

Computer- und Internetstrafrecht

von

Annette Marberth-Kubicki, Dr. Reinhard Gelhausen, Prof. Dr. Bernhard Weiner, Dr. Eduard Kunz, Gerhard Zellner

2. Auflage

[Computer- und Internetstrafrecht – Marberth-Kubicki / Gelhausen / Weiner / et al.](#)

schnell und portofrei erhältlich bei [beck-shop.de](#) DIE FACHBUCHHANDLUNG

Thematische Gliederung:

[Allgemeines](#)



Verlag C.H. Beck München 2010

Verlag C.H. Beck im Internet:

www.beck.de

ISBN 978 3 406 59505 9



Inhaltsverzeichnis

| | |
|---|----------|
| Inhaltsübersicht | VII |
| Abkürzungsverzeichnis | XIX |
| Literaturverzeichnis | XXV |
| A. Einleitung/Allgemeines | 1 |
| I. Vorbemerkung | 1 |
| II. Struktur des Internets | 3 |
| 1. Historischer Abriss | 3 |
| 2. Aufbau des Internets | 4 |
| 3. Funktionsweise | 4 |
| a) IP-Adresse | 4 |
| b) Port-Nummern | 5 |
| c) Transportprotokolle | 6 |
| d) Akteure des Internets | 7 |
| 4. Dienste im Internet | 7 |
| a) TELNET | 8 |
| b) World Wide Web | 8 |
| c) E-Mail | 9 |
| d) Web 2.0/Social Software | 10 |
| aa) Usenet/Newsgroups | 11 |
| bb) Internet Relay Chat (IRC) | 11 |
| cc) Online-Netzwerke | 11 |
| dd) Wikis, Weblogs, Foto- und Videoportale | 12 |
| ee) Virtuelle Welten | 12 |
| 5. Organisation und Verhalten im Netz | 13 |
| III. Datenschutz | 14 |
| 1. Kryptographie | 15 |
| 2. Steganographie | 15 |
| 3. AN.ON-Anonymität. Online | 15 |
| IV. Nationale und internationale Normen | 17 |
| 1. Nationale Normen | 17 |
| a) Telemediengesetz – TMG | 18 |
| b) Telekommunikationsgesetz – TKG | 19 |
| c) Telekommunikationsüberwachungsverordnung – TKÜV | 20 |
| d) Jugendschutzgesetz – JuSchG/Jugendmedienstaatsvertrag – JMStV | 20 |
| e) Urheberrechtsgesetz – UrhG | 21 |
| 2. Internationale Normen | 21 |
| a) Rahmenbeschluss des Rates über Angriffe auf Informationssysteme vom 24. 2. 2005 | 22 |
| b) Cyber-Crime Konvention | 23 |

| | |
|--|----|
| c) Gesetz zur Regelung der internationalen Rechtshilfe – IRG | 24 |
| d) Gesetz zum europäischen Haftbefehl – EUHfG | 24 |
| V. Anwendung deutschen Strafrechts | 25 |
| B. Materielles Recht/Erscheinungsformen | 27 |
| I. Straftaten gegen den Computer/das Internet | 27 |
| 1. Computerbetrug, § 263 a StGB | 27 |
| a) Rechtsgut | 28 |
| b) Tatbestand | 28 |
| aa) Tatgegenstand | 28 |
| bb) Tathandlung | 28 |
| (1) Unrichtige Gestaltung des Programms, § 263 a Abs. 1 | |
| 1. Var. StGB | 29 |
| (2) Verwendung unrichtiger oder unvollständiger Daten, | |
| § 263 a Abs. 1 2. Var. StGB | 30 |
| (3) Unbefugte Verwendung von Daten, § 263 a Abs. 1 | |
| 3. Var. StGB | 30 |
| (aa) Missbräuchliche Verwendung von Codekarten | 32 |
| (bb) Einsatz von Karten innerhalb automatisierter | |
| Zahlungssysteme | 33 |
| (cc) Unberechtigter Zugang zu Pay-TV-Programmen | 34 |
| (4) Sonstige unbefugte Einwirkung auf den Ablauf, | |
| § 263 a Abs. 1 4. Var. StGB | 34 |
| c) Spezifische Erscheinungsformen | 35 |
| aa) Phishing und Pharming | 35 |
| bb) Beteiligung am Phishing/Pharming | 38 |
| cc) Skimming | 39 |
| d) Besonderheiten des Computerbetrugs | 41 |
| aa) Strafbare Vorbereitungshandlung, § 263 a Abs. 3 StGB | 41 |
| bb) Strafantrag | 42 |
| 2. Ausspähen von Daten, § 202 a StGB | 42 |
| a) Rechtsgut | 43 |
| b) Tatbestand | 45 |
| aa) Tatgegenstand | 45 |
| (1) Nicht für den Täter bestimmt | 46 |
| (2) Besondere Zugangssicherung | 47 |
| bb) Tathandlung – Zugangsverschaffung | 48 |
| c) Spezifische Erscheinungsformen, Hackertechniken | 49 |
| aa) Technische Vorbereitungshandlungen | 50 |
| (1) Footprinting | 50 |
| (2) Ping-Scan | 50 |
| (3) Port-Scan | 50 |
| bb) Brute-Force Angriffe | 51 |
| cc) Ausnutzen von Systemlücken | 52 |
| dd) Trojaner | 53 |
| ee) Key-Logger | 54 |
| ff) Snifferprogramme | 54 |
| gg) Man in the Middle/Session Hijacking | 55 |

| | |
|--|----|
| hh) Tarnung der IP-Adresse | 55 |
| (1) Verschleierung | 55 |
| (2) Spoofing | 55 |
| ii) Wardriving | 56 |
| jj) Schwarz-Surfen | 57 |
| kk) Phishing | 57 |
| d) Keine Versuchsstrafbarkeit/Strafantrag | 58 |
| 3. Abfangen von Daten, § 202 b StGB | 58 |
| a) Rechtsgut | 58 |
| b) Tatbestand | 59 |
| aa) Tatgegenstand | 59 |
| bb) Tathandlung | 59 |
| c) Strafantrag | 60 |
| 4. Vorbereiten des Ausspähens und Abfangens von Daten, § 202 c StGB | 60 |
| a) Rechtgut | 60 |
| b) Tatbestand | 60 |
| aa) Passwörter und andere Sicherungscodes, § 202 c Nr. 1 StGB | 61 |
| bb) Hacker-Tools, § 202 c Nr. 2 StGB | 61 |
| cc) Phishing | 63 |
| c) (Kein) Strafantrag | 63 |
| 5. Datenveränderung, § 303 a StGB | 64 |
| a) Rechtsgut | 64 |
| b) Tatbestand | 64 |
| aa) Tatgegenstand/Fremdheit der Daten | 64 |
| (1) Rechte am Datenträger oder den Daten | 66 |
| (2) Urheberchaft | 68 |
| (3) In fremdem Auftrag erstellte Daten | 69 |
| bb) Tathandlung | 70 |
| (1) Löschen | 70 |
| (2) Unterdrücken | 70 |
| (3) Unbrauchbarmachen | 71 |
| (4) Verändern | 72 |
| cc) Vorbereitung | 72 |
| c) Spezifische Erscheinungsformen/Manipulationstechniken | 72 |
| aa) Einsatz von Schadprogrammen | 72 |
| (1) Viren | 73 |
| (2) Logische Bomben | 73 |
| (3) Hoax | 73 |
| (4) Würmer | 74 |
| bb) DOS- und DDOS-Attacken | 74 |
| cc) Spamming und Mailbombing | 75 |
| dd) Online-Demonstration | 77 |
| ee) Dialer | 78 |
| ff) Füllen eines leeren Speicherplatzes | 78 |
| gg) Cookies | 79 |
| d) Strafantrag | 79 |

Inhaltsverzeichnis

| | |
|--|----|
| 6. Computersabotage, § 303 b StGB | 79 |
| a) Rechtsgut | 79 |
| b) Tatbestand | 79 |
| aa) Tatgegenstand | 80 |
| (1) Datenverarbeitung | 80 |
| (2) Für einen Anderen von wesentlicher Bedeutung | 80 |
| bb) Tathandlung, § 303 b Abs. 1 StGB – Erhebliches Stören | 82 |
| (1) § 303 b Abs. 1 Nr. 1 StGB | 82 |
| (2) § 303 b Abs. 1 Nr. 2 StGB | 82 |
| (3) § 303 b Abs. 1 Nr. 3 StGB | 83 |
| cc) Qualifikation § 303 b Abs. 2 StGB | 84 |
| dd) Besonders schwere Fälle § 303 b Abs. 4 StGB | 85 |
| ee) Vorbereitungshandlung | 86 |
| c) Strafantrag | 86 |
| 7. Fälschung technischer Aufzeichnungen, § 268 StGB | 86 |
| a) Rechtsgut | 87 |
| b) Tatbestand | 87 |
| aa) Tatgegenstand | 87 |
| bb) Tathandlung | 87 |
| 8. Fälschung beweisereheblicher Daten, § 269 StGB | 88 |
| a) Rechtsgut | 88 |
| b) Tatbestand | 89 |
| aa) Tatgegenstand | 89 |
| bb) Tathandlung | 89 |
| (1) Speichern | 89 |
| (2) Verändern | 89 |
| (3) Gebrauchen | 90 |
| c) Spezifische Erscheinungsformen | 90 |
| aa) Versenden einer Phishing-Mail | 90 |
| bb) Verwenden einer falschen E-Mail-Adresse | 91 |
| 9. Täuschung im Rechtsverkehr bei der Datenverarbeitung, § 270 StGB | 92 |
| 10. Mittelbare Falschbeurkundung, §§ 271, 348 StGB | 92 |
| a) Rechtsgut | 92 |
| b) Tatbestand | 92 |
| aa) Tatgegenstand | 92 |
| bb) Tathandlung | 92 |
| 11. Urkundenunterdrückung, § 274 StGB | 93 |
| 12. Erschleichen von Leistungen, § 265 a StGB | 93 |
| a) Automatenmissbrauch | 93 |
| b) Missbrauch von Telekommunikationsnetzen | 94 |
| 13. Störung von Telekommunikationsanlagen, § 317 StGB | 95 |
| II. Straftaten mittels Computer/Internet | 95 |
| 1. Betrug, § 263 StGB | 95 |
| a) Rechtsgut | 96 |
| b) Tatbestand | 96 |
| aa) Täuschungshandlung | 96 |
| bb) Irrtum | 96 |

Inhaltsverzeichnis

| | |
|--|-----|
| cc) Vermögensverfügung | 97 |
| dd) Vermögensschaden. | 97 |
| c) Spezifische Erscheinungsformen | 97 |
| aa) Online-(Versand)-Handel. | 97 |
| bb) Online-Auktionen | 98 |
| cc) Installation von Dialerprogrammen. | 99 |
| dd) Nigeria-Connection | 99 |
| 2. Unerlaubte Veranstaltung eines Glücksspiels, § 284 StGB | 100 |
| a) Rechtsgut | 101 |
| b) Tatbestand | 102 |
| aa) Tatgegenstand | 102 |
| (1) Glücksspiel | 102 |
| (2) Geschicklichkeitsspiel. | 102 |
| (3) Wette | 102 |
| (4) Sport-, Renn- und Odsettwetten | 103 |
| (5) Öffentlichkeit des Glücksspiel. | 103 |
| bb) Tathandlung | 104 |
| (1) Veranstalten, Halten oder Bereitstellen der Einrichtung eines Glücksspiels | 104 |
| (2) Fehlen der behördlichen Erlaubnis | 104 |
| c) Besonderheiten der unerlaubten Veranstaltung eines Glücksspiels | 105 |
| aa) Anwendung deutschen Strafrechts | 105 |
| bb) Sperrverfügungen gegen Provider | 106 |
| 3. Besitz und Verbreitung pornographischer Schriften, § 184 StGB | 107 |
| a) Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Schriften, § 184 b und § 184 c StGB | 109 |
| aa) Rechtsgut | 110 |
| bb) Tatbestand. | 110 |
| (1) Tatgegenstand | 110 |
| (2) Tathandlungen. | 111 |
| (aa) Verbreiten | 111 |
| (bb) Zugänglichmachen | 111 |
| (cc) Vorbereitungshandlungen. | 112 |
| (dd) Besitz- und Besitzverschaffung | 112 |
| cc) Besonderheiten | 114 |
| (1) § 184 c StGB – eingeschränkte Tathandlung | 114 |
| (2) § 184 c StGB – Scheinerwachsene | 115 |
| (3) Ausnahmeregelung für bestimmte Personengruppen. | 115 |
| 4. Verbreitung pornographischer Darbietungen durch Rundfunk, Medien- oder Teledienste, § 184 d StGB | 116 |
| 5. Anleitung zu Straftaten, § 130 a StGB | 116 |
| 6. Volksverhetzung und Gewaltdarstellung, §§ 130, 131 StGB | 117 |
| 7. Beleidigung, § 185 StGB | 119 |
| 8. Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen, § 201 a StGB | 119 |

| | |
|---|-----|
| 9. Offenbarung und Verwertung fremder Geheimnisse, §§ 203, 204 StGB | 120 |
| 10. Verletzung des Post- und Fernmeldegeheimnisses, § 206 StGB | 120 |
| a) Rechtsgut | 121 |
| b) Tatbestand | 121 |
| aa) Tatgegenstand | 121 |
| bb) Tathandlung | 121 |
| c) Spezifische Erscheinungsformen | 122 |
| aa) Ausfiltern von E-Mails | 122 |
| bb) Entscheidung des OLG Karlsruhe – „Hochschulfall“ | 124 |
| cc) Geheime Mitarbeiterkontrollen | 125 |
| 11. Nachstellung, § 238 StGB | 127 |
| a) Rechtsgut | 127 |
| b) Tatbestand | 128 |
| aa) Tatgegenstand | 128 |
| bb) Tathandlung | 128 |
| c) Antragerfordernis und Prozessuales | 128 |
| 12. Urheberrechtsverletzungen, §§ 106, 108 a UrhG | 129 |
| a) Rechtsgut | 130 |
| b) Tatbestand des § 106 UrhG, unerlaubte Verwertung urheberrechtlich geschützter Werke | 131 |
| aa) Tatgegenstand | 131 |
| bb) Tathandlungen | 131 |
| (1) Vervielfältigen | 131 |
| (2) Verbreiten | 134 |
| (3) Öffentliche Wiedergabe | 134 |
| c) Tatbestand des § 108 UrhG, unerlaubte Eingriffe in verwandte Schutzrechte | 134 |
| d) Tatbestand des § 108 a UrhG, gewerbsmäßige unerlaubte Verwertung | 134 |
| e) Tatbestand des § 108 b UrhG, unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtswahrnehmung erforderlicher Informationen | 135 |
| f) Spezifische Erscheinungsformen | 136 |
| aa) Erstellen von Privatkopien | 136 |
| bb) Filesharing-Tauschbörsen | 138 |
| g) Besonderheiten bei Urheberrechtsverletzungen | 142 |
| aa) Identitätsermittlung | 142 |
| bb) Rolle der „privaten Ermittler“ | 145 |
| cc) Drittauskunftsanspruch, § 101 UrhG | 147 |
| dd) Strafantrag | 148 |
| 13. Markenrechtsverletzungen, § 143 MarkenG | 149 |
| 14. Verrat von Geschäfts- und Betriebsgeheimnissen, § 17 UWG | 149 |
| a) Rechtsgut | 149 |
| b) Tatbestand | 149 |
| aa) Tatgegenstand | 149 |
| bb) Tathandlungen | 150 |
| (1) Sich Verschaffen | 150 |

| | |
|---|-----|
| (2) Sicherung | 150 |
| (3) Verwertung | 150 |
| c) Besonderheiten | 151 |
| aa) Absicht | 151 |
| bb) Strafantrag | 151 |
| 15. Datenschutzverletzungen, §§ 3, 43, 44 BDSG | 151 |
| 16. Abhörverbot, §§ 89, 148 TKG | 153 |
| 17. Verstoß gegen Arzneimittelgesetz, §§ 95, 96 AMG | 154 |
| <hr/> | |
| C. Inanspruchnahme von Providern/Haftung für Inhalte | 155 |
| I. Datenspeicherung | 156 |
| 1. Daten | 156 |
| a) Inhaltsdaten | 156 |
| b) Verkehrsdaten/Nutzungsdaten | 156 |
| c) Abrechnungsdaten | 157 |
| d) Bestandsdaten/Benutzerdaten | 158 |
| e) Zugangsdaten | 159 |
| f) Standort-/Positions-/Geodaten | 159 |
| g) Zukünftige Daten | 159 |
| 2. Speicherung | 160 |
| a) Recht zur Speicherung | 160 |
| b) Pflicht zur Speicherung/Vorratsdatenspeicherung | 162 |
| aa) BVerfG – Beschl. v. 11. 3. 2008 | 163 |
| bb) BVerfG – Beschl. v. 28. 10. 2008 | 164 |
| cc) VG Berlin – Beschl. v. 17. 10. 2008 und 16. 1. 2009 | 165 |
| dd) VG Wiesbaden – Beschl. v. 27. 2. 2009 | 166 |
| ee) Kritik aus der Literatur | 166 |
| II. Auskunftserteilung | 167 |
| 1. Auskunft gem. § 100 g StPO – Erhebung von Verkehrsdaten | 168 |
| a) Anordnungsvoraussetzungen | 169 |
| aa) Materiell | 169 |
| bb) Formell | 169 |
| cc) Rechtsmittel | 170 |
| 2. Manuelles und automatisiertes Auskunftsverfahren, §§ 112, 113 TKG | 171 |
| 3. Auskunft über Anschlussinhaber hinter einer IP-Adresse | 172 |
| 4. Drittauskunftsanspruch, § 101 UrhG | 175 |
| III. Sperrverfügungen gegen Access- und Host-(Service) Provider | 175 |
| IV. Haftung für Inhalte/Privilegierung | 178 |
| 1. Dogmatische Zuordnung der Haftungsprivilegierungen | 178 |
| 2. Content-Provider, § 7 Abs. 1 TMG | 179 |
| 3. Access-Provider, § 8 TMG | 179 |
| 4. Caching, § 9 TMG | 182 |
| 5. Host-Provider, § 10 TMG | 183 |
| a) Kenntnis | 183 |
| b) Tätigwerden | 183 |
| c) Zumutbarkeit | 183 |
| 6. Einzelfragen | 184 |

Inhaltsverzeichnis

| | |
|--|-----|
| a) Hyperlinks | 184 |
| b) Gästebücher, Foren und Suchmaschinen | 185 |
| c) Weiterleitung von E-Mails | 186 |
| d) Urheberrechtsverletzungen – P2P-Netze | 187 |
| e) Anonymisierungsserver | 187 |
| D. Prozessuales Recht | 189 |
| I. Beweisgewinnung | 189 |
| 1. Ermittlungsmaßnahmen (national) | 190 |
| a) Telekommunikationsüberwachung, §§ 100 a–100 i, 101 StPO | 190 |
| aa) Eingriffsvoraussetzungen der Telekommunikations- überwachung, § 100 a StPO | 192 |
| (1) Bestimmter Tatverdacht, § 100 a StPO | 194 |
| (2) Kernbereichsschutz, § 100 a Abs. 4 StPO | 195 |
| bb) Anordnungsvoraussetzungen und Ausführung, § 100 b StPO | 196 |
| cc) Wohnraumüberwachung, §§ 100 c, 100 d, 100 e StPO | 199 |
| dd) Verkehrsdatenerhebung, § 100 g Abs. 1 StPO | 201 |
| ee) Funkzellenabfrage, § 100 g Abs. 2 S. 2 StPO | 204 |
| ff) Einsatz technischer Mittel, § 100 h StPO | 206 |
| (1) Herstellung von Bildaufnahmen | 207 |
| (2) Verwendung sonstiger technischer Mittel/GPS | 207 |
| gg) Einsatz technischer Mittel beim Mobilfunk/IMSI- Catcher, § 100 i StPO | 208 |
| hh) Benachrichtigung; Löschung personenbezogener Daten, § 101 StPO | 209 |
| ii) Ermittlungsmaßnahme bei Zeugnisverweigerungsrecht, § 160 a StPO | 209 |
| b) Durchsuchung und Beschlagnahme von Daten und EDV-Anlagen, §§ 98, 102, 103 StPO | 210 |
| aa) Durchsuchungsvoraussetzungen, §§ 102, 103 StPO | 211 |
| (1) Materiell-rechtlich, §§ 102, 103 StPO | 211 |
| (2) Formell-rechtlich, § 105 StPO | 212 |
| bb) Beschlagnahmeveraussetzungen, §§ 94 Abs. 2, 98 StPO | 212 |
| cc) Durchsuchungen bei Internet-Providern | 212 |
| dd) Umsetzungen in den Bundesländern | 213 |
| ee) Ablauf der Maßnahme | 215 |
| (1) Vorbereitung | 215 |
| (2) Durchsuchung – 1. Phase | 216 |
| (3) Durchsicht, § 110 StPO – 2. Phase | 216 |
| (aa) Durchsicht, § 110 Abs. 1 und Abs. 2 StPO | 216 |
| (bb) „Fern“-Durchsuchung, § 110 Abs. 3 StPO („Kleine“ Online-Durchsuchung) | 217 |
| (4) Sicherstellung/Beschlagnahme, §§ 94 ff. StPO – 3. Phase | 218 |
| (5) Verhältnismäßigkeit | 220 |
| (6) Sicherung und Auswertung | 221 |

| | |
|--|-----|
| (aa) Sicherung der Daten | 222 |
| (bb) Durchsicht und Auswertung | 222 |
| (7) Mitwirkungspflichten | 225 |
| (8) Verhaltenshinweise für Mandant und Verteidiger | 225 |
| ff) Akteneinsichts- und Besichtigungsrechte der Verteidigung | 226 |
| gg) Zufallsfunde, § 108 StPO | 228 |
| hh) Rechtsmittel | 229 |
| ii) Interventionsmöglichkeiten der Verteidigung | 229 |
| c) Zugriff auf elektronische Speichermedien, | |
| insbesondere E-Mails | 231 |
| aa) Zugriff beim Verdächtigten/Zeugen | 231 |
| bb) Zugriff beim Provider | 231 |
| d) Online-Durchsuchung/Quellentelekommunikations- überwachung | 237 |
| aa) Online-Durchsuchung | 237 |
| bb) Quellentelekommunikationsüberwachung | 239 |
| e) Recherche in Datennetzen | 240 |
| aa) Internetrecherche/Netzpatrouille | 241 |
| (1) Bisherige Praxis | 242 |
| (2) Eingriffsgrundlage | 244 |
| bb) Zugriff auf fremde Server und zugangsgeschützte Inhalte | 245 |
| (1) Präventiv | 247 |
| (2) Repressiv | 247 |
| (aa) Verdeckter Ermittler | 247 |
| (bb) „Fern“-Durchsuchung einer Mailbox | 251 |
| (cc) Interventionsmöglichkeiten der Verteidigung | 252 |
| 2. Ermittlungsmaßnahmen (international) | 254 |
| a) Rechtshilfeverkehr mit dem Ausland in Strafsachen | 254 |
| aa) Allgemeine Voraussetzungen der Rechtshilfe | 254 |
| bb) Rechtshilfeersuchen, § 59 IRG | 255 |
| cc) Einfluss der Cyber-Crime Konvention | 257 |
| b) Europäischer Haftbefehl | 257 |
| aa) Wichtige Regelungen des Rahmenbeschlusses zum Europäischen Haftbefehl | 258 |
| bb) Umsetzung des Rahmenbeschlusses in deutsches Recht .. | 260 |
| cc) Konkrete Ausgestaltung des Verfahrens | 262 |
| c) Fahndung via Internet | 263 |
| aa) Voraussetzungen | 264 |
| bb) Anordnungscompetenz | 265 |
| cc) Anfechtungsmöglichkeiten und Verwertbarkeit | 266 |
| 3. Technische Identifizierungsmöglichkeiten durch die Nutzung von E-Mail und Internet | 267 |
| a) Arten von Spuren | 267 |
| aa) Angaben im Impressum einer Website | 267 |
| bb) Angaben bei DENIC | 268 |
| cc) Personenbezogene Daten beim Provider | 268 |
| b) Spuren im World Wide Web | 268 |
| aa) Datenfluss | 269 |

Inhaltsverzeichnis

| | |
|---|-----|
| bb) IP-Spoofing | 271 |
| cc) Cookies | 272 |
| dd) Session-IDs | 273 |
| ee) Web-Bugs bzw. ClearGIFs | 273 |
| ff) Schnüffelprogramme: Spyware und Adware | 274 |
| gg) Lesezeichen im Internet-Explorer | 275 |
| hh) Bannerwerbung | 275 |
| ii) Smart-Browsing-Funktion im Netscape Communicator | 275 |
| jj) Portscanning | 275 |
| c) Spuren beim E-Mail-Verkehr | 276 |
| aa) Datenfluss | 276 |
| bb) Informationen der einzelnen Teile der E-Mail | 277 |
| (1) Briefkopf | 278 |
| (2) Technische Angaben | 278 |
| (3) Zustellvermerke | 279 |
| cc) Mailinglists | 279 |
| dd) Mail-Adressen | 280 |
| ee) Spam-Mails | 280 |
| ff) Funktionsweise einiger per E-Mail versandter Viren | 281 |
| d) News | 282 |
| aa) Datenfluss | 282 |
| bb) Archive | 282 |
| cc) News-Header | 283 |
| e) Internet Relay Chat (IRC) | 283 |
| aa) Datenfluss | 283 |
| bb) Robots | 283 |
| f) Selbstdatenschutz/Vermeidung von Spuren | 284 |
| aa) Internet | 284 |
| bb) E-Mail-Verkehr | 285 |
| II. Beweisverwertung | 286 |
| 1. Beweiswert elektronischer Daten | 286 |
| a) Beweiswert von E-Mails | 287 |
| b) Beweiswert von IP-Adressen | 289 |
| 2. Einführung in die Hauptverhandlung | 291 |
| a) Zeugenbeweis | 291 |
| b) Augenscheinsbeweis | 291 |
| c) Urkundenbeweis | 292 |
| 3. Beweisverwertungsverbote | 292 |
| a) Auslandsermittlungen | 293 |
| b) Verwertung von rechtswidrig vorgehaltenen (personenbezogenen) Daten | 295 |
| Technisches Glossar | 299 |
| Stichwortverzeichnis | 307 |