom*, S. 25; *Corporate Trust*, 2019, S. 11; *Drescher*, S. 54; *Janke*, S. 265.

höht.<sup>47</sup> **Weltweit** schätzt eine Studie der Beratungsgesellschaft Pricewaterhouse-Coopers schon für das Erhebungsjahr 2013 die Schäden bei Geheimnisverlust auf 749 Mrd. bis 2,2 Bill. Dollar.<sup>48</sup>

Der für die bundesrepublikanische Wirtschaft bezifferte Maximalschaden von 55 Mrd. EUR erscheint selbst bei zehnfacher Dunkelziffer **deutlich zu hoch** gegriffen, insbesondere wenn der Fokus einmal stärker auf den Mittelstand gerichtet wird.<sup>49</sup> Dies belegt bereits eine einfache Überschlagsrechnung in Anlehnung an die Fallzahlen der obigen polizeilichen Kriminalstatistiken (→ Rn. 7 Fn. 39). Wird hier die nicht eben geringe Gesamtsumme auf 4.000–7.500 Straftaten angesetzt,<sup>50</sup> so ergibt sich daraus bei partiell abgestufter Aufteilung der 50 Mrd. EUR in sechs willkürlich gegriffene Schadensstufen von 250, 125, 50, 25, 12,5 Mio. EUR und darunter folgende Beispielrechnung – 50 Fälle mit 200, 80 Fälle mit 125, 100 Fälle mit 50,<sup>51</sup> 200 Fälle mit 25 und 800 Fälle mit 12,5 Mio. EUR Schadenshöhe – für die verbleibenden maximal 6.250 Schadensfälle eine Restsumme von 15 Mrd. EUR mit einem Durchschnittsschaden von ca. 2,4–5,35 Mio. EUR. In den vergangenen drei Jahrzehnten ist eine jährliche Deliktsquote von über 400 Fällen mit einem Mindestschaden von 25, 50, 125 und 200 Mio. EUR selbst unter Einbeziehung etwaiger Zivilverfahren nie auch nur annähernd bekannt geworden. Aus allen publik gewordenen Fällen lassen sich deutschland- wie europaweit pro Jahr maximal 100 Fälle mit bis zu 100 Mio. EUR Einzelschaden identifizieren. Es ist daher angemessen, unter Einbeziehung einer gleichanteilig hohen Schadenssumme für nachrichtendienstliche Industriespionage die alljährliche **Gesamtschadenssumme auf 15–25 Mrd. EUR** zu reduzieren. Dies erscheint besser vertretbar, zumal mitunter einbezogene Plagiate und Patentverletzungen<sup>52</sup> häufig auf bloßer Nachahmung beruhen.

#### b) Individuelles Schadensspektrum

Auch im Hinblick auf die individuellen (geschätzten) Schadenssummen bestehen erhebliche Unklarheiten. Hier zeigt sich eine deutliche **Steigerungsquote**. Wurde vor 30 Jahren noch für 1998 ein Durchschnittsschaden von 1 Mio. DM angenommen,<sup>53</sup> bestätigte bereits zur Jahrtausendwende eine US-amerikanische Studie, dass die be-

47 American Society for Information Security (ASIS), vgl. Hbl. v. 4.7.2000, Nr. 126, 26; *Johnson/Kierkus/Barton*, I.P.Q. 2017, 152, 154.

48 Vgl. <https://www.pwc.com/gsis> 2015, S. 11; s. auch Hbl. v. 22.4.2015, Nr. 64, 4 f.; 21.7.2014, Nr. 137, 22.

49 *Nienaber*, Rn. 100 ff., 125 ff., 373 ff.

50 Dies entspricht etwa der Verfünffachung aller einschlägigen eindeutigen und hinzukommenden konkreten Verdachtsfälle der *PWC*, Studie 2016, S. 16 ff. Von mindestens 4000 Fällen geht auch *Drescher*, S. 91 aus.

51 Diese Schadensgruppe ist den in der *PWC*, Studie 2016, S. 16, 36 erwähnten 115 „gravierenden“ Schadensfällen nachempfunden. Massenmedial nachweisbar sind die Gesamtzahl und Schadenshöhe allerdings für keinen Berichtszeitraum.

52 *Bitkom*, S. 25; *Corporate Trust*, 2014, S. 22, 29 (11,8 Mrd. EUR ohne Einbeziehung).

53 *Tuck/Liebl/Liebl*, 1988, S. 109. So unverändert zuletzt auch noch für das Jahr 2014 die Studien von *BKA*, S. 54 f. und *Corporate Trust*, 2014, S. 8, 23; s. auch *Drescher*, S. 85 ff.

## Einl. A Geschäftsgeheimnisschutz – Daten und Fakten

fragten Unternehmen erlittene Ausspähungsschäden auf 15–50 Mio. Dollar je Angriff festsetzten.<sup>54</sup> Neue Berechnungen<sup>55</sup> und neuere Fälle wie „A2Mac1/GWM“,<sup>56</sup> „Enercon/Kenetech“,<sup>57</sup> „Heraeus und Lanxess“, „Mitec/Ford“,<sup>58</sup> „Nippon Steel/Posco“,<sup>59</sup> „Oracle/SAP“,<sup>60</sup> „Opel/VW“,<sup>61</sup> „Renault“,<sup>62</sup> „Thyssen Krupp“,<sup>63</sup> „Vietz/CNPC“,<sup>64</sup> „Vodafone Deutschland“,<sup>65</sup> „VW/FAW“<sup>66</sup> ergeben, dass die betroffenen Unternehmen durchaus ein- bis dreistellige Millionenverluste hatten<sup>67</sup> bzw. insolvent wurden.<sup>68</sup> Daran anknüpfend kann eine Schadens(ersatz-)summe zwischen 1 Mio. und 1 Mrd. EUR angesetzt werden, wobei die **Verlustquote** bis zu 10 Mio. EUR prozentual absolut dominiert.<sup>69</sup>

- 11 Die große Anzahl neuerer Fälle<sup>70</sup> verdeutlicht, dass die kriminelle Erlangung und Ausbeutung fremder Wirtschaftsgeheimnisse ein kostenreduzierender Faktor ist, der unter ökonomischen Gesichtspunkten zunehmend akzeptabel erscheint.<sup>71</sup> Wenn

54 American Society for Information Security (ASIS), Hbl. v. 4.7.2000, Nr. 126, 26.

55 Janke, S. 266 ff.; Nathusius, S. 4 ff.

56 Hbl. v. 9.1.2013, Nr. 6, 14.

57 Hbl. v. 25.1.2011, Nr. 17, 26; Schaaf, S. 19; Ulfkotte, S. 35 ff.

58 WiWo 47/2015, S. 40; Hbl. v. 30./31.10.2009, Nr. 210, 12; OLG Jena, BeckRS 2015, 20226.

59 Financial Times Deutschland v. 26.4.2012, S. 6; GRUR Int. 2017, 639.

60 Hbl. v. 23.3.2007, Nr. 59, 17; 25.11.2010, Nr. 229, 20 f.; WiWo 48/2010, S. 95 f.

61 Zu diesem Fall Nathusius, S. 7 ff. Das LG Darmstadt hat das gegen Lopez u. A. betriebene Strafverfahren gegen Zahlung von 590.000,- DM endgültig eingestellt; Hbl. v. 28.7.1998, Nr. 142, 15.

62 Hbl. v. 6.1.2011, Nr. 4, 24 f.; 19.1.2011, Nr. 13, 22.

63 *Corporate Trust*, 2019, S. 10.

64 Hbl. v. 29.9.2008, Nr. 189, 18; WiWo 8/2009, S. 68 ff.

65 Hbl. v. 13./14.9.2013, Nr. 177, 20.

66 Hbl. v. 27./28.7.2012, Nr. 144, 3, 8; WiWo 28/2013, S. 58, 60.

67 Aktuell: ASML/Xtal, Börsenzeitung 12.4.2019, Nr. 72, 9; Heraeus/Biomet, GRUR Int. 2018, 600 ff.; Schaumstoffsysteme, OLG Stuttgart, WRP 2021, 242 Rn. 25; Waymo/Uber, WiWo 7/2018, S. 46; s. auch die Fälle AMSC/Sinovel, <https://de.wikipedia.org/wiki/Sinovel> sowie Enercon, Opel (Rn. 10) oder Ferrari (Fn. 90) und die Zusammenstellungen bei Janke, S. 266 ff. und Nathusius, S. 4 ff.

68 ZB Geis-Kugellager Schweinfurt, WiWo 27/2005, S. 68; Mifa, Hbl. v. 2.–5.10.2014, Nr. 190, 19.

69 Durchschnittsschaden nach Unternehmensgröße: *Corporate Trust*, 2014, S. 8, 23: 0,01–1,2 Mio. EUR; Drescher, S. 85 ff., 91: 0,3 Mio. EUR; KPMG, e-Crime, S. 16: 0,61 Mio. EUR; PWC, Studie 2018, S. 21: 7,23 Mio. EUR. Laut KPMG, 2020, S. 15 kann eine stark ansteigende Zahl von Unternehmen (35%) die Schadenshöhe nur schwer bemessen.

70 Aldi Süd/Lidl, WiWo 15/2019, S. 16, 18, 22; AMSC/Sinovel, <https://de.wikipedia.org/wiki/Sinovel>; Bosch, WiWo 35/2016, S. 16, 18; 36/2016, S. 37; Compware Medical, Hbl. v. 28.11.2018, Nr. 230, 20 f.; Dyson/Bosch, FAZ v. 25.10.2012, Nr. 249, 14; Heraeus/Biomet, GRUR Int. 2018, 600 ff.; Himax, OGH Taiwan, GRUR Int. 2018, 576; Koenig&Bauer/Hebenstreit Metal Decorating, WiWo 14/2018, S. 50 f.; Lanxess, Hbl. v. 16./17./18.11.2018, Nr. 222, 25; Mars, Hbl. v. 25.5.2020, Nr. 99, 46; Nike, WiWo 51/2014, S. 13; Procter&Gamble/Unilever, WiWo 21/2004, S. 80; Rieder Faserbeton, WiWo 25/2010, S. 44, 48; Waymo/Uber, Hbl. v. 30.8.2019, Nr. 166, 27; WiWo 7/2018, S. 46.

71 Zuletzt zur Autobranche WiWo 23/2018, S. 66 ff.; Beiersdorf/Ave+Edam v. 12. Apr. 2021, vgl. [www.businessinsider.de/gruenderszene/health/nutzt-beiersdorf-know-how-von-startups-ave-edam-b/?utm\\_source=rss&utm\\_medium=rss&utm\\_campaign=nutzt-beiersdorf-know-how-von-startups-ave-edam-b](http://www.businessinsider.de/gruenderszene/health/nutzt-beiersdorf-know-how-von-startups-ave-edam-b/?utm_source=rss&utm_medium=rss&utm_campaign=nutzt-beiersdorf-know-how-von-startups-ave-edam-b). Volkswirtschaftlich ist der Nutzen ersparter Entwicklungskosten in staatlich gelenkten Wirtschaften natürlich ungleich höher.

zudem bedacht wird, dass sowohl schon vor über drei Jahrzehnten ebenso wie noch heutzutage mehr als die Hälfte aller Verfahren eingestellt, auf den Privatklageweg verwiesen oder mit Geldstrafen von 90–250 Tagessätzen sanktioniert wurde,<sup>72</sup> verwundert es nicht, dass das Ernten „fremder Früchte“ in manchen Bereichen (nicht immer aus betriebswirtschaftlichen Erwägungen heraus) zu einem verbreiteten Verhalten geworden ist.<sup>73</sup> Mitunter geht es sogar gänzlich unentgeltlich, beispielsweise durch Aneignung fremden (Haus-)Mülls oder „entsorgter“ Prototypen.<sup>74</sup>

### 3. Aktuelle Gefahrensituation

Gesteigerter Aufmerksamkeit bedürfen Geschäftsgeheimnisse vor allem aus zwei **12** Gründen:<sup>75</sup> wegen ihrer immensen Vielfältigkeit und ihrer besonderen **Anfälligkeit** für immer neue Angriffsweisen. Neue zukunftssträchtige Industrien und die inzwischen nahezu überall einzusetzenden **Informationstechnologien**<sup>76</sup> formen ein erschöpfliches Gefahrenbündel, dessen Gefährdungspotenzial durch die Themenbereiche „Big Data“<sup>77</sup> und „Industrie 4.0“<sup>78</sup> auf eine höhere Stufe gehoben wird.

#### a) Vielfalt der Angriffsziele

Die Angriffsziele der unerlaubten Erlangung, Offenlegung und Nutzung fremder **13** geheimer Kenntnisse expandieren gleichsam spiegelbildlich leicht zeitverschoben zur jeweiligen wirtschaftlichen Entwicklung mit zunehmender Geschwindigkeit. Waren **früher** technische Geheimnisse der chemischen, pharmazeutischen oder Maschinenbauindustrie die bevorzugten Angriffsziele privatseitig betriebener Spionagetätigkeit,<sup>79</sup> so sind in den letzten Jahrzehnten eine ganze Reihe **neuer**

72 *Brammsen*, Lauterkeitsstrafrecht, Vor §§ 17–19 Rn. 7; *Kilchling*, GSZ 2020, 57, 59 f., beide mwN.

73 Zur Autobranche WiWo 23/2018, S. 66 ff.; s. auch *Hambach/Berberich*, ZfWG 2017, 60 ff.

74 Zum „Trash Trawling“ als alternativer Informationsbeschaffung Hbl. v. 4.7.2000, Nr. 126, 26; WiWo 14/2018, S. 50 f.; 21/2004, S. 80; *Schaaf*, S. 55 f.; zur Aneignung „entsorgter“ Lehrwerkstatt-Prototypen *Denzer*, Hbl. v. 2.2.1998, Nr. 22, 45; s. auch BGH(Z), GRUR 2009, 1075 Rn. 1, 20 ff. – Betriebsbeobachtung.

75 Anschaulich *Brandau/Rehaag*, Kap. 2 Rn. 143 ff.; komprimierter *McGuire*, GRUR 2016, 1000 f.

76 Eingehender *Brammsen*, ZIP 2016, 2193, 2197 ff.; *Drescher*, S. 98 ff., 105 ff.; *Kochheim*, Rn. 180 ff., 243 ff.; s. auch BVerfGE 120, 274, 303 ff.

77 Dazu einführend: *Amstutz*, AcP 2018, 438 ff.; *Karikari*, S. 1 ff., 25 ff., 216 ff.; *Scheja*, CR 2018, 485 ff.; *Stender-Vorwachs/Steeger*, NJOZ 2018, 1361 ff.; *Wiebe/Schur*, ZUM 2017, 461 ff.; *Zech*, GRUR 2015, 1151 ff.; gebietsübergreifend *Taeger* (Hrsg.), Big Data & Co, 2014; *Lederer*, S. 226 ff. und passim; *Otte et al.*, Von Data Mining bis Big Data, 2020, S. 33 f. u. passim.

78 Statt vieler beispielhaft *Müllmann*, WRP 2018, 1177 ff.; *Söbbing*, S. 1 ff., 28 ff., 41 ff.; *Staffler*, NZWiSt 2018, 269 ff.

79 *Koenig&Bauer/Hebenstreit Metal Decorating*, WiWo 14/2018, S. 50 f.; *Procter&Gamble/Unilever*, WiWo 21/2004, S. 80; *Unilever/Dove*, Hbl. v. 28.4.2004, Nr. 82, 16; s. auch ÖOGH, WRP 2021, 503 Rn. 2 ff. – Flüsteraggregat; OLG Stuttgart, WRP 2021, 242 Rn. 2 ff., 110 ff. – Schaumstoffsysteme; OLG Düsseldorf, BeckRS 2020, 188 Rn. 51 ff. – Spritzgießwerkzeuge; Nordbayerischer Kurier v. 26.4.2019, Nr. 97, 8.

## Einl. A Geschäftsgeheimnisschutz – Daten und Fakten

**Dienstleistungs-, Industrie- und Produktionsbereiche** hinzugekommen:<sup>80</sup> Der Anlagen- und Betonbau,<sup>81</sup> die Datenbank-, Steuerungs- und Prüftechnik,<sup>82</sup> die Finanzbranche,<sup>83</sup> die Material-, Medizin-<sup>84</sup> und Umwelttechnik,<sup>85</sup> der Energiesektor mit der Solar- und Windenergie,<sup>86</sup> die Beschichtungs- und Biotechnologie<sup>87</sup> sowie die Produkte, Produktionen und Geschäftsmethoden der Flugzeug-<sup>88</sup> und Audioindustrie.<sup>89</sup> **Insbesondere** sind es aber die Fahr(zeug)-,<sup>90</sup> die Computer-<sup>91</sup> und die Telekommunikationsindustrie,<sup>92</sup> die aktuell den „Spionagemarkt“ absolut dominieren. Mit ihren hohen Entwicklungskosten und einem regelmäßig begrenzten Nutzungszeitraum stellen heute Computerprogramme (auch für maschinelles Lernen),<sup>93</sup> Mikrochips,<sup>94</sup> Diagnosetests,<sup>95</sup> Kodiervverfahren<sup>96</sup> uam. neben den klassischen Bran-

80 Komprimierter Überblick auch bei *Drescher*, S. 79 ff.

81 *Bitkom*, S. 17; OLG Hamm, WRP 2021, 223 Rn. 158, 160 – Stopfaggregate; Lanxess, Hbl. v. 16./17.11.2018, Nr. 222, 25; Nippon Steel/Posco, GRUR Int. 2017, 639; Rieder Faserbeton, WiWo 25/2010, S. 44, 48; s. auch BGH(Z), GRUR 2010, 536 Rn. 47 ff. – Modulgerüst II. Beispielhaft zur Einbeziehung von Gebäudedatenmodellen (Building Information Modeling, BIM) *Reinholz/Kraushaar*, K&R 2020, 788, 796 ff.

82 AMSC/Sinovel, <https://de.wikipedia.org/wiki/Sinovel>; Bosch (Fn. 70); s. auch BGH, wistra 2017, 101 Rn. 29 ff.; OLG Stuttgart, Die Justiz 2016, 382 Rn. 11 ff.; Hbl. v. 8.9.2010, Nr. 173, 54; WiWo 25/2010, S. 44 ff.

83 Hbl. v. 10.12.2019, Nr. 238, 28 f.; 28.1.2010, Nr. 19, 66; WiWo 25/2010, S. 44, 46; *KPMG, e-Crime*, S. 13 f.

84 Compware Medical (Fn. 70); S-Cape/Eizo Nanao, Hbl. v. 19.5.2014, Nr. 95, 18; BGH(Z), GRUR 2018, 1161 Rn. 28 ff. – Hohlfasermembran II.; BGH(Z), WRP 2018, 424 ff. u. 429 ff. – Knochenzement I u. II; BGH(Z), GRUR 2012, 1048 Rn. 13 ff. – Movicol.

85 Hbl. v. 28.1.2010, Nr. 19, 66; WiWo 25/2010, S. 44, 47.

86 AMSC/Sinovel, <https://de.wikipedia.org/wiki/Sinovel>; Enercon (Fn. 57); Hbl. v. 23./24.7.2010, Nr. 140, 20 f., 24 f.

87 Hbl. v. 7.10.2002, Nr. 192, 10.

88 Airbus, WiWo 25/2010, S. 44, 48.

89 Clearaudio, WiWo 43/2011, S. 102 f.

90 *Bitkom*, S. 17; A2Mac1/GWM (Fn. 56); Bosch (Fn. 70); Daimler/Yaxing-Benz, WiWo 51/2004, S. 46, 48 f.; Ferrari/McLaren, Hbl. v. 14.9.2007, Nr. 178, 28; Mitec/Ford (Fn. 58); Opel/VW (Fn. 61); Renault (Fn. 62); VW/FAW (Fn. 66); Erlikönige, Hbl. v. 1.11.2004, Nr. 212, 13; PKW-Kennzeichnung „Scheibengravur“, Spiegel 46/1994, 250 ff.; Fahrrad „Mifa/Hero Cycles“, Hbl. v. 2.–5.10.2014, Nr. 190, 19.

91 Uni Data/IT Competence, SZ v. 31.3.2001, Nr. 76, 63; Oracle/SAP (Fn. 60); Toshiba/Lexar Media, Hbl. v. 29.3.2005, Nr. 60, 14. Weitere Fälle: Hbl. v. 10./11.1.2014, Nr. 7, 52 f.; 7.7.2011, Nr. 129, 23; SZ v. 18.7.2012, 20.

92 Himax, OGH Taiwan, GRUR Int. 2018, 576; Huawei, Hbl. v. 26.8.2010, Nr. 164, 28; Lucent, Hbl. v. 4./5.5.2001, Nr. 86, 24; NTT Docomo, GRUR Int. 2017, 601 ff. Weitere Fälle: OLG Karlsruhe, WRP 2016, 751 Rn. 26 ff.; Hbl. v. 10./11.1.2014, Nr. 7, 52 f.; 7.7.2011, Nr. 129, 23; 5.2.2010, Nr. 25, 27; SZ v. 18.7.2012, 20.

93 Zu ihrem Geheimnischarakter BGH, BeckRS 2016, 17444 Rn. 36; OLG Stuttgart, BeckRS 2016, 52686 Rn. 11; schweiz. BGE, 111 IV 74, 79 f. Zu sog. „Machine Learning-Modellen“ prägnant *Apel/Kaulartz*, RD 2020, 24 ff. mwN.

94 Hbl. v. 5.2.2010, Nr. 25, 27; 29.3.2005, Nr. 60, 14; 9.3.2005, Nr. 48, B6.

95 Zu seltsamen Verhaltensweisen bei der Entwicklung eines Testverfahrens für den Hepatitis C Virus v. *Kekule*, Die Zeit 44/1989, 88.

96 ZB bei PKW-Kennzeichnungssystemen, Spiegel 46/1994, 250 ff.

chen Chemie, Gesundheit, Pharma und Handel<sup>97</sup> das mit Abstand größte Kontingent dar.<sup>98</sup> Trotz dieser unübersehbaren Techniklastigkeit finden immer wieder aber auch „klassische“ **Geschäftsgeheimnisse** wie Geschäftsunterlagen das Interesse unbefugter Dritter.<sup>99</sup> Spionage- und Verratsfälle wie „Amazon-BiblioFind“,<sup>100</sup> „Bankhaus Oddo Seydler/Yoc AG“,<sup>101</sup> „Bombardier“,<sup>102</sup> „Carto Travel/Mair Dumont“,<sup>103</sup> „CeWe Color/medienfabrik Gütersloh“,<sup>104</sup> „Coca-Cola“,<sup>105</sup> „Kirch/Breuer“,<sup>106</sup> „Mars“ (Fn. 70), „MLP/Simon“,<sup>107</sup> „Nike“ (Fn. 70), „Opel/VW“ (Fn. 61), „Oracle/SAP“ (Fn. 60), „Pfleiderer/Noe“,<sup>108</sup> „Rundstedt/Kienbaum“,<sup>109</sup> „S-Cape/Eizo Nanao“ (Fn. 84), „Siemens/Dassault“,<sup>110</sup> „Software AG“,<sup>111</sup> „Transrapid“<sup>112</sup> und „TWL (Technische Werke Ludwigshafen)“<sup>113</sup> sind dafür ein recht bedectes Beispiel.<sup>114</sup>

Das Interesse der nachrichtendienstlich organisierten **Industriespionage fremder Staaten** liegt traditionell schwerpunktmäßig auf der Rüstungs-, Luft- und Raumfahrtindustrie oder Energieunternehmen.<sup>115</sup> Neue „Geschäftsfelder“ wie die Auto- und Computerindustrie, die Finanzbranche, Lasertechnologie, Telekommunikation und – besonders aktuell – die Pharmaindustrie (Stichwort: Covid-19) werden daneben zunehmend verstärkt zur Beschaffung von „High-Tech-Wissen“ einbezogen,<sup>116</sup> was letztlich auch die bundesdeutsche Auflistung der schutzrelevanten „kritischen Infrastrukturen“ Energie, Informationstechnik, Telekommunikation, Transport,

97 Heraeus/Biomet, GRUR Int. 2018, 600 ff.; Lanxess, Hbl. v. 16./17./18.11.2018, Nr. 222, 25.

98 *Bitkom*, S. 17; *Corporate Trust*, 2014, S. 8, 17.

99 Eingehend zu Bedeutung und Schutz von Geschäftsgeheimnissen im Mittelstand *Nienaber*, Rn. 115 ff., 225 ff. u. passim.

100 Hbl. v. 7.3.2001, Nr. 47, 27.

101 WiWo 40/2015, S. 71.

102 WiWo 51/2004, S. 48 ff.; Hbl. v. 17.8.2005, Nr. 158, 16.

103 Hbl. v. 22.12.2004, Nr. 249, 15.

104 NRhZ – Flyer 56 v. 8.8.2006.

105 Hbl. v. 6.2.2007, Nr. 26, 10; 15.12.2006, Nr. 243, K 8.

106 BGH, NJW 2006, 830 ff.; s. auch LG Düsseldorf, NStZ-RR 2011, 84, 85; Hbl. v. 28.1.2014, Nr. 19, 26 f.

107 Hbl. v. 8.7.2003, Nr. 128, 16.

108 Hbl. v. 23.1.2008, Nr. 16, 17.

109 Hbl. v. 2.2.2012, Nr. 24, 5.

110 Hbl. v. 4.9.2008, Nr. 172, 11.

111 WiWo 44/2020, S. 52 ff.

112 WiWo 51/2004, S. 46 ff.; 50/2004, S. 8.

113 WiWo 44/2020, S. 52, 54; <https://eh-cybercrime/2020/09/09/cybersicherheit-in-unternehmen/>.

114 Zu den Angriffsbereichen Einkauf, Vertrieb, Finanzen und Personal komprimiert *Bitkom*, S. 20 f.; *Corporate Trust*, 2014, S. 9, 26 f.; *Drescher*, S. 77; *Ernst&Young*, 2018, S. 15; *KPMG*, e-Crime, S. 31 und *Tatort*, S. 16 f.; zum US-EEA *Johnson/Kierkus/Barton*, I.P.Q. 2017, 152, 162. Aktuell OLG Stuttgart, WRP 2021, 242 Rn. 176 ff. – Schaumstoffsysteme; LAG Frankfurt, ECLI:DE:LAGHE:2020:0527.18SA1109.19.00, Rn. 56 f.; Mars (Fn. 70) und Hbl. v. 10.12.2019, Nr. 238, 28 f.; Nordbayerischer Kurier v. 26.4.2019, Nr. 97, 8.

115 Verfassungsschutzbericht 2016, 265; 2014, 144 f., 231; Hbl. v. 28.1.2015, Nr. 19, 26 f.

116 WiWo 38/2020, S. 8; Verfassungsschutzbericht 2016, 261, 265; Hbl. v. 2./3.5.2014, Nr. 84, 15; *Drescher*, S. 184 ff.; *KPMG*, e-Crime, S. 17 ff.; *Söhner*, KJ 2015, 56 ff.; *Ulfkotte*, S. 75 ff.

## Einl. A Geschäftsgeheimnisschutz – Daten und Fakten

Verkehr, Wasser, Ernährung, Gesundheit, Finanz- und Versicherungswesen bestätigt.<sup>117</sup> Hier finden mitunter auch „Joint Ventures“ als operative Geschäftsmodelle Verwendung, vor allem in osteuropäischen, asiatischen und „Dritte-Welt-Ländern“.<sup>118</sup> Ihnen treten verstärkt verdeckte Gefahrenquellen in Gestalt ausländischer Produktprüfungsverfahren oder die zunehmend befürwortete Lizenzierung von geheimem Know-how an „rechtskreisfremde“ Konkurrenz hilfreich zur Seite.<sup>119</sup> So verwundert es nicht, dass die Ausnutzung fremder Geschäftsgeheimnisse ungeachtet ihrer Gegenständlichkeit inzwischen extrem verbreitet ist – allseits herrscht Hochkonjunktur. Staatlicherseits kann ihnen inzwischen nur noch durch ein zunehmend wachsendes Wirtschaftssicherheitsrecht von (Export-, Investitions-, Personal- und sonstigen) Kontroll- und Prüfungsverfahren, Schutzhilfen usw. begegnet werden, dessen Ausmaß sich dem der Unternehmensbetreiber immer mehr anpasst.<sup>120</sup>

### b) Aktuelle Angriffsweisen

#### aa) Faktische Zugriffsmethoden

- 15 In allen Bereichen des Dienstleistungsgewerbes, der Warenproduktion, des Vertriebs, der Freizeitindustrie usw. finden sich heute eine Vielzahl datenspeichernder, datenübertragender und datenverarbeitender Geräte, die zahllose **Angriffswege** auf fremde geheime Datenbestände eröffnen.<sup>121</sup> Deren „unentgeltliche Abtretung“ muss keineswegs eingefordert werden,<sup>122</sup> es geht viel einfacher und unauffälliger. Zum eigentlichen „Einfallstor“ der Daten- und Wirtschaftsspionage ist nämlich, gestützt von und im Verbund mit der mobilen Telekommunikation, erst das Internet geworden:<sup>123</sup> **Abrufen**, Kopieren und Auswerten gespeicherter Daten,<sup>124</sup> **Anzapfen** und Mitschneiden von Gesprächen und Datenübermittlungen (auch mittels Keylogger, Trojaner-Software etc.),<sup>125</sup> **Aufzeichnen** und Rekonstruieren elektronischer

117 Vgl. §§ 4 ff. BSI-KritisVO 2016 idF 1. BSI-KritisÄndVO v. 21.6.2017 (BGBl. I, 1903 ff.).

118 *Hofer/Weiß*, S. 57 ff.

119 CCC-Gütesiegel, WiWo 8/2009, S. 68, 72; Daimler/Yaxing-Benz (Fn. 90); VW/FAW (Fn. 66); Vietz/CNPC (Fn. 64); s. auch *Buxbaum/Cooter*, in: FS Ch. Kirchner, S. 681, 687 ff.

120 Einen aktuellen Überblick über das breite Spektrum additiven staatlichen Geschäftsgeheimnisschutzes geben *Borman/Ludwig*, DÖV 2020, 1061 ff.

121 Neuere Schätzungen: *Bitkom*, S. 15 ff.; *Ernst&Young*, Datenklau 2017, S. 14 f.; *PWC*, 2018, S. 19 ff.

122 Aktuell VW/Prevent, Hbl. v. 19./21.8.2016, Nr. 160, 1, 6 f.; s. auch WiWo 47/2015, S. 40 und 4/2015, S. 50 ff.

123 Instruktiv Hbl. v. 20.10.2014, Nr. 201, 19; 15.2.2012, Nr. 34, 20 f.; WiWo 28/2013, S. 58.

124 *Bitkom*, S. 15; WiWo 27/2011, S. 78 f.; 43/2011, S. 102; Hbl. v. 11./12.2.2011, Nr. 30, 4; BVerfGE 120, 274, 304 ff.; OLG Hamburg, GRUR-RR 2020, 18, 19 f., 21 f. Rn. 7.

125 Hbl. v. 2.3.2004, Nr. 43, 13 (RFID-Funkchips); 16.4.2008, Nr. 74, B6 (GPS-Funkwanzen); 23./24.7.2010, Nr. 140, 24 f. (USB-Sticks); 11.8.2011, Nr. 154, 20 f. (GPRS-Handy); 13./14.9.2013, Nr. 177, 14 (Bluetooth-Handy); WiWo 41/2005, S. 66 f. (Blackberry); 29/2012, S. 42 f.; 49/2010, S. 88 (Smartphone); 28/2013, S. 58 ff.

Abstrahlungen (etwa von Bildschirmterminals),<sup>126</sup> **Ausspähen** von (Kredit-)Kundendateien,<sup>127</sup> **„Cloud-Computing“**<sup>128</sup> (ins außereuropäische Ausland),<sup>129</sup> (auch staatliches) **„Hacken“** und Verwanzen<sup>130</sup> einschließlich Datendiebstahl und Darknet-Handel,<sup>131</sup> **Kenntnisverschaffen** und -verwerten bei verdeckter (Fernwartungs-) Schadstoffsoftware,<sup>132</sup> **Privatnutzung** von Diensthardware und umgekehrt,<sup>133</sup> **„Outsourcing“** von Datenverarbeitungsvorgängen,<sup>134</sup> **„Social media accounts“**<sup>135</sup> und vieles andere mehr bieten ein riesiges Reservoir für unauffällige externe Zugriffsmöglichkeiten.<sup>136</sup> Der klassische **Sachdiebstahl** von Gegenständen wie Festplatten, Handys, Laptops, Notebooks, Musterprozessoren und dergleichen hat deswegen heute allenfalls eine untergeordnete Bedeutung.<sup>137</sup>

bb) Erlaubte Zugriffe

Neben dem vermehrten Auftreten neuer wertversprechender Angriffsziele und dem in etwa zeitgleichen Entstehen immer variantenreicherer datentechnischer Zugriffsmöglichkeiten hat sich in den letzten Jahrzehnten ein weiterer folgenreicher Gefahrenherd entwickelt, dessen Verbreitung längst die Dimensionen „faktischer“ Geheimheitsdurchbrechungen erreicht hat. Angesprochen sind damit jene in den verschiedensten Ausgestaltungen anzutreffenden Berechtigungen, die anderen Per-

16

- 126 WiWo 49/2010, S. 87; Hbl. v. 11.12.2006, Nr. 239, 10 („Kraftwerk-Power Monitoring“); BVerfGE 120, 274, 310.
- 127 Hbl. v. 10.12.2019, Nr. 238, 28 f.; 2./3./4.8.2019, Nr. 147, 26 f. (Capital One); 23.11.2017, Nr. 226, 5 (Yahoo); 10./11.10.2014, Nr. 195, 29 (JP Morgan Chase); 8.5.2014, Nr. 88, 36 f. (Target).
- 128 *Drescher*, S. 120 ff.; Hbl. v. 2.7.2013, Nr. 124, 1, 4 f.; WiWo 30/2017, S. 68 ff. Zum „Cloud-Computing“ *Borges/Meents*, §§ 1 f., 6 ff.; *Busching*, S. 7 ff., 22 ff.; *Henrich*, S. 42 ff., 84 ff. u. passim; *Müller*, S. 33 ff., 48 ff.; *ders.*, DuD 2017, 371 ff.; (speziell zu § 203 StGB) *Cornelius*, StV 2016, 380 ff.; *Müller*, S. 229 ff.; *Wicker*, S. 35 ff., 99 ff., 241 ff. Zu Schutzmaßnahmen *Psaroudakis*, E.I.P.R. 2016, 344 ff.
- 129 *Borges/Meents*, §§ 15 f.; *Voigt*, MMR 2014, 158 ff.
- 130 Instrukтив BVerfGE 120, 274, 301 ff.; Hbl. v. 2.1.2020, Nr. 1, 27; 10.12.2019, Nr. 238, 28 f.; 19.8.2019, Nr. 158, 8 f.; 2./3./4.8.2019, Nr. 147, 26 f.; 15.8.2018, Nr. 156, 18 f.; 9.8.2017, Nr. 152, 16 f.; WiWo 50/2019, S. 75 ff.; 43/2019, S. 53 ff.; 19/2018, S. 38 ff.; 9/2018, S. 60 ff.; 51/2016, S. 17 ff.; *Drescher*, S. 107 ff.; *Schaaf*, S. 19 ff.
- 131 Anschaulich WiWo 44/2020, S. 52 ff.
- 132 *Bitkom*, S. 15 f., 19 f.; Hbl. v. 20.10.2014, Nr. 201, 19; 13./14.9.2013, Nr. 177, 14; WiWo 28/2013, S. 58 ff.; 21/2011, S. 64 ff.
- 133 Sog. „Bring your own device“; zu den Gefahren *Drescher*, S. 112 ff. und *Heldmann*, S. 15 ff., 80 ff. mwN.
- 134 Beispielhafte Angriffe: Hbl. v. 3.12.2018, Nr. 233, 53 (Marriott-Datenbank); 18.5.2010, Nr. 96, 24 (Sony-Datenbank); s. auch *Buxbaum/Cooter*, in: FS Ch. Kirchner, S. 681 ff. zu Unternehmenskooperationen und *Sendzik*, S. 121 ff. Zur Parallelproblematik bei § 203 StGB weiterführend *Conrad/Fechtner*, CR 2013, 137 ff.; *Kahler*, CR 2015, 153 ff.; *Kort*, NStZ 2011, 193 ff.
- 135 Stichwort: Who owns your follower? erläuternd *Surblyte*, GRUR Int. 2016, 1121 ff.
- 136 Ausführliche Zusammenstellungen: BVerfGE 120, 274, 301 ff.; MK-StGB/*Graf*, 3. Aufl. 2017, § 202a Rn. 82 ff., 89 ff.
- 137 Hbl. v. 8.9.2010, Nr. 173, 54; 12./13.8.2005, Nr. 155, K3; 12.4.1990, Nr. 73, 23; WiWo 24/2015, S. 78 f.; 12/2004, S. 86; 32/1997, S. 58; 12/1991, S. 126.

## Einl. A Geschäftsgeheimnisschutz – Daten und Fakten

sonen Zugang zu fremdseitig zugeordneten Geheimheiten gestatten. In nahezu allen Rechtsgebieten bzw. Lebensgebieten in immens vielfältigen Erscheinungsformen vertreten, haben sie inzwischen eine Häufigkeit erreicht, die es rechtfertigt, von einem nur noch „durchlöcherter“ oder sogar ausgeschlossenen Geheimnisschutz zu reden.<sup>138</sup>

- 17 An anderer Stelle bereits systematisch vorgeordnet in einerseits administrative Zugangs- und Verwertungsbefugnisse und andererseits privatseitige absolute oder relative Informations-, Transparenz- und Umsetzungsrechte dargestellt, ergeben sie in ihrer Gesamtheit ein kaum noch überschaubares Konvolut von Zugriffsregeln, das den grundrechtlich gewährleistenden Geschäftsgeheimnisschutz (→ § 1 Rn. 19) auszuhöhlen droht. Auf ihre dortigen Zusammenstellungen ist schon aus Raumgründen zu verweisen.<sup>139</sup> Ihnen sind zur weiteren Abrundung und Aktualisierung der Bandbreite der ungebrochenen gesetzgeberischen Umformungs- bzw. Neuordnungsbestrebungen einige besonders gewichtige Neuerungen hinzuzufügen.
- 18 Absoluter Vorrang bzw. die Tabellenspitze gebührt dabei den Einfügungen des GeschGehG zum sog. „Reverse Engineering“ öffentlich verfügbarer, dh. in den Verkehr gebrachter oder rechtmäßig und ohne Erlangungsverbot besessener Produkte oder Gegenstände (§ 3 Abs. 1 Nr. 2) und des „Whistleblowing“ (§ 5). Gegründet entweder auf „Innovationsförderung“ oder ein „allgemeines öffentliches Interesse“ entziehen beide Freistellungen den betroffenen Geheimnisschutzhabern mit unspezifizierten Generalisierungen jeglichen Rechtsschutz, erklären den Wissensvorsprung mithin allseitig (§ 5 Nr. 1, 2) oder partiell (§ 5 Nr. 3) für vogelfrei. Gleichermaßen genereller Freistellung erfreuen sich nunmehr: Anprangerungen festgestellter Hygienemängel unter Namensnennung<sup>140</sup> durch die öffentliche Verwaltung bei noch nicht einmal abgeschlossenen Verfahren (begrenzt auf eine halbjährige Zeitspanne),<sup>141</sup> die über vorgeschaltete „Compliance-Zwänge“<sup>142</sup> eröffnete Möglichkeit zur hoheitlichen „Indienstnahme“ privater Ermittlungshelfer bei „Internal Investigations“<sup>143</sup> oder die ungebrochen fragwürdigen<sup>144</sup> Praktiken im Umgang mit entwendeten Bankdaten (nunmehr in „Cum-ex-Geschäften“).<sup>145</sup>

138 *Brammsen*, ZIP 2016, 2193: „Durchlöcherter Bestandsschutz“.

139 Vgl. *Brammsen*, ZIP 2016, 2193, 2198 ff.; s. auch *Drescher*, S. 117 ff.

140 Kritisch zu den damit verbundenen Grundrechtseingriffen *Born*, K&R 2021, 13, 15 ff.

141 Vgl. § 40 LFGB idF des 1. Gesetzes zur Änderung des LFGB vom 13.3.2019, der sich inzwischen bereits ersten „Aushebelungsbestrebungen“ seitens der Online-Plattform „Topf Secret“ ausgesetzt sieht; vgl. OVG Münster, BeckRS 2020, 33891; BeckRS 2020, 292 Rn. 24 ff., 60 ff.; *Kluge*, ZLR 2019, 518, 524 ff.; *Lück/Penski*, DÖV 2020, 506, 510 ff., beide mwN. Zu Parallelen im Tierschutzrecht vgl. OVG Lüneburg v. 24.10.2017 – 10 LA 90/16 – juris (Rn. 17 ff., 26 ff.).

142 Die Gefahren frühzeitiger vorvertraglicher Kenntnisweitergaben an mögliche künftige externe (Sonder-)Berater veranschaulicht der Fall „VW/Freeh“; vgl. Hbl. v. 7./8./9.2.2020, Nr. 27, 63.

143 Zu dieser Einspannung *privater Ermittlungshelfer in staatliche Ermittlungstätigkeiten* BVerfG, NJW 2018, 2395 m. Anm. *Brammsen*, EWiR 2018, 669 f.; zu möglichen datenschutzrechtlichen Konsequenzen im Arbeitsrecht (Reichweite der Anonymität) anschaulich LAG Baden-Württemberg, NZA-RR 2019, 242 Rn. 160 ff., 178 ff. m. zust. Anm. *Fuhlrott*, NZA-RR 2019, 251, 252.

144 *Breitenbach*, S. 56 ff., 128 ff., 308 ff.; zuletzt FG Köln, BeckRS 2020, 41019 Rn. 85 ff.

145 *Sarazin/Seitz*, Hbl. v. 26.3.2019, Nr. 60, 30.