BOOK

Cybercrime and Internet Communication Law

Bilişim Suçları ve İnternet İletişim Hukuku

Murat Volkan Dülger

11th ed., Seçkin Publishing, Ankara, May 2025, 1008 pages, ISBN 9786253810702

Table of contents

Preface to the Eleventh Edition 6
Preface to the Tenth Edition 7
Preface to the Ninth Edition 9
Preface to the Eighth Edition 11
Preface to the Seventh Edition 12
Preface to the Sixth Edition 14
Preface to the Fifth Edition 16
Preface to the Fourth Edition 19
Preface to the Third Edition 22
Preface to the Second Edition 24
Preface to the First Edition 26
Abbreviations 51
Introduction 55

CHAPTER ONE
DEFINITION OF THE COMPUTER, INFORMATICS, CYBERCRIME AND RELATED CONCEPTS, AND THE HISTORY OF THE COMPUTER AND OF CYBERCRIME

I. TERM AND CONCEPT 61
A. The Computer 62
1. The Term Computer 62
2. Definition of the Computer 63
a. Definition Based on the Tasks and Functions Performed by the Computer 64
b. Definition Based on the Physical Characteristics of the Computer and the Tasks and Functions It Performs 65
c. Main Components of the Computer 66
aa. Central Processing Unit 67
bb. Read-Only Memory 67
cc. Random-Access Memory 67
dd. Peripheral Input – Output Units 68
ee. Operating Software 68
ff. Application Software 69
d. Types of Computer 69
e. Distinguishing Features and a Reconciling Definition 70
f. Assessment and My View 71
g. Operating Logic and System of the Computer 72
B. Informatics and the Information System 72
C. Cybercrime 76
1. The Problem of Terminology 76

2. Content of the Concept of Cybercrime 80
D. Data 83
E. The Internet 84
1. Definition 84
2. Technical Structure, Infrastructure and Governance of the Internet 87
a. Technical Structure of the Internet 87
aa. The TCP/IP Protocol 88
bb. The World Wide Web System 88
b. Infrastructure of the Internet 88
c. Governance of the Internet in General 89
II. HISTORICAL DEVELOPMENT 92
A. Historical Development of the Computer 92
1. First Period 94
2. Second Period 95
3. Third Period 95
4. Fourth Period 96
B. Historical Development of the Internet 97
C. Historical Development of Cybercrime 100

CHAPTER TWO

MODES OF COMMISSION OF CYBERCRIME, ITS RELATIONSHIP WITH CRIMINOLOGY, ECONOMIC OFFENCES AND TERRORISM, AND CYBERCRIME IN COMPARATIVE LAW

I. MODES OF COMMISSION OF CYBERCRIME 109
A. In General 109
B. Modes of Commission 110
1. Trojan Horse 110
2. Salami Technique 111
3. Breaking System Security and Gaining Entry (Hacking) 112
a. Computer Intruders Who Commit Offences (Hackers) 112
b. Former Computer Intruders Who Test System Security (Ethical Hackers) 115
4. Network Worms 115
5. Rabbits 116
6. Chameleons 117
7. Logic Bombs 117
8. Computer Viruses 118
9. Unsolicited Electronic Mail (Spam) 119
10. Offering Unlawful Content 122
11. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks 123
12. Phishing Attacks 123
13. Password-Cracking Attacks 123
14. Botnet Attack 124
15. Dumpster Diving (Scavenging) 125
16. Wrongful Misuse of the DNS 125
17. Web Page Redirection 126
18. Scanning 126
19. Cyberbullying 127
20. Ransomware 128

21. Other Methods 129

II. RELATIONSHIP OF CYBERCRIME WITH CRIMINOLOGY AND ECONOMIC OFFENCES 129

A. Relationship of Cybercrime with Criminology 129

1. In General 129

2. General Characteristics of Perpetrators of Cybercrime 132

B. Relationship of Cybercrime with Economic Offences 134

1. Economic Law 135

2. White-Collar Crime and the Economic Offence 137

a. White-Collar Crime 137

b. Concept and Definition of the Economic Offence 139

aa. Economic Offences from the Criminological – Sociological Perspective 140

bb. Economic Offences from the Perspective of the Rules of Criminal Procedure 141

cc. Economic Offences from the Perspective of the Legal Interest Protected by the Offence 141

c. Assessment and My View 142

3. Cybercrimes as Economic Offences 143

III. SOCIAL MEDIA 144

A. In General 144

B. Definition 145

C. Forms of Social Media 146

D. How Social Media Differs from Industrial Media 147

E. Effect of Social Media on Companies 148

F. Building Social Authority 149

G. Effects of Social Media on Internet Use 150

H. Possible Historical / Political Effects of Social Media 153

I. Economic Effects of the Social Marketing Arising from Social Media 153

İ. Effects of Social Media on Education 155

J. Ownership of the Content Making Up Social Media 156

K. Social Media and the COVID–19 Pandemic 156

L. Criticisms of Social Media 158

IV. THE EFFECT OF THE MASS MEDIA –IN PARTICULAR THE INTERNET– ON TERRORISM 159

A. Terrorism in General and the Definition of Terrorism 159

B. Effects on Terrorism of Developments in Technology and in Information Technologies in General 163

1. Effects on Terrorism of Technological Developments in Means of Transport 165

2. Effects on Terrorism of Developments in Weapons Technology 166

3. Effects on Terrorism of Developments in the Technology of Personal Communication Devices 167

4. Effects on Terrorism of Developments in Information Systems 168

C. Effects on Terrorism of Developments in the Mass Media 173

1. The Relationship between the Mass Media and Terrorism in General 173

2. Coverage of Terrorist Acts by the Mass Media 175

a. Coverage during the Act 178

b. Coverage after the Act 180

3. Assessment of the Debates on Mass Media Coverage of Terrorist Acts from the Perspective of Freedom of Expression and Freedom of the Press 180

a. The View that the Restriction Must Be Imposed by Law 181

b. The View that the Restriction Must Be Achieved through Self-Regulation 182

D. Cyberterrorism 183
1. Concept and Definition 183
2. Differences between Cyberterrorism and Traditional Terrorism and the Advantages of the Former 186
3. The Risk of Cyberterrorism and Methods of Attack 189
E. Cyberwarfare 191
F. Hacktivism and a Legal Assessment of Hacktivist Acts 193
G. Assessment and My View 194
V. THE INTERNATIONAL DIMENSION OF CYBERCRIME AND THE PROVISIONS ON CYBERCRIME IN INTERNATIONAL LAW AND IN FOREIGN NATIONAL LAWS 198
A. The International Dimension of Cybercrime 198
1. The Need for International Cooperation in Combating Cybercrime 198
2. Reasons Why Cybercrimes Are Transnational Offences 199
3. Relationship of Cybercrime with International Criminal Law 201
4. Assessment and My View 205
B. Cybercrime in International Law 207
1. Work of the Council of Europe on Cybercrime 207
a. The Convention on Cybercrime 208
b. Additional Protocol to the Convention on Cybercrime concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems 212
2. Legal Bases of International Mutual Legal Assistance from the Perspective of Türkiye 213
a. Basic Principles of Mutual Legal Assistance 215
aa. Requests Are Executed in Accordance with the Legislation of the Requested State 215
bb. As a Rule, No Costs Are Charged 215
cc. The Request and Its Annexes Are Translated into the Official Language of the Requested State 215
b. Grounds for Refusing a Request for Mutual Legal Assistance 215
aa. The Requested State Considers the Request to Concern Political Offences or Fiscal Offences 215
bb. The Requested State Considers Execution of the Request Contrary to Its Sovereignty, Public Order or Other Interests 216
c. The Requirement of Dual Criminality 216
3. Mutual Legal Assistance under the Convention on Cybercrime 216
a. Articles of the Convention Concerning Mutual Legal Assistance 216
b. Requests for Mutual Legal Assistance to Obtain Traffic Data / IP Numbers in Cybercrime Cases 218
c. Problems in Cybercrime Cases Arising from the Place of Commission of the Offence or the Whereabouts of the Suspect Being Unknown 219
d. Situations in Which Judicial Authorities May Obtain IP Information and Traffic Data Directly 220
e. International Letters Rogatory within the 24/7 Framework in Cybercrime Cases 221
4. Work of the European Union on Cybercrime 222
5. Work of Other Supranational Organisations on Cybercrime 223
C. Cybercrime in National Laws 223
1. In General 223
2. Cybercrime in US Law 224
a. The Computer Fraud and Abuse Act 225
b. The Communications Decency Act 226
c. The Child Pornography Prevention Act 226

d. The Child Online Protection Act 227
e. The Electronic Communications Privacy Act 228
f. The Internet Gambling Prohibition Act 228
g. The Identity Theft Act 229
h. The Anti-Terrorism Act 229
ı. Provisions on Information Security Expertise 230
3. Cybercrime in German Law 232
4. Cybercrime in English Law 233
5. Cybercrime in French Law 234
6. Cybercrime in Italian Law 235
7. Cybercrime in the Laws of Other Countries 236

CHAPTER THREE
CYBERCRIMES PROVIDED FOR IN THE TURKISH CRIMINAL CODE

I. FORMATION OF THE TURKISH CRIMINAL CODE (TCK), ITS STRUCTURE IN GENERAL AND COMPARISON OF THE OFFENCE TYPES 241
A. Formation of the TCK 241
B. Structure of the TCK in General 242
C. Classification of the Cybercrimes Provided for in the TCK 248
II. OFFENCE TYPES PROVIDED FOR IN THE CHAPTER ON OFFENCES IN THE FIELD OF INFORMATICS 249
A. The Offence of Unlawfully Accessing an Information System or Remaining in the System (Art. 243(1)–(3)) 249
1. In General 249
2. Legal Interest Protected by the Offence 253
a. The Problem of the Change in the Protected Legal Interest 253
b. Protected Legal Interests 257
3. Conformity with the Statutory Definition of the Offence 260
a. Material (Objective) Elements of the Statutory Definition of the Offence 261
aa. Perpetrator 261
aaa. The Perpetrator in General 261
bbb. The Question Whether Legal Persons Can Be Perpetrators 263
aaaa. Liability of Legal Persons from the Perspective of the Principle of the Personal Nature of Penalties 263
bbbb. Criminal Liability of Legal Persons from the Perspective of the Principle of Culpability 265
cccc. Criminal Liability of Legal Persons from the Perspective of the Theory of the Act 266
dddd. Assessment and Our View 266
eeee. The Position of Legal Persons with Regard to Cybercrime 269
bb. Victim 270
cc. Object of the Offence 271
dd. Conduct (Act) 271
ee. No Separate Result Is Required for This Offence 278
ff. The Form of the Offence Aggravated by Its Result: Destruction or Alteration of the Data Contained in the System as a Result of the Commission of the Offence (Art. 243(3)) 279
gg. Qualified Forms of the Offence 281
aaa. In General 281
bbb. Commission of the Offence in Respect of Systems That May Be Used Against Payment (Art. 243(2)) 283

ccc. Where the Perpetrator's Conduct Fulfils Both the Qualified Form and the Form Aggravated by Its Result (Art. 243(2)–(3)) 288
ddd. Commission of the Offence for Terrorist Purposes (Arts. 4, 5 of the Anti-Terror Law No. 3713 (TMK)) 289
b. Mental (Subjective) Element of the Statutory Definition of the Offence 290
4. The Element of Unlawfulness 294
a. In General 294
b. The Function of Including the Expression "Unlawfully" among the Elements of the Offence 296
aa. The View of Special Unlawfulness 297
bb. The Doctrine of Elements Evaluating the Act as a Whole and the Solution Based on Differentiation 298
cc. Our View 299
c. Consent of the Victim 303
d. Application of a Statutory Provision 304
e. Is Self-Defence Possible? 304
f. The Practice of Journalism Does Not Constitute the Ground of Justification of Exercise of a Right for Accessing a System without Authorisation 305
g. Exceeding the Limits of Grounds of Justification 307
5. Culpability 307
a. In General 307
b. Force and Threat 310
c. Carrying Out an Unlawful Binding Order 311
6. Special Forms of Appearance of the Offence 312
a. Attempt 312
b. Participation 313
c. Concurrence 314
7. Sanction, Investigation and Prosecution 319
B. The Offence of Interception (Art. 243(4)) 324
1. In General 324
2. Legal Interest Protected by the Offence 326
3. Conformity with the Statutory Definition of the Offence 326
a. Material (Objective) Elements of the Statutory Definition of the Offence 326
aa. Perpetrator 326
bb. Victim 327
cc. Object of the Offence 327
dd. Conduct (Act) 329
ee. Qualified Forms of the Offence 330
b. Mental (Subjective) Elements of the Statutory Definition of the Offence 330
4. Unlawfulness 330
5. Special Forms of Appearance of the Offence 332
a. Attempt 332
b. Participation 332
c. Concurrence 332
6. Sanction, Investigation and Prosecution 333
C. The Offence of Hindering or Disrupting the Functioning of an Information System and the Offence of Destroying or Altering Data (Art. 244(1)–(2)) 333
1. In General 333
2. Legal Interests Protected by the Offences 335

3. Conformity with the Statutory Definition of the Offence 338
a. Material (Objective) Elements of the Statutory Definition of the Offence 338
aa. Perpetrator 338
bb. Victim 339
cc. Object of the Offences 339
aaa. In General 339
bbb. Whether Subjects and Objects in Virtual Reality Games Can Constitute the Object of the Offence 340
dd. Conduct (Act) 341
aaa. Acts Provided for in Art. 244(1) 342
aaaa. Hindering the Functioning of an Information System 342
bbbb. Disrupting the Functioning of an Information System 343
bbb. Acts Provided for in Art. 244(2) 345
aaaa. Damaging Data 345
bbbb. Destroying Data 345
cccc. Altering Data 347
dddd. Rendering Data Inaccessible 347
eeee. Introducing Data into an Information System 350
ffff. Sending Data Existing in an Information System Elsewhere 351
ccc. Assessment and My View 352
ddd. Parallels between the Acts in the Offence Definition and the Convention on Cybercrime (ASSS) 353
eee. The Difference between the Acts in Paragraphs 1 and 2 of Article 244 and Their Application 354
ee. Result 354
ff. Qualified Forms of the Offence 355
aaa. Commission of the Offence on an Information System Belonging to a Bank or Credit Institution or to a Public Institution or Body (Art. 244(3)) 355
bbb. Commission of the Offence for Terrorist Purposes (Arts. 4, 5 of the Anti-Terror Law No. 3713 (TMK)) 357
b. Mental (Subjective) Elements of the Statutory Definition of the Offence 357
4. The Element of Unlawfulness 357
5. Special Forms of Appearance of the Offence 359
a. Attempt 359
b. Participation 359
c. Concurrence 360
6. Sanction, Investigation and Prosecution 362
D. **The Offence of Obtaining an Unlawful Benefit by Means of an Information System (Art. 244(4))** 363
1. In General 363
2. Legal Interest Protected by the Offence 365
3. Conformity with the Statutory Definition of the Offence 366
a. Material (Objective) Elements of the Statutory Definition of the Offence 366
aa. Perpetrator 366
bb. Victim 367
cc. Object of the Offence 368
dd. Conduct (Act) 368
ee. Result 373
b. Mental (Subjective) Elements of the Statutory Definition of the Offence 375

4. The Element of Unlawfulness 377
5. Special Forms of Appearance of the Offence 377
a. Attempt 377
b. Participation 380
c. Concurrence 380
6. Sanction, Investigation and Prosecution 381
E. The Offences of Misuse of Bank or Credit Cards (Art. 245) 382
1. In General 382
2. Legal Interest Protected by the Offence 384
3. Conformity with the Statutory Definition of the Offence 387
a. Material (Objective) Elements of the Statutory Definition of the Offence 387
aa. Perpetrator 387
bb. Victim 388
cc. Object of the Offence 394
aaa. Bank Card 394
bbb. Credit Card 395
ccc. The Bank Card, the Credit Card and the Benefit Obtained as the Object of the Offence 395
ddd. The Bank or Credit Card Belonging to Another Person 396
dd. Conduct (Act) 397
aaa. Obtaining an Unlawful Benefit with a Bank or Credit Card Belonging to Another Person (Art. 245(1)) 398
aaaa. It Is a Combined-Act and Free-Form Offence 398
bbbb. The Acts of Acquiring and Possessing 399
cccc. The Acts of Using and Causing to Be Used 401
dddd. Obtaining a Benefit with a Card Not Yet Delivered to Its Holder 401
eeee. Use of Bank or Credit Cards Belonging to Another Person for Purchases 403
ffff. Obtaining and Using a Supplementary Card Linked to Another Person's Credit Card 408
gggg. Card Purchases over Virtual Networks 409
hhhh. Use of Cards in Excess of the Amount Specified in the Agreement with the Holder 410
IIII. Use of ATMs to Obtain an Unjust Benefit 411
iiii. Withdrawal of Money or Salary from the Account of a Deceased Person by Using His or Her Bank Card 412
jjjj. Use of Another Person's Bank or Credit Card at a Member Merchant by Producing a Sales Slip 413
bbb. Producing, Selling, Transferring, Purchasing or Accepting Counterfeit Bank or Credit Cards Linked to Bank Accounts Belonging to Others (Art. 245(2)) 414
ccc. Obtaining a Benefit by Using a Counterfeit or Falsified Bank or Credit Card (Art. 245(3)) 418
aaaa. It Is a Free-Form Offence 418
bbbb. Obtaining a Benefit with a Card Issued on the Basis of Untrue, Forged Documents 419
cccc. Issuing Fictitious Sales Documents with Counterfeit Cards 424
dddd. Use of Counterfeit Cards for Purchases 426
eeee. Use of a Counterfeit Bank or Credit Card at a Member Merchant by Producing a Sales Slip 427
ee. Result 427

aaa. The Result with Regard to the Offences in Paragraphs 1 – 3 of Article 245 427
bbb. The Result with Regard to the Offence in Paragraph 2 of Article 245 429
b. Mental (Subjective) Elements of the Statutory Definition of the Offence 429
4. The Element of Unlawfulness 430
5. Special Forms of Appearance of the Offence 432
a. Attempt 432
b. Participation 439
c. Concurrence 443
aa. In General 443
bb. Application of the Rule on the Continuing Offence 444
aaa. Application of the Continuing Offence with Regard to Art. 245(1) 444
bbb. Application of the Continuing Offence with Regard to Art. 245(2) 450
ccc. Application of the Continuing Offence with Regard to Art. 245(3) 450
cc. Various Problems of Concurrence Arising in Relation to Article 245 452
aaa. Can the Offence of Obtaining an Unlawful Benefit with a Bank or Credit Card Belonging to Another Person (Art. 245(1)) and the Offence of Theft (Art. 141) Be Applied Together to the Same Act? 452
aaaa. The Decision of the General Criminal Assembly of the Court of Cassation (YCGK) on the Matter 452
bbbb. Assessment and My View 456
bbb. Where the Bank Card Is Obtained on the Pretext of Helping and the Money Is Taken by the Perpetrator, the Offence of Theft Is Committed 457
ccc. The Relationship between the Offence of Obtaining an Unlawful Benefit with a Bank or Credit Card Belonging to Another Person (Art. 245(1)) and the Offence of Fraud (Art. 157) 461
ddd. The Relationship between the Offence of Obtaining an Unlawful Benefit with a Bank or Credit Card Belonging to Another Person (Art. 245(1)) and the Offence of Qualified Fraud (Art. 158(1)(f)) 472
eee. The Relationship between the Offence of Obtaining an Unlawful Benefit with a Bank or Credit Card Belonging to Another Person (Art. 245(1)) and the Offence of Breach of Trust (Art. 155) 475
fff. The Relationship between Producing, Selling, Transferring, Purchasing or Accepting Counterfeit Bank or Credit Cards Linked to Bank Accounts Belonging to Others (Art. 245(2)) and the Offence of Forgery of Documents (Arts. 204 – 207) 478
ggg. The Relationship between the Offence of Obtaining an Unlawful Benefit with a Counterfeit Bank or Credit Card (Art. 245(3)) and the Offence of Qualified Fraud (Art. 158(1)(f)) 480
hhh. Commission of Paragraph 2 and Paragraph 3 of Article 245 Together 482
III. Commission of Article 245 Together with Articles 135 and 136 488
6. Personal Grounds for Exemption from Punishment and Personal Grounds Extinguishing Punishment 489
a. The Relationship between Perpetrator and Victim 490
b. Effective Remorse 492
7. Sanction, Investigation and Prosecution 497
F. **The Offence of Producing and Trading in Prohibited Devices and Programs (Art. 245/A) 500**
1. In General 500
2. Protected Legal Interest 504
3. Conformity with the Statutory Definition of the Offence 504
a. Material (Objective) Elements of the Statutory Definition of the Offence 504
aa. Perpetrator 504

bb. Victim 504
cc. Object of the Offence 504
dd. Conduct (Act) 505
b. Mental (Subjective) Elements of the Statutory Definition of the Offence 506
4. The Element of Unlawfulness 507
5. Special Forms of Appearance of the Offence 507
a. Attempt 507
b. Participation 508
c. Concurrence 508
6. Sanction, Investigation and Prosecution 508
III. CYBERCRIMES AMONG THE OFFENCES AGAINST PROPERTY 509
A. The Offence of Theft Committed by Using an Information System (Art. 142(2)(e)) 509
1. In General 509
2. Protected Legal Interest 512
3. Conformity with the Statutory Definition of the Offence 512
a. Material (Objective) Elements of the Statutory Definition of the Offence 512
aa. Perpetrator 512
bb. Victim 512
cc. Object of the Offence 512
aaa. Data as the Object of the Offence 512
bbb. Views on Whether Data Can Constitute the Qualified Form of the Offence of Theft and the Decisions of the Court of Cassation on the Matter 513
aaaa. The View that Data Can Be the Object of the Qualified Form of the Offence of Theft and the Decisions of the Court of Cassation 513
bbbb. The View that Data Cannot Be the Object of the Qualified Form of the Offence of Theft and the Decisions of the Court of Cassation 514
cccc. The Decision of the YCGK that Data Can Be the Object of the Qualified Form of the Offence of Theft and the Decisions of the Court of Cassation to the Same Effect 515
dddd. Assessment and My View 517
dd. Conduct (Act) 521
ee. Result 523
ff. Qualified Form of the Offence 523
b. Mental (Subjective) Elements of the Statutory Definition of the Offence 523
4. The Element of Unlawfulness 523
5. Special Forms of Appearance of the Offence 524
a. Attempt 524
b. Participation 524
c. Concurrence 524
6. Sanction, Investigation and Prosecution 526
B. The Offence of Fraud Committed by Using an Information System (Art. 158(1)(f)) 526
1. Information Systems as Constituting the Qualified Form of the Offence of Fraud, in General 526
2. Is Commission of the Offence of Fraud through Online Shopping Sites a Qualified Form? 537
3. Assessment and My View 539
4. Personal Grounds Extinguishing or Reducing Punishment 539
IV. OTHER OFFENCE TYPES THAT MAY BE COMMITTED BY MEANS OF INFORMATION SYSTEMS 540
A. The Offence of Hindering Communication (Art. 124) 540
B. The Offence of Insult (Art. 125) 541

C. The Offence of Persistent Stalking (Art. 123/A) 545
1. Introduction 545
a. The Need for a Provision on Persistent Stalking 545
b. How the Acts Constituting the Offence of Persistent Stalking First Emerged 549
c. The Importance of Normative Regulation 552
2. Protected Legal Interest 555
3. Conformity with the Statutory Definition of the Offence 556
a. Material (Objective) Elements of the Statutory Definition of the Offence 556
aa. Perpetrator 556
bb. Victim 556
cc. Object of the Offence 556
dd. Conduct (Act) 557
aaa. Nature of the Act 557
bbb. Persisting 558
ccc. Physically Following 560
ddd. Attempting to Establish Contact with the Victim 562
aaaa. Using Means of Correspondence and Communication 563
bbbb. Using Information Systems 563
cccc. Using Third Parties 564
ee. Result 565
aaa. Causing Serious Distress to the Victim 565
bbb. The Victim Fearing for His or Her Own Safety or That of a Person Close to Him or Her 567
ff. Qualified Form of the Offence 568
aaa. Commission of the Offence against a Child 568
bbb. Commission of the Offence against a Spouse from Whom the Perpetrator Is Judicially Separated or Divorced 569
ccc. The Offence Causing the Victim to Change School, Workplace or Home, or to Leave School or Work 570
ddd. Commission of the Offence by a Perpetrator Subject to a Removal Order or to an Order Not to Approach the Home, School or Workplace 570
eee. A Missing Qualifying Element: The Hate Motive 571
b. Mental (Subjective) Element of the Statutory Definition of the Offence 572
4. The Element of Unlawfulness 572
5. Special Forms of Appearance of the Offence 572
a. Attempt 572
b. Participation 573
c. Concurrence 574
6. Sanction, Investigation and Prosecution 575
D. The Offence of Violating the Confidentiality of Communications (Art. 132) 578
E. The Offence of Listening to or Recording Conversations between Persons (Art. 133) 580
F. The Offence of Violating the Privacy of Private Life (Art. 134) 582
G. The Offence of Obscenity (Art. 226) 584
H. Providing a Place and Facilities for Gambling by Using Information Systems (Art. 228(3)) 588

CHAPTER FOUR

CYBERCRIMES PROVIDED FOR IN THE LAW ON INTELLECTUAL AND ARTISTIC WORKS AND IN THE ELECTRONIC SIGNATURE LAW

I. CYBERCRIMES PROVIDED FOR IN THE LAW ON INTELLECTUAL AND ARTISTIC WORKS 591

A. In General 591

B. Offences of Infringement of Economic, Moral and Related Rights (Art. 71) 593

1. In General 593

2. Legal Interest Protected by the Offence 594

3. Conformity with the Statutory Definition of the Offence 595

a. Material (Objective) Elements of the Statutory Definition of the Offence 595

aa. Perpetrator 595

bb. Victim 596

cc. Object of the Offence 598

dd. Conduct (Act) 599

aaa. Acts Constituting the Offence against Moral Rights 599

aaaa. Communicating to the Public and Publishing 599

bbbb. Giving Information about the Content of a Work Not Yet Made Public 601

cccc. Putting a Name to the Work 601

dddd. Distributing, Disseminating and Publishing the Work under the Name of a Well-Known Other Person 601

eeee. Failure to Cite the Source Quoted, or Citing a Wrong, Inadequate or Misleading Source 601

ffff. Modification of the Work 602

bbb. Acts against Economic Rights 602

aaaa. Adaptation of the Work 602

bbbb. Reproduction of the Work 602

cccc. Offering for Sale Copies of the Work Reproduced by the Perpetrator Himself or Herself 603

dddd. Distribution of the Work by Rental or Public Lending 603

eeee. Importation of the Work 604

ffff. Performance of the Work 604

gggg. Dissemination and Publication of the Work over a Data Transmission Network 604

hhhh. Purchase of the Work for Commercial Purposes 605

IIII. Possession and Storage of the Work Other than for Personal Purposes 605

ccc. Acts against Related Rights 605

ee. Result 606

b. Mental (Subjective) Elements of the Statutory Definition of the Offence 606

4. The Element of Unlawfulness 606

5. Special Forms of Appearance of the Offence 608

a. Attempt 608

b. Participation 608

c. Concurrence 609

6. Effective Remorse 610

7. Sanction, Investigation and Prosecution 611

C. The Offence of Unauthorised Removal or Alteration of Information Appearing When the Work Is Presented to the Public and of the Numbers or Codes Representing That Information (Art. 71(2)) 613

D. The Offence of Preparatory Acts Aimed at Rendering Protective Programs Ineffective (Art. 72) 614

II. CYBERCRIMES PROVIDED FOR IN THE ELECTRONIC SIGNATURE LAW 615
A. Offences in the Electronic Signature Law (EİK) (Arts. 16 – 17) 615
B. Legal Interest Protected by the Offence 618
C. Conformity with the Statutory Definition of the Offence 619
1. Material (Objective) Elements of the Statutory Definition of the Offence 619
a. Perpetrator 619
b. Victim 619
c. Object of the Offence 620
d. Conduct (Act) 622
aa. With Regard to the Offence of Unauthorised Use of Electronic Signature Creation Data (Art. 16 EİK) 622
aaa. In General 622
bbb. Obtaining the Data or the Device 623
ccc. Giving the Data or the Device 623
ddd. Copying the Data or the Device 624
eee. Recreating the Signature Creation Device 624
fff. Creating an Electronic Signature without Authorisation 624
bb. With Regard to the Offence of Forgery of Electronic Certificates (Art. 17 EİK) 625
aaa. In General 625
bbb. Creating a False Electronic Certificate 626
ccc. Imitating Valid Certificates 626
ddd. Falsifying Valid Certificates 627
eee. Using a False Certificate 627
e. Result 628
f. Qualified Form of the Offence 628
2. Mental (Subjective) Elements of the Statutory Definition of the Offence 628
D. The Element of Unlawfulness 629
E. Special Forms of Appearance of the Offence 630
1. Attempt 630
2. Participation 630
3. Concurrence 630
F. Sanction, Investigation and Prosecution 631
G. Misdemeanours under the Electronic Signature Law (EİK) (Art. 18) 631

CHAPTER FIVE

COERCIVE MEASURES OF CRIMINAL PROCEDURE WITH REGARD TO CYBERCRIME, DIGITAL FORENSICS AND MEASURES TO BE TAKEN IN COMBATING CYBERCRIME

I. IN GENERAL 635
II. COERCIVE MEASURES OF CRIMINAL PROCEDURE DIRECTED AT INFORMATION SYSTEMS 636
A. Search, Copying and Seizure in Information Systems 636
1. Legal Basis 636
2. Existence of Strong Grounds for Suspicion Based on Concrete Evidence 638
3. Impossibility of Obtaining Evidence by Other Means 640
4. The Measure of Search and Copying 642
5. The Measure of Seizure 642
6. Objection to the Decision Ordering the Measure 645
7. Art. 134 of the Code of Criminal Procedure (CMK) Is a Special Provision 645

8. Criticisms Raised in Practice and the Method Applied 646
B. Legislative Innovations and Shortcomings in Investigation and Prosecution 648
1. The Convention on Cybercrime (ASSS) Becoming Part of Our Domestic Law 648
2. The Amendment Introduced with regard to Investigations by Art. 3(4) of Law No. 5651 and the Situation after the Annulment of Paragraph 4 by the Constitutional Court (AYM) 649
3. The Uncertainty as to What Is to Be Done at the End of the Proceedings with Forensic Images Taken under Art. 134 CMK Should Be Removed 650
4. The Failure to Mention Cybercrime in Art. 135 CMK Leads to Deficient Investigations or to Unlawfully Obtained Evidence 651
C. An IP Address Alone Does Not Identify the Perpetrator 652
D. The Perpetrator Cannot Be Reached without an IP Address 657
E. NAT IP and Port Information Must Be Obtained in Order to Identify the Perpetrator Fully and Correctly 658
F. What Needs to Be Done in Investigation and Prosecution 661
III. DIGITAL FORENSICS 664
A. Introduction 664
B. The Science of Computer Criminalistics 665
C. The Concept of Digital Forensics 665
1. Definition 665
2. Benefits of the Digital Forensics Methodology 667
D. Digital Evidence and Types of Digital Evidence 668
1. What Is Digital (Electronic) Evidence? 668
2. Conditions Required for Digital Evidence to Be Usable 671
3. Media on Which Digital Evidence Is Found 672
a. Motherboard 673
b. Processor 673
c. Memory: RAM (Random Access Memory) – ROM (Read Only Memory) – Cache Memory 674
d. Hard Disk (Hard Disk Drive) 675
e. Floppy Disks and CD/DVD/Blu-ray 676
f. Memory Cards 676
g. Digital Storage Devices 676
h. Mobile Phones 676
ı. Digital Video and Still Cameras 677
i. MP3 Players/iPod 677
j. Handheld Computers (PDA, PALM, Pocket PC) 677
k. Portable Memory Devices (Flash Memory) 677
l. Printers, Fax Machines, Photocopiers and Other Hardware 678
4. The Council of Europe Electronic Evidence Guide 678
E. Stages of Digital Forensics 680
1. The Crime Scene – Collection and Preservation of Evidence 680
2. Points to Be Observed before Starting to Collect Evidence 680
a. First Step 680
b. Second Step 681
3. What Must Not Be Done at the Crime Scene 682
a. Mistake 1 – Operating the Computer 682
b. Mistake 2 – Asking the Owner of the Computer for Help 682
c. Mistake 3 – Failing to Check for Computer Viruses 682
d. Mistake 4 – Taking No Precautions during the Transport of Electronic Evidence 682

4. Live Analysis 682
5. Packaging – Transport – Preservation 684
6. The Latent Nature of Electronic Evidence 684
F. The Digital Forensics Expert's Approach to Electronic Evidence 685
1. In General 685
2. Examination 685
a. Disk Write Protection 685
b. Forensic Imaging 686
c. Hash Value 688
d. Result of the Examination 689
3. Interpretation (Evaluation/Analysis) 690
a. Stages of Computer Analysis 690
b. Stages of Mobile Phone Analysis 690
c. Stages of Network Traffic Data Analysis 691
d. Stages of Analysis of External Disks, CD/DVDs, Memory Cards and Flash Drives 692
e. User-Protected Files 693
f. Anti-Forensics and Concealment Methods 693
4. General Principles to Be Observed by Experts 694
5. Data Recovery 694
6. Features and Preparation of the Digital Forensics Report 694
IV. MEASURES TO BE TAKEN IN COMBATING CYBERCRIME 695
A. Measures to Be Taken by Individuals and/or Institutions 695
1. In General 695
2. Ensuring and Testing System Security 697
B. Measures to Be Taken by States 699
1. Establishment and Training of Units Prosecuting Cybercrime 699
a. General Remarks 699
b. The Example of the USA 699
c. The Situation in Our Country 700
2. Measures Taken against the Phenomenon of Cyberterrorism 702
3. State Control of Cyberspace 702
4. International Cooperation 704
5. The Relationship between Organised Crime and Cybercrime 704
V. CYBERCRIME DE LEGE FERENDA 708
A. From the Perspective of Criminal Law 708
B. From the Perspective of the Law of Criminal Procedure 711

CHAPTER SIX
INTERNET COMMUNICATION LAW

I. INTRODUCTION 715
II. THE MEANING AND LIMITS OF FREEDOM OF THOUGHT (EXPRESSION) AND ITS IMPORTANCE FOR THE INTERNET 717
A. Concept 718
B. Content of Freedom of Thought (Expression) 721
C. Freedom of Expression under the European Convention on Human Rights (ECHR) 722
1. The Origin of the ECHR and Its Entry into the Turkish Legal Order 722

2. Meaning and Application of Freedom of Expression 724
a. The Concept of Freedom of Expression in the ECHR 724
b. Art. 10(1) ECHR: Content of Freedom of Expression 724
c. Art. 10(2) ECHR: Cases in Which Freedom of Expression May Be Restricted 728
d. Art. 10(2) ECHR: The Limit of Restriction 733
3. The Approach of the European Court of Human Rights (ECtHR) to the Internet in the Context of Freedom of Expression 735
D. Assessment and Our View 736
III. DISTINCTIONS CONCERNING THE BLOCKING OF INTERNET COMMUNICATION 740
A. The Distinction between Blocking of Access to the Internet and Blocking of Internet Communication 740
B. The Distinction between the Technical and the Legal Possibility of Blocking Internet Communication 742
1. Scope of the Distinction 742
2. Technical Methods of Blocking 742
C. The Distinction as to the Possibility of Blocking Internet Communication by the Methods of "General Blocking – Specific Blocking" 748
IV. PROVISIONS INTRODUCED BY LAW NO. 5651 "ON THE REGULATION OF PUBLICATIONS ON THE INTERNET AND COMBATING OFFENCES COMMITTED BY MEANS OF SUCH PUBLICATIONS" 749
A. Drafting Process, Purpose and Scope of the Law 749
1. Drafting Process of the Law 749
2. Purpose and Scope 752
3. Legal Nature of the Measures Provided for in Law No. 5651 753
B. Institutions Involved in the Governance of the Internet 754
1. The Information and Communication Technologies Authority 754
2. The Internet Development Board 758
C. Definitions 758
D. Obligation to Inform the Public 759
E. Duty to Collect and Transmit Traffic Data 764
F. Liability of Internet Actors 769
1. In General 769
2. The Example of Germany 769
3. The Regulation in Law No. 5651 771
a. Responsibilities and Obligations of Content Providers 771
b. Responsibilities and Obligations of Hosting Providers 780
i. Hosting Providers' Non-Liability for Content 780
ii. Hosting Providers' Responsibility to Retain Traffic Data 782
iii. Sanctions for Breach of Obligations 782
iv. Classification and Differentiation of Hosting Providers 783
c. Responsibilities and Obligations of Access Providers 784
d. The Union of Access Providers 787
e. Responsibilities and Obligations of Mass-Use Providers 790
f. Assessment and My View 792
V. GENERAL BLOCKING OF INTERNET ACCESS (FILTERING) 793
A. The Internet Is a Field Subject to Legal Regulation 795
B. Governance of the Internet 797
C. Models for the Regulation of Cyberspace 800

1. Regulation at National Level 801
2. Regulation by International Conventions 801
3. Regulation through International Organisations 802
4. Self-Regulation 802
5. Our View on the Models of Regulation 803
D. The Internet as a Medium of Mass Communication and the Blocking of Its Communication 804
1. The Concept of Mass Communication in General 804
2. The Phenomenon of Misuse of Internet Communication 805
3. Views on the General Blocking of Internet Communication 807
4. State Regulation of Cyberspace and General Filtering 808
E. An Administrative Practice of General Blocking of Internet Communication – The Powers of the Telecommunications Authority over the Internet and the Decisions It Has Taken 810
F. General Blocking of Internet Communication under Law No. 5651 on the Regulation of Internet Publications 812
VI. SPECIFIC BLOCKING OF INTERNET ACCESS (BLOCKING OF ACCESS) 818
A. Blocking of Internet Communication by Court Decision 818
1. A Case Study on the Blocking of Internet Communication by Court Decision 819
2. Assessment of the Case Study on the Blocking of Internet Communication by Court Decision 821
3. The ECtHR Judgment Holding That Law No. 5651 Violates Article 10 of the ECHR 823
4. The Constitutional Court Judgment Holding That the Decision of the Presidency of Telecommunication and Communication (TİB) to Block Communication Violated Freedom of Expression 828
a. As to Admissibility 828
b. As to the Merits 829
c. Assessment and Our View 834
5. The Constitutional Court Judgment of 26/12/2019, Published in the Official Gazette on 20/01/2020, on the Application of Wikimedia Foundation Inc. and Others 835
a. As to Admissibility 835
b. As to the Merits 837
c. Assessment and Our View 839
6. The Constitutional Court Judgment of 27/10/2021, Published in the Official Gazette on 07/01/2022, on the Application of Keskin Kalem Yayıncılık ve Ticaret A.Ş. and Others 840
a. As to Admissibility 844
b. As to the Merits 844
c. Assessment and Our View 857
B. Blocking of Internet Communication by Administrative Practice – The Example of Blocking of Communication by Decision of the Telecommunications Board 858
1. A Case Study on the Blocking of Internet Communication by Administrative Practice 858
2. Assessment of the Case Study on the Blocking of Internet Communication by Administrative Practice 860
C. Blocking of Internet Communication by a "Legal Person Governed by Private Law" – The Example of Blocking of Communication by Decision of the Turkish Football Federation 863
VII. ASSESSMENT OF LAW NO. 5651 WITH REGARD TO THE SPECIFIC BLOCKING OF INTERNET COMMUNICATION (REMOVAL OF CONTENT AND/OR BLOCKING OF ACCESS) 865
A. Types of Offence for Which a Decision to Remove Content and/or Block Access May Be Issued 865
1. In General 865
2. Obscene Publications 869
3. Providing a Place and Facilities for Gambling 874
4. Offences Relating to the Law on Football and Other Sports Competitions 876

5. Offences Committed against Atatürk 877
6. Offences Relating to the Law on Taxes, Funds and Shares Levied on the Proceeds of Games of Chance 878
7. Additional Article 4 of the Law on Intellectual and Artistic Works (FSEK) 878
B. **The Decision to Remove Content and/or Block Access as a Coercive Measure** 879
1. Legal Basis 879
2. Who May Issue the Decision 879
a. Judge and Public Prosecutor 879
b. The Power of the President of the TİB 880
3. The Procedure to Be Applied 882
4. Lifting of the Measure 883
5. Sanction 885
6. The Situation in Practice and Our View 885
C. **The Decision to Remove Content and/or Block Access as an Administrative Measure** 889
1. Legal Basis 889
2. Who May Issue the Decision 889
3. Legal Nature of Blocking of Access as an Administrative Measure 891
4. The Procedure to Be Applied 899
5. Sanction 900
D. **Compensation for Unjustified Blocking Decisions** 901
E. **Removal of Content and Blocking of Access in Cases Where Delay Is Prejudicial (Art. 8/A)** 901
F. **Removal of Unlawful Content from Publication and Blocking of Access (Art. 9)** 903
G. **Blocking of Access to Content on Grounds of Privacy (Art. 9/A)** 908
H. **The Competent Court** 909
VIII. **LEGAL REGIME OF SOCIAL NETWORK PROVIDERS** 909
A. **The Need to Regulate Social Network Providers** 909
B. **Legal Regime of Social Network Providers under the Internet Law** 912
1. In General 912
2. Obligation to Appoint a Representative, and the Representative's Qualifications and Responsibilities 912
3. Liability of Social Network Providers in Respect of Applications Made under Art. 9/A of the Internet Law 914
4. Obligation to Submit to the Authority Reports on the Implementation of Decisions to Remove Content and/or Block Access 914
5. Obligation to Provide Information on Certain Offences to the Authorities Competent for Investigation and Prosecution 915
6. Obligation to Store Data in Turkey 916
7. Obligation to Take the Necessary Measures to Provide Differentiated Services Specific to Children 917
8. Sanctions Applicable to Social Network Providers in Connection with Blocking of Access and Removal of Content 918
9. Sanction for Failure to Comply with a Decision to Remove Content and/or Block Access Issued by the President of the Information and Communication Technologies Authority (BTK) 918
10. Obligation to Comply with the Rules on User Rights 920
11. Liability for Damages on Account of Unlawful Content 921
12. Obligation to Establish an Effective Application Mechanism for the Removal of Hashtags and Featured Content by Way of Notice and Takedown 921
13. Notification to Law Enforcement of Content Endangering the Safety of Life and Property of Persons 921

14. Obligations of Social Network Providers as Content and Hosting Providers under the Internet Law 922
15. The BTK's Power to Request Information and Conduct On-Site Inspections 922
16. Obligation to Draw Up a Crisis Plan 923
17. Secondary Legislation 923
18. Transitional Provision 924
C. Assessment and Our View 925
IX. LEGAL REGIME OF INTERNET NEWS SITES 927
A. The Question of the Applicability of the Rules of Press Law to Internet Publishing 927
B. Legal Regime of Internet News Sites under the Press Law 929
1. In General 929
2. Definition 929
3. Freedom and Its Limit 930
4. Obligation to Display Information on the Site 930
5. Obligation to Display News and Content Updates Clearly on the Site 931
6. Consequences of Treating Internet News Sites as Periodicals 932
a. General Obligations Arising from the Press Law 932
b. Obligation to File a Declaration and Its Consequences 933
c. Loss of the Rights relating to Official Announcements and Advertisements and to Employees' Press Cards as a Consequence of Filing the Declaration 934
7. Obligation to Preserve Content Published on an Internet News Site in a Manner Ensuring Its Accuracy and Integrity 937
8. Right of Correction and Reply 938
9. The Manner of Reporting News of Sexual Assault, Murder and Encouragement of Suicide 939
10. Time Limits and Procedure for Prosecution and Investigation 940
X. LEGAL REGIME OF OVER-THE-TOP SERVICE PROVIDERS 940
A. Definition and Concept 940
B. Rights and Obligations 941
C. Sanction 944
XI. ASSESSMENT AND OUR VIEW 945
Bibliography 957
Table of Cases 989
Subject Index 999
Author's Curriculum Vitae 1007

This document is the table of contents of the book, translated from Turkish; page numbers refer to the printed book. Page of the book: www.dulger.av.tr/en/publications/bilisim-suclari-ve-internet-iletisim-hukuku/