

Table of Contents

Agnieszka Gryszczyńska

Preface 11

Ferenc Sántha

Chapter 1. Definition and Systematisation of Cybercrimes	27
1.1. Introduction	27
1.2. Single Definitions of Cybercrimes	29
1.3. The Definitions Refer to Different Categories of Relevant Crimes	30
1.3.1. Dichotomies of Cybercrimes	31
1.3.2. Trichotomies of Cybercrimes	31
1.4. Definitions Based on the Systematisation of Cybercrimes (Taxonomies of Cybercrimes)	34
1.5. Overview: Cyber-Dependent Crimes in Hungarian Criminal Law	38
1.5.1. Article 423 of the HCC – Breach of an Information System or Data	39
1.5.2. Article 424 of the HCC – Circumvention of Technical Measures for the Protection of the Information System	41
1.5.3. Article 422 of the HCC – Illegal Access to Data	42
1.5.4. Article 375 of the HCC – Fraud Committed by Means of an Information System	42
1.6. Closing Remarks	43
REFERENCES	44

Agnieszka Gryszczyńska

Chapter 2. The Scope of Criminalisation of Cybercrime in Poland	47
2.1. Introduction	47
2.2. The Most Common Cyber Security Incidents Occurring in Poland	49
2.3. The Substantive Basis for the Criminalisation of Cybercrime in Poland	55
2.3.1. Introductory Remarks	55
2.3.2. Cyber-Dependent Crimes in the Polish Criminal Law	59
2.3.3. Cyber-Enabled Crimes in Polish Criminal Law	63
2.3.3.1. Computer Fraud – Article 287 CC	63
2.3.3.2. Fraud – Article 286 CC	65
2.3.3.3. Identity Theft – Article 190a § 2 CC	67
2.4. The New Regulation Concerning Abuse of Electronic Communications	68
2.5. The Scope of Criminalisation of Cybercrime in Poland in Comparison to International Regulations	70
2.6. Summary and Conclusions	72
REFERENCES	74

Judit Jacsó

Chapter 3. New Developments and Challenges in the Fight Against Money Laundering by Means of Cybercrime – Methods and Risks	79
3.1. Introduction	79
3.2. Anti-Money Laundering Regulation (AML) – Historical Overview and International Legal Framework	81
3.2.1. Source and First Regulation of Money Laundering	81
3.2.2. International Legal Framework	83
3.2.2.1. United Nations Legal Framework	83
3.2.2.2. Relevant Conventions of the Council of Europe (Strasbourg Convention and Warsaw Convention)	84
3.2.2.3. Universal Anti-Money Standards (FATF)	87
3.2.2.4. Legal Framework of the European Union	88

3.3.	Methods and Stages of Money Laundering in Cyberspace	89
3.3.1.	Stages of Money Laundering in Cyberspace	89
3.3.2.	Cash Couriers and the Money Mule Phenomenon	91
3.4.	Connection Between Money Laundering and Cybercrime	94
3.4.1.	Basic Remarks about Cybercrime	94
3.4.2.	The Meaning of Cyber-Laundering	96
3.4.3.	AML Potential Risk of Virtual Currencies and Crypto Assets	99
3.4.3.1.	Conceptual Clarification of Definitions	99
3.4.3.2.	Potential Risks Associated with Cryptocurrency	103
3.5.	Conclusion and Proposals	104
	REFERENCES	106

Judit Jacsó

	Chapter 4. Preventive Means Against Cyber-Laundering in the European Union	111
4.1.	Introduction	111
4.2.	Global Standard (FATF Recommendations) in Connection to VAs and VASPs	113
4.2.1.	Regulatory Development	113
4.2.2.	FATF Recommendation No. 15 and FATF Recommendation No. 16 (Travel Rule)	116
4.3.	Development of the AML Regulation in the European Union	118
4.3.1.	Main Characteristics of the AML Regulation Framework in the EU	118
4.3.2.	Requirement to Report Suspicious Transactions and the Role of the Financial Intelligence Unit (FIU)	122
4.3.3.	The Fight Against Money Laundering by Criminal Law	124
4.4.	New Developments in the European Union	125
4.4.1.	Action Plan of the European Commission 2020 and Legislative Package 2021	125

4.4.2.	Amendments of the IV. AML Directive to Prevent Cyber-Laundering	127
4.5.	Summary and Conclusion	129
	REFERENCES	130
<i>Ferenc Sántha</i>		
	Chapter 5. Problems of Jurisdiction in Cybercrimes Cases	133
5.1.	Introduction	133
5.2.	The Concept of Jurisdiction	135
5.3.	The Principles of Jurisdiction	136
5.4.	Conflicts of Jurisdictions	141
5.5.	Conflicts of Jurisdiction and the Institutions of International Cooperation in Criminal Matters	145
5.5.1.	The Detected Location of the Cyber-Attack Is Hungary	146
5.5.2.	The Detected Location of the Cyber-Attack Is a Member State of the European Union	148
5.5.3.	The Detected Location of the Cyber-Attack Is a Third Country Outside the European Union	149
5.6.	Conclusion	150
	REFERENCES	151
<i>Piotr Burczaniuk</i>		
	Chapter 6. Pre-Trial Activities of Intelligence Service and Law Enforcement Agencies	153
6.1.	Introduction	153
6.2.	Impact of the Cybersecurity System on the Fight Against Cybercrime	154
6.3.	Types and Scope of Law Enforcement Intelligence Gathering Activities to Combat Cybercrime – Current Status and Challenges	166
6.4.	International Information and Operational Cooperation in the Fight Against Cybercrime	182
6.5.	Conclusions	188
	REFERENCES	189

Erika Róth

Chapter 7. Application of Coercive Measures in Cybercrime Cases	193
7.1. Introduction	193
7.2. General Rules for the Application of Coercive Measures	195
7.3. Coercive Measures Affecting Personal Liberty	196
7.4. Coercive Measures Affecting Assets	197
7.4.1. Search	197
7.4.2. Body Search	200
7.4.3. Seizure	200
7.4.3.1. General Rules of Seizure	201
7.4.3.2. Seizure of Electronic Data and Ordering the Preservation of Electronic Data	202
7.4.3.3. Ordering the Preservation of Electronic Data	206
7.4.4. Sequestration	208
7.4.5. Rendering Electronic Data Temporarily Inaccessible	209
7.5. <i>The Lege Ferenda</i> Proposals	211
7.6. Conclusion	212
REFERENCES	213

Erika Róth

Chapter 8. Particulars of Evidence in Cybercrime Cases	215
8.1. Introduction	215
8.2. General Rules of Evidence	216
8.3. Means of Gathering Evidence	217
8.3.1. Means of Evidence	218
8.3.2. Evidentiary Acts	220
8.3.2.1. Inspection	220
8.3.2.2. On-Site Interrogation	221
8.3.2.3. Reconstruction of a Criminal Offence	222
8.3.2.4. Presentation for Identification	222
8.3.2.5. Confrontation	222
8.3.3. Obtaining the Evidence	223
8.4. Particulars of Evidence Used in Cybercrime Cases	224

8.4.1.	Electronic Data as a Means of Evidence	226
8.4.2.	IT Expert in Criminal Proceedings	230
8.4.3.	Covert Methods Used for Obtaining Evidence in Cybercrime Cases	231
8.5.	<i>De Lege Ferenda</i> Proposals	233
8.6.	Conclusion	234
	REFERENCES	235

Rafał Wielki

Chapter 9. Data Retention and Legal Problems of Investigating Cybercrime		239
9.1.	Introduction	239
9.2.	Law on Data Retention in European Union	240
9.3.	Polish Approach to Data Retention	243
9.4.	Some Comments about the Future	246
9.5.	Conclusions	249
	REFERENCES	250

Rafał Wielki

Chapter 10. Crime Analysis Against the Challenges of Cybercrime		253
10.1.	Introduction	253
10.2.	Characteristics of Cybercrime	254
10.3.	Crime Analysis in Cybercrime Cases	264
10.4.	Techniques of Crime Analysis	270
10.5.	Conclusions	277
	REFERENCES	279