

IT-Strafrecht

Cyberdelikte und Ermittlungsbefugnisse

von

Dr. Susanne Reindl-Krauskopf

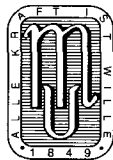
Universitätsprofessorin und Vorstand des Instituts für Strafrecht und Kriminologie der Universität
Wien, Honorarprofessorin an der University of Queensland

Dr. Farsam Salimi

Assistenzprofessor am Institut für Strafrecht und Kriminologie der Universität Wien

Dr. Martin Stricker

Ehemaliger wissenschaftlicher Mitarbeiter am Institut für Strafrecht und Kriminologie der
Universität Wien



Wien 2018

MANZ'sche Verlags- und Universitätsbuchhandlung

Inhaltsverzeichnis

| | |
|---|----|
| 1. Kapitel Einführung | 1 |
| I. Der Begriff Cybercrime | 1 |
| II. Besonderheiten von Cybercrime | 2 |
| III. Praktische Bedeutung von Cybercrime | 3 |
| IV. Zur nationalen und internationalen Entwicklung des IT-Strafrechts | 6 |
| 2. Kapitel Materielles Strafrecht und Cybercrime | 11 |
| I. Angriffe auf Informationssysteme und Datenmanipulationen | 11 |
| A. Allgemeines | 11 |
| B. Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB) | 12 |
| 1. Objektiver Tatbestand | 13 |
| a) Das Tatobjekt | 13 |
| aa) Computersystem und Teil eines solchen | 13 |
| bb) Verfügungsbefugnis über das Computersystem | 14 |
| b) Die Tathandlung | 16 |
| aa) Zugang-Verschaffen | 16 |
| bb) Überwinden spezifischer Sicherheitsvorkehrungen im Computersystem | 16 |
| 2. Subjektive Tatseite | 20 |
| a) „Bloße“ Spionageabsicht | 20 |
| b) Datenbezogene Verwendungsabsicht | 21 |
| c) Systembezogene Verwendungsabsicht | 22 |
| 3. Qualifikationen | 23 |
| a) Zugriff auf kritische Infrastrukturen | 23 |
| b) Kriminelle Vereinigung | 24 |
| 4. Sonstiges | 25 |
| C. Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB) | 25 |
| 1. Allgemeines | 26 |
| 2. Objektiver Tatbestand | 27 |
| a) Angebrachte oder empfangsbereite Vorrichtung | 27 |
| b) Telekommunikationsanlage | 30 |
| c) Computersystem | 30 |
| d) Benützen | 30 |
| 3. Subjektiver Tatbestand | 31 |
| a) Tatbildvorsatz | 31 |
| b) Erweiterter Vorsatz | 31 |
| aa) Absicht, sich oder einem anderen Unbefugten Kenntnis zu verschaffen | 31 |
| bb) Geschützte Nachrichten | 32 |
| 4. Abgrenzung zum Telekommunikationsgesetz 2003 (TKG) | 33 |
| D. Missbräuchliches Abfangen von Daten (§ 119a StGB) | 34 |
| 1. Abfangen von Daten (§ 119a Abs 1 Fall 1 StGB) | 35 |
| a) Der objektive Tatbestand | 35 |
| b) Der subjektive Tatbestand | 36 |
| 2. Abfangen der Abstrahlung (§ 119a Abs 1 Fall 2 StGB) | 36 |
| a) Der objektive Tatbestand | 36 |
| b) Der subjektive Tatbestand | 38 |
| 3. Sonstiges | 38 |
| E. Missbrauch von Tonaufnahme- und Abhörgeräten (§ 120 Abs 2a StGB) | 38 |

| | |
|---|----|
| 1. Der objektive Tatbestand | 39 |
| 2. Der subjektive Tatbestand | 41 |
| 3. Weitere Anmerkungen | 41 |
| F. Auskundschaften eines Geschäfts- oder Betriebsgeheimnisses (§§ 123 und 124 StGB) | 41 |
| 1. Allgemeines | 42 |
| 2. Objektiver Tatbestand | 43 |
| a) Tatobjekt | 43 |
| b) Tathandlung | 44 |
| aa) Auskundschaften | 44 |
| bb) Preisgeben | 45 |
| 3. Subjektiver Tatbestand | 45 |
| a) Tatbildvorsatz | 45 |
| b) Erweiterter Vorsatz | 45 |
| 4. Abgrenzung und Konkurrenzen | 46 |
| G. Datenbeschädigung (§ 126 a StGB) | 47 |
| 1. Allgemeines | 48 |
| 2. Objektiver Tatbestand | 48 |
| a) Tatobjekt | 49 |
| b) Tathandlung | 51 |
| c) Schaden | 53 |
| 3. Subjektiver Tatbestand | 54 |
| 4. Qualifikationen | 55 |
| 5. Abgrenzung und Konkurrenzen | 56 |
| H. Funktionsstörung eines Computersystems (§ 126 b StGB) | 58 |
| 1. Der objektive Tatbestand | 59 |
| a) Computersystem als geschütztes Rechtsgut | 59 |
| b) Störung der Funktionsfähigkeit | 60 |
| c) Störung durch Dateneingabe oder Übermittlung | 62 |
| 2. Der subjektive Tatbestand | 62 |
| 3. Qualifikationen | 62 |
| a) Längere Zeit andauernde Störung | 62 |
| b) Störung vieler Computersysteme | 63 |
| c) Wertqualifikation | 63 |
| d) Angriff auf kritische Infrastruktur | 64 |
| e) Tatbegehung als Mitglied einer kriminellen Vereinigung | 64 |
| 4. Sonstiges | 64 |
| a) Subsidiaritätsklausel | 64 |
| b) Spam-Verbot | 64 |
| I. Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126 c StGB) | 65 |
| 1. Der objektive Tatbestand | 65 |
| a) Beschränkung auf bestimmte Delikte | 65 |
| b) Verpönte Tatobjekte | 66 |
| c) Tathandlungen | 67 |
| 2. Der subjektive Tatbestand | 68 |
| 3. Strafaufhebung nach § 126 c Abs 2 StGB | 69 |
| J. Datenfälschung (§ 225 a StGB) | 70 |
| 1. Der objektive Tatbestand | 70 |
| a) Das Tatobjekt – Daten | 70 |
| aa) Falsche Daten | 70 |
| bb) Verfälschte Daten | 71 |
| cc) Lugdaten | 72 |
| dd) Verkörperung der Inhalte auf Datenträgern | 72 |

| | |
|--|-----|
| ee) Rechtserheblichkeit | 73 |
| ff) Erkennbarkeit des Ausstellers | 73 |
| gg) Original und Kopie | 75 |
| b) Tathandlung | 75 |
| 2. Der subjektive Tatbestand | 76 |
| 3. Tätige Reue | 77 |
| K. Übergreifende Beispiele | 78 |
| II. Angriffe auf fremdes Vermögen | 80 |
| A. Vorbemerkungen | 80 |
| B. Betrug (§ 146 StGB) | 81 |
| 1. Allgemeines | 82 |
| a) Objektiver Tatbestand | 82 |
| b) Subjektiver Tatbestand | 85 |
| c) Qualifikationen | 86 |
| 2. Erscheinungsformen im Cybercrime | 89 |
| a) Phishing | 89 |
| b) Online-Kauf mit fremder Kreditkarte oder fremden Kreditkartendaten .. | 90 |
| c) Telebanking | 91 |
| d) Betrügerischer Online-Handel mit Waren und Dienstleistungen | 93 |
| e) Versprochene Gewinne beim Besuch einer bestimmten Website | 94 |
| f) Fehlbuchung und Fehlüberweisung | 94 |
| C. Betrügerischer Datenverarbeitungsmissbrauch (§ 148a StGB) | 96 |
| 1. Allgemeines | 96 |
| 2. Objektiver Tatbestand | 97 |
| 3. Subjektiver Tatbestand | 102 |
| 4. Qualifikationen | 102 |
| 5. Abgrenzung und Konkurrenz | 103 |
| 6. Erscheinungsformen im Cybercrime | 104 |
| a) Online-Kauf mit fremder Kreditkarte oder fremden Kreditkartendaten .. | 104 |
| b) Telebanking | 105 |
| c) Zahlungen mit fremder Bankomatkarte | 106 |
| d) Behebungen am Bankomaten mit fremder bzw eigener Bankomatkarte .. | 106 |
| e) Missbräuche bei Kommunikationsdienstleistungen | 108 |
| D. Glücks- (§ 168 StGB) und Ketten- oder Pyramidenspiele (§ 168a StGB) | 110 |
| 1. Allgemeines | 111 |
| 2. Objektiver Tatbestand | 111 |
| a) Tatobjekt | 111 |
| b) Tathandlung | 112 |
| 3. Subjektiver Tatbestand | 114 |
| 4. Qualifikation | 114 |
| 5. Straflosigkeitsgründe | 115 |
| 6. Glücks- oder Pyramidenspiele im Internet | 116 |
| E. Schutz unbarer Zahlungsmittel (§§ 241 a ff StGB) | 118 |
| 1. Fälschung unbarer Zahlungsmittel (§ 241 a StGB) | 119 |
| a) Allgemeines | 119 |
| b) Objektiver Tatbestand | 119 |
| c) Subjektiver Tatbestand | 122 |
| d) Qualifikationen | 123 |
| 2. Annahme, Weitergabe oder Besitz falscher oder verfälschter unbarer Zah- | |
| lungsmittel (§ 241 b StGB) | 124 |
| a) Allgemeines | 125 |
| b) Objektiver Tatbestand | 125 |
| c) Subjektiver Tatbestand | 127 |

| | |
|---|-----|
| 3. Vorbereitung der Fälschung unbarer Zahlungsmittel (§ 241 c StGB) | 128 |
| a) Allgemeines | 128 |
| b) Objektiver Tatbestand | 128 |
| c) Subjektiver Tatbestand | 130 |
| d) Tätige Reue (§ 241 d StGB) | 130 |
| 4. Entfremdung unbarer Zahlungsmittel (§ 241 e StGB) | 131 |
| a) Allgemeines | 132 |
| b) Objektiver Tatbestand | 132 |
| c) Subjektiver Tatbestand | 134 |
| d) Qualifikationen | 135 |
| e) Verwertung und Konkurrenz | 136 |
| 5. Annahme, Weitergabe oder Besitz entfremdeter unbarer Zahlungsmittel (§ 241 f StGB) | 137 |
| a) Allgemeines | 137 |
| b) Objektiver Tatbestand | 138 |
| c) Subjektiver Tatbestand | 138 |
| d) Tätige Reue | 139 |
| 6. Ausspähen von Daten eines unbaren Zahlungsmittels (§ 241 h StGB) | 140 |
| a) Allgemeines | 140 |
| b) Objektiver Tatbestand | 140 |
| c) Subjektiver Tatbestand | 144 |
| d) Qualifikationen | 144 |
| e) Tätige Reue | 146 |
| F. Zugangskontrollgesetz (§ 10 ZuKG) | 146 |
| III. Angriffe auf Persönlichkeit und Ehre | 148 |
| A. Allgemeines zu den Ehrschutzdelikten (§§ 111 ff StGB) | 148 |
| B. Üble Nachrede (§§ 111 f StGB) | 150 |
| 1. Objektiver Tatbestand | 150 |
| a) Verhaltens-, Eigenschafts- oder Gesinnungsvorwurf | 150 |
| aa) Verächtliche Eigenschaft oder Gesinnung: Schmähung (§ 111 Abs 1 Fall 1 StGB) | 151 |
| bb) Unehrenhaftes oder sittenwidriges Verhalten (§ 111 Abs 1 Fall 2 StGB) | 152 |
| b) Wahrnehmbarkeit für Dritte | 156 |
| 2. Subjektiver Tatbestand | 157 |
| 3. Qualifikation des § 111 Abs 2 StGB | 157 |
| 4. Wahrheitsbeweis/Gutgläubensbeweis (§ 111 Abs 3 und § 112 StGB) | 158 |
| a) Wahrheitsbeweis | 159 |
| b) Gutgläubensbeweis | 159 |
| c) Beweisthemenvorbot (§ 112 StGB) | 160 |
| d) Medieninhaltsdelikt | 161 |
| C. Beleidigung (§ 115 StGB) | 161 |
| 1. Objektiver Tatbestand | 162 |
| a) Allgemeines | 162 |
| b) Beschimpfen | 162 |
| c) Verspotten | 163 |
| d) Bedrohen mit Misshandlung | 163 |
| e) Öffentliche Begehung oder Begehung vor mehreren Leuten | 164 |
| aa) Öffentlichkeit | 164 |
| bb) Vor mehreren Leuten | 164 |
| 2. Subjektiver Tatbestand | 164 |
| 3. Entrüstungsbeleidigung | 165 |
| D. Cybermobbing (§ 107 c StGB) | 165 |
| 1. Allgemeines | 166 |

| | |
|---|-----|
| 2. Objektiver Tatbestand | 167 |
| a) Tathandlungen | 167 |
| aa) Verletzung der Ehre | 167 |
| bb) Wahrnehmbar-Machen von Tatsachen oder Bildaufnahmen des höchstpersönlichen Lebensbereichs | 167 |
| b) IKT-Bezug und Mindestpublizität | 168 |
| c) Dauer und Handlungswiederholung: über längere Zeit hindurch fortgesetzt | 169 |
| d) Gefährlichkeit: Eignung, die Lebensweise unzumutbar zu beeinträchtigen | 170 |
| e) Problem der Tätermehrheit | 171 |
| 3. Subjektiver Tatbestand | 172 |
| 4. Qualifikation: Suizid oder Suizidversuch | 172 |
| E. Schutz personenbezogener Daten (§ 63 DSGVO) | 172 |
| 1. Allgemeines | 173 |
| 2. Objektiver Tatbestand | 174 |
| a) Tatobjekt | 174 |
| aa) Personenbezogene Daten | 174 |
| bb) Bestehen eines schutzwürdigen Geheimhaltungsinteresses | 177 |
| b) Täterkreis | 178 |
| aa) Zugang aufgrund berufsmäßiger Beschäftigung | 178 |
| bb) Widerrechtliche Verschaffung | 179 |
| c) Tathandlungen | 180 |
| aa) Benützen | 181 |
| bb) Einem anderen zugänglich machen | 182 |
| cc) Veröffentlichen | 183 |
| 3. Subjektiver Tatbestand | 183 |
| a) Tatbestandsvorsatz | 183 |
| b) Erweiterter Vorsatz | 183 |
| aa) Bereicherungsvorsatz | 183 |
| bb) Absicht auf Schädigung des Geheimhaltungsanspruchs | 184 |
| 4. Rechtfertigung durch Art 6ff DSGVO | 184 |
| 5. Subsidiaritätsklausel | 185 |
| 6. Anwendbarkeit auf journalistische, wissenschaftliche, künstlerische oder literarische Tätigkeit? | 186 |
| F. Täuschung (§ 108 StGB) und personenbezogene Daten | 187 |
| G. Bildnisschutz | 189 |
| 1. Schutz durch geltendes Recht | 189 |
| a) Kein eigener Straftatbestand | 189 |
| b) Nur partielle Abdeckung durch andere Strafnormen | 190 |
| 2. Rechtspolitische Bewertung | 191 |
| IV. Angriffe auf den öffentlichen Frieden | 191 |
| A. Allgemeines | 191 |
| B. Anleitung zur Begehung einer terroristischen Straftat (§ 278f StGB) | 192 |
| 1. Objektiver Tatbestand | 192 |
| a) Abs 1: Verbreiten der einschlägigen Informationen | 192 |
| aa) Medienwerk oder Informationen | 192 |
| bb) Terrorismusbezogener Inhalt | 193 |
| cc) Tathandlungen | 194 |
| b) Abs 2: Sich Verschaffen der Informationen | 195 |
| 2. Subjektiver Tatbestand | 195 |
| a) Abs 1: Absicht auf Aufreizung zu einer terroristischen Straftat | 196 |
| b) Abs 2: Absicht auf Begehung einer terroristischen Straftat | 196 |
| C. Aufforderung zu und Gutheißung von mit Strafe bedrohten Handlungen (§ 282 StGB) | 196 |

| | |
|--|-----|
| 1. Objektiver Tatbestand | 197 |
| a) Aufforderung zu mit Strafe bedrohten Handlungen | 197 |
| aa) Aufforderung zu mit Strafe bedrohter Handlung | 197 |
| bb) Publizität | 198 |
| cc) Vorrang der Beteiligungstäterschaft | 199 |
| b) Gutheißung mit Strafe bedrohter Handlungen | 199 |
| aa) Gutheißung einer Straftat | 199 |
| bb) Schwere der Straftat | 200 |
| cc) Eignung der Störung des allgemeinen Rechtsempfindens oder zur Aufreizung zur Tatbegehung | 200 |
| 2. Subjektiver Tatbestand | 200 |
| D. Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten (§ 282a StGB) | 200 |
| 1. Objektiver Tatbestand | 201 |
| a) Aufforderung zu terroristischer Straftat | 201 |
| aa) Terroristische Straftat | 201 |
| bb) Publizität | 202 |
| cc) Vorrang der Beteiligungstäterschaft | 202 |
| b) Gutheißung einer terroristischen Straftat | 203 |
| 2. Subjektiver Tatbestand | 203 |
| E. Verhetzung (§ 283 StGB) | 203 |
| 1. Allgemeines | 204 |
| 2. Objektiver Tatbestand des Abs 1 | 205 |
| a) Z 1: Gewaltaufforderung oder Aufstachelung zu Hass gegen Gruppen und Einzelpersonen | 205 |
| aa) Geschützte Gruppen | 205 |
| bb) Hetze gegen Einzelpersonen wegen Gruppenzugehörigkeit | 208 |
| cc) Tathandlungen | 208 |
| b) Z 2: Beschimpfen von Gruppen | 209 |
| aa) Beschimpfen und Eignung der Herabsetzung oder Verächtlichmachung | 209 |
| bb) Absicht auf Verletzung in der Menschenwürde | 209 |
| c) Z 3: Leugnung bestimmter Verbrechen | 210 |
| aa) Verbrechen iSd §§ 321 – 321f StGB | 211 |
| bb) Tathandlungen | 212 |
| cc) Eignung zur Aufstachelung zu Gewalt und Hass | 212 |
| d) Mindestpublizität | 212 |
| 3. Subjektiver Tatbestand | 213 |
| 4. Erhöhte Publizität: Qualifikation nach Abs 2 | 213 |
| 5. Erfolgsqualifikation nach Abs 3 | 213 |
| 6. Abs 4: Publikation und Weiterverbreitung hetzerischer Inhalte | 214 |
| a) Verbreitung bestimmter Inhalte | 214 |
| b) Tathandlungen | 215 |
| c) Gutheißende oder rechtfertigende Weise | 215 |
| d) Publizität | 215 |
| e) Subsidiarität gegenüber Beteiligungstäterschaft | 215 |
| F. Strafbarkeit nach dem Verbotsgesetz | 216 |
| 1. Allgemeines | 217 |
| 2. Aufforderungen, Aneifern oder Verleiten zu verbotenen Handlungen nach §§ 1 und 3 VG | 217 |
| 3. Sonstige Wiederbetätigung (§ 3g VG) | 218 |
| 4. Leugnung, Verharmlosung, Gutheißung und Rechtfertigung nationalsozialistischer Verbrechen (§ 3h VG) | 220 |

| | |
|---|-----|
| V. Angriffe auf die sexuelle Integrität und Selbstbestimmung | 221 |
| A. Pornographische Darstellungen Minderjähriger (§ 207a StGB) | 221 |
| 1. Allgemeines | 223 |
| 2. Objektiver Tatbestand | 223 |
| a) Altersgrenzen | 223 |
| b) Formen der Pornographie | 224 |
| aa) Realpornographie (Abs 4 Z 1 und Z 3 lit a Fall 1) | 225 |
| bb) Anscheinpornographie (Abs 4 Z 2 und Z 3 lit a Fall 2) | 226 |
| cc) Reißerische Darstellung der Genitalien oder Schamgegend (Abs 4 Z 3 lit b) | 226 |
| dd) Virtuelle Pornographie (Abs 4 Z 4) | 227 |
| c) Tathandlungen | 227 |
| 3. Subjektiver Tatbestand | 230 |
| 4. Strafausschluss nach Abs 5 und Abs 6 | 230 |
| a) Herstellung und Besitz von Pornographie mündiger Minderjähriger mit Zustimmung – Abs 5 Z 1 | 230 |
| b) Besitz und Herstellung von virtueller Pornographie mit mündigen Minderjährigen – Abs 5 Z 2 | 231 |
| c) Straflosigkeit des Sexting – Abs 6 Z 1 | 231 |
| d) Besitz von Darstellungen Unmündiger von sich selbst nach Erreichen der Strafmündigkeit – Abs 6 Z 2 | 232 |
| 5. Qualifikationen | 233 |
| B. Sittliche Gefährdung von Personen unter sechzehn Jahren (§ 208 StGB) | 234 |
| 1. Objektiver Tatbestand | 234 |
| 2. Subjektiver Tatbestand | 235 |
| 3. Alterstoleranzklausel | 236 |
| C. Anbahnung von Sexualkontakten zu Unmündigen (§ 208a StGB) | 236 |
| 1. Allgemeines | 236 |
| 2. Grooming (§ 208a Abs 1 StGB) | 237 |
| a) Objektiver Tatbestand | 237 |
| aa) Vorschlagen oder Vereinbarung des Treffens | 237 |
| bb) Konkrete Vorbereitungshandlung | 238 |
| b) Subjektiver Tatbestand | 238 |
| c) Versuchsproblematik | 239 |
| 3. Kontaktaufnahme mit Unmündigen (§ 208a Abs 1 a StGB) | 240 |
| a) Objektiver Tatbestand | 240 |
| b) Subjektiver Tatbestand | 240 |
| 4. Tätige Reue | 241 |
| D. Pornographische Darbietungen Minderjähriger (§ 215a Abs 2a StGB) | 241 |
| 1. Allgemeines | 242 |
| 2. Objektiver Tatbestand | 242 |
| 3. Subjektiver Tatbestand | 244 |
| 4. Kein Strafausschließungsgrund | 244 |
| E. Strafbarkeit nach dem Pornographiegesetz | 244 |
| 1. Verbreitung unzüchtiger Pornographie (§ 1 PornG) | 244 |
| a) Objektiver Tatbestand | 245 |
| aa) Tatobjekt | 245 |
| bb) Begriff der Unzüchtigkeit | 245 |
| cc) Tathandlungen | 247 |
| dd) Subjektiver Tatbestand | 248 |
| 2. Gefährdung von Jugendlichen durch Pornographie (§ 2 PornG) | 248 |
| a) Allgemeines | 249 |
| b) Objektiver Tatbestand der lit a | 249 |

| | |
|--|------------|
| c) Objektiver Tatbestand der lit b | 250 |
| d) Subjektiver Tatbestand | 250 |
| 3. Kapitel Haftung der Provider | 251 |
| I. Provider-Kategorien | 251 |
| II. Prinzip der Haftungsregeln | 253 |
| III. Ausschluss der Verantwortlichkeit bei Durchleitung | 253 |
| IV. Ausschluss der Verantwortlichkeit bei Suchmaschinen | 254 |
| V. Ausschluss der Verantwortlichkeit bei Zwischenspeicherungen (Caching) | 256 |
| VI. Ausschluss der Verantwortlichkeit bei Speicherungen fremder Inhalte (Hosting) .. | 258 |
| VII. Ausschluss der Verantwortlichkeit bei Links | 259 |
| 4. Kapitel Strafanwendungsrecht | 263 |
| I. Allgemeines | 263 |
| II. Inländischer Tatort (§ 62 iVm § 67 Abs 2 StGB) | 263 |
| A. Allgemeines | 263 |
| B. Inländischer Tatort bei allgemeinen Erfolgsdelikten | 263 |
| C. Inländischer Tatort bei Äußerungs- und Medieninhaltsdelikten | 264 |
| 1. Allgemeines | 264 |
| 2. Erweiterungskonzepte | 264 |
| a) Exzessives Verständnis des Handlungsorts | 264 |
| b) Exzessives Verständnis des Erfolgsorts | 266 |
| c) Lösungsansatz: Differenzierte Tatbestandslösung | 266 |
| 3. Begrenzungskonzepte | 270 |
| a) Begrenzung aufgrund der Täterintention | 270 |
| b) Unterscheidung zwischen „Push- und Pull-Technologie“ | 271 |
| c) Begrenzung auf Fälle mit besonderem Inlandsbezug | 271 |
| d) Die „Sonderregel“ des § 51 MedienG | 272 |
| aa) Herkunftslandprinzip und Internet-Provider | 273 |
| III. Ausländischer Tatort (§§ 64, 65 StGB) | 274 |
| A. Anknüpfung unabhängig von der Strafbarkeit am Tatort (§ 64 StGB) | 276 |
| B. Anknüpfung bei Vorliegen identer Norm (§ 65 StGB) | 277 |
| 5. Kapitel Ermittlungen und Cybercrime | 279 |
| I. Allgemeines | 279 |
| II. Strafprozessuale Ermittlungen | 279 |
| A. Sicherstellung und Beschlagnahme (§§ 110ff StPO) | 279 |
| 1. Allgemeines | 282 |
| 2. Lokale Sicherstellung von Datenträgern und Daten beim Betroffenen | 282 |
| 3. Sicherstellung von Daten auf externen Datenträgern durch Fernzugriff: „Cloudcomputing“ | 284 |
| 4. Sicherstellung als Zugriff auf im Zeitpunkt des Zugriffs abgespeicherte Daten | 286 |
| 5. Subsidiarität (§ 110 Abs 4 StPO) | 288 |
| 6. Formelle Voraussetzungen der Sicherstellung | 289 |
| 7. Beschlagnahme nach § 115 StPO | 289 |
| 8. Sonderfall: Sicherstellung und Beschlagnahme von Domain-Namen? | 290 |
| B. Durchsuchung von Orten und Gegenständen (§§ 119ff StPO) | 291 |
| C. Verdeckte Ermittlung und Scheingeschäft (§§ 131f StPO) | 292 |
| 1. Allgemeines | 294 |
| 2. Verdeckte Ermittlungen im Internet | 295 |
| 3. Straftaten durch verdeckte Ermittler und Lockspitzelverbot | 296 |
| a) Verbotene Tatprovokation | 296 |
| b) Verbotene Verleitung zu einem Geständnis | 298 |

| | |
|---|-----|
| D. Auskunft über Stamm- und Zugangsdaten (§ 76a StPO) | 299 |
| 1. Allgemeines | 299 |
| 2. Stammdatenauskunft nach § 76a Abs 1 StPO | 300 |
| 3. Zugangsdatenauskunft (§ 76a Abs 2 StPO) | 301 |
| a) Auskunft zu dynamischen IP-Adressen (§ 76a Abs 2 Z 1 StPO) | 301 |
| b) Auskunft von E-Maildaten (§ 76a Abs 2 Z 2 bis Z 4 StPO) | 302 |
| c) Formelle Voraussetzungen | 302 |
| d) Löschungspflicht versus Speicherpflicht | 303 |
| E. Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübertragung, Lokalisierung einer technischen Einrichtung, Anlassdatenspeicherung, Überwachung von Nachrichten und Überwachung verschlüsselter Nachrichten (§ 135 StPO u § 135a StPO) | 304 |
| 1. Geltendes Recht | 304 |
| a) Beschlagnahme von Briefen | 308 |
| aa) Aktuelle Bedeutung iZm Cybercrime | 308 |
| bb) Materielle und formelle Voraussetzungen | 308 |
| b) Allgemeines zur weiteren Kommunikationsüberwachung | 308 |
| c) Auskunft über Daten einer Nachrichtenüberwachung | 311 |
| aa) Definition | 311 |
| bb) Materielle Voraussetzungen | 314 |
| cc) Formelle Voraussetzungen | 315 |
| dd) Weitere Durchführung | 316 |
| d) Lokalisierung einer technischen Einrichtung | 317 |
| aa) Definition | 317 |
| bb) Materielle und formelle Voraussetzungen | 318 |
| e) Anlassdatenspeicherung | 318 |
| aa) Definition | 318 |
| bb) Materielle und formelle Voraussetzungen | 319 |
| f) Überwachung von Nachrichten | 321 |
| aa) Definition | 321 |
| bb) Materielle Voraussetzungen | 324 |
| g) Verfahrensregeln | 328 |
| 2. Ausblick: Überwachen verschlüsselter Nachrichten | 329 |
| a) Allgemeines | 332 |
| b) Überwachung verschlüsselter Nachrichten | 334 |
| aa) Definition | 334 |
| bb) Materielle und formelle Voraussetzungen | 335 |
| cc) Weitere Durchführung | 336 |
| dd) Ausblick | 337 |
| F. Der Sonderfall „Vorratsdatenspeicherung“ | 337 |
| 1. Allgemeines | 337 |
| 2. Mögliche Nachfolgeregelung? | 339 |
| G. Optische und akustische Überwachung (§ 136 StPO) | 344 |
| 1. Allgemeines | 346 |
| 2. Objekt der Überwachung | 346 |
| 3. Einsatz technischer Hilfsmittel | 348 |
| 4. Varianten des Lausch- und Spähangriffs | 348 |
| a) Der „große Lauschangriff“ (§ 136 Abs 1 Z 3 StPO) | 348 |
| aa) Materielle Voraussetzungen | 348 |
| bb) Formelle Voraussetzungen | 350 |
| cc) Eindringen in Wohnungen und vom Hausrecht geschützte Räumlichkeiten (§ 136 Abs 2 StPO) | 350 |
| dd) Verwendung der Webcam der Zielperson? | 351 |
| b) Optische Überwachung/der „Spähangriff“ (§ 136 Abs 3 StPO) | 351 |

| | |
|--|-----|
| H. Rechtsschutz | 352 |
| 1. Einspruch wegen Rechtsverletzung (§ 106 StPO) | 352 |
| 2. Beschwerde (§§ 87ff StPO) | 355 |
| a) Allgemeines | 356 |
| b) Einbindung des Rechtsschutzbeauftragten der Justiz | 357 |
| III. Sicherheitspolizeiliche Ermittlungen | 358 |
| A. Allgemeines | 358 |
| B. Ausgewählte Aufgaben im Zusammenhang mit Cybercrime | 359 |
| 1. Abwehr gefährlicher Angriffe | 359 |
| 2. Abwehr krimineller Verbindungen | 361 |
| C. Besondere Befugnisse im Zusammenhang mit Cybercrime | 362 |
| 1. Ermittlung von Stamm- und Verbindungsdaten (§ 53 Abs 3a SPG) | 362 |
| a) Beauskunftung von Telefonie-Stammdaten (§ 53 Abs 3a Z 1 SPG) | 363 |
| b) Beauskunftung von IP-Adressen und Übermittlungszeitpunkt zu bestimmten Nachrichten (§ 53 Abs 3a Z 2 SPG) | 364 |
| c) Beauskunftung von Name und Anschrift zu einer dynamischen IP-Adresse (§ 53 Abs 3a Z 3 SPG) | 365 |
| d) Punktuelle Rufdatenerfassung (§ 53 Abs 3a Z 4 SPG) | 365 |
| 2. Ermittlung von Standortdaten (§ 53 Abs 3b SPG) | 366 |
| 3. Ermittlung von personenbezogenen Daten aus anderen verfügbaren Quellen (§ 53 Abs 4 SPG) | 368 |
| 4. Verwendung von durch Dritte ermittelte personenbezogene Bilddaten (§ 53 Abs 5 SPG) | 370 |
| 5. Verdeckte Ermittlungen im Internet (§ 54 Abs 3 SPG) | 373 |
| 6. Einsatz von Bild- und Tonaufzeichnungsgeräten (§ 54 Abs 4 SPG) | 375 |
| D. Besonderer Rechtsschutz | 377 |
| 1. Allgemeiner Rechtsschutz | 381 |
| 2. Besonderer Rechtsschutz: Der Rechtsschutzbeauftragte | 381 |
| IV. Staatsschutzermittlungen | 383 |
| A. Allgemeines zum PStSG | 383 |
| B. Staatsschutzaufgaben im Zusammenhang mit Cybercrime | 384 |
| 1. Erweiterte Gefahrenerforschung (§ 6 Abs 1 Z 1 PStSG) | 384 |
| 2. Schutz vor verfassungsgefährdenden Angriffen (§ 6 Abs 1 Z 2 iVm Abs 2 PStSG) | 386 |
| 3. Schutz vor verfassungsgefährdenden Angriffen durch ausländische Gefährder mittels Informationsspeicherung (§ 6 Abs 1 Z 3 PStSG) | 388 |
| V. Besondere Befugnisse des Staatsschutzes | 389 |
| A. Allgemeines | 393 |
| B. Besondere Ermittlungsmaßnahmen des PStSG | 394 |
| 1. Observation (§ 11 Abs 1 Z 1 PStSG) | 394 |
| 2. Verdeckte Ermittlung (§ 11 Abs 1 Z 2 PStSG) | 395 |
| 3. Einsatz von Bild- und Tonaufzeichnungsgeräten (§ 11 Abs 1 Z 3 PStSG) | 395 |
| 4. Einsatz von Kennzeichenerkennungsgeräten für Fahrzeugkontrollen (§ 11 Abs 1 Z 4 PStSG) | 395 |
| 5. Einholen von Stammdaten, Standortdaten und Daten zu IP-Adressen (§ 11 Abs 1 Z 5 PStSG) | 396 |
| 6. Einholen von taxativ aufgezählten Daten bei Beförderungsunternehmen (§ 11 Abs 1 Z 6 PStSG) | 397 |
| 7. Einholen von Verbindungsdaten (§ 11 Abs 1 Z 7 PStSG) | 398 |
| 8. Datenverarbeitungen (§ 12 PStSG) | 399 |
| C. Lösungsverpflichtung und Rechtsschutz | 399 |
| 1. Lösungsverpflichtung | 399 |
| 2. Rechtsschutz | 400 |