

Computerkriminalität und Recht der Internetkommunikation

Bilişim Suçları ve İnternet İletişim Hukuku

Murat Volkan Dülger

11. Aufl., Seçkin Verlag, Ankara, Mai 2025, 1008 Seiten, ISBN 9786253810702

■ Inhaltsverzeichnis

Vorwort zur elften Auflage	6
Vorwort zur zehnten Auflage	7
Vorwort zur neunten Auflage	9
Vorwort zur achten Auflage	11
Vorwort zur siebten Auflage	12
Vorwort zur sechsten Auflage	14
Vorwort zur fünften Auflage	16
Vorwort zur vierten Auflage	19
Vorwort zur dritten Auflage	22
Vorwort zur zweiten Auflage	24
Vorwort zur ersten Auflage	26
Abkürzungen	51
Einleitung	55

ERSTES KAPITEL

DEFINITION DES COMPUTERS, DER INFORMATIK, DER COMPUTERKRIMINALITÄT UND DER ZUGEHÖRIGEN BEGRIFFE SOWIE GESCHICHTE DES COMPUTERS UND DER COMPUTERKRIMINALITÄT

I. TERMINUS UND BEGRIFF	61
A. Computer	62
1. Der Terminus „Computer“	62
2. Definition des Computers	63
a. Definition nach den Aufgaben und Funktionen des Computers	64
b. Definition nach den physischen Eigenschaften sowie den Aufgaben und Funktionen des Computers	65
c. Hauptbestandteile des Computers	66
aa. Hauptprozessor	67
bb. Nur-Lese-Speicher	67
cc. Speicher mit wahlfreiem Zugriff	67
dd. Periphere Ein- und Ausgabeeinheiten	68
ee. Betriebssystem	68
ff. Anwendungssoftware	69
d. Arten von Computern	69
e. Unterscheidungsmerkmale und vermittelnde Definition	70
f. Bewertung und eigene Auffassung	71
g. Arbeitslogik und Arbeitsweise des Computers	72
B. Informatik und informationstechnisches System	72

C.	Computerkriminalität	76
1.	Das Terminologieproblem	76
2.	Inhalt des Begriffs der Computerkriminalität	80
D.	Daten	83
E.	Internet	84
1.	Definition	84
2.	Technischer Aufbau, Infrastruktur und Verwaltungsform des Internets	87
a.	Technischer Aufbau des Internets	87
aa.	Das TCP/IP-Protokoll	88
bb.	Das System des World Wide Web	88
b.	Infrastruktur des Internets	88
c.	Die Verwaltungsform des Internets im Allgemeinen	89
II.	GESCHICHTLICHE ENTWICKLUNG	92
A.	Geschichtliche Entwicklung des Computers	92
1.	Erste Phase	94
2.	Zweite Phase	95
3.	Dritte Phase	95
4.	Vierte Phase	96
B.	Geschichtliche Entwicklung des Internets	97
C.	Geschichtliche Entwicklung der Computerkriminalität	100

ZWEITES KAPITEL

BEGEHUNGSWEISEN DER COMPUTERKRIMINALITÄT, IHR VERHÄLTNIS ZUR KRIMINOLOGIE, ZUR WIRTSCHAFTSKRIMINALITÄT UND ZUM TERRORISMUS SOWIE COMPUTERKRIMINALITÄT IM RECHTSVERGLEICH

I.	BEGEHUNGSWEISEN DER COMPUTERKRIMINALITÄT	109
A.	Allgemeines	109
B.	Begehungsweisen	110
1.	Trojanisches Pferd (Trojan Horse)	110
2.	Salami-Technik	111
3.	Überwindung der Systemsicherheit und Eindringen in das System (Hacking)	112
a.	Straftaten begehende Computerpiraten (Hacker)	112
b.	Ehemalige Computerpiraten, die die Systemsicherheit testen (Ethical Hacker)	115
4.	Netzwerkwürmer (Network Worms)	115
5.	Kaninchen (Rabbits)	116
6.	Chamäleons (Chameleons)	117
7.	Logische Bomben (Logic Bombs)	117
8.	Computerviren	118
9.	Unverlangt empfangene E-Mails (Spam)	119
10.	Anbieten rechtswidriger Inhalte	122
11.	Dienstverweigerungsangriffe (DoS) und verteilte Dienstverweigerungsangriffe (DDoS)	123
12.	Köderangriffe (Phishing)	123
13.	Angriffe zum Knacken von Passwörtern	123
14.	Botnetz-Angriff	124
15.	Mülltauchen (Scavenging)	125
16.	Unrechtmäßiger Missbrauch des DNS	125
17.	Umleitung von Webseiten	126

18.	Scannen	126
19.	Cybermobbing (Cyberbullying)	127
20.	Erpressungssoftware (Ransomware)	128
21.	Sonstige Methoden	129
II.	DAS VERHÄLTNISS DER COMPUTERKRIMINALITÄT ZUR KRIMINOLOGIE UND ZUR WIRTSCHAFTSKRIMINALITÄT	129
A.	Das Verhältnis der Computerkriminalität zur Kriminologie	129
1.	Allgemeines	129
2.	Allgemeine Merkmale der Computerstraftäter	132
B.	Das Verhältnis der Computerkriminalität zur Wirtschaftskriminalität	134
1.	Wirtschaftsrecht	135
2.	Weißer-Kragen-Kriminalität und Wirtschaftsstraftat	137
a.	Weißer-Kragen-Kriminalität	137
b.	Begriff und Definition der Wirtschaftsstraftat	139
aa.	Wirtschaftsstraftaten aus kriminologisch-soziologischer Sicht	140
bb.	Wirtschaftsstraftaten aus Sicht der Regeln des Strafverfahrens	141
cc.	Wirtschaftsstraftaten aus Sicht des durch den Straftatbestand geschützten Rechtsguts	141
c.	Bewertung und eigene Auffassung	142
3.	Computerkriminalität als Wirtschaftskriminalität	143
III.	SOZIALE MEDIEN	144
A.	Allgemeines	144
B.	Definition	145
C.	Formen der sozialen Medien	146
D.	Unterschied der sozialen Medien zu den industriellen Medien	147
E.	Einfluss der sozialen Medien auf Unternehmen	148
F.	Aufbau sozialer Autorität	149
G.	Auswirkungen der sozialen Medien auf die Internetnutzung	150
H.	Mögliche historische / politische Auswirkungen der sozialen Medien	153
I.	Wirtschaftliche Auswirkungen des aus den sozialen Medien hervorgegangenen sozialen Marketings	153
i.	Auswirkungen der sozialen Medien auf die Bildung	155
J.	Inhaberschaft an den Inhalten, aus denen die sozialen Medien bestehen	156
K.	Soziale Medien und die COVID-19-Pandemie	156
L.	Kritik an den sozialen Medien	158
IV.	DER EINFLUSS DER MASSEN MEDIEN – INSBESONDERE DES INTERNETS – AUF DEN TERRORISMUS	159
A.	Terrorismus im Allgemeinen und Definition des Terrorismus	159
B.	Auswirkungen der Entwicklungen in der Technologie und in den Informationstechnologien auf den Terrorismus im Allgemeinen	163
1.	Auswirkungen der technologischen Entwicklungen bei den Verkehrsmitteln auf den Terrorismus	165
2.	Auswirkungen der Entwicklungen in der Waffentechnologie auf den Terrorismus	166
3.	Auswirkungen der Entwicklungen in der Technologie der individuellen Kommunikationsmittel auf den Terrorismus	167
4.	Auswirkungen der Entwicklungen bei den informationstechnischen Systemen auf den Terrorismus	168
C.	Auswirkungen der Entwicklungen bei den Massenmedien auf den Terrorismus	173
1.	Das Verhältnis zwischen Massenmedien und Terrorismus im Allgemeinen	173

2.	Die Berichterstattung der Massenmedien über Terrorakte	175
a.	Berichterstattung während der Tat	178
b.	Berichterstattung nach der Tat	180
3.	Bewertung der Diskussionen über die Berichterstattung der Massenmedien über Terrorakte unter dem Gesichtspunkt der Meinungs- und Pressefreiheit	180
a.	Die Auffassung, dass die Beschränkung durch Gesetz erfolgen müsse	181
b.	Die Auffassung, dass die Beschränkung durch Selbstkontrolle erfolgen müsse	182
D.	Cyberterrorismus	183
1.	Begriff und Definition	183
2.	Unterschiede und Vorteile des Cyberterrors gegenüber dem herkömmlichen Terror	186
3.	Risiko und Angriffsmethoden des Cyberterrors	189
E.	Cyberkrieg	191
F.	Hackivismus und rechtliche Bewertung hackivistischer Aktionen	193
G.	Bewertung und eigene Auffassung	194
V.	DIE INTERNATIONALE DIMENSION DER COMPUTERKRIMINALITÄT, REGELUNGEN ZUR COMPUTERKRIMINALITÄT IM INTERNATIONALEN RECHT UND IN AUSLÄNDISCHEN NATIONALEN RECHTSORDNUNGEN	198
A.	Die internationale Dimension der Computerkriminalität	198
1.	Notwendigkeit internationaler Zusammenarbeit bei der Bekämpfung der Computerkriminalität	198
2.	Gründe für den grenzüberschreitenden Charakter der Computerkriminalität	199
3.	Das Verhältnis der Computerkriminalität zum internationalen Strafrecht	201
4.	Bewertung und eigene Auffassung	205
B.	Computerkriminalität im internationalen Recht	207
1.	Arbeiten des Europarats zur Computerkriminalität	207
a.	Europäisches Übereinkommen über Computerkriminalität	208
b.	Zusatzprotokoll zum Europäischen Übereinkommen über Computerkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art	212
2.	Rechtsgrundlagen der internationalen Rechtshilfe aus Sicht der Türkei	213
a.	Grundprinzipien der Rechtshilfe	215
aa.	Ersuchen werden nach den Rechtsvorschriften des ersuchten Staates erledigt	215
bb.	Grundsätzlich werden keine Kosten erhoben	215
cc.	Das Ersuchen und seine Anlagen werden in die Amtssprache des ersuchten Staates übersetzt	215
b.	Gründe für die Ablehnung eines Rechtshilfeersuchens	215
aa.	Der ersuchte Staat sieht das Ersuchen als auf politische oder fiskalische Straftaten bezogen an	215
bb.	Der ersuchte Staat hält die Erledigung des Ersuchens für unvereinbar mit seiner Souveränität, seiner öffentlichen Ordnung oder seinen sonstigen Interessen	216
c.	Voraussetzung der beiderseitigen Strafbarkeit	216
3.	Rechtshilfe im Rahmen des Europäischen Übereinkommens über Computerkriminalität	216
a.	Die Rechtshilfe betreffende Artikel des Übereinkommens	216
b.	Rechtshilfeersuchen zur Erlangung von Verkehrsdaten / der IP-Nummer bei Computerkriminalität	218
c.	Probleme bei Computerkriminalität, die daraus entstehen, dass der Tatort oder der Aufenthaltort des Beschuldigten unbekannt ist	219
d.	Fälle, in denen die Justizbehörden IP-Informationen und Verkehrsdaten unmittelbar erlangen können	220

e.	Internationale Rechtshilfeersuchen im Rahmen von 7/24 bei Computerkriminalität	221
4.	Arbeiten der Europäischen Union zur Computerkriminalität	222
5.	Arbeiten anderer supranationaler Organisationen zur Computerkriminalität	223
C.	Computerkriminalität in den nationalen Rechtsordnungen	223
1.	Allgemeines	223
2.	Computerkriminalität im US-amerikanischen Recht	224
a.	Gesetz über Computerbetrug und Computermisbrauch	225
b.	Gesetz über den Anstand in der Kommunikation	226
c.	Gesetz zur Verhinderung von Kinderpornografie	226
d.	Gesetz zum Schutz von Kindern vor Online-Veröffentlichungen	227
e.	Gesetz über die Vertraulichkeit der elektronischen Kommunikation	228
f.	Gesetz zur Verhinderung des Glücksspiels im Internet	228
g.	Gesetz über Identitätsdiebstahl	229
h.	Gesetz zur Bekämpfung des Terrorismus	229
i.	Regelungen zur IT-Sicherheitsexpertise	230
3.	Computerkriminalität im deutschen Recht	232
4.	Computerkriminalität im englischen Recht	233
5.	Computerkriminalität im französischen Recht	234
6.	Computerkriminalität im italienischen Recht	235
7.	Computerkriminalität in den Rechtsordnungen anderer Länder	236

DRITTES KAPITEL

DIE IM TÜRKISCHEN STRAFGESETZBUCH GEREGLTEN COMPUTERSTRAFTATEN

I.	ENTSTEHUNG DES TCK, SEIN AUFBAU IM ALLGEMEINEN UND VERGLEICH DER STRAFTATBESTÄNDE	241
A.	Entstehung des TCK	241
B.	Aufbau des TCK im Allgemeinen	242
C.	Einteilung der im TCK geregelten Computerstraftaten	248
II.	DIE IM ABSCHNITT „STRAFTATEN IM BEREICH DER INFORMATIK“ GEREGLTEN STRAFTATBESTÄNDE	249
A.	Die Straftat des rechtswidrigen Zugangs zu einem informationstechnischen System oder des rechtswidrigen Verbleibens im System (Art. 243 Abs. 1–3)	249
1.	Allgemeines	249
2.	Durch den Straftatbestand geschütztes Rechtsgut	253
a.	Das Problem des Wandels des geschützten Rechtsguts	253
b.	Geschützte Rechtsgüter	257
3.	Tatbestandsmäßigkeit	260
a.	Äußere (objektive) Tatbestandsmerkmale	261
aa.	Täter	261
aaa.	Der Täter im Allgemeinen	261
bbb.	Die Frage, ob juristische Personen Täter sein können	263
aaaa.	Verantwortlichkeit juristischer Personen im Hinblick auf den Grundsatz der Höchstpersönlichkeit der Strafe	263
bbbb.	Strafrechtliche Verantwortlichkeit juristischer Personen im Hinblick auf das Schuldprinzip	265
cccc.	Strafrechtliche Verantwortlichkeit juristischer Personen im Hinblick auf die Handlungslehre	266
dddd.	Bewertung und eigene Auffassung	266
eeee.	Die Stellung juristischer Personen im Hinblick auf die Computerkriminalität	269

bb.	Opfer	270
cc.	Tatobjekt	271
dd.	Tat (Handlung)	271
ee.	Ein gesonderter Erfolg ist für diese Straftat nicht erforderlich	278
ff.	Erfolgsqualifizierte Form der Straftat: Verlust oder Veränderung der im System enthaltenen Daten infolge der Tatbegehung (Art. 243 Abs. 3)	279
gg.	Qualifikationen der Straftat	281
aaa.	Allgemeines	281
bbb.	Begehung der Straftat in Bezug auf entgeltlich nutzbare Systeme (Art. 243 Abs. 2)	283
ccc.	Der Fall, dass die Tat des Täters sowohl die Qualifikation als auch die Erfolgsqualifikation verwirklicht (Art. 243 Abs. 2–3)	288
ddd.	Begehung der Straftat zu terroristischen Zwecken (Art. 4, 5 des Antiterrorgesetzes Nr. 3713 – TMK)	289
b.	Inneres (subjektives) Tatbestandsmerkmal	290
4.	Das Merkmal der Rechtswidrigkeit	294
a.	Allgemeines	294
b.	Die Funktion der Aufnahme der Wendung „rechtswidrig“ in die Merkmale der Straftat	296
aa.	Die Auffassung von der besonderen Rechtswidrigkeit	297
bb.	Die Lehre von den gesamttatbewertenden Merkmalen und die differenzierende Lösung	298
cc.	Eigene Auffassung	299
c.	Einwilligung des Opfers	303
d.	Anwendung einer Gesetzesbestimmung	304
e.	Ist Notwehr möglich?	304
f.	Die Ausübung des Journalistenberufs begründet für das unbefugte Eindringen in ein System nicht den Rechtfertigungsgrund der Ausübung eines Rechts	305
g.	Überschreitung der Grenzen der Rechtfertigungsgründe	307
5.	Schuld	307
a.	Allgemeines	307
b.	Gewalt und Drohung	310
c.	Ausführung eines rechtswidrigen verbindlichen Befehls	311
6.	Besondere Erscheinungsformen der Straftat	312
a.	Versuch	312
b.	Beteiligung	313
c.	Konkurrenzen	314
7.	Sanktion, Ermittlungsverfahren und gerichtliches Verfahren	319
B.	Die Straftat des Abfangens von Daten (Art. 243 Abs. 4)	324
1.	Allgemeines	324
2.	Durch den Straftatbestand geschütztes Rechtsgut	326
3.	Tatbestandsmäßigkeit	326
a.	Äußere (objektive) Tatbestandsmerkmale	326
aa.	Täter	326
bb.	Opfer	327
cc.	Tatobjekt	327
dd.	Tat (Handlung)	329
ee.	Qualifikationen der Straftat	330
b.	Innere (subjektive) Tatbestandsmerkmale	330
4.	Rechtswidrigkeit	330

5.	Besondere Erscheinungsformen der Straftat	332
a.	Versuch	332
b.	Beteiligung	332
c.	Konkurrenzen	332
6.	Sanktion, Ermittlungsverfahren und gerichtliches Verfahren	333
C.	Die Straftat der Behinderung oder Störung des Betriebs eines informationstechnischen Systems und die Straftat der Vernichtung oder Veränderung von Daten (Art. 244 Abs. 1–2)	333
1.	Allgemeines	333
2.	Durch die Straftatbestände geschützte Rechtsgüter	335
3.	Tatbestandsmäßigkeit	338
a.	Äußere (objektive) Tatbestandsmerkmale	338
aa.	Täter	338
bb.	Opfer	339
cc.	Tatobjekt der Straftaten	339
aaa.	Allgemeines	339
bbb.	Die Frage, ob Subjekte und Objekte in Virtual-Reality-Spielen Tatobjekt sein können	340
dd.	Tat (Handlung)	341
aaa.	Die in Art. 244 Abs. 1 geregelten Handlungen	342
aaaa.	Behinderung des Betriebs eines informationstechnischen Systems	342
bbbb.	Störung des Betriebs eines informationstechnischen Systems	343
bbb.	Die in Art. 244 Abs. 2 geregelten Handlungen	345
aaaa.	Beschädigung von Daten	345
bbbb.	Vernichtung von Daten	345
cccc.	Veränderung von Daten	347
dddd.	Unzugänglichmachen von Daten	347
eeee.	Einbringen von Daten in ein informationstechnisches System	350
ffff.	Übermittlung der in einem informationstechnischen System vorhandenen Daten an einen anderen Ort	351
ccc.	Bewertung und eigene Auffassung	352
ddd.	Parallelität der im Straftatbestand enthaltenen Handlungen zum Europäischen Übereinkommen über Computerkriminalität (ASSS)	353
eee.	Unterschied zwischen den Handlungen in Art. 244 Abs. 1 und Abs. 2 und ihre Anwendung	354
ee.	Erfolg	354
ff.	Qualifikationen der Straftat	355
aaa.	Begehung der Straftat an einem informationstechnischen System einer Bank oder eines Kreditinstituts oder einer öffentlichen Behörde oder Einrichtung (Art. 244 Abs. 3)	355
bbb.	Begehung der Straftat zu terroristischen Zwecken (Art. 4, 5 des Antiterrorgesetzes Nr. 3713 – TMK)	357
b.	Innere (subjektive) Tatbestandsmerkmale	357
4.	Das Merkmal der Rechtswidrigkeit	357
5.	Besondere Erscheinungsformen der Straftat	359
a.	Versuch	359
b.	Beteiligung	359
c.	Konkurrenzen	360
6.	Sanktion, Ermittlungsverfahren und gerichtliches Verfahren	362

D.	Die Straftat der Erlangung eines rechtswidrigen Vorteils mittels eines informationstechnischen Systems (Art. 244 Abs. 4)	363
1.	Allgemeines	363
2.	Durch den Straftatbestand geschütztes Rechtsgut	365
3.	Tatbestandsmäßigkeit	366
a.	Äußere (objektive) Tatbestandsmerkmale	366
aa.	Täter	366
bb.	Opfer	367
cc.	Tatobjekt	368
dd.	Tat (Handlung)	368
ee.	Erfolg	373
b.	Innere (subjektive) Tatbestandsmerkmale	375
4.	Das Merkmal der Rechtswidrigkeit	377
5.	Besondere Erscheinungsformen der Straftat	377
a.	Versuch	377
b.	Beteiligung	380
c.	Konkurrenzen	380
6.	Sanktion, Ermittlungsverfahren und gerichtliches Verfahren	381
E.	Die Straftaten des Missbrauchs von Bank- oder Kreditkarten (Art. 245)	382
1.	Allgemeines	382
2.	Durch den Straftatbestand geschütztes Rechtsgut	384
3.	Tatbestandsmäßigkeit	387
a.	Äußere (objektive) Tatbestandsmerkmale	387
aa.	Täter	387
bb.	Opfer	388
cc.	Tatobjekt	394
aaa.	Bankkarte	394
bbb.	Kreditkarte	395
ccc.	Bankkarte, Kreditkarte und erlangter Vorteil als Tatobjekt	395
ddd.	Fremdheit der Bank- oder Kreditkarte	396
dd.	Tat (Handlung)	397
aaa.	Erlangung eines rechtswidrigen Vorteils mit einer fremden Bank- oder Kreditkarte (Art. 245 Abs. 1)	398
aaaa.	Es handelt sich um ein mehraktiges und verhaltensungebundenes Delikt	398
bbbb.	Die Handlungen des Sichverschaffens und des Innehabens	399
cccc.	Die Handlungen des Gebrauchs und des Gebrauchenlassens	401
dddd.	Vorteilerlangung mit einer dem Inhaber noch nicht ausgehändigten Karte	401
eeee.	Verwendung fremder Bank- oder Kreditkarten beim Einkauf	403
ffff.	Ausstellenlassen und Verwendung einer Zusatzkarte zu einer fremden Kreditkarte	408
gggg.	Einkauf mit der Karte in virtuellen Netzen	409
hhhh.	Verwendung der Karten über den in der Vereinbarung mit dem Inhaber festgelegten Betrag hinaus	410
iiii.	Verwendung von Geldautomaten zur Erlangung eines unrechtmäßigen Vorteils	411
iiii.	Abhebung von Geld oder Gehalt vom Konto eines Verstorbenen unter Verwendung seiner Bankkarte	412
jjjj.	Verwendung einer fremden Bank- oder Kreditkarte durch Ausstellen eines Belastungsbelegs in einem Vertragsunternehmen	413

bbb.	Herstellung, Verkauf, Übertragung, Ankauf oder Annahme gefälschter Bank- oder Kreditkarten, die mit fremden Bankkonten verknüpft werden (Art. 245 Abs. 2)	414
ccc.	Vorteilserlangung durch Verwendung einer fälschlich hergestellten oder verfälschten Bank- oder Kreditkarte (Art. 245 Abs. 3)	418
aaaa.	Es handelt sich um ein verhaltensungebundenes Delikt	418
bbbb.	Vorteilserlangung mit einer Karte, die mittels unwahrer, gefälschter Unterlagen ausgestellt wurde	419
cccc.	Ausstellung fiktiver Verkaufsbelege mit gefälschten Karten	424
dddd.	Verwendung gefälschter Karten beim Einkauf	426
eeee.	Verwendung einer gefälschten Bank- oder Kreditkarte durch Ausstellen eines Belastungsbelegs in einem Vertragsunternehmen	427
ee.	Erfolg	427
aaa.	Der Erfolg bei den Straftaten in Art. 245 Abs. 1 – 3	427
bbb.	Der Erfolg bei der Straftat in Art. 245 Abs. 2	429
b.	Innere (subjektive) Tatbestandsmerkmale	429
4.	Das Merkmal der Rechtswidrigkeit	430
5.	Besondere Erscheinungsformen der Straftat	432
a.	Versuch	432
b.	Beteiligung	439
c.	Konkurrenzen	443
aa.	Allgemeines	443
bb.	Anwendung der Regel über die fortgesetzte Tat	444
aaa.	Anwendung der fortgesetzten Tat im Hinblick auf Art. 245 Abs. 1	444
bbb.	Anwendung der fortgesetzten Tat im Hinblick auf Art. 245 Abs. 2	450
ccc.	Anwendung der fortgesetzten Tat im Hinblick auf Art. 245 Abs. 3	450
cc.	Verschiedene Konkurrenzprobleme im Zusammenhang mit Art. 245	452
aaa.	Können die Straftat der Erlangung eines rechtswidrigen Vorteils mit einer fremden Bank- oder Kreditkarte (Art. 245 Abs. 1) und der Diebstahl (Art. 141) nebeneinander auf dieselbe Tat angewendet werden?	452
aaaa.	Die einschlägige Entscheidung des Großen Strafsenats des Kassationshofs (YCGK)	452
bbbb.	Bewertung und eigene Auffassung	456
bbb.	Wird die Bankkarte unter dem Vorwand der Hilfeleistung erlangt und das Geld vom Täter an sich genommen, liegt Diebstahl vor	457
ccc.	Das Verhältnis zwischen der Straftat der Erlangung eines rechtswidrigen Vorteils mit einer fremden Bank- oder Kreditkarte (Art. 245 Abs. 1) und dem Betrug (Art. 157)	461
ddd.	Das Verhältnis zwischen der Straftat der Erlangung eines rechtswidrigen Vorteils mit einer fremden Bank- oder Kreditkarte (Art. 245 Abs. 1) und dem qualifizierten Betrug (Art. 158 Abs. 1 Buchst. f)	472
eee.	Das Verhältnis zwischen der Straftat der Erlangung eines rechtswidrigen Vorteils mit einer fremden Bank- oder Kreditkarte (Art. 245 Abs. 1) und dem Vertrauensmissbrauch (Art. 155)	475
fff.	Das Verhältnis zwischen der Herstellung, dem Verkauf, der Übertragung, dem Ankauf oder der Annahme gefälschter, mit fremden Bankkonten verknüpfter Bank- oder Kreditkarten (Art. 245 Abs. 2) und der Urkundenfälschung (Art. 204–207)	478
ggg.	Das Verhältnis zwischen der Straftat der Erlangung eines rechtswidrigen Vorteils mit einer gefälschten Bank- oder Kreditkarte (Art. 245 Abs. 3) und dem qualifizierten Betrug (Art. 158 Abs. 1 Buchst. f)	480
hhh.	Gemeinsame Begehung der Taten nach Art. 245 Abs. 2 und Abs. 3	482
iii.	Gemeinsame Begehung der Taten nach Art. 245 und nach Art. 135 und 136	488

6.	Persönliche Strafausschließungsgründe und persönliche Strafaufhebungsgründe	489
a.	Die Beziehung zwischen Täter und Opfer	490
b.	Tätige Reue	492
7.	Sanktion, Ermittlungsverfahren und gerichtliches Verfahren	497
F.	Die Straftat der Herstellung von und des Handels mit verbotenen Geräten und Programmen (Art. 245/A)	500
1.	Allgemeines	500
2.	Geschütztes Rechtsgut	504
3.	Tatbestandsmäßigkeit	504
a.	Äußere (objektive) Tatbestandsmerkmale	504
aa.	Täter	504
bb.	Opfer	504
cc.	Tatobjekt	504
dd.	Tat (Handlung)	505
b.	Innere (subjektive) Tatbestandsmerkmale	506
4.	Das Merkmal der Rechtswidrigkeit	507
5.	Besondere Erscheinungsformen der Straftat	507
a.	Versuch	507
b.	Beteiligung	508
c.	Konkurrenzen	508
6.	Sanktion, Ermittlungsverfahren und gerichtliches Verfahren	508
III.	COMPUTERSTRAFTATEN UNTER DEN STRAFTATEN GEGEN DAS VERMÖGEN	509
A.	Der unter Verwendung eines informationstechnischen Systems begangene Diebstahl (Art. 142 Abs. 2 Buchst. e)	509
1.	Allgemeines	509
2.	Geschütztes Rechtsgut	512
3.	Tatbestandsmäßigkeit	512
a.	Äußere (objektive) Tatbestandsmerkmale	512
aa.	Täter	512
bb.	Opfer	512
cc.	Tatobjekt	512
aaa.	Daten als Tatobjekt	512
bbb.	Auffassungen zu der Frage, ob Daten die Qualifikation des Diebstahls begründen können, und die einschlägigen Entscheidungen des Kassationshofs	513
aaaa.	Die Auffassung, dass Daten Tatobjekt der Qualifikation des Diebstahls sein können, und Entscheidungen des Kassationshofs	513
bbbb.	Die Auffassung, dass Daten nicht Tatobjekt der Qualifikation des Diebstahls sein können, und Entscheidungen des Kassationshofs	514
cccc.	Die Entscheidung des YCGK, wonach Daten Tatobjekt der Qualifikation des Diebstahls sein können, und die Entscheidungen des Kassationshofs in diesem Sinne	515
dddd.	Bewertung und eigene Auffassung	517
dd.	Tat (Handlung)	521
ee.	Erfolg	523
ff.	Qualifikation der Straftat	523
b.	Innere (subjektive) Tatbestandsmerkmale	523
4.	Das Merkmal der Rechtswidrigkeit	523
5.	Besondere Erscheinungsformen der Straftat	524

a.	Versuch	524
b.	Beteiligung	524
c.	Konkurrenzen	524
6.	Sanktion, Ermittlungsverfahren und gerichtliches Verfahren	526
B.	Der unter Verwendung eines informationstechnischen Systems begangene Betrug (Art. 158 Abs. 1 Buchst. f)	526
1.	Informationstechnische Systeme als Qualifikation des Betrugs im Allgemeinen	526
2.	Ist die Begehung des Betrugs über Internet-Einkaufsseiten eine Qualifikation?	537
3.	Bewertung und eigene Auffassung	539
4.	Persönliche Strafaufhebungs- oder Strafmilderungsgründe	539
IV.	SONSTIGE STRAFTATBESTÄNDE, DIE MITTELS INFORMATIONSTECHNISCHER SYSTEME VERWIRKLICHT WERDEN KÖNNEN	540
A.	Die Straftat der Behinderung der Kommunikation (Art. 124)	540
B.	Die Straftat der Beleidigung (Art. 125)	541
C.	Die Straftat der Nachstellung (Art. 123/A)	545
1.	Einleitung	545
a.	Das Bedürfnis nach einer Regelung der Nachstellung	545
b.	Der Prozess des erstmaligen Auftretens der Handlungen, die Gegenstand der Straftat der Nachstellung sind	549
c.	Die Bedeutung einer normativen Regelung	552
2.	Geschütztes Rechtsgut	555
3.	Tatbestandsmäßigkeit	556
a.	Äußere (objektive) Tatbestandsmerkmale	556
aa.	Täter	556
bb.	Opfer	556
cc.	Tatobjekt	556
dd.	Tat (Handlung)	557
aaa.	Charakter der Handlung	557
bbb.	Beharrlichkeit	558
ccc.	Physisches Verfolgen	560
ddd.	Der Versuch, Kontakt zum Opfer herzustellen	562
aaaa.	Verwendung von Telekommunikations- und Kommunikationsmitteln	563
bbbbb.	Verwendung informationstechnischer Systeme	563
cccc.	Einsatz dritter Personen	564
ee.	Erfolg	565
aaa.	Hervorrufen einer ernsthaften Beunruhigung beim Opfer	565
bbb.	Besorgnis des Opfers um die eigene Sicherheit oder die einer ihm nahestehenden Person	567
ff.	Qualifikation der Straftat	568
aaa.	Begehung der Straftat gegen ein Kind	568
bbb.	Begehung der Straftat gegen den gerichtlich getrennt lebenden oder den geschiedenen Ehegatten	569
ccc.	Der Fall, dass die Straftat das Opfer veranlasst, die Schule, den Arbeitsplatz oder die Wohnung zu wechseln oder die Schule oder die Arbeit aufzugeben	570
ddd.	Begehung der Straftat durch einen Täter, gegen den eine Wegweisung oder ein Verbot der Annäherung an Wohnung, Schule oder Arbeitsplatz angeordnet wurde	570
eee.	Fehlendes Qualifikationsmerkmal: Hassmotiv	571
b.	Inneres (subjektives) Tatbestandsmerkmal	572

4.	Das Merkmal der Rechtswidrigkeit	572
5.	Besondere Erscheinungsformen der Straftat	572
a.	Versuch	572
b.	Beteiligung	573
c.	Konkurrenzen	574
6.	Sanktion, Ermittlungsverfahren und gerichtliches Verfahren	575
D.	Die Straftat der Verletzung der Vertraulichkeit der Kommunikation (Art. 132)	578
E.	Die Straftat des Abhörens oder Aufzeichnens von Gesprächen zwischen Personen (Art. 133)	580
F.	Die Straftat der Verletzung der Privatsphäre (Art. 134)	582
G.	Die Straftat der Obszönität (Art. 226)	584
H.	Bereitstellung von Ort und Gelegenheit zum Glücksspiel unter Verwendung informationstechnischer Systeme (Art. 228 Abs. 3)	588

VIERTES KAPITEL

DIE IM GESETZ ÜBER GEISTES- UND KUNSTWERKE UND IM GESETZ ÜBER DIE ELEKTRONISCHE SIGNATUR GEREGELTEN COMPUTERSTRAFTATEN

I.	DIE IM GESETZ ÜBER GEISTES- UND KUNSTWERKE GEREGELTEN COMPUTERSTRAFTATEN	591
A.	Allgemeines	591
B.	Die Straftaten der Verletzung von Verwertungsrechten, Urheberpersönlichkeitsrechten und verwandten Schutzrechten (Art. 71)	593
1.	Allgemeines	593
2.	Durch den Straftatbestand geschütztes Rechtsgut	594
3.	Tatbestandsmäßigkeit	595
a.	Äußere (objektive) Tatbestandsmerkmale	595
aa.	Täter	595
bb.	Opfer	596
cc.	Tatobjekt	598
dd.	Tat (Handlung)	599
aaa.	Handlungen, die die Straftat gegen die Urheberpersönlichkeitsrechte begründen	599
aaaa.	Öffentliche Wiedergabe und Veröffentlichung	599
bbbbb.	Mitteilung des Inhalts eines noch nicht veröffentlichten Werkes	601
cccc.	Anbringen eines Namens auf dem Werk	601
dddd.	Verteilung, Verbreitung und Veröffentlichung des Werkes unter Anbringung des Namens eines bekannten Dritten	601
eeee.	Unterlassene Angabe der zitierten Quelle sowie falsche, unzureichende oder irreführende Quellenangabe	601
ffff.	Änderung des Werkes	602
bbb.	Handlungen gegen die Verwertungsrechte	602
aaaa.	Bearbeitung des Werkes	602
bbbbb.	Vervielfältigung des Werkes	602
cccc.	Anbieten der vom Täter selbst hergestellten Vervielfältigungsstücke des Werkes zum Verkauf	603
dddd.	Verbreitung des Werkes durch Vermietung oder öffentlichen Verleih	603
eeee.	Einfuhr des Werkes	604
ffff.	Aufführung des Werkes	604
gggg.	Verbreitung und Veröffentlichung des Werkes über ein Datenübertragungsnetz	604
hhhh.	Ankauf des Werkes zu gewerblichen Zwecken	605

iii. Besitz und Lagerung des Werkes zu anderen als persönlichen Zwecken	605
ccc. Handlungen gegen die verwandten Schutzrechte	605
ee. Erfolg	606
b. Innere (subjektive) Tatbestandsmerkmale	606
4. Das Merkmal der Rechtswidrigkeit	606
5. Besondere Erscheinungsformen der Straftat	608
a. Versuch	608
b. Beteiligung	608
c. Konkurrenzen	609
6. Tätige Reue	610
7. Sanktion, Ermittlungsverfahren und gerichtliches Verfahren	611
C. Die Straftat der unbefugten Entfernung oder Änderung von Informationen, die bei der Zugänglichmachung des Werkes für die Öffentlichkeit erscheinen, sowie von Zahlen oder Codes, die diese Informationen darstellen (Art. 71 Abs. 2)	613
D. Die Straftat der auf das Unwirksammachen von Schutzprogrammen gerichteten Vorbereitungshandlungen (Art. 72)	614
II. DIE IM GESETZ ÜBER DIE ELEKTRONISCHE SIGNATUR GEREGLTEN COMPUTERSTRAFTATEN	615
A. Die im Eik enthaltenen Straftaten (Art. 16–17)	615
B. Durch den Straftatbestand geschütztes Rechtsgut	618
C. Tatbestandsmäßigkeit	619
1. Äußere (objektive) Tatbestandsmerkmale	619
a. Täter	619
b. Opfer	619
c. Tatobjekt	620
d. Tat (Handlung)	622
aa. Im Hinblick auf die Straftat der unbefugten Verwendung von Signaturerstellungsdaten (Art. 16 Eik)	622
aaa. Allgemeines	622
bbb. Erlangung der Daten oder der Signaturerstellungseinheit	623
ccc. Weitergabe der Daten oder der Signaturerstellungseinheit	623
ddd. Kopieren der Daten oder der Signaturerstellungseinheit	624
eee. Nachbildung der Signaturerstellungseinheit	624
fff. Unbefugte Erstellung einer elektronischen Signatur	624
bb. Im Hinblick auf die Straftat der Fälschung elektronischer Zertifikate (Art. 17 Eik)	625
aaa. Allgemeines	625
bbb. Erstellung eines gefälschten elektronischen Zertifikats	626
ccc. Nachahmung gültiger Zertifikate	626
ddd. Verfälschung gültiger Zertifikate	627
eee. Verwendung eines gefälschten Zertifikats	627
e. Erfolg	628
f. Qualifikation der Straftat	628
2. Innere (subjektive) Tatbestandsmerkmale	628
D. Das Merkmal der Rechtswidrigkeit	629
E. Besondere Erscheinungsformen der Straftat	630
1. Versuch	630
2. Beteiligung	630
3. Konkurrenzen	630
F. Sanktion, Ermittlungsverfahren und gerichtliches Verfahren	631

FÜNFTES KAPITEL

STRAFPROZESSUALE ZWANGSMASSNAHMEN BEI COMPUTERKRIMINALITÄT, IT-FORENSIK UND ERFORDERLICHE MASSNAHMEN ZUR BEKÄMPFUNG DER COMPUTERKRIMINALITÄT

I.	ALLGEMEINES	635
II.	STRAFPROZESSUALE ZWANGSMASSNAHMEN GEGENÜBER INFORMATIONSTECHNISCHEN SYSTEMEN	636
A.	Durchsuchung, Anfertigung von Kopien und Beschlagnahme bei informationstechnischen Systemen	636
1.	Gesetzliche Grundlage	636
2.	Vorliegen eines auf konkrete Beweise gestützten dringenden Tatverdachts	638
3.	Fehlen einer anderweitigen Möglichkeit der Beweiserlangung	640
4.	Die Maßnahme der Durchsuchung und der Anfertigung von Kopien	642
5.	Die Maßnahme der Beschlagnahme	642
6.	Beschwerde gegen die Anordnung der Maßnahme	645
7.	Art. 134 der türkischen Strafprozessordnung (CMK) ist eine Sonderregelung	645
8.	Kritikpunkte in der Praxis und angewandte Vorgehensweise	646
B.	Gesetzgebungsbedingte Neuerungen und Defizite im Ermittlungsverfahren und im gerichtlichen Verfahren	648
1.	Die Eingliederung des Übereinkommens über Computerkriminalität (ASSS) in unser innerstaatliches Recht	648
2.	Die durch Art. 3 Abs. 4 des Gesetzes Nr. 5651 für das Ermittlungsverfahren eingeführte Änderung und die Rechtslage nach der Aufhebung des Absatzes 4 durch das Verfassungsgericht (AYM)	649
3.	Die Ungewissheit darüber, was mit den nach Art. 134 CMK angefertigten Images nach Abschluss des Verfahrens zu geschehen hat, muss beseitigt werden	650
4.	Die fehlende Nennung der Computerstraftaten in Art. 135 CMK führt zu lückenhaften Ermittlungen oder zur Erlangung rechtswidriger Beweise	651
C.	Die IP-Adresse allein weist den Täter nicht aus	652
D.	Ohne IP-Adresse lässt sich der Täter nicht ermitteln	657
E.	Für die vollständige und zutreffende Ermittlung des Täters ist der Zugriff auf NAT-IP- und Portdaten erforderlich	658
F.	Erforderliche Schritte im Ermittlungsverfahren und im gerichtlichen Verfahren	661
III.	IT-FORENSIK	664
A.	Einleitung	664
B.	Die Wissenschaft der Computerkriminalistik	665
C.	Der Begriff der IT-Forensik	665
1.	Definition	665
2.	Nutzen der IT-forensischen Methodik	667
D.	Digitale Beweismittel und ihre Arten	668
1.	Was ist ein digitales (elektronisches) Beweismittel?	668
2.	Voraussetzungen für die Verwertbarkeit digitaler Beweismittel	671
3.	Medien, auf denen sich digitale Beweismittel befinden	672
a.	Hauptplatine	673
b.	Prozessor	673
c.	Speicher: RAM (Random Access Memory) – ROM (Read Only Memory) – Zwischenspeicher (Cache Memory)	674
d.	Hard Disk (Festplattenlaufwerk)	675

e.	Diskette und CD/DVD/Blu-ray	676
f.	Speicherkarten	676
g.	Digitale Speichereinheiten	676
h.	Mobiltelefone	676
i.	Digitale Kameras und Fotoapparate	677
i.	MP3-Player/iPod	677
j.	Handheld-Computer (PDA, PALM, Pocket PC)	677
k.	Wechselspeicher (Flash Memory)	677
l.	Drucker, Faxgeräte, Kopiergeräte und sonstige Hardware	678
4.	Leitfaden des Europarats zu elektronischen Beweismitteln	678
E.	Phasen der IT-Forensik	680
1.	Tatort – Sammlung und Sicherung von Beweismitteln	680
2.	Vor Beginn der Beweissammlung zu beachtende Punkte	680
a.	Erste Stufe	680
b.	Zweite Stufe	681
3.	Was am Tatort zu unterlassen ist	682
a.	Fehler 1 – Einschalten des Computers	682
b.	Fehler 2 – Den Inhaber des Computers um Hilfe bitten	682
c.	Fehler 3 – Unterlassene Prüfung auf Computerviren	682
d.	Fehler 4 – Keinerlei Vorkehrungen beim Transport elektronischer Beweismittel	682
4.	Live-Analyse	682
5.	Verpackung – Transport – Aufbewahrung	684
6.	Die verborgene Struktur elektronischer Beweismittel	684
F.	Die Herangehensweise des IT-Forensikers an elektronische Beweismittel	685
1.	Allgemeines	685
2.	Untersuchung	685
a.	Einrichtung des Schreibschutzes für den Datenträger	685
b.	Forensische Datensicherung (Image)	686
c.	Hashwert	688
d.	Ergebnis der Untersuchung	689
3.	Auswertung (Bewertung/Analyse)	690
a.	Phasen der Computeranalyse	690
b.	Phasen der Mobiltelefonanalyse	690
c.	Phasen der Analyse von Netzwerkverkehrsdaten	691
d.	Phasen der Analyse von externen Festplatten, CDs/DVDs, Speicherkarten und Flash-Speichern	692
e.	Benutzergeschützte Dateien	693
f.	Anti-Forensics und Verschleierungsmethoden	693
4.	Allgemeine Grundsätze, die die Fachleute zu beachten haben	694
5.	Datenwiederherstellung	694
6.	Merkmale und Erstellung des IT-forensischen Berichts	694
IV.	ERFORDERLICHE MASSNAHMEN ZUR BEKÄMPFUNG DER COMPUTERKRIMINALITÄT	695
A.	Von Personen und/oder Institutionen zu treffende Maßnahmen	695
1.	Allgemeines	695
2.	Gewährleistung und Prüfung der Systemsicherheit	697
B.	Von den Staaten zu treffende Maßnahmen	699
1.	Einrichtung und Schulung von Einheiten zur Verfolgung von Computerstraftaten	699

a.	Allgemeine Erläuterungen	699
b.	Das Beispiel der USA	699
c.	Die Lage in unserem Land	700
2.	Maßnahmen gegen das Phänomen des Cyberterrorismus	702
3.	Die Kontrolle des virtuellen Raums durch die Staaten	702
4.	Internationale Zusammenarbeit	704
5.	Das Verhältnis zwischen organisierter Kriminalität und Computerkriminalität	704
V.	COMPUTERKRIMINALITÄT DE LEGE FERENDA	708
A.	Aus strafrechtlicher Sicht	708
B.	Aus strafprozessrechtlicher Sicht	711

SECHSTES KAPITEL INTERNETKOMMUNIKATIONSRECHT

I.	EINLEITUNG	715
II.	BEDEUTUNG UND GRENZEN DER GEDANKENFREIHEIT (MEINUNGSFREIHEIT) SOWIE IHR STELLENWERT FÜR DAS INTERNET	717
A.	Begriff	718
B.	Inhalt der Gedankenfreiheit (Meinungsfreiheit)	721
C.	Die Meinungsfreiheit in der EMRK	722
1.	Entstehung der EMRK und ihre Aufnahme in die türkische Rechtsordnung	722
2.	Bedeutung und Anwendung der Meinungsfreiheit	724
a.	Der Begriff der Meinungsfreiheit in der EMRK	724
b.	Art. 10 Abs. 1 EMRK: Inhalt der Meinungsfreiheit	724
c.	Art. 10 Abs. 2 EMRK: Fälle, in denen die Meinungsfreiheit eingeschränkt werden kann	728
d.	Art. 10 Abs. 2 EMRK: Grenzen der Einschränkung	733
3.	Die Sicht des EGMR auf das Internet im Kontext der Meinungsfreiheit	735
D.	Würdigung und eigene Auffassung	736
III.	UNTERSCHIEDUNGEN BEI DER SPERRUNG DER INTERNETKOMMUNIKATION	740
A.	Die Unterscheidung zwischen der Sperrung des Zugangs zum Internet und der Sperrung der Internetkommunikation	740
B.	Die Unterscheidung zwischen technischer und rechtlicher Sperrbarkeit der Internetkommunikation	742
1.	Umfang der Unterscheidung	742
2.	Technische Sperrmethoden	742
C.	Die Unterscheidung der Sperrbarkeit der Internetkommunikation nach den Methoden „allgemeine Sperrung – besondere Sperrung“	748
IV.	DIE REGELUNGEN DES GESETZES NR. 5651 „ÜBER DIE REGELUNG DER IM INTERNET VERBREITETEN VERÖFFENTLICHUNGEN UND DIE BEKÄMPFUNG DER DURCH DIESE VERÖFFENTLICHUNGEN BEGANGENEN STRAFTATEN“	749
A.	Entstehungsgeschichte, Zweck und Anwendungsbereich des Gesetzes	749
1.	Entstehungsgeschichte des Gesetzes	749
2.	Zweck und Anwendungsbereich	752
3.	Rechtsnatur der im Gesetz Nr. 5651 vorgesehenen Maßnahmen	753
B.	An der Verwaltung des Internets beteiligte Institutionen	754
1.	Behörde für Informationstechnologien und Kommunikation	754
2.	Rat für Internetentwicklung	758
C.	Begriffsbestimmungen	758

D.	Pflicht zur Information der Öffentlichkeit	759
E.	Pflicht zur Erhebung und Übermittlung von Verkehrsdaten	764
F.	Verantwortlichkeit der Internetakteure	769
1.	Allgemeines	769
2.	Das Beispiel Deutschlands	769
3.	Die Regelung im Gesetz Nr. 5651	771
a.	Verantwortlichkeit und Pflichten der Inhaltsanbieter	771
b.	Verantwortlichkeit und Pflichten der Hostprovider	780
i.	Keine Verantwortlichkeit der Hostprovider für Inhalte	780
ii.	Verantwortlichkeit der Hostprovider für die Speicherung von Verkehrsdaten	782
iii.	Sanktionen bei Pflichtverstößen	782
iv.	Klassifizierung und Differenzierung der Hostprovider	783
c.	Verantwortlichkeit und Pflichten der Zugangsanbieter	784
d.	Verband der Zugangsanbieter	787
e.	Verantwortlichkeit und Pflichten der Anbieter gemeinschaftlicher Internetnutzung	790
f.	Würdigung und eigene Auffassung	792
V.	ALLGEMEINE SPERRUNG DES INTERNETZUGANGS (FILTERUNG)	793
A.	Das Internet ist ein Bereich, der rechtlichen Regelungen unterliegt	795
B.	Die Verwaltung des Internets	797
C.	Modelle zur Regulierung des virtuellen Raums	800
1.	Regulierung auf nationaler Ebene	801
2.	Regulierung durch internationale Übereinkommen	801
3.	Regulierung durch internationale Organisationen	802
4.	Selbstregulierung (Self-Regulation)	802
5.	Eigene Auffassung zu den Regulierungsmodellen	803
D.	Das Internet als Massenkommunikationsmittel und die Sperrung seiner Kommunikation	804
1.	Der Begriff der Massenkommunikation im Allgemeinen	804
2.	Das Phänomen des Missbrauchs der Internetkommunikation	805
3.	Überlegungen zur allgemeinen Sperrung der Internetkommunikation	807
4.	Die Regulierung des virtuellen Raums durch die Staaten und die allgemeine Filterung	808
E.	Eine Verwaltungspraxis der allgemeinen Sperrung der Internetkommunikation – Die Befugnisse der Telekommunikationsbehörde im Internet und ihre Entscheidungen	810
F.	Die allgemeine Sperrung der Internetkommunikation nach dem Gesetz Nr. 5651 über die Regelung von Internetveröffentlichungen	812
VI.	BESONDERE SPERRUNG DES INTERNETZUGANGS (ZUGANGSSPERRE)	818
A.	Sperrung der Internetkommunikation durch gerichtliche Entscheidung	818
1.	Fallbeispiel zur Sperrung der Internetkommunikation durch gerichtliche Entscheidung	819
2.	Würdigung des Fallbeispiels zur Sperrung der Internetkommunikation durch gerichtliche Entscheidung	821
3.	Das Urteil des EGMR, wonach das Gesetz Nr. 5651 Art. 10 EMRK verletzt	823
4.	Die Entscheidung des Verfassungsgerichts, wonach die Sperrentscheidung des Präsidiums für Telekommunikation und Kommunikation (TİB) die Meinungsfreiheit verletzt	828
a.	Zur Zulässigkeit	828
b.	Zur Begründetheit	829
c.	Würdigung und eigene Auffassung	834
5.	Die Entscheidung des Verfassungsgerichts vom 26/12/2019 über die Beschwerde der Wikimedia Foundation Inc. und anderer, veröffentlicht im Amtsblatt (Resmî Gazete) vom 20/01/2020	835

a.	Zur Zulässigkeit	835
b.	Zur Begründetheit	837
c.	Würdigung und eigene Auffassung	839
6.	Die Entscheidung des Verfassungsgerichts vom 27/10/2021 über die Beschwerde der Keskin Kalem Yayıncılık ve Ticaret A.Ş. und anderer, veröffentlicht im Amtsblatt (Resmî Gazete) vom 07/01/2022	840
a.	Zur Zulässigkeit	844
b.	Zur Begründetheit	844
c.	Würdigung und eigene Auffassung	857
B.	Sperrung der Internetkommunikation durch Verwaltungspraxis – Das Beispiel der Sperrung der Kommunikation durch Entscheidung des Telekommunikationsausschusses	858
1.	Fallbeispiel zur Sperrung der Internetkommunikation durch Verwaltungspraxis	858
2.	Würdigung des Fallbeispiels zur Sperrung der Internetkommunikation durch Verwaltungspraxis	860
C.	Sperrung der Internetkommunikation durch eine „dem Privatrecht unterliegende juristische Person“ – Das Beispiel der Sperrung der Kommunikation durch Entscheidung des Türkischen Fußballverbands	863
VII.	WÜRDIGUNG DES GESETZES NR. 5651 IM HINBLICK AUF DIE BESONDERE SPERRUNG DER INTERNETKOMMUNIKATION (ENTFERNUNG VON INHALTEN UND/ODER ZUGANGSSPERRE)	865
A.	Straftatbestände, bei denen die Entfernung von Inhalten und/oder die Zugangssperre angeordnet werden kann	865
1.	Allgemeines	865
2.	Obszöne Veröffentlichungen	869
3.	Bereitstellung von Ort und Gelegenheit zum Glücksspiel	874
4.	Straftaten im Zusammenhang mit dem Gesetz über Fußball- und andere Sportwettkämpfe	876
5.	Straftaten gegen Atatürk	877
6.	Straftaten im Zusammenhang mit dem Gesetz über die aus den Einnahmen von Glücksspielen erhobenen Steuern, Fonds und Anteile	878
7.	Zusatzartikel 4 FSEK	878
B.	Die Anordnung der Entfernung von Inhalten und/oder der Zugangssperre als Zwangsmaßnahme	879
1.	Gesetzliche Grundlage	879
2.	Zur Anordnung Befugte	879
a.	Richter und Staatsanwalt	879
b.	Die Befugnis des Präsidenten des TİB	880
3.	Anzuwendendes Verfahren	882
4.	Außerkräfttreten der Maßnahmenanordnung	883
5.	Sanktion	885
6.	Die Lage in der Praxis und eigene Auffassung	885
C.	Die Anordnung der Entfernung von Inhalten und/oder der Zugangssperre als Verwaltungsmaßnahme	889
1.	Gesetzliche Grundlage	889
2.	Zur Anordnung Befugte	889
3.	Rechtsnatur der Zugangssperre als Verwaltungsmaßnahme	891
4.	Anzuwendendes Verfahren	899
5.	Sanktion	900
D.	Entschädigung wegen unrechtmäßiger Sperranordnung	901
E.	Entfernung von Inhalten und Zugangssperre bei Gefahr im Verzug (Art. 8/A)	901
F.	Entfernung rechtswidriger Inhalte aus der Veröffentlichung und Zugangssperre (Art. 9)	903

G.	Sperrung des Zugangs zu Inhalten aus Gründen des Schutzes des Privatlebens (Art. 9/A)	908
H.	Sachlich zuständiges Gericht	909
VIII.	DAS RECHTSREGIME DER ANBIETER SOZIALER NETZWERKE	909
A.	Die Notwendigkeit einer Regelung für Anbieter sozialer Netzwerke	909
B.	Das Rechtsregime der Anbieter sozialer Netzwerke nach dem Internetgesetz	912
1.	Allgemeines	912
2.	Pflicht zur Benennung eines Vertreters, dessen Eigenschaften und Verantwortlichkeiten	912
3.	Verantwortlichkeit der Anbieter sozialer Netzwerke bei Anträgen nach Art. 9/A des Internetgesetzes	914
4.	Pflicht, der Behörde Berichte über die Umsetzung von Anordnungen der Entfernung von Inhalten und/oder der Zugangssperre zu übermitteln	914
5.	Pflicht zur Übermittlung von Informationen über bestimmte Straftaten an die für das Ermittlungsverfahren und das gerichtliche Verfahren zuständigen Stellen	915
6.	Pflicht zur Speicherung der Daten in der Türkei	916
7.	Pflicht, die erforderlichen Maßnahmen für das Angebot eines gesonderten, kindgerechten Dienstes zu treffen	917
8.	Sanktionen gegen Anbieter sozialer Netzwerke im Zusammenhang mit Zugangssperre und Entfernung von Inhalten	918
9.	Sanktion bei Nichtbefolgung der vom Präsidenten der BTK erlassenen Anordnung der Entfernung von Inhalten und/oder der Zugangssperre	918
10.	Pflicht zur Einhaltung der Regelungen über Nutzerrechte	920
11.	Schadensersatzhaftung für rechtswidrige Inhalte	921
12.	Pflicht zur Einrichtung eines wirksamen Antragsmechanismus für die Entfernung von Hashtags und hervorgehobenen Inhalten im Melde- und Abhilfeverfahren	921
13.	Meldung von Inhalten, die die Sicherheit von Leben und Eigentum von Personen gefährden, an die Polizei	921
14.	Pflichten der Anbieter sozialer Netzwerke als Inhaltsanbieter und Hostprovider nach dem Internetgesetz	922
15.	Auskunftersuchen der BTK und ihre Befugnis zur Prüfung vor Ort	922
16.	Pflicht zur Erstellung eines Krisenplans	923
17.	Untergesetzliche Regelungen	923
18.	Übergangsregelung	924
C.	Würdigung und eigene Auffassung	925
IX.	DAS RECHTSREGIME DER INTERNET-NACHRICHTENSEITEN	927
A.	Das Problem der Anwendbarkeit presserechtlicher Vorschriften auf Internetpublikationen	927
B.	Das Rechtsregime der Internet-Nachrichtenseiten nach dem Pressegesetz	929
1.	Allgemeines	929
2.	Definition	929
3.	Freiheit und ihre Grenze	930
4.	Pflicht, die Angaben auf der Website bereitzuhalten	930
5.	Pflicht, Aktualisierungen von Nachrichten und Inhalten deutlich erkennbar auf der Website bereitzuhalten	931
6.	Folgen der Einstufung von Internet-Nachrichtenseiten als periodische Veröffentlichungen	932
a.	Allgemeine Pflichten aus dem Pressegesetz	932
b.	Pflicht zur Abgabe einer Anmeldeerklärung und ihre Folgen	933
c.	Wegfall der Rechte in Bezug auf amtliche Bekanntmachungen und Anzeigen sowie auf den Presseausweis der Beschäftigten als Folge der Abgabe der Anmeldeerklärung	934
7.	Pflicht, die auf der Internet-Nachrichtenseite veröffentlichten Inhalte unter Gewährleistung ihrer Richtigkeit und Integrität aufzubewahren	937

8.	Recht auf Berichtigung und Gegendarstellung	938
9.	Form der Berichterstattung über sexuelle Übergriffe, Tötungsdelikte und die Verleitung zum Suizid	939
10.	Fristen und Verfahrensweise für das gerichtliche Verfahren und das Ermittlungsverfahren	940
X.	DAS RECHTSREGIME DER ANBIETER VON OVER-THE-TOP-DIENSTEN	940
A.	Definition und Begriff	940
B.	Rechte und Pflichten	941
C.	Sanktion	944
XI.	WÜRDIGUNG UND EIGENE AUFFASSUNG	945
	Literaturverzeichnis	957
	Verzeichnis der Gerichtsentscheidungen	989
	Sachverzeichnis	999
	Lebenslauf des Verfassers	1007

Dieses Dokument ist das aus dem Türkischen übersetzte Inhaltsverzeichnis des Buches; die Seitenzahlen beziehen sich auf das gedruckte Buch. Seite des Buches: www.dulger.av.tr/de/publikationen/bilisim-suclari-ve-internet-iletisim-hukuku/