

TABLE OF CONTENTS

1 SECURITY ARCHITECTURE AND THE INTERCEPTION OF TELECOMMUNICATION	11
1.1 National Security Architecture – Two Frameworks of Interception.....	11
1.2 Powers for interception of telecommunication – Legislative grounds	14
1.2.1 <i>The law of criminal procedure</i>	14
1.2.2 <i>Law of intelligence agencies</i>	18
1.2.3 <i>Financial and Customs Investigation Service</i>	19
1.3 Responsibility for the technical performance of interception measures – a general overview	20
1.4 Legitimacy of data transfers between different security services	25
1.5 Statistics on Telecommunication Interception	27
2 CONSTITUTIONAL AND STATUTORY SAFEGUARDS OF TELECOMMUNICATIONS	31
2.1 Areas of constitutional protection	31
2.2 Proportionality of access to data.....	36
2.2.1 <i>Secrecy of telecommunications</i>	40
2.2.2 <i>Secrecy of retained traffic data</i>	41
2.2.3 <i>Secrecy of information systems</i>	46
2.3 Statutory consequences of constitutional protection.....	47
2.3.1 <i>Protection of the secrecy of telecommunications</i>	48
2.3.2 <i>Protection of the confidentiality and integrity of information systems</i>	49
2.3.3 <i>Protection of the core area of privacy</i>	50
2.3.4 <i>Criminal liability for the unlawful infringement of the telecommunication secrecy</i>	51
2.3.5 <i>Protection of professional secrets in criminal procedural law</i>	53
2.3.6 <i>The principle of the “purpose limitation of personal data”</i>	55
3 POWERS FOR ACCESSING TELECOMMUNICATION DATA	57
3.1 Overview	57
3.2 Requirement of (reasonable) clarity for powers in the law of criminal procedure.....	58
3.3 Differentiation and classification of powers in the law of criminal procedure.....	63

4	INTERCEPTION OF CONTENT DATA	65
4.1	Object of interception.....	65
4.2	Special protection of confidential communication content.....	68
4.3	Execution of telecommunication interception.....	69
4.4	Duties of telecommunication service providers to cooperate.....	70
4.5	Formal prerequisites of interception orders.....	73
4.6	Substantive prerequisites of interception orders.....	76
4.7	Consent by a communication participant to the measure	79
4.8	Duties to record, report, and destroy.....	80
4.9	Notification duties and remedies	81
4.10	Confidentiality requirements	82
5	COLLECTION AND USE OF TRAFFIC AND SUBSCRIBER DATA	83
5.1	Collection of traffic data.....	83
5.2	Collection of subscriber data	85
5.3	“Data retention”	86
6	ACCESS TO (TEMPORARILY) STORED COMMUNICATION DATA	89
6.1	Online searches with the help of remote forensic software.....	89
6.2	Search and seizure of stored communication data	90
6.3	Duties to cooperate: production and decryption orders.....	91
7	USE OF ELECTRONIC COMMUNICATION DATA IN JUDICIAL PROCEEDINGS	93
7.1	Use of electronic communication data in the law of criminal procedure.....	93
7.2	Inadmissibility of evidence as a consequence of inappropriate collection	95
7.3	Use of data outside the main proceedings.....	101
7.3.1	<i>Data from other criminal investigations</i>	101
7.3.2	<i>Data from preventive investigations</i>	102
7.3.3	<i>Data from foreign jurisdictions</i>	104
7.4	Challenging the probity of intercepted data	105

8 DIFFERENTIAL COMPARATIVE NOTE: SLOVAKIA	107
8.1 Security Architecture and the Interception of Telecommunication	107
8.1.1 <i>National Security architecture – Two Frameworks of Interception</i>	107
8.1.2 <i>Legislative grounds</i>	110
8.1.3 <i>Responsibility for the technical performance and legitimacy of data transfers between different security services</i>	117
8.1.4 <i>Statistics on Telecommunication Interception</i>	118
8.2 Constitutional Safeguards of Telecommunication.....	123
8.2.1 <i>Areas of constitutional protection</i>	123
8.2.2 <i>Proportionality of access to data</i>	125
8.2.3 <i>Consequences for the interception of telecommunication</i>	127
8.2.4 <i>Statutory protection of personal data</i>	132
8.3 Powers for Accessing Telecommunication Data.....	138
8.3.1 <i>Overview</i>	138
8.3.2 <i>Requirement of (reasonable) clarity for powers in the law of criminal procedure</i>	139
8.3.3 <i>Differentiation and classification of powers in the law of criminal procedure</i>	141
8.4 Interception of Content Data.....	142
8.4.1 <i>Object of interception, special protection of confidential communication content and execution of telecommunication interception</i>	142
8.4.2 <i>Duties of telecommunication service providers to cooperate</i>	143
8.4.3 <i>Prerequisites of interception orders</i>	144
8.4.4 <i>Duties to record, report, and destroy</i>	147
8.5 Collection and use of traffic data and subscriber data.....	148
8.6 Access to (temporarily) stored communication data.....	150
8.7 Use of electronic communication data in judicial proceedings	151
8.7.1 <i>Use of electronic communication data in the law of criminal procedure</i>	151
8.7.2 <i>Inadmissibility of evidence as a consequence inappropriate collection</i>	152
8.7.3 <i>Use of data outside the main proceedings</i>	155
8.7.4 <i>Challenging the probity of intercepted data</i>	156
 Bibliography.....	 159
Appendix: Collection of Relevant Legal Provisions	167