

Industriespionage

HERAUSGEGEBEN VON

Dr. Stefan Albiez

MMag. Thomas Hartl

LexisNexis'

Inhaltsverzeichnis

| | |
|------------------------------|--------------|
| Vorwort der Herausgeber..... | V |
| Abkürzungsverzeichnis..... | XV |
| Autorenverzeichnis..... | 1..... ; XXI |

Die wirtschaftliche Dimension und Bedeutung von Wirtschaftsspionage

| | |
|--|----------|
| (Philip Aumüller/Alfred Heiter)..... | 1 |
| 1. Die wirtschaftliche Dimension der Wirtschaftsspionage und strafrechtliche Ableitungen de lege ferenda..... | -..... 1 |
| 1.1. Die wirtschaftliche Dimension der Wirtschaftsspionage | 1 |
| 1.1.1. Die Bedeutung wissensbasierter Vermögenswerte in Unternehmen..... | 1 |
| 1.1.2. Der Schutz von Geschäftsgeheimnissen als Innovationsmotor und Grundlage für Kooperation..... | 2 |
| 1.1.3. Faktische Ausgangslage..... | 3 |
| 1.1.4. Formen der Wirtschaftsspionage..... | 4 |
| 1.1.4.1. Wirtschaftsspionage unter Ausnutzung von Humankapital..... | 4 |
| 1.1.4.1.1. Untermehmensinterne Wirtschaftsspionage..... | 4 |
| 1.1.4.1.2. Untermehmensexteme Wirtschaftsspionage..... | 5 |
| 1.1.4.2. Digitale Formen der Wirtschaftsspionage..... | 7 |
| 1.1.4.2.1. Malware..... | 7 |
| 1.1.4.2.2. Keylogger..... | 8 |
| 1.1.4.2.3. Phishing Mail..... | 8 |
| 1.1.4.2.4. Apps..... | 8 |
| 1.1.4.2.5. Cloud-Computing..... | 9 |
| 1.1.4.2.6. Darknet..... | 9 |
| 1.1.4.2.7. Abhörgeräte..... | 10 |
| 1.1.5. Fallstudien..... | 10 |
| 1.1.5.1. Fall 1..... | 10 |
| 1.1.5.2. Fall 2..... | 10 |
| 1.1.5.3. Fall 3..... | 11 |
| 1.1.5.4. Fall 4..... | 11 |
| 1.1.5.5. Fall 5..... | 11 |
| 1.1.5.6. Fall 6..... | 11 |
| 1.1.5.7. Fall 7..... | 12 |
| 1.1.5.8. Fall 8..... | 12 |
| 1.2. Strafrechtliche Ableitungen de lege ferenda..... | 12 |
| 1.2.1. Materielle rechtliche Fragen..... | 13 |
| 1.2.1.1. Sedes Material im UWG und sachlicher Anwendungsbereich..... | 13 |
| 1.2.1.2. Im europäischen und internationalen Vergleich zu niedriger Strafraumen..... | 14 |
| 1.2.2. Prozessuale Fragen..... | 16 |
| 1.2.2.1. Privatanklage- vs Offizialdelikt..... | 16 |
| 1.2.2.2. Zuständige Staatsanwaltschaft..... | 18 |
| 1.2.2.3. Zuständiges Gericht..... | 19 |

Inhaltsverzeichnis

| | |
|---|-----------|
| 1.3. Conclusio und Ausblick..... | 20 |
| 2. Literatur (Auswahl)..... | 21 |
| Der Schutz vor Wirtschaftsspionage aus strafrechtlicher und zivilrechtlicher Sicht (Stefan Albiez/Thomas Hartl)..... | 23 |
| 1. Was sind Geschäfts- und Betriebsgeheimnisse?..... | 23 |
| 2. Der strafrechtliche Schutz von Geschäftsgeheimnissen..... | 26 |
| 2.1. Die Tatbestände des allgemeinen Strafgesetzbuchs..... | 26 |
| 2.1.1. § 122 StGB: Verletzung eines Geschäfts- oder Betriebsgeheimnisses | 27 |
| 2.1.2. § 123 StGB: Auskundschaften eines Geschäfts- oder Betriebsgeheimnisses..... | 29 |
| 2.1.3. § 124 StGB: Auskundschaften eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslands..... | 30 |
| 2.2. Spezialgesetzliche Strafbestimmungen zum Geheimnisschutz | 32 |
| 2.2.1. § 11 UWG: Verletzung von Geschäfts- oder Betriebsgeheimnissen..... | 32 |
| 2.2.2. § 12 UWG: Missbrauch anvertrauter Vorlagen und technischer Vorschriften..... | 34 |
| 2.2.3. § 101 BWG: Verletzung des Bankgeheimnisses..... | 35 |
| 3. Leitfaden für die Anspruchsverfolgung..... | 35 |
| 3.1. Anspruchsverfolgung im Strafverfahren..... | 36 |
| 3.1.1. Ablauf des Strafverfahrens - Überblick..... | 36 |
| 3.1.2. Besonderheiten bei Privatanklagedelikten..... | 37 |
| 3.1.3. Praxisleitfaden Privatbeteiligung..... | 39 |
| 3.2. Anspruchsverfolgung im Zivilverfahren..... | 43 |
| 3.2.1. Zivilrechtliche Ansprüche zum Schutz von Geschäftsgeheimnissen..... | 43 |
| 3.2.1.1. Überblick..... | 43 |
| 3.2.1.2. Rechtswidrige Handlungen..... | 43 |
| 3.2.1.3. Rechtmäßige Handlungen..... | 44 |
| 3.2.1.4. Unterlassung..... | 45 |
| 3.2.1.5. Beseitigung..... | 46 |
| 3.2.1.6. Angemessene Entschädigung anstelle von Unterlassung/ Beseitigung..... | 46 |
| 3.2.1.7. Schadenersatz..... | 47 |
| 4. Verfahrensrechtlicher Schutz von Geschäftsgeheimnissen..... | 47 |
| 4.1. Aussageverweigerung..... | 49 |
| 4.2. Verweigerung der Urkundenvorlage..... | 50 |
| 4.3. Ausschluss der Öffentlichkeit im Zivil- und Strafverfahren..... | 51 |
| 5. Literatur (Auswahl) | 52 |
| Der neue materielle rechtliche Schutz von Geschäftsgeheimnissen (Ivo Rungg/Adrian Ramon Ploner) | 53 |
| 1. Einleitung..... | 53 |
| 2. Grundlagen..... | 53 |

| | | |
|----------|---|----|
| 3. | Der neue materiellrechtliche Schutz von Geschäftsgeheimnissen..... | 55 |
| 3.1. | Rechtswidrige Tathandlungen..... | 55 |
| 3.1.1. | Rechtswidriger Erwerb..... | 56 |
| 3.1.2. | Rechtswidrige Nutzung oder Offenlegung..... | 59 |
| 3.1.3. | Exkurs: Vertraulichkeitsvereinbarung und Geschäftsgeheimnisse..... | 61 |
| 3.1.3.1. | Entsprechende und angemessene Geheimhaltungsmaßnahme..... | 61 |
| 3.1.3.2. | Zulässige Weitergabe von Informationen..... | 62 |
| 3.1.3.3. | Bestimmungen zum „Reverse Engineering“..... | 63 |
| 3.1.4. | Erwerb, Nutzung oder Offenlegung durch eine andere Person..... | 63 |
| 3.1.5. | Rechtsverletzende Produkte..... | 64 |
| 3.2. | Rechtmäßige Tathandlungen..... | 65 |
| 3.2.1. | Rechtmäßiger Erwerb, Nutzung oder Offenlegung durch Zustimmung..... | 66 |
| 3.2.2. | Rechtmäßiger Erwerb..... | 66 |
| 3.3. | Ausnahmen..... | 69 |
| 4. | Abgrenzung zu den Immaterialgüterrechten..... | 72 |
| 5. | Literatur (Auswahl) | 75 |

Datenschutz und Wirtschaftsspionage (Angelika Pallwein-Prettner/Stefan Frank-Woda) 77

| | | |
|----------|---|----|
| 1. | Datenschutzrechtliche Aspekte interner Untersuchungen..... | 77 |
| 1.1. | Einleitung..... | 77 |
| 1.2. | Rechtliche Grundlagen..... | 78 |
| 1.2.1. | Das neue Datenschutzregime der DS-GVO..... | 78 |
| 1.2.2. | Was sind personenbezogene Daten?..... | 78 |
| 1.2.2.1. | Allgemein..... | 78 |
| 1.2.2.2. | Besondere Kategorien personenbezogener Daten..... | 79 |
| 1.2.2.3. | Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten..... | 80 |
| 1.2.3. | Rollenverteilung im Datenschutz..... | 81 |
| 1.2.3.1. | Verantwortlicher..... | 81 |
| 1.2.3.2. | Auftragsverarbeiter..... | 81 |
| 1.2.4. | Grundsätze der Datenverarbeitung..... | 81 |
| 1.2.5. | Verbotsprinzip/Erlaubnistatbestände..... | 82 |
| 1.2.6. | Grundlegende Pflichten des Verantwortlichen..... | 83 |
| 1.2.6.1. | Information an betroffene Personen..... | 83 |
| 1.2.6.2. | Verzeichnis der Verarbeitungstätigkeiten..... | 84 |
| 1.2.6.3. | Datenschutz-Folgenabschätzung (DSFA)..... | 84 |
| 1.2.6.4. | Technische und organisatorische Sicherheitsmaßnahmen..... | 86 |
| 1.2.6.5. | Auftragsverarbeitungsvertrag..... | 86 |
| 1.2.7. | Rechte der Betroffenen..... | 87 |
| 1.2.7.1. | Auskunft..... | 87 |
| 1.2.7.2. | Löschung..... | 88 |
| 1.2.7.3. | Widerspruch..... | 88 |
| 1.2.8. | Datenverarbeitung im Beschäftigungskontext..... | 89 |
| 1.2.8.1. | Grundlagen..... | 89 |
| 1.2.8.2. | Betriebsvereinbarungen..... | 89 |

Inhaltsverzeichnis

| | |
|--|------------|
| 1.2.9. Strafen..... | 91 |
| 1.2.9.1. Strafhöhe..... | 91 |
| 1.2.9.2. Haftung..... | 92 |
| 1.3. Discovery..... | 92 |
| 1.3.1. Allgemeines..... | 92 |
| 1.3.2. Videoüberwachung..... | 93 |
| 1.3.2.1. Allgemeines/Einsatzbereich..... | 93 |
| 1.3.2.2. Zulässigkeit und Voraussetzungen..... | 94 |
| 1.3.2.3. Sicherheitsmaßnahmen und Kennzeichnung..... | 95 |
| 1.3.3. Whistleblowing-Systeme..... | 96 |
| 1.3.3.1. Allgemeines/Einsatzbereich..... | 96 |
| 1.3.3.2. Zulässigkeit..... | 97 |
| 1.3.3.3. Umsetzung..... | 100 |
| 1.4. Ermittlung und Reaktion..... | 100 |
| 1.4.1. Interne Untersuchung..... | 100 |
| 1.4.2. Übermittlung von personenbezogenen Daten..... | 102 |
| 1.4.2.1. Zulässigkeit..... | 102 |
| 1.4.2.2. Transfer in Drittstaaten..... | 104 |
| 1.4.3. Data Breach Notification..... | 106 |
| 1.5. Zusammenfassung..... | 108 |
| 2. Literatur (Auswahl)..... | 108 |
| Besonderheiten des Computerstrafrechts (Clemens Thiele)..... | 111 |
| 1. Einleitung..... | 111 |
| 2. Grundlagen und Überblick..... | 111 |
| 3. Grundbegriffe des Computerstrafrechts..... | 113 |
| 3.1. Hardware..... | 113 |
| 3.2. Software..... | 113 |
| 3.3. Hacking..... | 114 |
| 3.4. Kriminalpolitische Aspekte und Kritik..... | 115 |
| 4. Angriffe auf Wirtschaftsdaten und Computersysteme..... | 116 |
| 4.1. Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB)..... | 116 |
| 4.2. Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB)..... | 119 |
| 4.3. Missbräuchliches Abfangen von Daten (§ 119a StGB)..... | 122 |
| 4.4. Missbrauch von Tonaufnahme- oder Abhörgeräten (§ 120 StGB)..... | 125 |
| 5. Störung und Beschädigungen von Computersystemen..... | 127 |
| 5.1. Datenbeschädigung (§ 126a StGB)..... | 127 |
| 5.2. Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB)..... | 131 |
| 5.3. Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB)..... | 133 |
| 6. Computerbezogener Betrug und Datenfälschung..... | 136 |
| 6.1. Betrügerischer Datenverarbeitungsmissbrauch (§ 148a StGB)..... | 137 |
| 6.2. Datenfälschung (§ 225a StGB)..... | 142 |
| 7. Verstoß gegen das Zugangskontrollgesetz..... | 146 |

| | |
|--|------------|
| 8. Prozessuale Aspekte..... | 149 |
| 8.1. Zuständigkeit und Opferbegriff..... | 149 |
| 8.2. Einstellung und Diversion..... | 150 |
| 8.3. Akteneinsicht..... | 150 |
| 8.4. Strafzumessungsgesichtspunkte..... | 151 |
| 8.5. Einziehung..... | 151 |
| 8.6. Verbandsverantwortlichkeit..... | 151 |
| 9. Gerichtliches Computerstrafverfahren..... | 152 |
| 9.1. Inländische Gerichtsbarkeit..... | 152 |
| 9.2. Zuständigkeit und Verfahrensgang..... | 153 |
| 9.3. Strafgerichtlicher Instanzenzug..... | 154 |
| 10. Doppelverfolgungsverbot..... | 155 |
| 10.1. Strafcharakter der Sanktion..... | 155 |
| 10.2. Identität..... | 157 |
| 10.3. Keine Sperrwirkung..... | 157 |
| 11. Checkliste | 158 |
| 12. Literatur (Auswahl)..... | 159 |
| IT-Security (Benjamin Böck)..... | 161 |
| 1. Einleitung..... | 161 |
| 2. Wer sind Ihre Feinde? | 161 |
| 2.1. Weltweite Überwachung von Internet und Kommunikation..... | 162 |
| 3. Erkennung und Abwehr von Industriespionage..... | 163 |
| 3.1. Wesentliche Prinzipien der Informationssicherheit..... | 163 |
| 3.1.1. Principle of least Privilege/Need-to-know..... | 163 |
| 3.1.2. Blacklisting und Whitelisting..... | 163 |
| 3.1.3. Responsible Disclosure | 164 |
| 3.2. Technische Schutzmaßnahmen..... | 165 |
| 3.2.1. IDS/IPS..... | 165 |
| 3.2.2. Web Application Firewall (WAF)..... | 166 |
| 3.2.3. Security Information and Event Management (SIEM)..... | 166 |
| 3.2.4. Durchführung von Penetrationstests..... | 167 |
| 3.2.5. Verteidigung gegen Advanced Persistent Threats (APT)..... | 168 |
| 3.2.6. Sicherer Fernzugriff..... | 169 |
| 3.3. Umgang mit Schwachstellen..... | 170 |
| 3.3.1. Kontrolle des Handels mit Schwachstellen..... | 170 |
| 3.3.2. Open Source..... | 171 |
| 3.4. Angriffe auf den „Faktor Mensch“..... | 173 |
| 3.4.1. Social Engineering..... | 173 |
| 4. Aufbau eines Informationssicherheitsmanagementsystems (ISMS)..... | 174 |
| 4.1. ISO/IEC 27001 | 174 |
| 4.2. ISO/IEC 27002..... | 176 |
| 5. Checkliste Industriespionage: IT-Security..... | 187 |
| 5.1. Das Wichtigste zuerst..... | 187 |
| 5.2. Der „Faktor Mensch“..... | 188 |
| 5.3. Technische Sicherheitsmaßnahmen | 189 |

5.4. Physische Sicherheit..... 190
 5.5. Umgang mit Schwachstellen..... 192
 5.6. Kryptografische Verschlüsselungsverfahren.....1 192
 6. Zusammenfassung.....194

Arbeitsrechtliche Aspekte des Geheimnisschutzes (Saskia Albiez).....197

1. Einleitung..... 197
 2. Gesetzliche Verschwiegenheitspflicht und deren Ausnahmen..... 198
 2.1. Verschwiegenheitspflicht aufgrund Treuepflicht..... 198
 2.2. Informationsrecht der Arbeitnehmer..... 198
 2.3. Whistleblowing..... 199
 2.4. Aufgaben der Arbeitnehmervertreter..... 200
 3. Notwendigkeit eines strukturierten Know-how-Schutzes..... 200
 3.1. Angemessene Geheimhaltungsmaßnahmen..... 200
 3.2. Abgrenzungsfragen..... 201
 3.3. Mehrschichtiges Schutzsystem..... 201
 3.3.1. Sensibilisierung der Mitarbeiter und Dokumentation der Maßnahmen..... 201
 3.3.2. Kennzeichnung geheimer Informationen..... 202
 3.3.3. Identifikation von Know-how-Trägern..... 202
 3.3.4. Automatisierung von Schutz- und Kontrollsystemen..... 202
 3.3.5. Geheimhaltungsvereinbarungen..... 202
 3.3.5.1. Möglicher Regelungsinhalt und Risiken..... 202
 3.3.5.2. Musterklausel..... 204
 4. Sanktionierung von Verstößen..... 205
 4.1. Mögliche Rechtsfolgen eines Verstoßes..... 205
 4.2. Beendigung des Dienstverhältnisses..... 206
 4.2.1. Geheimnisverletzung als Entlassungsgrund..... 206
 4.2.2. Beispiele aus der Judikatur..... 207
 4.2.3. Formalitäten und Wirkung der Entlassung..... 208
 4.2.4. Beweislast..... 209
 5. Literatur (Auswahl)..... 210

Öffentliches Interesse schaffen und Reputation sichern. Oder: Litigation-Communications bei Wirtschaftsspionage als Erfolgsfaktor (Harald Schiff)..... 211

1. Einleitung..... 211
 1.1. Litigation-Communications - eine Provokation?..... 211
 1.2. Litigation-Communications ist selbstverständlicher strategischer Bestandteil juristischer Auseinandersetzungen..... 212
 1.2.1. Der Anfang von Litigation-Communications 213
 1.2.2. Wozu Litigation-Communications?..... 213
 1.2.2.1. „Man kann nicht nicht kommunizieren!“..... 214
 1.2.2.2. Recht und Medien - zwei Welten..... 214
 1.2.2.2.1. Recht wird wieder moralisch..... 215
 1.2.2.3. Journalisten als wichtige Zielgruppe..... 216

| | | |
|------------|--|------------|
| 1.2.2.4. | Die neue Medienwelt | 216 |
| 1.2.2.4.1. | Im digitalen Zeitalter wird nichts mehr vergessen..... | 217 |
| 1.2.2.4.2. | „Klassische Medien“ verlieren an Glaubwürdigkeit..... | 218 |
| 1.3. | Generelles Ziel von Litigation-Communications..... | 219 |
| 1.3.1. | Kommunikation auch bei Industriespionage? | 220 |
| 1.3.1.1. | Eigentümergeführte Unternehmen und ihre besonderen Herausforderungen..... | 220 |
| 1.3.2. | Der Schutz der Reputation..... | 221 |
| 1.3.3. | Juristischer und öffentlicher Druck auf die Gegner..... | 221 |
| 1.3.4. | Aktiv oder Passiv?..... | 222 |
| 1.3.4.1. | Was für Passiv/Reaktiv spricht..... | 222 |
| 1.3.4.1.1. | Was für Aktiv spricht..... | 222 |
| 1.3.5. | Chancen-Risiken-Analyse | 223 |
| 1.3.6. | Wahrheit oder Unwahrheit?..... | 223 |
| 1.3.7. | Die „Klage-Dramaturgie“..... | 223 |
| 1.3.7.1. | Mögliche Aktivitäten des Klägers, um Druck auszuüben..... | 224 |
| 2. | Litigation-Communications bei Unternehmensspionage konkret..... | 224 |
| 2.1. | Frühzeitige Einbindung der Litigation-Communications-Profis..... | 224 |
| 2.2. | Am Anfang viele Fragen | 225 |
| 2.2.1. | Die Dialoggruppen - wer sind die Adressaten?..... | 225 |
| 2.2.2. | Definition der Inhalte und Botschaften..... | 226 |
| 2.2.2.1. | „Framing“ - ein Zauberwort..... | 226 |
| 2.2.3. | Gemeinsame Strategie für Recht und Kommunikation..... | 226 |
| 2.2.4. | Langer Atem ist gefragt..... | 227 |
| 2.3. | Fakten! Fakten! Fakten!..... | 227 |
| 2.3.1. | Es gilt die Unschuldsvermutung..... | 228 |
| 2.4. | Der richtige Zeitpunkt entscheidet..... | 229 |
| 2.5. | Vorberichterstattung als Druckmittel..... | 229 |
| 2.6. | Was ist konkret möglich?..... | 230 |
| 3. | Ein Plädoyer für den Einsatz von Experten..... | 230 |
| 4. | Literatur (Auswahl)..... | 230 |
| | Stichwortverzeichnis | 233 |