

# Inhaltsverzeichnis

|                                                          |    |
|----------------------------------------------------------|----|
| Abkürzungsverzeichnis                                    | 17 |
| Kapitel 1: Einleitung                                    | 27 |
| Kapitel 2: Grundlagen der IT-Forensik                    | 35 |
| A. Informatische Grundbegriffe                           | 35 |
| I. Digitale Daten                                        | 35 |
| II. Dateien                                              | 36 |
| III. Datenträger                                         | 36 |
| IV. IT-System                                            | 38 |
| V. Rechnernetze                                          | 39 |
| VI. Cloud-Computing                                      | 40 |
| VII. Künstliche Intelligenz                              | 42 |
| VIII. Digitalisierung                                    | 44 |
| B. Begriff der IT-Forensik                               | 45 |
| I. Allgemeine Forensik                                   | 45 |
| 1. Zweck                                                 | 46 |
| 2. Grundprinzip                                          | 47 |
| 3. Rekonstruktionsprozess                                | 48 |
| II. Besonderheiten der Teildisziplin „IT“-Forensik       | 49 |
| 1. Digitale Spuren                                       | 49 |
| a) Flüchtigkeit                                          | 50 |
| b) Vermeidbarkeit                                        | 52 |
| c) Manipulier- und Nachvollziehbarkeit                   | 52 |
| d) Kopierbarkeit                                         | 53 |
| 2. Digitales Austauschprinzip                            | 53 |
| 3. Zweck der IT-Forensik und Abgrenzung                  | 54 |
| III. Definition von IT-Forensik                          | 55 |
| IV. Die Beziehung zwischen IT-Forensik und Kriminalistik | 57 |
| C. Fazit zu Kapitel 2                                    | 58 |

|                                                            |    |
|------------------------------------------------------------|----|
| Kapitel 3: SAP-Modell                                      | 61 |
| A. Sicherung                                               | 61 |
| I. Allgemeines                                             | 63 |
| 1. Umfassende Stoffsammlung                                | 63 |
| 2. Integrität und Authentizität                            | 64 |
| II. Sicherungsansätze                                      | 65 |
| 1. Post-Mortem-Sicherung                                   | 66 |
| a) Begriff                                                 | 66 |
| b) Anwendungsbereich                                       | 66 |
| c) Sonderfall: Cold Boot Attack                            | 68 |
| d) Vorgehen                                                | 69 |
| aa) Magnetische Festplatten                                | 70 |
| bb) Flash-Speicher                                         | 72 |
| cc) Mobilfunkgeräte                                        | 73 |
| (1) SIM-Karten                                             | 73 |
| (2) Interne und externe Speichermedien                     | 74 |
| dd) Navigationsgeräte                                      | 75 |
| e) Anforderungen an das Vorgehen                           | 76 |
| aa) Behebung von Leseproblemen                             | 76 |
| bb) Sicherungs- und Arbeitskopien                          | 77 |
| cc) Integrität und Authentizität                           | 78 |
| f) Sicherungsresistenzen                                   | 79 |
| aa) Auffindbarkeit der Datenträger                         | 80 |
| bb) Datenträgerverschlüsselung und<br>Beweisvereitelung    | 80 |
| cc) Einbindung des Datenträgers                            | 81 |
| dd) Datenvolumen                                           | 82 |
| ee) Cloud-Computing                                        | 83 |
| 2. Live-Sicherung                                          | 84 |
| a) Ausschließlich: Systemeigenes Benutzerinterface         | 85 |
| b) Kombination: Betriebssystem und importierte<br>Software | 85 |
| c) Hardware-basierte Variante                              | 86 |
| d) Netzwerkforensik (insbesondere Daten-TKÜ)               | 86 |
| e) Online-Durchsuchung und Quellen-TKÜ                     | 88 |
| f) Probleme der Live-Sicherung                             | 90 |

|                                                       |         |
|-------------------------------------------------------|---------|
| B. Analyse                                            | 91      |
| I. Umfang                                             | 91      |
| II. Selektion der Daten                               | 92      |
| 1. Filterung nach Metadaten und Stichwortsuche        | 93      |
| 2. Schlag- bzw. Stichwortsuche                        | 93      |
| 3. Hash-Wert-Datenbanken                              | 94      |
| 4. Künstliche Intelligenz                             | 94      |
| III. Auswertung                                       | 95      |
| IV. Praxisbeispiele                                   | 96      |
| C. Präsentation                                       | 98      |
| D. Risikofaktoren                                     | 100     |
| I. Anti-Forensik                                      | 100     |
| II. Fähigkeiten und Qualifikationen der Ermittler     | 101     |
| III. Ressourcen                                       | 102     |
| E. Fazit zu Kapitel 3                                 | 103     |
| <br>Kapitel 4: Digitale Beweisführung und Beweisrecht | <br>105 |
| A. Beweismittel                                       | 106     |
| I. Einlassung des Beschuldigten                       | 106     |
| II. Zeugen                                            | 107     |
| III. Sachverständige                                  | 109     |
| IV. Urkunden                                          | 111     |
| V. Richterlicher Augenschein                          | 113     |
| B. Würdigung digitaler Beweismittel                   | 115     |
| I. Grundsatz: freie Beweiswürdigung                   | 115     |
| II. Grenzen der freien Beweiswürdigung                | 116     |
| 1. Denkgesetze und Erfahrungssätze                    | 116     |
| 2. Beweisverbote                                      | 118     |
| III. Beweiswertermittlung                             | 123     |
| 1. Kriterien                                          | 123     |
| a) Vollständigkeit                                    | 124     |
| b) Darstellbarkeit                                    | 124     |
| c) Wissenschaftlich-technische Grundlage              | 124     |
| d) Integrität und Authentizität                       | 126     |
| e) Nachvollziehbarkeit und Nachprüfbarkeit            | 126     |
| f) Glaubwürdigkeit des Personalbeweises               | 127     |

|                                                                                                   |     |
|---------------------------------------------------------------------------------------------------|-----|
| 2. Leitfaden IT-Forensik                                                                          | 128 |
| 3. Bewertung der IT-forensischen Sicherungsansätze                                                | 129 |
| C. Fazit zu Kapitel 4                                                                             | 130 |
| Kapitel 5: Sicherungs- und Auswertungsbefugnisse                                                  | 133 |
| A. Einfluss der Grundrechte                                                                       | 133 |
| I. Betroffene Grundrechte                                                                         | 133 |
| 1. Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG)                                              | 134 |
| 2. Eigentumsfreiheit (Art. 14 Abs. 1 GG)                                                          | 135 |
| 3. Fernmeldegeheimnis (Art. 10 Abs. 1 Var. 3 GG)                                                  | 138 |
| 4. Allgemeines Persönlichkeitsrecht (Art. 2 Abs. 1 GG<br>i.V.m. Art. 1 Abs. 1 GG)                 | 143 |
| a) Recht auf informationelle Selbstbestimmung                                                     | 144 |
| b) Recht auf Gewährleistung der Vertraulichkeit und<br>Integrität informationstechnischer Systeme | 146 |
| II. Absoluter Schutz des Kernbereichs privater<br>Lebensgestaltung                                | 148 |
| III. Rechtsgrundlagen für strafprozessuale<br>Grundrechtseingriffe mittels IT-Forensik            | 151 |
| 1. Vorbehalt des Gesetzes                                                                         | 151 |
| 2. Eingriffsbefugnisse der Strafprozessordnung und Lehre<br>von der Annexkompetenz                | 153 |
| IV. Rechtmäßigkeitsanforderungen (insbesondere<br>Verhältnismäßigkeit)                            | 154 |
| B. Durchsuchung, §§ 102 ff. StPO                                                                  | 155 |
| I. Allgemeine Voraussetzungen des § 102 StPO                                                      | 156 |
| II. Reichweite der Durchsuchungsbefugnis                                                          | 158 |
| III. Besonderheiten des § 103 StPO                                                                | 159 |
| IV. Abgrenzung zwischen § 102 und § 103 StPO                                                      | 160 |
| 1. Abgrenzungskriterium: Gewahrsam                                                                | 160 |
| 2. Abgrenzungsfragen beim Einsatz von IT-Forensik                                                 | 161 |
| a) Gemeinschaftlich genutzte Räumlichkeiten und IT-<br>Systeme                                    | 161 |
| b) Durchsuchung beim Cloud-Nutzer                                                                 | 161 |
| c) Durchsuchung beim Cloud-Anbieter                                                               | 163 |

|                                                                                   |     |
|-----------------------------------------------------------------------------------|-----|
| V. Einzelne IT-forensische Maßnahmen zur Identifikation von IT-Systemen und Daten | 163 |
| 1. Suche nach Datenträgern und IT-Systemen                                        | 163 |
| 2. Suche nach Daten innerhalb eines IT-Systems                                    | 164 |
| 3. Inbetriebnahme und Benutzung von IT-Systemen                                   | 166 |
| 4. Installieren eigener Software                                                  | 168 |
| 5. Überwindung von Datenverschlüsselung                                           | 169 |
| a) Nutzung der Zugangsdaten                                                       | 169 |
| b) Anwendung von Entschlüsselungstechniken                                        | 170 |
| 6. Durchsicht des Datenbestandes, § 110 Abs. 3 S. 1 StPO                          | 172 |
| a) Allgemeines zur Durchsicht                                                     | 172 |
| b) Vorläufige Mitnahme und Sicherung zur Durchsicht                               | 174 |
| aa) Vorläufige Mitnahme von IT-Systemen                                           | 175 |
| bb) Vorläufige Sicherung von Daten                                                | 175 |
| cc) Zwischenergebnis                                                              | 176 |
| c) Ferndurchsuchung                                                               | 177 |
| aa) Allgemeines                                                                   | 177 |
| bb) „Transborder Searches“                                                        | 178 |
| d) Höchstdauer der Durchsicht                                                     | 183 |
| VI. Fazit zur Durchsuchung                                                        | 184 |
| C. Sicherstellung, §§ 94 ff. StPO                                                 | 185 |
| I. Allgemeines                                                                    | 185 |
| II. Sicherstellungsfähige Gegenstände                                             | 186 |
| III. Potenzielle Beweisbedeutung                                                  | 187 |
| IV. Mitwirkungspflichten nicht-verdächtiger Personen                              | 188 |
| V. Fazit zur Sicherstellung                                                       | 191 |
| D. TKÜ, § 100a StPO                                                               | 192 |
| I. Allgemeines                                                                    | 192 |
| II. Beschränkung auf laufende Telekommunikationsvorgänge                          | 195 |
| III. Voraussetzungen der klassischen Daten-TKÜ                                    | 198 |
| IV. Sonderform: Quellen-TKÜ                                                       | 200 |
| 1. Überwachung laufender Kommunikation, § 100a Abs. 1 S. 2 StPO                   | 201 |
| 2. Überwachung gespeicherter Daten, § 100a Abs. 1 S. 3 StPO                       | 203 |
| 3. Technische Anforderungen, § 100a Abs. 5 StPO                                   | 203 |
| 4. Protokollierungspflichten, § 100a Abs. 6 StPO                                  | 205 |

|                                                                              |     |
|------------------------------------------------------------------------------|-----|
| 5. Teilweise Verfassungswidrigkeit von § 100a Abs. 1 S. 2<br>und 3 StPO      | 206 |
| V. Fazit zur TKÜ                                                             | 208 |
| E. Online-Durchsuchung, § 100b StPO                                          | 209 |
| F. Auswertungsbefugnis                                                       | 214 |
| G. Grenzen IT-forensischer Sicherungs- und Auswertungsbefugnisse             | 215 |
| I. Kernbereich privater Lebensgestaltung                                     | 216 |
| 1. Zweistufiges Schutzkonzept des<br>Bundesverfassungsgerichts               | 217 |
| a) Erste Stufe: Datenerhebung                                                | 218 |
| b) Zweite Stufe: Datenaus- und verwertung                                    | 219 |
| 2. Anwendung des zweistufigen Schutzkonzepts                                 | 220 |
| II. Verfassungsrechtlich geschützte Beziehungen                              | 222 |
| 1. Beschlagnahmeverbot, § 97 StPO                                            | 223 |
| a) Verbot der Suche nach und der Beschlagnahme von<br>Daten und Datenträgern | 223 |
| b) Untersuchungsergebnisse aus IT-forensischen<br>Internal Investigations    | 224 |
| 2. Überwachungsverbot, § 100d Abs. 5 StPO                                    | 226 |
| 3. Allgemeine Beweisverbote, § 160a Abs. 1 und 2 StPO                        | 226 |
| III. Keine gezielte Suche nach Zufallsfunden                                 | 227 |
| IV. Verhältnismäßigkeit und Grundrechte                                      | 230 |
| 1. Physische Mitnahme eines IT-Systems                                       | 230 |
| 2. Komplettsicherung des aufgefundenen Datenmaterials                        | 231 |
| a) Geeignetheit                                                              | 232 |
| b) Erforderlichkeit                                                          | 232 |
| aa) Grundsatz: Vorrang der partiellen Sicherung                              | 232 |
| bb) Erste Ausnahme: Keine Unterscheidbarkeit                                 | 233 |
| cc) Zweite Ausnahme: Drohende<br>Beweiswerteinbußen                          | 233 |
| dd) Dritte Ausnahme: Unzumutbarer Aufwand                                    | 234 |
| V. Herausgabe- und Löschungspflichten                                        | 235 |
| 1. Normierte Pflichten der Strafprozessordnung                               | 235 |
| a) Herausgabe verfahrensirrelevanter Datenträger                             | 236 |
| b) Löschungspflichten                                                        | 236 |
| aa) (Quellen-)TKÜ und Online-Durchsuchung                                    | 236 |
| bb) Sonstige Ermittlungsmaßnahmen                                            | 237 |
| cc) Behördeninterne Dateien                                                  | 238 |

|                                                                                |     |
|--------------------------------------------------------------------------------|-----|
| 2. Datenschutzrechtliche Löschungspflicht                                      | 239 |
| 3. Ungeschriebene Herausgabe- und Löschungspflicht                             | 240 |
| VI. Fazit zu den Grenzen IT-forensischer Sicherungs- und Auswertungsbefugnisse | 241 |
| H. Reformbedarf beim offenen Zugriff auf IT-Systeme                            | 242 |
| I. Ausgangspunkt                                                               | 242 |
| II. Diskussion rund um den 74. Deutschen Juristentag                           | 244 |
| 1. Kritik: Schutz- und Regelungsdefizite                                       | 244 |
| 2. Reformvorschläge                                                            | 245 |
| III. Stellungnahme                                                             | 247 |
| 1. Zur Reformdiskussion im Allgemeinen                                         | 247 |
| 2. Zu den Impulsen des 74. Deutschen Juristentages                             | 251 |
| I. Fazit zu Kapitel 5                                                          | 254 |
| Kapitel 6: Kompetenzen                                                         | 257 |
| A. Anordnungscompetenz                                                         | 257 |
| I. Allgemeines                                                                 | 257 |
| II. Durchsuchung (§ 105 StPO) und Beschlagnahme (§ 98 StPO)                    | 258 |
| 1. Anordnungscompetenz                                                         | 258 |
| 2. Inhaltliche Anforderungen                                                   | 259 |
| III. (Quellen-)TKÜ und Online-Durchsuchung, § 100e StPO                        | 261 |
| 1. Anordnungscompetenz                                                         | 261 |
| 2. Inhaltliche Anforderungen                                                   | 262 |
| B. Vollzugscompetenz                                                           | 263 |
| I. Staatsanwaltschaft                                                          | 263 |
| II. Ermittlungspersonen und sonstige Polizeibeamte                             | 265 |
| III. Privatpersonen                                                            | 267 |
| 1. Problemaufriss: Privatisierungstendenzen                                    | 267 |
| 2. Grundlagen der Privatisierung staatlicher Aufgaben                          | 269 |
| a) Vermögensprivatisierung                                                     | 270 |
| b) Organisationsprivatisierung                                                 | 270 |
| c) Aufgabenprivatisierung                                                      | 271 |
| d) Erfüllungsprivatisierung                                                    | 272 |
| e) Zwischenergebnis                                                            | 273 |

|                                                                                |     |
|--------------------------------------------------------------------------------|-----|
| 3. IT-Forensik als Sachverständigentätigkeit                                   | 273 |
| a) Voraussetzung: Erfordernis der besonderen Sachkunde                         | 274 |
| b) Bewertung typischer IT-forensischer Aufgabenstellungen                      | 275 |
| aa) Datensichtung                                                              | 276 |
| bb) Vollständigkeitsprüfung                                                    | 276 |
| cc) Datenaufbereitung                                                          | 277 |
| dd) Durchsicht der Daten                                                       | 279 |
| c) Ermittlungshoheit und Neutralität als Grenzen der Sachverständigentätigkeit | 280 |
| d) Rechtsfolgen der faktischen Beleihung                                       | 281 |
| e) Zwischenergebnis                                                            | 282 |
| 4. De lege ferenda: Schaffung eines Beleihungstatbestandes?                    | 284 |
| a) Vereinbarkeit mit Art. 33 Abs. 4 GG                                         | 284 |
| aa) Der Funktionsvorbehalt als Beleihungsschranke                              | 284 |
| bb) Grenzen des Funktionsvorbehalts                                            | 287 |
| (1) Lediglich vorübergehende Aufgabenübertragung                               | 287 |
| (2) Regel-Ausnahme-Prinzip                                                     | 287 |
| b) Zwischenergebnis                                                            | 291 |
| C. Fazit zu Kapitel 6                                                          | 292 |
| Kapitel 7: Zusammenfassung der Ergebnisse und Gesamtbetrachtung                | 295 |
| Literaturverzeichnis                                                           | 301 |