

Inhaltsverzeichnis

<i>Vorwort</i>	Seite V
<i>Abkürzungsverzeichnis</i>	XIII
Einleitung	1
Kapitel 1: Herausforderungen bei der Bekämpfung der Internetkriminalität	5
I. Einleitung	7
1. Abhängigkeit der Gesellschaft von der Verfügbarkeit der Informationstechnologie	8
2. Die Gewährleistung einer effektiven Strafverfolgung	9
3. Möglichkeiten der Strafverfolgungsbehörden	9
4. Die Notwendigkeit einer Berücksichtigung der Herausforderungen	11
II. Überblick und Einzelaspekte	13
1. Grad der Abhängigkeit der Informationsgesellschaft von der Verfügbarkeit der Informations- und Kommunikationsinfrastruktur	13
2. Quantität von Nutzern, Information und Diensten	14
3. Verfügbarkeit von Tatwerkzeugen	16
4. Verfügbarkeit von Internetzugängen zur Tatbegehung	19
5. Anonymität	20
6. Verfügbarkeit von Informationen zur Tatbegehung	23
7. Fehlende Kontrollinstrumente	26
8. Automatisierung	29
9. Ressourcen	31
10. Unabhängigkeit von Tat- und Handlungsort/ Transnationale Dimension	33
11. Geschwindigkeit der Datenübertragung	36
12. Computerdaten als Beweismittel	38
13. Verschlüsselungstechnologie	39
Kapitel 2: Entwicklung der rechtlichen Rahmenbedingungen des Internetstrafrechts	44
I. Entwicklung der gesetzlichen Grundlagen in Deutschland	47
1. Zweites Gesetz zur Bekämpfung der Wirtschafts- kriminalität (1986)	47
2. Informations- und Kommunikationsdienstegesetz (1997) ..	48
3. Erstes Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft (2003)	49
4. Gesetz zur Änderung der Strafprozessordnung (2001)	49
5. Zweites Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft (2007)	50
6. Gesetz zur Neuregelung der Telekommunikations- überwachung (2007)	50
7. 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (2007)	51

Inhaltsverzeichnis

a)	Umgehung wirksamer technischer Schutzmaßnahmen (§ 108b Abs. 1 Nr. 1 UrhG)	208
b)	Veränderung von Informationen zur Rechte- wahrnehmung (§ 108b Abs. 1 Nr. 2a) UrhG)	213
c)	Verbreitung von manipulierten Werken (§ 108b Abs. 1 Nr. 2b) UrhG)	218
d)	Interaktion mit Tatwerkzeugen (§ 108b Abs. 2 UrhG)	220
11.	Strafschärfung für gewerbsmäßige Handlungen (§ 108a UrhG)	224
12.	Prozessuale Besonderheiten	225
a)	Zuständigkeit der Gerichte	225
b)	Strafantrag (§ 109 UrhG)	225
c)	Privatklage	226
d)	Nebenklage	227
e)	Adhäsionsverfahren.	227
f)	Einziehung (§ 110 UrhG)	227
g)	Beschränkung der Durchführung von Ermittlungen.	228
Kapitel 4: Verantwortlichkeit der Diensteanbieter		232
I.	Einleitung	234
II.	Entwicklung der primärrechtlichen Regelungen zur Verantwortlichkeit	236
III.	Bedeutung der Verantwortlichkeitsregelungen für die Praxis.	237
IV.	Systematik.	238
1.	Das TMG und seine Abgrenzung zu anderen Regelungswerken	238
a)	Abgrenzung zum Rundfunk.	239
b)	Abgrenzung zum TKG.	240
c)	Telekommunikationsgestützte Dienste gemäß § 3 Nr. 25 TKG	240
d)	Reine Telekommunikationsdienste gemäß § 3 Nr. 24 TKG	241
2.	Rechtsgebietsspezifischer Anwendungsbereich	242
3.	Dogmatische Einordnung.	242
a)	Integrationslösung.	243
b)	Vorfilterlösung	243
4.	Persönlicher Anwendungsbereich	243
5.	Funktionsspezifischer Anwendungsbereich und Details der Verantwortlichkeit	244
a)	Content-Provider (§ 7 Abs.1 TMG).	245
b)	Hosting-Provider (§ 10 TMG).	247
c)	Access-Provider (§ 8 Abs. 1 TMG)	251
d)	Technisch bedingte Zwischenspeicherung (§ 8 Abs. 2 TMG)	255
e)	Caching- und Proxy-Provider (§ 9 TMG)	256
f)	Verantwortlichkeit für Hyperlinks.	258
g)	Verantwortlichkeit für Suchmaschinen	261

Kapitel 5: Strafprozessrecht	262
I. Einleitung	268
II. Terminologie	269
III. Ermittlungsmaßnahmen	270
1. Zugriff auf Bestandsdaten	271
a) Zugriff bei Telemedienanbietern	271
b) Zugriff bei Telekommunikationsanbietern	272
c) Sonderfall: Rasterfahndung	283
d) Datenschutzrechtliche Aspekte	287
2. Zugriff auf Nutzungs- und Verkehrsdaten	291
a) Vorfragen	291
b) Zugriff bei Telemedienanbietern	294
c) Zugriff bei Telekommunikationsanbietern	295
d) Zugriff bei Teilnehmern einer Telekommunikation	308
e) Datenschutzrechtliche Aspekte	308
3. Zugriff auf Inhaltsdaten	314
a) Zugriff auf frei zugängliche Daten	315
b) Zugriff mit Hilfe von Nutzern	316
c) Zugriff auf Daten beim Provider	317
d) Heimliche Online-Zugriffe auf informationstechnische Systeme	336
e) Quellen-Telekommunikationsüberwachung	347
f) Datenschutzrechtliche Aspekte	350
4. Umgehungs- und Verschleierungsmöglichkeiten	351
a) Anonymer Internet-Access	352
b) Anonyme Nutzung von Internet-Diensten	355
c) Anonymität auf Rechner Ebene	362
5. Internet-Fahndung	363
a) Ausschreibung zur Festnahme	364
b) Aufenthaltsermittlung	365
c) Besonderheiten für Abbildungen	366
d) Umsetzung der Maßnahmen	366
6. Zugriff auf körperliche Gegenstände	366
a) Durchsuchung und Beschlagnahme	367
b) Untersuchung und Verwertung	372
IV. Computerdaten als Beweismittel	374
1. Beweiseinführung	374
2. Forensisches Verfahren	375
3. Beweisverwertungsverbote	382
V. Praktische Verhaltenshinweise	383
1. Beschuldigte	383
2. Opfer und Anzeigenerstatter	384
3. Zeugen und unbeteiligte Dritte	385
<i>Stichwortverzeichnis</i>	389