universität wien

DISSERTATION

Remote Forensic Investigations

Verfasser
Mag. iur. Wolfgang Bärnthaler

angestrebter akademischer Grad
Doktor der Rechtswissenschaften

Wien, März 2011

Studienkennzahl lt. Studienblatt:	A 083 101
Dissertationsgebiet lt. Studienblatt:	Rechtswissenschaften
Betreuerin / Betreuer:	ao. Univ.-Prof. Mag. DDr. Erich Schweighofer

Content

Introduction ... 7
1 General Aspects – Defining the Object of Interest ... 15
1.1 Technology and Law ... 15
1.2 Remote Forensic Investigation (RFI) ... 16
1.2.1 Field of Application ... 17
1.2.2 Timeframe of Application ... 19
2 Technical Aspects of RFI ... 23
2.1 Malware ... 23
2.1.1 Introduction ... 23
2.1.2 Computer Virus ... 25
2.1.3 Worms ... 29
2.1.4 Spyware ... 31
2.2 Telecommunication ... 41
2.2.1 Introduction ... 41
2.2.2 Types of Communication ... 42
2.2.3 Communication Systems ... 43
2.3 Encryption and Decryption ... 46
2.3.1 Introduction ... 46
2.3.2 Symmetric Cryptography ... 49
2.3.3 Asymmetric Cryptography ... 51
2.3.4 Summary ... 52
2.4 Examination of a Computer – Computer Forensics ... 53
2.4.1 Introduction ... 53
2.4.2 Procedures established for Examinations ... 56
2.4.3 Hardware and Software Tools ... 63
2.5 Potential Procedures of RFI ... 66
2.5.1 Obtaining Access ... 67
2.5.2 Exploiting an Obtained Access ... 72
2.6 Conclusion and Summary ... 74
3 Legal Aspects of RFI ... 79
3.1 Introduction ... 79
3.2 RFI and the Austrian Constitution ... 80
3.2.1 State of Law ... 80
3.2.2 Fundamental and Human Rights ... 81
3.2.3 Reservation of Statuary Powers and the Principle of Proportionality ... 84
3.2.4 Federation vs. Federal States (Laender) ... 88
3.2.5 Criminal Police vs. Public Security Police ... 89
3.3 Substantive Criminal Law ... 91
3.3.1 The Convention on Cybercrime ... 91
3.3.2 Penalized Behavior ... 93
3.3.3 Offenses Following Hacking Attacks ... 100
3.4 Austrian Code of Criminal Procedure ... 104
3.4.1 Introduction ... 104
3.4.2 Search of Locations and Objects ... 112
3.4.3 Conclusion: Realization of an RFI ... 125
3.4.4 Surveillance of Communication ... 128
3.4.5 Surveillance of Data and Communication ... 133
3.4.6 Conclusion: Realization of an RFI ... 141
3.4.7 Disclosure of Transmission Data ... 145
3.4.8 Conclusion: Realization of an RFI ... 150
3.4.9 Surveillance of Persons ... 151
3.4.10 Conclusion: Realization of an RFI ... 167
3.5 Security Police Law ... 169
3.5.1 Introduction Task and Competences of the Public Security Police ... 169
3.5.2 Tasks ... 171
3.5.3 Competence Regarding Averting of Danger ... 176
3.5.4 Conclusion: Realization of an RFI ... 183

4 Prevention and Criminal (Procedural) Law ... 187
4.1 General Aspects of Prevention ... 189
4.1.1 From A State of Nature to a State of Prevention ... 189
4.1.2 Issues Challenging A State of Law ... 191
4.2 Public Security Police vs. Criminal Police ... 193
4.2.1. Diminishing Separation ... 196
4.2.2. Protection of Human Rights ... 197
4.3 Systematic Failures ... 199
4.4 Substantive Criminal Law ... 200
4.4.1 Criminal Organizations and Terrorist Associations ... 201
4.5 Strong Suspicion ... 204
Conclusion ... 213
Sources ... 219
- Internet Sources ... 219
- Literature ... 222
- Judgements ... 227
- Legislative Materials ... 230
- Commentaries ... 230
Abstract ... 231
Abstract German ... 234
Curriculum Vitae Autoris ... 237

List of Abbreviations

- ACPO Association of Chief Police Officers
- ARPA Advanced Research Project Agency
- BGH Bundesgerichtshof
- BlgNR Beilagen zu den Stenographischen Protokollen des Nationalrats
- BMI Bundesministerium für
- BMJ Bundesministerium für Justiz
- BVerfG Bundesverfassungsgericht
- CCC Convention on Cybercrime
- CCTV Closed Circuit Television.
- cf. confer
- EBRV Erläuternde Bemerkungen zur Regierungsvorlage
- e.g. exempli gratia, for example
- EMRK Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten
- ENFSI European Network of Forensic Science Institutes
- et seq. et sequentes; and the following ones
- EvBl Evidenzblatt
- FIT Forensic Information Technology
- FS Festschrift
- GP Gesetzgebungsperiode
- HFR Humbold Forum Recht
- Ibid. ibidem, in the same place
- i.e. id est
- IOCE International Organization on Computer Evidence
- IP Internet Protocol
- ITRB Der IT Rechtsberater
- JR Juristische Rundschau
- JuS Juristische Schulung
- JZ JuristenZeitung
- KH Oberster Gerichts- und Kassationshof
- KritV Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft
- LAN Local Area Network
- LG Landesgericht
- MN Margin Number
- no. number
- NJI National Institute of Justice
- ÖJZ Österreichische Juristen-Zeitung
- p. page
- para. paragraph
- pp. pages
- POTS Plain Old Telephone Service
- PSW Password Stealing Ware
- PIN Personal Identification Number
- RFI Remote Forensic Investigation
- RFS Remote Forensic Software

- StGG Staatsgrundgesetz
- SSt Entscheidungen des Obersten Gerichtshofs in Strafsachen und Disziplinarangelegenheiten
- TAN Transaction Number
- TCP/IP Transmission Control Protocol/Internet Protocol
- VfSlg Verfassungssammlung
- VOIP Voice over Internet Protocol
- VwGH Verwaltungsgerichtshof
- VwSlg Verwaltungssammlung
- WK-StGB Wiener Kommentar zum Strafgesetzbuch
- WK-StPO Wiener Kommentar zur Strafprozessordnung

Introduction

Throughout the world, the increasing use of electronic data processing and storage devices has created new phenomena. Nowadays, there is hardly an area of social life not penetrated by electronic means and its possibilities of rapid information exchange. The development in the field of electronics over the last two decades is astonishing. The single fact that e.g. storage space increased from around 100 MB to currently approximate 2 TB[1] is absolutely mind boggling as is the similar development of working memory (RAM)[2]. Within 20 years the possible storage space and working memory/speed of computers multiplied enormously. Thanks to these technical improvements, the Internet could be 'established' as a communication network for everybody. Globalization is the magic word in this context and it triggered a 'reflattening' of the world, as Thomas Friedman called this.[3] The reshaping of the world and the communication process over the last two decades was carried out by geo-economics as well as the already mentioned technological improvements. In a globalized world, borders and other physical barriers are in the process of being diminished. It does not matter anymore where you are as all necessary information, tools and software is available in an easy and affordable manner. For the common good, one might say; and indeed, the common good can be seen everywhere: communication networks work faster, letters (e-mails) are being delivered within seconds to any part of the planet, people in different places on the Earth can attend (online or video) conferences in real time without getting out their office, as long as there is a connection to the Internet. People are able to handle their banking affairs, shop for their groceries or purchase any other item via the World Wide Web. Governments conduct research in order to establish a cheaper and more efficient public administration via e-government; so do many international corporations and a lot of other businesses. The Internet offers a lot of opportunities and everyone can benefit, be it used as a sales market (e-commerce), as an outsourcing option or just as a communication platform.

---

1 One Megabyte is 106 Byte = 1.000.000 Byte meaning that 100 Megabyte are 100.000.000 Byte; on the contrary to this modern computers do have a storage capacity of 2 Terabyte meaning 2 x 1012 Byte = 2.000.000.000.000 Byte; thus it is 20.000 time higher than 20 years ago.

2 In 1981 a personal computer had the capacity to proceed 640 KB (640.000 Byte), in 1994 4 MB (4.000.000 Byte) and nowadays already 8 GB (8.000.000.000 Byte), thus its speed multiplied by 12.500 over the last 30 years, cf. <http://www.arbeitsspeicher-info.de/die-entwicklung.html> retrieved 15 February, 2010.

3 cf. Friedman, Thomas L., 'It's a Flat World, After All', New York Times 3 April, 2005; he points out 10 flatteners (e.g. the breakthrough of the Microsoft Windows 3.0 operating program; the dot.com boom; 'Outsourcing'; 'Off shoring'; 'Open-Sourcing'; etc) merging in 2000 and building up a new playing field – the globalized world we know today.

However, the brighter the light, the deeper the shadow. All these benefits mentioned above, can have inherent negative outcomes as information could be used for other purposes. Everybody knows the annoying consequence of simple, cheap and fast communications means – spam. Who has never been bothered by such e-mails? Furthermore criminals all over the world use the technology provided for their unlawful needs: 'phishing' attacks intended to collect passwords, PINs and TANs[4], fraud committed via computers (Internet fraud) or hacking attacks with the aim to spy on secret data or communication, are just a few examples. Legislators in many countries responded to these often devastating threats and established not only corresponding provisions in their criminal codes but also a close cooperation between the investigation authorities. Today, a multitude of provisions is in force dealing with computer crime.

In addition, investigating authorities obtained powerful procedural competence in order to use the same electronic tools for their investigations. However, as investigation and monitoring devices can interfere massively with fundamental and human rights of the affected persons, highly controversial questions might pop up. Especially since the attacks in September 2001, the discussions in this matter are omnipresent. Governments try to weight the justified freedoms of the individual with the no less justified interests of the public order and peace. Every person scarifies parts of his/her freedom for the greater common good. For instance, digital CCTV[5] cameras are ever present and people have already gotten used to them. The main argument in favor of such surveillance methods is crime prevention, but also the solving of crimes is mentioned as justification for the application of cameras. The question whether it is a beneficial tool to prevent criminal incidences, respectively whether the individual feels safer due to these cameras, is something completely different. Furthermore, it is to point out that the rising danger of terrorist attacks has provoked legislators all over the world to establish special provisions. Besides the old methods of wiretapping, or the employment of undercover agents, visual as well as acoustical surveillance can be implemented in certain circumstances. However, these procedural tools are seemingly still too weak to sustain the current need and demand for security. Hence, in order to maintain and preserve security and freedom, the Austrian government wants to establish a new method. For the government, 'remote forensic investigations' are the key to counter terrorism and other serious crimes, and a lot of effort has been put in, in order to path the way for it.

---

4 Personal Identification Number (PIN) and Transaction Number (TAN).
5 Closed Circuit Television.

Content and Purpose of this Thesis

The purpose of this thesis is to provide an introduction and general overview of the newly developed method of remote forensic investigations. It intends to present RFIs in a rather broad and general way. The first chapter is solemnly intended to give a clear definition of the object of interest, involving a distinction between technology and law, a clarification of the term remote forensic investigation and its potential fields of application.

The intentions behind this analysis are distinct and include principal technical questions and sole legal issues. Hence, both, the technical, as well as the legal requirements for remote forensic investigations are illustrated.

The main question the author tried to answer was, whether it is possible from a technical point of view to apply an RFI without the target person's knowledge. Thus, it is analyzed whether this method of investigation would work in the field or only on paper. The main argument against the possible implementation is certainly that there is a broad range of different anti-spyware programs capable to prevent spying attacks on computers. Therefore, the second part of this thesis is dedicated to the technical aspects of a remote forensic investigation: It starts with the presentations of software programs potentially capable to be applied in such investigations. The terms of 'malware' and 'viruses' are also clarified, as are the expressions 'spyware' and the various forms of 'Trojan horses'. Special attention is given to the technical issues and properties of telecommunication as well as to that of decryption and encryption.[6] In order to show how a computer has to be searched physically by law enforcement agencies, the author gives a brief introduction into computer forensics. This is especially important as there should be no qualitative difference between an actual physical search and a remote search of a computer. The illustration includes a description of the established procedures for the investigation authorities and the various principles the process is based on. Furthermore, a brief overview of the special hardware as well as software tools is given. Thereafter, a presentation of the potential application of a remote forensic investigation in regards to its two

[6] Note that the awareness of the technical properties and the consequent differences are of great importance when evaluating remote forensic investigations from a legal point of view. In addition, this presentation will give the reader a broader view on the technical properties and permit a sophisticated insight into the whole matter.

main purposes, i.e. obtaining access to a computer and the exploitation of that access. The chapter is finished off with a summary of the findings and the conclusion that can be drawn. Special attention is given to presently available anti-spyware programs and the author presents an answer to the above mentioned, technical question of whether such protective tools are useful against an RFI. In this context, gaining remote access to a target computer is of particular interest and the most pressing question. Is it possible to secretly install and run remote forensic software tools without the knowledge of the user of the target computer?

The second major topic, investigated by the author, deals with a solemnly legal issue: would the conduction of an RFI by the Austrian security agencies be legal under the current law. In order to investigate this issue the author provides the fundamentals, thus with a brief overview on the framework of constitutional provisions at the beginning of chapter 3. In this context, especially the principle of a State of Law in respect to fundamental and human rights, and the corresponding question of proportionality are illustrated. The relationship between the Austrian Federation and the Federal States (Laender) is another aspect presented, as well as the difference between criminal police and public security police. To present the problems without any procedural provision for the security agencies, the author gives a summary of important substantive law provisions. This is necessary in order to show that the security agencies would – without empowerment to conduct a remote forensic investigation – commit a criminal act and would therefore be liable for it as well. In this context, the international framework, i.e. the Convention on Cybercrime is also presented and so is the national provision on computer hacking or illegal interception of data etc.

In a state of law, the security agencies have to follow certain procedures in order for their actions to be considered within their legal limits. This is also true for all measures taken during criminal investigations. Hence, a large portion of the legal part in this thesis is dedicated to procedural provisions in the Austrian legal system. In order to answer the raised question a detailed examination of the provisions in question has to be done. Such provisions can be found in the Austrian Code of Criminal Procedure as well as the Austrian Security Police Act. However, before going any further certain common principles of criminal law have to be illustrated. After an introduction into criminal procedures law, involving an illustration of general principles – such as the principle of indictment, or the system of warrants – the relationship between the criminal police, the public prosecution and the court

as well as their special tasks and competences, the provisions in regard to remote forensic investigations are pointed out extensively. As remote forensic investigations can be conducted for three different purposes,[7] the presentation is oriented towards these purposes. The author examines in the first place the provision of the Austrian Code of Criminal Procedure and thereafter the potentially relevant provisions in the Austrian Security Police Act.

In concrete terms this means that the procedural regulations for a search of locations and objects are displayed. This includes the requirements in regard to the demanded degree of suspicion, and the rights of the people affected by the process. Moreover, the question of what happens to items found but not searched for (accidental discoveries), and the aspects of danger in delay are set out as well.

Second of all, the provisions in respect to surveillance of communication are taken into account and due to their importance a major part of this thesis is dedicated to them. Following an illustration of the formal requirements for surveillance and its general principles, the three main methods are presented. The Austrian Code of Criminal Procedure offers the option of surveillance of data and communication, a disclosure of transmission data, and an optical and acoustical surveillance of persons – also known as major, respectively minor electronic eavesdropping operation.

This presentation is followed by an illustration of the Austrian Security Police Act. After a short introduction, the competences of the security agencies in respect to remote forensic investigations are presented. These competences contain inter alia, the competence to enter and search premises, rooms and vehicles, or the legitimacy to process personal data and other special regulations in respect of investigations. Thus, the competences of the security police appear to be quite similar. However, the major differences between the two will be illustrated.

The subchapters in the third part are concluded by an extensive effort to subsume a remote forensic investigation under the presented procedural provision. Hence, the realization of an RFI with the illustrated procedural provision is examined and therefore the provisions potential capability to ‘host’ an RFI is verified.

Without anticipation, this attempt proved to be more difficult than expected mainly due to the fact that there are only some good starting points. However, in every illustration a component

---

7 Firstly, in order to search remotely a computer; secondly, in order to monitor the activities set out via a computer; and thirdly, in order to monitor telecommunication; cf. below for further details.

is missing in order to achieve a sound and proper outcome – i.e. a clear and distinct subsumption. This means that none of the present provisions provide the necessary legal framework in order to allow the conduction of a remote forensic investigation or alike.

The final question of this thesis deals with the inherent problem of a remote forensic investigation. Besides its pure repressive character, RFIs do have a certain preventative touch. Therefore, the author researched whether and in which form prevention is legally possible, respectively who is responsible for the prevention of incidences and which tools does this agency have to act upon these situations effectively. In this regard it may be noted that the author does not believe that the prevention of a criminal incident can be legally conducted within the framework of the Austrian Code of Criminal Procedure[8]. Hence, in order to find a conclusion to this question, the forth part deals with the delicate relationship between the task of preventing criminal incidences and the competences set out under criminal procedural law. The author presents his doubts of the fact that the prevention is a task of the criminal police by pointing out the difficulties of this special relationship. It will be shown that prevention is a manifold issue and not easy to handle. A simple empowerment of the criminal police with preventive powers does not work and should be subject to closer investigation. Special focus should be on four diverging aspects, which have to be taken into account when establishing a new provision to deal with these special cases.

In the first place the connection and relationship between the principles of the public security police and that of the criminal police, respectively their tasks and competences are examined. Since their functions and duties are only alike on the first sight, serious problems on how to effectively deal with crime prevention arise. It is to show that the responsibilities of the criminal police do have a pure repressive character, while the duties of the public security police are partly preventive.

Secondly, it is pointed out that this provision[9] could possibly constitute a systematic failure within the Austrian legal framework. Due to the fact that the method of a remote forensic investigation is intended to be applied in a repressive as well as in a preventive way constitutional problems occur.

---

8 Note in this respect, that the Austrian legislator intends to establish a corresponding 'RFI provision' within the Austrian Code of Criminal Procedure.

9 Not only this but also some established earlier.

Thirdly, to a certain extent substantive provisions within the Austrian Criminal Code deal with questions of prevention, or involve at least a particular semblance in this regard. The difficulties arising from these provisions are illustrated, raising awareness to them.

The last but probably most important point of critique deals with the issue of general suspicion. It investigates the level of suspicion that is required in order for authorities to conduct a remote forensic investigation. It is commonly agreed that the more serious the crime, the more serious the repression. The same is true for investigations, meaning that the more serious the crime, the more severe (i.e. interfering with fundamental/human rights) the investigation method can be. However, since in certain instance a crime has not even been committed and the 'investigations' are only based on assumptions, the degree of suspicion plays an important role.

These four parts give an extensive overview of the difficulties and controversies remote forensic investigations are facing within the Austrian legal system. Not only is this investigation method highly debatable with regard to human and fundamental rights[11] but there are great concerns in respect to procedural and constitutional principles as well.

The author wants to point out that this thesis does not deal with questions rooted in the area of fundamental rights, but rather with issues of procedural questions. The reason for this is that the topic of fundamental rights is already one of advanced discussion and literature. The contributions of German lawyers have to especially be mentioned in this context. Hence, the author refers the interested reader to further reading materials.

In regard to the technical part of this thesis it is to say that the author intended to provide a broad overview on numerous aspects. Certainly, there are many more interesting facets, which could be elaborated on in the course of this thesis; however, due to the highly technical nature of the topic, the author only illustrates the basic information necessary for comprehensive purposes. Most importantly in this regard is that the author does not claim the completeness of all aspects. The interested reader is once again referred to technical essays dealing with this issue. In addition, it is to mention at this stage that the author tried to obtain information from

[11] The author is aware of the difference between fundamental and human rights. Both expressions are used synonymic throughout the thesis.

the Austrian Ministry of the Interior on how customary searches of electronic devices are conducted and whether there is something like a good handbook for officers. The existence and the use of such guidelines were confirmed by e-mail in August 2009. Unfortunately, these guidelines are only for the internal use, hence not publicly available. However, the author is confident that the ‘good practice guide’ presented in the technical chapter of this thesis gives a good and comprehensive insight on the work of investigating authorities and the corresponding proper principles for conducting a search.

1 General Aspects – Defining the Object of Interest

Before going into further detail, it is mandatory to define some fundamental terms this thesis is dealing with. This is especially true since ambiguous terms are being used. First of all, there is an absence of a universal terminology in this respect, meaning that, in particular the media is mixing and misusing terms and meanings quite often. This has been leading to a lot of confusion. Second of all, techno-legal terms have a high potential to cause even further misunderstandings on both sides – on that of technicians as well as that of lawyers. Thirdly, in general minor but important distinctions have to be made on both, the technical and the legal side. These differentiations imply different outcomes as well as technical and legal consequences.

1.1 Technology and Law

From a technical point of view, there are physical boundaries due to the laws of nature. These borders are final, meaning that you cannot overcome them, just because you want to. If something is physically not possible, then it is not working. With law it is the other way round, however, there are limited boundaries. If we talk about boundaries in a legal context, in most cases, we mean human rights or principles of law binding legislators to a framework of what is possible and what is not.

The relationship between technology and law is an interesting aspect. In general it can be said that technology is always one, if not two or more steps ahead of its corresponding legal regulations. Technical progress is too fast for lawmakers to keep up the pace. A good example for this time lag is the enormous development of the Internet over the last 15 to 20 years, which is still ongoing. It took legislators all over the world quite a while to respond to the things going on the Internet. Even today, with no end of this expansion in sight, lawmakers everywhere are still behind on the concept of what is and will be technically possible. This indicates that legislators are always in a defensive position, as their main agenda is to react to technical phenomena and to implement them into the legal framework. On the other hand, it is to note that not everything that is legal is possible from a technical standpoint.

The intended goal for this brief introduction into the bizarre relationship between law and technology is to raise awareness for the sophisticated relationship, its interactions and the variety of potential outcomes.

1.2 Remote Forensic Investigation (RFI)

In general, this thesis is dealing with three fields of application, which can be subsumed under the umbrella term of remote forensic investigation[s]. RFI is neither in a technological nor in a legal sense a fixed term. There are various expressions used for more or less the same kind of investigation. Hence, there is need for a clarification and a definition of the terminology. The cornerstones of this investigating method for law enforcement agencies can be drawn out of the debate, which has lasted several years in Austria and Germany as follows:

RFI is the employment of technical devices (soft- as well as hardware), which are secretly installed on a certain computer in order to gather knowledge about the content of the hard drive, to monitor sent and received e-mails, or to monitor the page view of certain Internet sites. It is important to note that the user of that specific computer is unaware of the ongoing RFI.[12] During a parliamentary request session, August. Hanning, secretary of State and the coordinator for intelligence services of the German government, defined an RFI as a search for criminal act relevant content data on a data carrier to which there is no physical access for the law enforcement agencies, so that the access has to be established via telecommunication networks.[13] An RFI is a technical means to search and/or survey data carrier for data relevant in criminal proceedings, without the need of physical presence of the investigative officer. With the assistance of technical devices it is possible for the law enforcement agencies to obtain data in a remote way and to use them for their investigations. Furthermore, the investigation is done without the knowledge of the computers user – the potential suspect.

---

12 cf. Vortrag an den Ministerrat der Republik Österreich durch das Bundesministerium für Justiz und das Bundesministerium für Inneres hinsichtlich der Erweiterung des Ermittlungsinstrumentariums zur Bekämpfung schwerer, organisierter und terroristischer Kriminalitätsformen („Online-Durchsuchung'), 17 October, 2007.

13 cf. furthermore BT-Drs. 16/3231, p. 11 at <http://dip21.bundestag.de/dip21/btd/16/032/1603231.pdf> retrieved 21 October, 2009.

1.2.1 Field of Application

Remote forensic devices – be it soft- or hardware – can technically be used in various ways. Generally speaking, three main ways of application have evolved for the law enforcement agencies. Each one of these fields needs certain technological and legal input; thus entailing certain technological and legal consequences. Hence, it is important to keep the differences between the applications in mind when dealing with an RFI. Apart from the similarities of the remote forensic devices, they result in fundamental distinctive legal and technical outcomes if used for different purposes[14]. Law enforcement agencies can use remote forensic devices for:

- remote access to a suspects computer in order to make a search,
- (real time) surveillance of the activities done with a certain computer, or
- (real time) surveillance of the telecommunication done with a certain computer over the Internet

1.2.1.1 Remote Access for Search Purposes[15]

In order for law enforcement agencies to obtain information stored on electronic devices it is legally mandatory to first confiscate the physical device and to search this seized data carrier afterward. This procedure is time consuming and involves numerous people. An RFI would offer a rather uncomplicated way to achieve the same results – a snapshot of the hard drive's content.[16] From a technical point of view, there are two different options to execute an RFI for search purposes: First of all, via the (remote) installation of a Trojan horse it would be possible for the law enforcement to search the suspects hard drive live – thus in real time. A remote access enables the investigating officer to search files, data and information on the computer, as this search would be conducted (physically present) on site. The big advantage of this approach is that a search conducted in such a manner offers access to nearly everything, as the use of encryption software does not matter to such an extent[17].

---

14 There is a difference between a one-time access and surveillance of a computer; not only does this involve different legal precondition but also must there be different technical support.

15 cf. BMJ/BMI (2008), p. 9.

16 e.g., Buermeyer, Ulf, Die „Online-Durchsuchung'. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 4/2007, p. 160.

17 cf. for further details Buermeyer, Technischer Hintergrund, p. 160.

Secondly, a special electronic device could physically be installed on the suspect's computer and this device creates a copy of the hard drive. Afterward, this copy only needs to be transmitted to the law enforcement agencies and finally searched for relevant information.

1.2.1.2 Surveillance of Activities[18]

This field of application means the continued recording of data. Contrary to an image of a hard drive, continued surveillance of the activities is not like a snapshot but rather prolonged information on what happened in the course of time. Each alteration, manipulation etc. of data is recorded, trusting that sooner or later, suspects will use passwords in order to decipher their files. Thus, if this method is conducted long enough, a good copy of the hard drive may be created.[19] Furthermore, monitoring in such fashion enable law enforcement to record files that are stored only temporarily. Concerning this, particularly a temporary storage area – cache – has to be brought up, offering a useful tool to reconstruct online activities.[20]

1.2.1.3 Surveillance of Telecommunication

From a legal perspective, communication over the Internet is in fact a special form of telecommunication.[21] Therefore, it is rather not surprising that the legal regulations concerning the surveillance of customary telecommunication are applicable as well. Examples for telecommunication realized via the Internet can be Internet telephone services, e-mail messages, as well as the participation in instant messaging chats and the participation in online games, inquiries in databases and the customary surfing of the World Wide Web.[22] The provisions of the 'offline' world can be transferred directly into the online world.

From a technical point of view it is to state that there is a huge difference between the surveillance of customary and that of Internet telecommunication. Not only is it necessary to

---

18 cf. BMJ/BMI (2008), p. 9.

19 cf. for further details Buermeyer, Technischer Hintergrund, p. 161.

20 In such areas, abundant data is stored for fast access. If data is stored in the cache, it is faster in the future to use the copy (in the cache) than to recompute the original data; cf. further Buermeyer, Technischer Hintergrund, p. 161.

21 However, there are technical differences which are going to be presented below.

22 Rux, Johannes, Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden, in JZ 6/2007, p. 287.

encrypt communication in the latter case, there is also a special need for law enforcement agencies to have direct access to the terminal of the receiver or sender. This necessity is required due to the technical properties of the Internet and how communication on it works. The interception of Internet telecommunications via the assistance of an access provider is not satisfying. Therefore no method is more suitable than an RFI to intercept Internet phone calls. The goal is to install surveillance devices directly onto the terminals of receiver and/or sender, or to have at least direct access to these terminals. Otherwise the content data of the telecommunication cannot be obtained. From a technical point of view the interception of an Internet telecommunication is a more powerful interference than a simple analogue or 'offline' interception.

In short, the surveillance of telecommunication over a longer period of time enables the collection of data on conducted information flow. This can be far more relevant, comprehensive, and valuable that a simple 'snapshot' of data.

1.2.2 Timeframe of Application

There are two questions in regards to RFI and a timeframe. One is how many times an RFI is conducted, the other is when: This will consequently also answer the question of when the law enforcement agencies will start their investigation. The exact point of time, i.e. at which stage of a criminal activity, when law enforcement agencies start their activities implies not only the question of the legal basis of their acting[23] but also it involves the very interesting field of the different grounds of justification.[24] There are three different kinds of investigations distinguished by their launching time. Generally, the RFI techniques can be applied before, while or after a criminal act was committed.[25]

---

[23] e.g., can the single act be classified as prevention of a criminal act or is it already an investigation, etc? The former would be governed in Austria by the Security Police Act (Sicherheitspolizeigesetz) and by section 3 of the Austrian Criminal Code (self-defense) while the latter is regulated by the Austrian Criminal Procedure Code. For further clarification cf. the legal section of this thesis.

[24] cf. previous footnote.

[25] cf. regarding the distinction: Rux, p. 287.

1.2.2.1 Preliminary Stage of a Criminal Act

The averting of danger prior to the actual criminal act[26] is one of the most important tasks of security agencies. The prevention of criminal acts is always better than solving them because nobody was harmed and there are no actual damages. Hence, prevention in general occupies a crucial part in the daily work of the police forces. Furthermore, it is to state that there is hardly a strategic concept leaving questions of crime prevention aside.[27] In fact, an RFI is (according to its proponents) all about prevention, as it is intended to become the most vital part in the prevention of serious, organized or terrorist crimes.[28] Hence, at this stage an RFI supports crime prevention.

1.2.2.2 Averting of Danger[29]

At this stage, the actual offender has already started to commit a criminal act, meaning that the physical elements of a crime have been put in place. The law-breaking act is in progress by the time a law enforcement agency starts an RFI. Logically, an RFI at this stage can only be conducted if it continues and lasts at least for some time. Therefore, only criminal acts lasting for some time or constant/continued activities representing a criminal act[30] can be investigated via an RFI. Otherwise, if the criminal act is completed, there is no need for the averting of danger, as the danger is already gone. At this stage, an RFI helps to overcome or lessen the amount of danger in case of an attack.

1.2.2.3 Post-crime Investigation

When the actual threat is over, the criminal act committed and the law enforcement agency commences its investigation, the purpose of RFI changed once again. There is nothing to prevent or lessen anymore; from this point of time onward, an investigation is purely dedicated to the prosecution of an offender. After a criminal act is committed, collecting

---

26 Thus, when the actual criminal act has not yet happen and the offender is still in the process of preparation.

27 cf. homepage of the Austrian Federal Ministry for Internal Affairs at <http://www.bmi.gv.at/cms/BK/praevention_neu/wir_ueber_uns.aspx> retrieved 22 October, 2009.

28 cf. the titel of BMJ/BMI (2008).

29 Note that this is not a legal expression and therefore 'nothing' to do with the task of the public security police.

30 e.g. an offender persevered in committing the criminal act.

evidence and tracking the criminal is the main goal of an RFI.

2 Technical Aspects of RFI

Having clarified the relationship between technology on the one, and law on the other hand as well as having defined the object of interest and all its aspects, the next chapter deals with the technical aspects of RFI. Software and hardware tools are illustrated as well as a description of potential methods to conduct an RFI is given. The chapter is concluded by a brief presentation of the potential application of an RFI in regard to its main purposes, namely access obtaining and exploiting such.

2.1 Malware

2.1.1 Introduction

The term malware is a combination of the words malicious and software. It is used for software designed to infiltrate or harm computer systems. Malicious software can be divided into subgroups and is distinguished by its aims and goals as well as by its technical functions/abilities. Therefore, a distinction is made between Trojan horses, worms and computer viruses[31]. These three main subgroups are often not distinguished explicitly but rather used incorrectly in public discussion and by the press. For example, the term computer virus is commonly brought into play for all sorts of different malware without acknowledging that there are differences and that not all malicious software programs are viruses. Furthermore, it is to mention that adware, root kits and spyware as well as the various tools of hackers[32] can also be subsumed under the term malware. Hence, malware is the general expression for harmful computer software. Another phrase utilized in this context is ‘rouge program’ which is, in general, the same as malware.

Although this thesis is mainly focused on Trojan horses and similar programs, which offer the ability to spy (spyware) on a target computer system as their main focus, it is the intention of the author to give a brief overview on the other groups of malware. This information is

---

31 Klaeren Herbert, Viren, Würmer und Trojaner (2006), pp. 102-103.

32 There are three different ways to comprehend the term hacker, with slightly different meanings in nearly the same circumstances. In this context I will use the expression hacker in the sense of a person who is using programs to enter a computer system with the intention to commit a crime of whatever substance (illegal access, theft, fraud, data or system interference etc).

essential for the reader's comprehension and his/her better understanding of the bigger picture.

In general, there are minor differences between all these computer programs, tools and electronic devices. Each of them can obey different orders. Furthermore, various mixtures and hybrids have been designed over time in order to cause greater damage or to guarantee better surveillance. Having said this, it is to be noted that the following overview shall not be regarded as a final, everlasting list of devices. It is rather intended as presentation of not only the tools themselves but also the basic technical concepts, ideas and purposes behind their invention.

2.1.1.1 Intentions Behind Malware

The intentions behind the invention of malicious software vary based on the ideas of their creators. There were also shifts in the course of time: at the beginning of the development there were two main reasons coining the creation of malware, i.e. on the one hand, the purposes for programs, nowadays seen as rouge ones, were mainly harmless experiments. For instance, the first official[33] Internet worm – the Morris worm[34] – was intended to gauge the size of the Internet. On the other hand, these programs were meant as pranks, people trying to annoy colleagues without any bad intentions – such as causing serious damage to computers. The early viruses were the product of 'virologists', computer scientist who studied these new extraordinary phenomena. They tried to learn by programming viruses, thus learning by doing. As it is commonly known, however, everything has a backside and as it can easily be imagined the difference between a beneficial, purely scientific approach of the matter and an unlawful, i.e. criminal handling is minimal. The distinction lays only in the intention of the user/creator. Somehow, it is like a customary kitchen knife, which can be used in two ways – to chop vegetable, or to harm or even murder somebody. Thus, it is really not surprising that more and more criminals were attracted by the discoveries in the field of malware and that even well minded scientists changed the side of the law.

---

33 Or better the first one, which got broad media attention.

34 It infected 6.000 computer systems in the U.S. (mass infection) – at that time approximate 10 per cent of all servers of the ARPANET-network, which was the predecessor of the today Internet. One of its victims was the server of the NASA. cf. further Robens Daniel, Internet-Spionage – der Sicherheitsratgeber für Ihren PC (2000), p. 26 and Kaspersky Eugene, Malware (2008), p. 108.

2.1.1.2 Changing the Side

When it comes to the intention of a suspect we are dealing with delicate situations. What matters is the intention behind an act. If a person engages in an activity that could be of illegal nature, but his/her actions as such are permitted by law, the person cannot be held accountable for them.[35] Hence, it is important to note in this context that the change of affiliation is working in both directions. From the early days, hackers saw the whole matter of malware as playing a game. They were searching for gaps in the security systems of networks or single computers with the intention to overcome the hurdles, to hack into the system and to show that the programmer had failed to protect it efficiently. This was mainly the intention of early hackers. These goals have hardly changed in recent years and there are still enthusiasts playing this kind of game. The fact that hacking is not necessarily a harmful act but rather one with beneficial consequences, led to controversial discussions regarding the treatment of hackers. As history shows, hackers often changed sides after becoming convicted of computer crimes. Big corporations or even public entities were, and are still looking for these criminals in order to hire them. The main reason is that these criminals have gathered so much knowledge and experiences of networks, their security, potential gaps and weaknesses that they are the ideal partners to assist in improving these systems. Other hackers came out of illegality to sell their know-how to major companies such as Microsoft. They founded their own companies and sell their anti-virus programs.[36] It is further not surprising that the evolution and expansion of the anti-virus industry went along with the increasing number of appearing malware.

2.1.2 Computer Virus

A virus (the expression steams from Latin and means ‘poison’ or ‘toxin’) in the biological context is not a living organism - it is more a collection of genetic material. This material is

---

35 cf. as well the conclusions of this chapter and Posch, Reinhard, 'Technische Aspekte zur Online-Durchsuchung ' in Online-Durchsuchung (2008), p. 40

36 A good example is the creator of the Morris worm, Robert T. Morris Jr. - ironically enough son of a chief executive of the National Security Agency (NSA). His worm, reasoned by an error in programming, caused damages of approximately 10 – 100 million US Dollar. He was sentenced to three years imprisonment on parole, 400 hours of charitable activity as well as a 10.000 US Dollar fine. He co-founded Viaweb, an e-commerce hosting service, which was later sold to Yahoo and he became an associated professor at Massachusetts Institute of Technology; cf. further Klaeren, pp. 100-101; Robens (2000), p. 34; moreover Robert Morris biography at <http://pdos.csail.mit.edu/~rtm/> retrieved 14 May, 2008

capable of infiltrating into cells, modify their DNA and alter these cells into virus producing ones. Hence, a virus is not able to reproduce itself outside a host cell. In the context of computers, this means that viruses are programs which copy themselves in the form of Trojan horses[37] into other programs in order to alter the function of these programs. Then they use these infiltrated programs as newly created virus distributing engines. The original function of the now infiltrated programs (the new distributing programs) rests unchanged.

Gregory Benford mentioned computer viruses for the first time in 1970. In an article he warned that such viruses would be established soon and he recommended the invention of a vaccine. Furthermore, he designed some viruses himself in order to support his theory. His viruses were only intended to spread around but not to cause damage to the infected computer.[38]

Generally, it is to say that a modern virus has at least two different functions: firstly, a reproducing function afflicting other programs and integrating itself as Trojan horse. Secondly, there is the harmful purpose, which could be activated immediately. In most cases the latter function will not be exercised until a certain event or date. Sometimes viruses are programmed to wait for a remote order. Originally, viruses only spread via the exchange of discs and other external data carrier but nowadays viruses circulate mainly through the Internet, which offers a brilliant breeding ground.[39] Computer viruses have three different life phases: activation, reproduction and manipulation. Activation is the moment when the virus logs into a computer for the first time – mostly via a common source. Reproduction is the phase where the virus is trying to infect as many victims as possible. The moment a virus enters into force is called manipulation. This enforcement depends on the programmer's intention and can be connected to a certain date or another incident.[40]

2.1.2.1 Classical vs. Contemporary Viruses

In a recent study, Eugene Kaspersky pointed out that, as a distinguishing character between

---

37 cf. below.
38 cf. Klaeren (2006), p. 104.
39 cf. Klaeren (2006), p. 104.
40 Chirillo John, Der Hacker-Angriff (2004), p. 315.

other forms of malware – especially worms – classical viruses[41] do not use network services to get into computers. The reproduction of a virus attains only in other computers if the infected object (i.e. another program) is activated, for reasons not in conjunction with the function of the virus. Kaspersky provides the following examples: a user who is sending e-mail with an infected attachment; the case of a virus copying itself on removable media or on infecting files on such media.[42] Furthermore, he shows that new viruses have properties of other kinds of malware, as for instance, viruses containing components of Trojan horses in order to harm or damage computers. The development from the classical viruses (which do not need the resources of networks) to the modern day viruses (the combinations between more types of malware) is based on various reasons. One of them is that the development of rouge programs became more and more inspired by criminal intentions. A growing number of criminals are seeking easier and more efficient means for their unlawful purposes in cyberspace.[43] Nevertheless, the methods by which viruses infect files are still applied. Especially within contemporary worms and Trojan horses which were programmed for criminal purposes. Present day worms and Trojans horses are designed to harm the computer through the infection of files of the operation system (e.g. Windows) in order to aggravate the detection of the malware and its removal from the system.[44]

2.1.2.2 Classification of Viruses

Traditional viruses can be classified by two characteristics: the environment where they occur and the method of infection.

The former refers to the make-up of a computer, such as the operation system or application, required in order to infect files.[45] In this context four kinds of viruses,[46] can be differentiated,

---

41 e.g. the Michelangelo-virus, which spread only via disk. Detailed information can be found at Robens (2000), pp. 43 and 282-284.

42 Kaspersky (2008), p. 51.

43 This is a metaphor for the Internet. The term itself is a combination of the words cybernetics and space, and was coined by William Gibson in his scientific novel ‘Burning Chrome’ (1982).

44 Kaspersky (2008), pp. 51-52.

45 cf. <http://www.viruslist.com/en/virusesdescribed?chapter=152540474> retrieved 15 May, 2008.

46 cf. Kaspersky (2008), pp. 56-57; for further detailed information cf. http://www.kaspersky.com/virusinfo> retrieved 15 May, 2008.

namely

- file viruses – occurring in file systems
- boot sector viruses – occurring in boot sectors[47]
- macro viruses – occurring in macro environments[48] and
- script viruses – occurring in script hosts.

The latter criterion classifies the different forms of viruses by the employed tricks and used techniques to infiltrate a target and inject the virus code into an object.[49] Hence, the above shown types can be further divided.

The most significant types are file viruses. They have been used for over 20 years in order to comprehend the technology behind viruses. Due to this popularity, hackers and other programmers of viruses invented ever more-newer methods. Hence, today there is a very broad scope of different levels of viruses. They reach from simple and even primitive ones to technical highly developed approaches, able to infect the source codes. Seven types and targets of viruses can be distinguished:[50]

- Overwriting virus – it is the simplest form of infection and means that the virus replaces the code of the file by his own code. The original file is useless and it is not possible to restore it.
- Parasitic virus – it is the most widespread category of all file viruses. They alter the code of the infected file. This modification can influence the functionality of the host file. Within this group there are four further sub-categories, namely perpending[51],

---

47 As their name let one divine these viruses infect the boot sectors of media such as floppy disks of hard disks (Master Boot Record – MBR) and further Kaspersky (2008), p. 61 and <http://www.viruslist.com/en/virusesdescribed?chapter=152540474> retrieved 15 May, 2008.

48 The most widespread macro viruses are for Microsoft Office applications (Word, Excel and PowerPoint) which save information on OLE2 (Object Linking and Embedding) format. Viruses for other applications are relatively rare. cf. Kaspersky (2008), p. 62 and <http://www.viruslist.com/en/virusesdescribed?chapter=152540474> retrieved 15 May, 2008.

49 cf. <http://www.viruslist.com/en/virusesdescribed?chapter=152540474> retrieved 15 May, 2008.

50 cf. Kaspersky (2008), pp. 58-61 and <http://www.viruslist.com/en/virusesdescribed?chapter=152540474> retrieved 15 May, 2008.

51 Meaning the malicious code is written to the beginning of the file. This is the easiest method because the virus is shifting the whole content of the file backwards and inserts his own code at the created space. cf. as well Kaspersky (2008), p. 59 and <http://www.viruslist.com/en/virusesdescribed?chapter=152540474> retrieved 15 May, 2008.

appending,[52] inserting,[53]and entry point obscuring (EPO) viruses.[54]

- Companion virus – this category does not alter the code of the file. It is just duplicating the infected file, which contains its own code. Launching the file will open the duplicate file containing the virus.
- Link viruses
- Object modules (OBJ)
- Compiling libraries (LIB)
- Application source code

The harmful results of viruses on computers and networks can vary immensely. They range from a slight, not even noticeable, higher volume of sent data,[55] to a total breakdown of the whole system, or a complete loss of data. Furthermore, viruses can result in simple data-theft or even identity-theft. Thus, the (monetary) measurable extend of damage goes along with the intention of the malware programmer. In addition, it can be said that quite often the effects of the viruses are not even noticed by the actual user of the infected computer. Hence, it is somehow always a matter of luck to detect injures.[56]

2.1.3 Worms

In the contemporary western world, everybody has come across the term ‘computer worm’. The main distinguishing criterion among the different types of worms lays in their method of spreading, meaning the manner of how worms copy themselves onto other computers. Worms can be diverted by the technique used to infiltrate a system and how computers execute their

---

52 Meaning the malicious code is written to the end of the file. Most of the viruses fall under this category. cf. further Kaspersky (2008), p. 59 and <http://www.viruslist.com/en/virusesdescribed?chapter=152540474> retrieved 15 May, 2008.

53 Meaning the malicious code is inserted in the middle of the file. cf. further Kaspersky (2008), p. 59 and <http://www.viruslist.com/en/virusesdescribed?chapter=152540474> retrieved 15 May, 2008.

54 These include both appending and inserting viruses and are highly complex. Further information can be found at Kaspersky (2008), pp. 59-60 and <http://www.viruslist.com/en/virusesdescribed?chapter=152540474> retrieved 15 May, 2008.

55 e.g., if a Trojan horse uses the infected computer to send spam; cf. Kaspersky (2008), p. 43.

56 cf. Kaspersky (2008), p. 43. For further detailed information cf. ibid pp. 43-47.

copies. Moreover, other features also found in other groups of malware, can be used for distinction purposes.[57]

The most commonly known category of worms is the e-mail worm. Quite surprisingly, this kind is spreading by electronic mail. The worm is sending a copy of itself as attachment, respectively the sent message includes a link to a specially prepared website. The worm is activated, in the first case when the user tries to open the attached (and infected) file or as it is with the second case, when the file is downloaded from the contagious website, i.e. when the user clicks the provided link. In both cases, the e-mail itself is only the transmitting medium. Well-recognized e-mail worms were for instance the Melissa[58] or the LoveLetter worm.

Worms in instant messengers such as ICQ or MSN spread through the use of these vehicles. They are sending messages with links to infected websites to everybody on the local contact list. Thus, only the broadcasting means diverts this method from the e-mail approach. Similar to this strategy, worms spread out through Internet relay chats as well.[59]

Other distributional techniques for worms are

- to copy it on networked resources,
- to exploit operating system vulnerabilities to penetrate computers and/or networks,
- to penetrate public networks or
- the use of other malware to act as a carrier for the worm.[60]

These manners of spreading can stand-alone, but in many cases copies of worms distribute simultaneously in different ways throughout networks, as the worm Nimda showed in 2001.[61] Furthermore, it has to be mentioned that worms use also file-sharing networks. In order to

---

57 cf. Kaspersky (2008), p. 53.

58 In 1999 this worm e-mailed copies of itself to the first 50 people in a victims Outlook address book and caused in this way massive break- and shutdowns of e-mail networks, even that of Microsoft. Through its practice it caused $ 80 billion on damages; cf. further <http://articles.winferno.com/antivirus/computer-worms/> retrieved 19 May, 2008.

59 cf. further Kaspersy (2008), p. 54.

60 cf. Kaspersky (2008), p. 54 and <http://www.viruslist.com/en/virusesdescribed?chapter=152540408> retrieved 19 May, 2008.

61 The Nimda worm – backward spelled Admin – was so effective because it used three different ways to infect other computers: i.e. it spread via e-mail, it copied itself on open network shares and it used as well compromised web sites; cf. Kaspersky (2008), p. 55.

spread, the worm places a copy of itself – usually under a different, unsuspecting name – into a shared folder. Due to the technique used by peer-to-peer networks (P2P) other users gain knowledge that a new file is available and they are able to download it directly from a user's computer. Hence the P2P client as external service provider grants the distribution resource.[62]

2.1.4 Spyware

Spyware is a specific subgroup of malware.[63] It includes several more or less different tools and techniques, which enable to 'spy' on a target person. These applications are dedicated to the gathering of information of people's electronic data, their electronic communication or their habits using electronic devices. While the original intentions for the invention of most of these tools were focused on well-meant goals,[64] the image of these tools has altered in the course of time. This was mainly due to their changed use, particularly their employment for negative and even criminal purposes. Hence, the various, once praised items became the condemned ones. This is also expressed in a verbal way – the branding as spyware; although one still profits from their positive outcomes.

Spyware can be either soft- or hardware and accomplish quite different tasks. The effects of the various tools reach from key logging devices, noticing and storing every pushed button on a keyboard, to the installation of 'backdoors', which enable hackers to enter as system undiscovered. Another example is the screening of people's surfing habits for the purpose of direct advertising. However, the last mentioned scenario could potentially reach a point at which identity thefts become possible. This means that the criminal gathered so much information about a person that the data can be used to 'live that person's life': for instance to get a second mortgage on the victims house, pay with their credit card or even sell the victim's house. Identity thefts are mainly the outcome of the accumulated usage of different spyware programs and are highly dangerous for the victims as they could lose everything.

---

62 cf. Kaspersky (2008), p. 56.

63 As Kaspersky points it out, spying programs are already included in the category of adverse, unwanted and potential dangerous software (i.e. malware) and the term has not a autonomous, technical meaning rather than it is a marketing expression; cf. Kapersky (2008), p. 75.

64 e.g., there was the intention to enhance security, especially data security through storing all processes and inputs. Further it is to note that these tools were applied as well for educational reasons, such as to figure out how users work with their computers and to show them afterwards in which way they could improve the application of the device.

Usually, a computer, when bought is not infected with spyware. Thus, these programs have to be installed afterward. This is mainly done by users – the victims - themselves. In most cases spyware comes as a Trojan horse along with unsuspecting software downloadable for free via the internet, but it can also be included in image files on a website. Barely recognizable, the application runs in the background and reports the demanded information to the creator of the program. As mentioned earlier, the potential application of spyware is quite broad. Hence, the functions of the different tools divert among each other as well as the grade of intrusion ranges from low to high.

2.1.4.1 Trojan Horses

The right term for these tools is Trojan horses and not just simply Trojans as suggested. The short form is not only incorrect, but was also chosen ambiguously: In the Greek mythology the city of Troy was besieged by the Greeks during the Trojan War. During this event the Greeks only conquered the town of Troy through a trick. They bluffed the Trojans (inhabitants of Troy) with a present – a giant wooden horse. The Greeks left this horse in front of the city gate and pretended to leave. As the Trojans believed that they had won the war, they brought this horse behind the city walls into their town and celebrated their victory, unaware that the mightiest of the Greek soldiers were hidden within the horse. For those soldiers it was very easy – especially because of the celebrations – to leave their concealment, overrun the guards and open the city gates for their fellow soldiers.[65] This clearly indicated that the Trojans were the victims rather than the method. Hence, the only right expression for this kind of spyware is Trojan horse because it is the means, which cheats and smuggles the ‘enemy’ into ones computer.

Trojan horses are nowadays one of the most widespread and dangerous group of malware. They contain programs, which perform various functions in secret, such as deleting or altering of data, the damage of the computer’s functions or the abuse of computer recourses for criminal purposes.[66] As it is in general with all malware, it is also possible to divide Trojan horses into several subgroups. The main distinctive criterion for categorization is the

---

65 cf. Robens (2000), p. 293.
66 Kaspersky (2008), p. 52.

intentions behind the Trojan horse program, i.e. a distinction by their behavior and functions they execute on an infected workstation. For instance, there are several applications of Trojan horses, which cause damage to remote-computers, or within networks without harming the performance and functionality of the infected computer. This kind of Trojan horses is used for compact attacks on other computers, or designed especially for sending Spam. Briefly, there are the following kinds of Trojan horses:

2.1.4.1.1 Backdoors

Backdoors work similar to customary, lawful programs used for the remote management of a computer in a network, also known as system administration. Via remote management programs, the system administrator of a network is able to maintain all computers of the network from a distance, This means that the authorized persons are not forced to leave their workstation in order to maintain another workstation – system administrators have direct but remote access via their own computer. Hence it is possible to monitor every action taken on a computer respective to perform every function[67] of the victim computer remotely and secretly. Attackers of a computer system establish such backdoors in order to return later to collect the gathered data of an earlier installed sniffing program. Due to the fact that hackers are concerned that 'their' backdoor will be discovered and closed, they often create a further backdoor, either via a secret server process or an additional administrator account on the target computer.[68] The difference between a legal and illegal use is simple the lacking knowledge and/or consent of the affected person about the installation. In order to find activated backdoor programs, it is advisable to have a look on the list of open network ports.[69]

2.1.4.1.2 Trojan PSW

PSW stands for 'Password Stealing Ware' and includes Trojan horses, which are designed to

---

[67] e.g. a criminal can use the victim computer to send or receive, to open, delete or execute files, to display notification, to delete information stored on the computer or simply to reboot the computer etc. Backdoors combine the functionality of most other types of Trojan horses in one package and this fact makes them for one thing so powerful and for another thing so dangerous. cf. further Kaspersky (2008), pp. 63-64 and <http://www.viruslist.com/en/virusesdescribed?chapter=152540521> retrieved 20 May, 2008.

[68] cf. Geschonneck, Alexander, Computer Forensik – Systemeinbrüche erkennen, ermitteln, aufklären (2006), 2nd edition, pp. 27-28.

[69] cf. Geschonneck (2006), p. 77.

‘steal’ various information of a target computer, especially system passwords. The Trojan horse – or sniffer as it is further called – is programmed to monitor and protocol the whole traffic of a network and to search for files containing secret information such as phone or PIN numbers[70] and send this data to an e-mail address.

2.1.4.1.3 Trojan Clickers

A Trojan clicker is used to promote certain websites; i.e. this subgroup forwards the victims computer to certain websites. They are doing so by sending either the needed command to the Internet browser or by replacing the standard Internet URLs.[71] The goals behind these actions are to increase the hit-count, thus for pure advertising purposes, to organize Denial of Service attacks[72] or to spread viruses and Trojan horses.[73]

2.1.4.1.4 Trojan Downloaders

Trojan Downloaders are something like an ‘update service’ for malware. They are downloading new versions of malicious software and installing them unnoticed by the computer user.

2.1.4.1.5 Trojan Droppers

Trojan Droppers are employed for the covert installation of other malware. They transfer the

---

70 Further potential targeted types of information can be certain details of the computer system (memory, disc space or operating system details), IP-address or passwords for online games. cf. Kaspersky (2008), p. 64 and <http://www.viruslist.com/en/virusesdescribed?chapter=152540521> retrieved 20 May, 2008.

71 The website to which one is directed when one opens his/her browser.

72 Denial of Service (DoS) attacks are intended to arrange an ‘overheating’ of a server. Hence, if there are too many clicks on a website within a short time, it can happen that a host server will not able (technically) to provide this source any longer and it might crash and have a breakdown. Such a breakdown can cause serious damages to the company providing the web service because it cannot offer its service any longer. e.g. imagine such an attack on Amazon.com, if its server will break down, it might not be online for a couple of hours or even a day … the loses (the potential profits gathered, if it would have been online) might be quite serious. Moreover Distributed Denial of Service (DDoS) Trojan horses are spread around and infect numerous computers. As they are designed to visit a certain website at a specific time (or on command of the ‘master’), they are used for blackmail. Regarding this cf. especially Kaspersky (2008), p. 65.

73 As mentioned above under worms.

newly downloaded applications to a special location on a computer where these will be launched. Trojan Droppers can act covertly, i.e. without notification of the download or they can use deception for the installation. The latter means that they portray fake messages, such as errors etc. Usually, this kind of Trojan horses contains, next to the malicious, of at least one element that appears to be useful (a picture, a joke or a game) and which is intended to distract the attention of the user. The aim of this element is only to cover the ongoing process of installation. Besides the purpose of a hidden installation of other malware, Trojan Droppers are also intended to mislead antivirus programs, which are technically incapable to investigate all elements and to find the malicious code within the Trojan Dropper.[74]

2.1.4.1.6 Trojan Notifiers

The simple purpose of Trojan Notifiers is to confirm a successful infection of a victim's engine. They send a message to their 'master' and include regularly information about IP-addresses or open port numbers. Generally, Trojan notifiers are included into a complete Trojan horse package and do not stand alone, since this would not make any sense.

2.1.4.1.7 Trojan Proxies

The intention of Trojan proxies is to achieve secret access to Internet services. Trojan proxies serve as a proxy server. These programs are especially used for mass e-mailing, thus for spamming.

2.1.4.1.8 Root kits

The expression 'root kit' originates from the Unix[75] world in which the term root means the same as the term administrator in the Microsoft world. If somebody logs on as an administrator, a root, they have special power over a computer. It is possible for these certain

---

74 cf. Kaspersky (2008), p. 66.

75 Unix is a computer operating system (OS), hence the software section of a computer system in charge for the coordination and management of all activities of the computer. Another OS would be e.g. Microsoft Windows or Mac OS X.

‘users’ to change the various settings of a computer, to add or delete users and to govern their sphere of action, where each user can store their files and so on. A root is a certain empowered ‘user’ of a computer whose function is to manage it.

Root kits are in general words, a compilation of programs employed by a hacker to evade discovery while the criminals are seeking access to the remote computer. Usually a hacker installs the root kit after customary user-level access is obtained. In most cases cracking passwords or taking advantages of other weaknesses of the computer enables this access. Once the status of a regular user-level is achieved, it will be used to collect further user IDs of the workstation and finally access as root, respective administrator to the system.[76]

2.1.4.1.9 ArcBombs

ArcBombs are Trojan horses that are designed to sabotage the decompressor as well as the virus-scan programs. The ArcBombs themselves are archived files and if they are clicked on in order to open them, a computer might crash or slows down its processing speed. A further great danger stems from ArcBombs intended to influence file or e-mail server, especially if these servers use a system of automatic manipulation of incoming information. This is especially dangerous because these Trojan horses can easily bring servers to a 'thrashing', i.e. the server crashes.

There are three different types of ArcBombs: the incorrect header in the archive, the repeating data and a series of identical files in the archive.[77]

2.1.4.1.10 Trojan Spies

The most dangerous subgroup of the Trojan Horse is that of Trojan Spies. This group includes programs, which gather secret data, monitor every act of a user, assemble these actions and transfer the information to an unauthorized user. The range of data collected reaches from secret banking data, such as the access code to an account, over the listing of the visited websites to the control of the keyboard and which keys have been pressed, as well as simple

---

76 cf. further Kaspersky (2008), pp. 68-69.

77 cf. Kaspersky (2008), p. 69 and <http://www.viruslist.com/en/virusesdescribed?chapter=152540521> retrieved 9 June, 2008.

screen shots, logs of active applications or other user actions.[78] Trojan spies include a wide variety of spy programs created to track and save all activities of a computer user.

The intentions behind this are, for instance that it is necessary for direct advertising to know the surfing customs of the user. Thus, these programs are designed to collect, store and transmit information about the visited websites. This is already invasive but not as intrusive as the gathering and transfer of passwords by a key logging device.

To sum up, it can be said that Trojan horses, can be grouped according to the activities they exercise on the infected computer. Furthermore, these groups can be divided into further subgroups based on the seriousness of the damage they are inflicting. The harmfulness of Trojan Clickers, Downloaders, Droppers, Proxies and Notifiers is not that serious, since they not only support other malware but often carry out additional, more positive, functions[79]. The other programs mentioned above, on the other hand, have the potential to influence not only the computer as a machine but also the personal life of the user in a far more drastic way. Root kits, Backdoors, PSW Trojans, and especially Trojan Spies and ArcBombs can have far reaching consequences to the single user and its computer. They can cause great harm and damage to computers as they might be designed to destroy or alter all data. Apart from this surely unwelcome effect, which can end in massive financial loss, they have further the capability to ‘erase’ the existence of the user or at least their basis of life. With the help of sniffing and spying programs, criminals may obtain a huge amount of data, enabling them to become a great threat to people’s lives – the criminal is not only able to steal the victim’s money but also his identity.

2.1.4.2 Keyloggers

As previously mentioned, another possibility for hackers to spy on somebody is the usage of so-called key loggers. The term itself is neutral and describes simply the main function of the device’s respective program. Basically one is assuming a software tool, which was created to covertly observe as well as record all strokes on a keyboard done by the user of the computer. Although the vast majority of key loggers is software, some of them come in the form of a

---

78 cf. <http://www.viruslist.com/en/virusesdescribed?chapter=152540521> retrieved 9 June, 2008.

79 As giving notice to the master that a computer was infected; cf. above at Trojan Notifiers.

physical apparatus. This fact needs to be taken into consideration because the two different tools can cause distinctive consequences. Another important fact in this context is that unlike most other malware, key loggers do not harm the computer system itself. Its only goal is to spy on the user which makes the threat different but not less dangerous.

Once again, the discrepancy between a positive and a negative key logger lays in the intention of the user. Similar to other malware, the creators of early key loggers had nothing criminal in mind. On the contrary, their goal was to enhance security, especially data security, by storing all inputs made by the user, or they were driven by educational purposes. In the latter case, the instructor – by a look into the key logging transcript – was enabled, on one hand, to figure out what went wrong[80] and on the other hand to help the user to correct his errors. Hence, the instructor can reproduce all the user's operations and can present solutions for a better use and thereby enhance productivity. The good intentions, however, did not hinder criminals to use these freely available programs and devices in a law-breaking manner – as for instance, in order to steal passwords. Nevertheless once again, there is a very fine line between the positive and negative usage of key loggers.

Legal soft- as well as hardware sold via the Internet or in customary stores is often advertised as a legitimate tool to investigate computer history, justifying that parents should be allowed to get knowledge about the online or simple computer habits of their children. Furthermore, network and especially company security are catchwords for vendors as it is possible to monitor the habits of the company's employees. This can be seen as having the necessary control over one's own resources such as the company laptop or computer network. Hence, the employer is able to see and control whether their employees behave in accordance with their employment contract. Another advertising trick for key logger promotion targets jealous and or mistrusting people telling them that it is possible to track their potentially cheating partner. This instance is legally a bit trickier and might be located already in a juristic gray area. These examples show that it is not so easy to solve the problem of key loggers and one must always – as it is in the field of legal studies – take the purpose and intention of the performer into account. It can be pointed out, however, that nowadays, key loggers are primarily applied with fraudulent, i.e. criminal intentions and that the broad majority of newly

[80] e.g. whether it was a handling error caused by incorrect use or an error of the applied program itself.

created key loggers are written for these very purposes only[81].

As mentioned earlier and as the name key logger lets one assume, their applications are used for monitoring keystrokes and sending the gathered information to the creator of the malware. In general there are a several different types of key loggers:

Firstly, key loggers on a target data processor are software programs and designed to operate on the targeted computer. These key loggers can be 'kernel'[82] or 'hook'[83] based. Secondly, there are hardware key loggers, which are small inline[84] devices. These apparatuses are regularly placed somewhere in between the computer and the computer keyboard. Due to their size it is really hard to find them and often they stay undetected for long periods of time. Hardware key loggers' advantage over a software one is that the hardware device is independent of the computers operating system. This means that it is not impairing other programs running on the computer. Thirdly, there are wireless key logger sniffers, which are created to gather transmitted information between a wireless input device and its receiver. The last group of key loggers is acoustic key loggers. They operate on a sound analyzing basis.

Similar to other malicious programs, key loggers can be spread through different methods. For instance, they can be installed on a target computer when the user opens a file recently received via e-mail. Furthermore, the same can happen when the user is launching a file directly from an open-access directory on a P2P[85] network. Another possibility for the secret installation of a key logger is if a web page script utilizes the weakness of a browser. In this case the key logger itself will be launched when a certain, infected website will be visited. Another possibility is that other installed malware is installing key loggers, if it was designed to do so.[86] In this context it is crucial to mention that a lot of key loggers include the function of a root kit as well, empowering them to hide themselves and letting them become a Trojan horse program.[87]

---

81 cf. as well the section above about Trojan Spies, which track user activity, save the information to the user's hard disk and then forward it to the author or 'master' of the Trojan

82 These key loggers are located at the kernel level, hence practically invisible. If such a type is used, the key logger can function e.g. like a keyboard driver and thus gather all information which was type on the keyboard; cf. further <http://www.securityfocus.com/infocus/1829> retrieved 11 June, 2008.

83 These kind hook the keyboard with aid of the operating system; cf. further <http://www.securityfocus.com/infocus/1829> retrieved 11 June, 2008.

84 cf. at <http://www.securityfocus.com/infocus/1829> retrieved 11 June, 2008.

85 Peer to Peer is a special kind of network, mostly these networks are just ad hoc.

86 cf. above Trojan downloaders.

87 cf. <http://www.viruslist.com/en/analysis?pubid=204791931> retrieved 10 June, 2008.

2.1.4.3 Computer Protection Software

The technical properties of programs designed to prevent spying attacks, also known as anti-spyware tools are of crucial importance in this context. Currently available programs are largely capable of detecting malicious software while the infected data is accessed (on-access-scan). These same programs can also search for infected files stored on a computer while they are not being accessed. In order to become aware of infected files, anti-spyware programs use a variety of different strategies.

On the one hand, anti-spyware programs rely on the signatures of a file which describes its function and type. Therefore it covers the name of the function, its parameters as well as the type of the file.[88] Signatures can be seen as the fingerprints of files. Due to the fact that signatures also identify the functions of Trojan Horses etc, anti-spyware program are capable to find these files and notify the user of the computer, who then, in return becomes aware of the fact and is not accessing the file preventing the Trojan Horse from being activated. However, the big disadvantage of the signature based detection method is that infected files can only be found if the spyware's signature is already known to the anti-spyware software. The various anti-spyware producers update their database constantly, but due to the fast-paced development of computer programs and spyware, they are always a step behind. Hence, even if the anti-spyware scan is updated regularly, this does not guarantee absolute safety. Neither is signature based detection effective against newly created and therefore unknown spyware.

The second approach to identify spyware is called heuristic detection. The typical behavior of spyware builds the basis for its detection. Heuristic detection is quicker than the detection by signature, as it includes the search for characteristic performance of software. If this method is applied, anti-spyware program notifies the user in case it identifies suspicious activities on a program. However, this approach does involve also a certain level of uncertainty because it only notifies suspicious behavior. Thus, the anti-spyware scan notifies the user even when it only assumes that something is spyware. This can lead to false alarms and therefore, the user may not take notifications seriously enough.

---

[88] Note that depending on the programming language signatures contain once more and once less different information, such as the function's return, the return value, errors it can pass back or the type of its arguments.

2.1.4.4 Summary

In summary, the first part of this chapter dealt with the main objective of this thesis and presented many technical tools and devices intended to be used for remote forensic investigations. More technical details will be presented when the information becomes crucial to the understanding of future topics. Moreover, it can be concluded that the most obvious technical device to conduct a remote forensic investigation is a Trojan Horse. However, as shown above, there is a variety of different options as well as various combinations of such possible. The question whether it is possible for anti-spyware programs to prevent remote forensic investigations cannot yet be answered definitely. It may, however, be assumed – based on the investigated technical properties and functional principles of these tools – that they are quite capable of doing so.

2.2 Telecommunication

2.2.1 Introduction

We live in the age of telecommunication. The nature of telecommunication its properties and technical functionality as well as its integral part in RFI are of great importance in this context. In the following chapter the author will be discussing telecommunication devices, their commands and how gathered information is transmitted to a third party. It will also show the steps that have to be taken and the procedures that have to be followed in order to identify a potential suspect, prosecute the guilty and defend the innocent

In order to protect their privacy, people all over the world have always tried to conceal relevant information. They invented special codes to communicate or locked their documents in a vault. Nowadays, as these documents are increasingly stored on electronic devices, the question of cryptology plays an important role. Not only is it of up-most importance for law enforcement agencies to crack the code in order to obtain data, but cryptography also offers a wide variety of techniques to ensure that the gathered evidence can be used in a criminal trial. Later on, the author will give a short overview on de- and encryption.

In general terms, telecommunication is nothing more than regular and customary communication. The relatively young term telecommunication etymologically consists of 'tele', a Greek prefix meaning 'distant' or 'far off' and the Latin word 'communicare' meaning 'to share' or 'speak'.[89] On the one hand, the term 'tele' is a synonym for the medial opening of distances, thus a media bound communication with another place – independent where it is located. It is possible for various people to work simultaneously in the same media – for instance via computer-based action on a draft for a tenement – while they do not have to be at the same place. The pioneering technology for this was telegraphy.[90] On the other hand, the modes of communication in general changed in the course of time. As B.P. Lathi illustrated it: '*In the past, runners, carrier pigeons, drum beats and torches have carried messages. These schemes were adequate for the distances and 'data rates' of that age. In most parts of the world, these modes of communication have been superseded by electrical communication systems, which can transmit signals over much longer distances (even to distant planets and galaxies) and at the speed of light.*'[91] To sum up, it can be said that telecommunication is the transfer of information (communication) from a transmitter or sender to a receiver across a distance (tele).

2.2.2 Types of Communication

Communication can happen in a variety of ways:

First of all, there is a divergence between synchronous and asynchronous communication and secondly, between one-way and two-way communication. Synchronous communication means that the information is transferred simultaneously from sender to receiver, for instance a face-to-face conversation, a phone call or a live broadcast. If the flow of information is not simultaneously it is called asynchronously. This means that the sender does not know whether it will get any feedback on the sent information from the receiver. An archiving media is needed do have asynchronous communication.[92] The main distinction between synchronous and asynchronous communication is time. The difference between one-way and two-way communication, is simple the number of channels used for the purpose of communication. In

---

89 cf. as well New Oxford American Dictionary 2nd ed. (2005).

90 Brandl (2001), p. 26.

91 B.P., Lathi, Modern Digital and Analog Commuication Systems (1998), 3rd edtion, p. 1.

92 Examples for this type of communication are books, journals, newspaper or e-mail; cf. further Brandl (2001), p. 26.

the former case information can only be transmitted in one pre-assigned direction. A two-way communication (or duplex communication)[93] means that both ends can either send or receive information, thus the endpoints could change.[94] An example for a typical one-way communication is for instance the mass media, such as radio, newspaper or TV where the person receiving the message has no means to respond. Face-to-face conversations or phone calls are not only synchronous but also two-way communications. The Internet as the most modern tool for communication can be used for both as one-way and two-way communication media. Customary 'surfing' on the Internet can be seen as the typical one-way form[95] while Voice over Internet Protocol (VoIP)[96] and chat applications are seen as classical two-way communications.[97]

2.2.3 Communication Systems

Modern communication systems consist of the following components: the source, the transmitter and a receiver. The source is the origin of a message, such as a human voice, a television picture or data. If the data is no electrical – such as human voice or a television picture – it must be converted by an input transducer into an electrical waveform referred to as the baseband signal or message signal. The transmitter, also known as the sender or source,[98] modifies this signal for efficient transmission and a medium – the channel[99] or circuit[100] – such as a wire, coaxial cable or a radio link is used to send the output of the transmitter. At the other end of the 'line'[101] is a receiver[102] processing the signals received from the channel. The receiver does so by decoding the signals' modifications made by the transmitter and the channel. Thereafter, the receiver's output is fed to the output transducer,

---

93 The term duplex is only used in communication between two parties or devices.

94 A two-way communication can happen in two different forms: alternating which means that the endpoints of the communication cannot send and receive at the same time, and simultaneous which means that the just mentioned actions are possible, thus one can listen and talk at the same time.

95 Despite the fact that, reasoned by the technical circumstances (i.e. the Internet Protocols), nowadays a two-way communication is necessary. cf. further Brandl (2001), p. 27.

96 Note that VOIP is not a communication rather than it is a protocol describing how communication works.

97 Brandl (2001), pp. 26-27.

98 Horak, Ray, Telecommunication and Data Communications Handbook (2007), p. 2.

99 In formal standards terms, a channel is a means of one-way connection between transmitter and receiver, therefore, a one-way circuit or signal path. cf. for further clarification Horak (2007), p. 4.

100 A circuit is a communication path, over an established medium between two or more points, form end to end, between transmitter and receiver. cf. Horak (2007), p. 2.

101 cf. for further clarification Horak (2007), p. 3.

102 The receiver, also known as the sink, is the target device, or destination device, that receives the information transfer. cf. further Horak (2007), p. 2.

which converts the electric signals into its original form – the message.[103]

2.2.3.1 Analogue vs. Digital

Electronic communications systems or better electronic transmission systems can further also be differentiated between digital and analogue. While in the analogue form of electronic communications, information is represented as a continuous electromagnetic waveform, digital communications involves modulation (i.e. changing) of this waveform. This is done to represent information in binary form (1s and 0s) through a series of blips or pulses of discrete values, as measured at precise points in time or intervals of time.[104] Both transmission systems work but it is necessary that within an analogue system, all components have to operate in continuous-waveform (analogue) mode. The same is true for digital transmission systems which has to be digital from one end to the other. However, a network can consist of both systems requiring adoption in order to resolve the incompatibility. Both, analogue as well as digital communications systems have their advantages and appropriate applications.[105]

2.2.3.2 The Internet – Circuit vs. Packet-Switched

When speaking of the Internet and other related forms of communication, one has to mention that the modes of transmission from the originator to the receiver have changed dramatically over the last century. In the late nineteenth century, the traditional land line telephone system – the plain old telephone service (POTS) – involved only a permanent wired connection between two telephone instruments. This wired connection consisting of a twisted pair of wires (two wire circuit) – the telephone line – handled the signaling and the audio information at the same time. After more and more people wanted to be set up with a telephone it became increasingly inconvenient to connect every station set[106] with one another and a solution had to be found. Initially manual switchboards and later on switching machines were

---

103 Lathi (1998), pp. 1-2.
104 Horak (2007), p. 12.
105 cf. for a detailed overview on the single advantage Horak (2007), p. 16.
106 A telephone instrument is often called a station set. cf. Lathi (1998), p. 430.

established.[107] The development moved on, new inventions were made and finally analogue communication was replaced by digital. The main difference between a regular phone call and a modern telecommunication via the Internet lies in a different mode of data transmission. While the transmission during a regular phone call is circuit-oriented – i.e. there is an ongoing stream of data[108] – the transmission via the Internet is packet-oriented. This means that in the former case there is no buffering, neither with analogue nor digital technique.[109]

Since circuit switching was far too inefficient and expensive for intensive computer communications a new solution had to be found, which packet switching was. In order to set up an interactive, asynchronous computer-to-computer communication, the US Advanced Research Project Agency (ARPA) network established ARPANET, the first deployed packet switching in 1971. The ARPANET and its successors, such as the Internet – using the Transmission Control Protocol/Internet Protocol (TCP/IP)[110] – work by the transmission of data formed into packets and sent across a shared network.[111] This means that a message or information is split into packets of data prior to the transmission and after this transformation they are handed over into the Internet, along with other information of other users.[112] Each of these blocks of data is sent independently of each other through the net and arrives individually at the designated receiver. The receiver's job is then to reassemble the packets in the right (original) order. The single packet – also known as cell – consists of an information part (payload) in the trunk and a navigation part as its header. The information part of the packet contains its origin, destination, length, etc.[113] To sum up, packet-switched transmissions require routing control and packet assembly and disassembling.[114]

When examining such a packet-transmission on an IP basis, it is clear that there is no actual connection at all between the two 'communicating' partners. The 'senders' direct IP packages

---

107 For a detailed overview on the development please cf. Lathi (1998), p. 430.

108 Circuit switched: a fixed circuit is set up end to end and maintained during the period of use. cf. Lathi (1998), p. 368.

109 Nölle, Jochen, Voice Over IP - Grundlagen, Protokolle, Migration (2005), 2rd edition, p. 35.

110 The TCP/IP is not only essential for the functionality of the Internet, it serves also as basis for a number of developing high-speed packet networks optimized for voice, currently challenging the traditional circuit-switched PSTN (Public Switched Telephone Networks) for dominance. For further information cf. Horak (2007), p. 34.

111 Horak (2007), pp. 33-34.

112 Ebner, Gerhard, Voice Over IP – Grundlagen, Einrichtungen und Konfiguration (2006), p. 3.

113 Brandl (2001), p. 68.

114 Lathi (1998), p. 368.

into the Internet without noticing whether and when their packages reach the receivers. This characteristic of IP networks can be compared to the distributional network of regular mail: If you post a letter at your local post office, you do not know if and when your letter will reach the designated receiver. Only when the originator takes further steps – for instance a phone call – he/she can be sure that the letter found its way. Which way the letter took, however, will remain uncertain – whether the letter was transported via lorry, airmail, ship or train is not sure. The same is true if the originator posts several letters. Hence, the originator will never know whether the letters arrive simultaneously or via the same way at the addressee.[115]

2.3 Encryption and Decryption

2.3.1 Introduction

While the last chapter dealt with communication itself, this next chapter will focus on other vital aspects in this matter, such as confidentiality of sent messages.

Since the Internet as such was established as a pure network for scientific and educational purposes, all participants (universities, scientists, etc) were glad to have such media to communicate with each other. Nobody was even thinking of potential threats, as we know them today. These threats, due to the millions of worldwide Internet users, can be divided into two subgroups, namely active and passive attacks:

2.3.1.1 Active vs. Passive Attacks

Passive attacks are in general quite hard to pull off, since it is difficult to access data of a phone line – as you have to tap the wire or open the circuit distribution box. It is, however, rather simple and less dangerous to access data on the Internet. For instance, within a LAN[116] packets are sent in a broadcast mode, meaning that everybody having access to this LAN can easily gain access to the sent information as well. Since the number of wireless LANs is

---

115 Example taken from Nölle (2005), pp. 36-37.

116 Local Area Network: a computer network which covers a rather small physical area (group of buildings, an airport or just a home) – on the contrary to WAN's, Wide-Area Networks.

increasing rapidly, these problems have become a real threat.[117] Active attacks, on the other hand, manipulate data accessible on, or packets sent via the Internet. This can be done using different techniques.[118] Overall it can be said that, ever since communication has existed, people are looking for confidentiality and they have tried hard to achieve this goal. Neither the sender nor the receiver wants some uninvolved third person to have access to their messages. Therefore, various proceedings and techniques were established in order to keep secrets concealed.[119]

2.3.1.2 Protection of Confidentiality

In principal, three different measures on how to protect confidentiality could be adopted: organizational, physical, and cryptographic measures. An organizational measure is taken by a walk through the woods for the purpose of getting engaged, or to hand over a 'confidential matter' document to a reliable runner. Secondly, physical measures can be deployed in form of storing a document in a safe or sending a letter sealed. Thirdly, cryptographic measures can be used, which means that the message is distorted so that it appears completely absurd to an outsider.[120]

2.3.1.3 Cryptography

The scientific field dealing with confidentiality problems is called cryptology. Cryptology works on keeping secrets secret using codes. This brief introduction is imminent in order to understand why the legislator wants to empower its security agencies to conduct RFIs. The main reason for the establishment of this investigation method is for agencies to have direct access to a suspect's computer/electronic device and to read its content. Only at the sender's

---

117 According to press releases – cf. e.g. <http://www.openpr.de/news/111062/Mit-der-Chipsdose-im-WWW-surfen.html> retrieved 10 July, 2009 – it is possible to follow all communications happening within a wireless LAN with via real simple means; cf. further Schwenk, Jörg, Sicherheit und Kryptographie im Internet – Von sicherer E-mail bis zu IP-Verschlüsselung (2005), 2nd edition, pp. 4 and 180-183.

118 e.g. IP Spoofing, Port Scans, DNS Poisoning or Denial of Service Attacks; cf. for details Schwenk, (2005), p. 5.

119 e.g., people used lemon juice to as ink to write a letter or they codified the message with a prior agreed code so that the receiver could read it. cf. further Beutelspacher, Albrecht et al, Kryptografie in Theorie und Praxis – Mathematischen Grundlagen für Elektronisches Geld, Internetsicherheit und Mobilfunk (2005), p. 1.

120 Beutelspacher, Albrecht et al, Moderne Verfahren der Kryptographie (2006), 6th edition, p. 1.

receiving device is the confident message readable because this is the place where the message is encrypted respectively decrypted. On the other hand, access to a suspect's computer offers the option to gather the encrypting code etc.

As it can be easily imagined, its first employment was for military and political purposes as well as for Secret Service matters. There are numerous cases known in ancient Greece and Rome, which dealt with the hiding and codifying of messages.[121] However, it was not until the age of Renaissance that cryptology was further developed in Europe. Throughout history, there has always been a struggle between those who wanted to keep a message secret and those who wanted to crack the code of the messages intercepted.[122]

The term cryptology is derived from the Greek words 'κρυπτός, *kryptos*' meaning 'hidden' or 'secret' and 'λογία, -logia' meaning to 'speak' or 'word'. Furthermore cryptology is divided into:

cryptography – 'γράφω, -grapho' ('write') means the science of writing secret messages, or the science of mathematical lock and key

- cryptoanalysis – the science/art of deciphering encrypted messages
- steganography – the discipline of hiding information and
- steganalysis[123]

Steganography is intended to hide information, while cryptography encrypts it and therefore hides the meaning, but not the information itself. Hence, cryptography is overt secret writing, while steganography is covert secret writing.[124] Today, cryptography has established itself as a mathematical sub-discipline, which is not astonishing, since mathematics is most suitable to deal with and solve cryptographic question.[125]

---

121 e.g., Julius Caesar used a simple system of substituting one letter for another to send secret messages to his generals. He used a cyclic movement of letters by a certain amount of places – e.g. they replace 'a' by 'd', 'b' by 'e' and so forth. This code is known as Ceasar-Chiffre. cf. further Curtin, Matt, Brute Force – Cracking the Data Encryption Standard (2005), p. 3 and Beutelspacher (2005), p. 13.

122 Beutelspacher (2005), p. 1.; Wätjen, Dietmar, Kryptographie – Grundlagen, Algorithmen, Protokolle (2008), 2nd edition, p. 1.

123 Salomon, David, Data Privacy and Security (2003), p. 4.

124 Salomon (2003), p. 4.

125 Beutelspacher (2005), p. 1.

Encrypted messages come along with a number of properties:

- Confidentiality: only an authorized person can read an encrypted message. The authorized person is able to read the original message due to secret extra information (the 'key').
- Authentication: It is distinguished between the authentication of the participants and that of the message/information. In the former case the participants confirm each other's identity while in the latter the participants can confirm the origin and destination of the message. Authentication is needed to ensure that both, receiver and sender, are who they claim to be.[126]
- Integrity: This means that the message cannot be altered or modified in any way, not while stored or in transit. Such incidents would be detected.[127]
- No repudiation: The sender is unable to deny having sent the message.[128]
- Anonymity: Encrypted messages can be used to conceal someone's identity (either that of the sender or the receiver or even both) or to cover the fact that there was any form of communication between them.[129]

Sounds like a good thing, doesn't it? However, readers might ask themselves now, how does cryptography work and are there different methods and techniques to encrypt? The author will try to give a brief overview on the main and substantial ways.

2.3.2 Symmetric Cryptography

This is one of the oldest methods for secret communications and was already used by Julius Caesar in information exchanges with his generals. Symmetric cryptography requests that both, sender and receiver, know how do decrypt and encrypted messages, meaning that both have the same cryptographic key. In order to do so, it is necessary that they have contact with each other prior to the first secret communication because they have to exchange this cryptographic key. Symmetric cryptography is only (successfully) possible within bigger IT systems, because it requires a radial communication structure. This means that there is one big player in the middle having a lot of partners surrounding him. This center can provide its

126 cf. Beutelspacher (2005), p. 2, and Salomon (2003), p. 212.
127 Salomon (2003), p. 212.
128 A send B a message. This message is formally binding, if B can proof to C afterwards that this message originates from A. cf. Beutelspacher (2005), p. 2.
129 Beutelspacher (2005), p. 2.

partners with their personal key, while keeping its slave key. Thereby both partners – i.e. the big player and his counterpart – are able to communicate with each other secretly, as they can encrypt their and decrypt the others message. The keys of both participants are identical in such proceeding.[130] This principal is called Kerckhoffs principal[131] which claims that the important part of a secret code is not the encryption algorithm but the cryptographic key.[132] Kerckhoffs himself put it this way: '*One should assume that the opponent knows the method used to encipher data, and that security must lie in the choice of key. This does not necessarily imply that the method should be public, just that it is considered public during its creation.*'[133]

2.3.2.1 Algorithm

The algorithm used in symmetric encryption of data can be divided into two subgroups, namely block cipher and stream cipher. Block cipher encrypts a message by breaking it up into small blocks (typically 64 bit), encrypting each single block individually and turning each block of plain text (plainblock) into a block of cipher text (cipher block) that has the same size.[134] Examples for block ciphers are DES (Data Encryption Standard), its successor AES (Advanced Encryption Standard) and IDEA (International Data Encryption Algorithm). Contrary to this, stream cipher encrypts messages one bit a time. Therefore, a key-stream encodes the bits of a binary string one at a time, using a very simple rule. Stream ciphers are faster and easier to implement than block ciphers, especially in hardware. They are a natural choice in cases where the binary string has to be encrypted and transmitted at a constant rate.[135] The prototype of all stream ciphers is the One-Time-Pad.[136]

2.3.2.2 Hash Function

Hash functions are used in symmetric cryptography[137] in order to create non-manipulable

---

130 Buchmann, Johannes, Einführung in die Kryptographie (2003), 3rd edition, p. 61.
131 Named after Dr. Auguste Kerckhoffs, a Dutch cryptographer and linguist. Also known as Kerckhoffs' assumption, axiom or law.
132 Salomon (2003), p. ix.
133 Auguste Kerckhoffs, as quoted in Salomon (2003), p. 15.
134 Salomon (2003), p. 155.
135 Salomon (2003), p. 134.
136 cf. Beutelspacher (2005), p. 9.
137 Schwenk (2006), p. 11.

'fingerprints' of messages. A one-way[138] hash function is a collision-free (minimized collisions)[139] one-way function compressing messages into a hash table of a fixed length (normally either 128 or 160 bit). One-way hash functions are also called cryptographic hash functions. Such functions match exactly the function of a regular fingerprint: a fingerprint does not indicate who it belongs to but there are never two people having the same.[140] Hash tables are intended to protect sets of data from being altered and therefore they have certain properties:

- to compute the set of date out of a hash table (one-way function)
- to find a set of data equal to another set of data (collisions-free, minimized collisions) and
- to possess two sets of data having the same hash table.

Practically impossible, in this context, means that it is not possible to calculate this, neither with today's technology nor with computers in the near future, within a reasonable time frame.[141] Hash functions are part of symmetric cryptography.

Examples for the use of symmetric cryptography – or private key cryptography as it is also known – can be found widely in the telecommunication or pay TV business.[142]

2.3.3 Asymmetric Cryptography

Ever since cryptography was established it was proceeded on the assumption that it is necessary for the sender to have a secret key in order to communicate with the receiver. This key has to be equal to that of the receiver. Hence, the central problem occurring in symmetric cryptography was always the distribution and administration of the keys. It has always been necessary to exchange the key prior to a secret communication and therefore there has to be a secure channel for this exchange. Either a courier has to deliver the key or another solution has to be found. The problem is further increasing with the number of participants in the

---

138 cf. below.
139 cf. Salomon (2003), p. 378.
140 cf. further Beutelspacher (2006), p. 12.
141 cf. Schwenk (2006), pp. 11-12 and Buchmann (2003), pp. 191-192.
142 Schwenk (2006), p. 7.

communication network.[143] For many years it was believed that there would not be any satisfactory solution to this dilemma.

In the 1970s, however, there was a breakthrough – a simple and ideal solution was found which would become the basis for modern day cryptography:[144] asymmetric cryptography. Asymmetric cryptography works, to put it simply, as follows: Every participant in a system gets a private key as well as a public key. As it can be easily imagined, only the private key is to be kept secret because it is the actual key. Contrary to the private key, the public key is accessible to as many people as possible. In order to send a secret message to a particular participant, it is necessary to figure out the receiver's public key. This public key is then used to encrypt the message, which can than only be opened by the owner of the corresponding private key – i.e. the receiver. Thus, the sender encrypts a message and puts it into a publicly accessible mailbox, equivalent to the public key and it is only the owner of this particular mailbox who can open and therefore read the message.[145] In asymmetric cryptography systems, there is no need for key exchange between the users because encryption keys are listed in public directories and although everybody may read those directories, they must be protected from unauthorized usage. [146]

Due to its mechanism, asymmetric cryptography is also called public-key cryptography. Examples for public-key algorithms are for instance the RSA proceeding,[147] the first and still the most important encryption proceeding, ElGamal,[148] DSS (Digital Signature Standard) and DSA.[149] As mentioned, this technique is mainly used for secure communication over the Internet, especially for digital signatures.

2.3.4 Summary

Summarizing, it can be said that both, private and public-key cryptography have their

---

143 cf. for potential solutions to this problem Buchmann (2003), p. 133.

144 Diffie/Hellmann established a public-key cryptography algorithm that generates a shared secret key between two entities after they publicly share some randomly-generated data; cf. Diffie, W. and Hellmann M. E.New Directions in Cryptography, IEEE Transactions of Information Theory, 6 November, 1976, 644-654.

145 cf. further Schwenk (2006), pp. 13-14; Buchmann (2003), pp. 133-162.

146 cf. Buchmann, Johannes A., Introduction to Cryptography (2003), 2nd edition, p. 164.

147 Named after its inventors Ron Rivest, Adi Shamir and Len Adleman, cf. Buchmann (2003), p. 137.

148 ElGamal, T., A Public Key Cryptosystem and a Signature Scheme based on Diskrete Logarithms. IEEE Transactions on Information Theory, Vol. IT-31 (1985), pp. 469-472; cf. Buchmann (2003), pp. 156-160.

149 A special highly effective modification of ElGamal, invented by C. Schnorr and further developed by the NSA; cf. Schwenk (2006), pp. 17-18.

advantages as well as their disadvantages:[150]

	Advantages	Disadvantages
Private key	• de- and encryption algorithms can be fast in soft- as well as in hardware • keys are relatively short • ciphers can be used to generate pseudo-random numbers, hash functions and digital signatures • ciphers can be combined to create very secure encryption	• Key distribution problem • key must be replaced quite often • digital signature algorithms require large keys
Public key	• Solves the key-distribution problem • key does not have to be replaced often • in a large network, only a small number of keys needed • supports efficient digital signature algorithms	• Encryption algorithms are much slower than symmetric ciphers • keys are much longer

2.4 Examination of a Computer – Computer Forensics[151]

2.4.1 Introduction

To search the scene of a crime requires some special techniques, rules and principles.[152] This is especially true if the collected evidence is needed later to identify suspects, prosecute the

150 cf. for further details Salomon (2003), p. 133.

151 According to Judd Robins, computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud. Computer specialists can draw on an array of methods for discovering data that resides in a computer system, or recovering deleted, encrypted, or damaged file information. Any or all of this information may help during discovery, depositions, or actual litigation; cf. <http://www.computerforensics.net/forensics.htm> retrieved 12 August, 2009.

152 In this context the author wants to refer again to an e-mail received in August 2009 from the Austrian Ministry of the Interior confirming the existence and the use of guidelines; unfortunately, these guidelines are only for the internal use, hence not publicly available.

guilty and defend the innocent. Speaking in general terms, forensic science provides such principles and techniques facilitating investigations and prosecution of criminal offenses. During a criminal investigation, anything being applied to identify, recover or to analyze evidence is part of forensic science. This may include various scientific principles or scientific techniques. Which are used for:

- to detect and examine fingerprints and DNA
- to invest the authenticity or source of a document
- to recover damaged or deleted data from a computer hard drive
- to make copies of digital evidence
- to collect digital data transmitted through networks
- to verify that digital evidence has not been modified
- to affirm that digital evidence is authentic
- to define the unique characteristics of a piece of digital evidence[153]

In court procedures there is no real difference between digital and physical evidence, except for the fact that the former is less tangible. Contrary to their physical counterpart, digital evidence is made of magnetic fields and electronic pulses that can be collected and analyzed using special tools and techniques.[154] A computer is therefore the carrier of evidence and can be searched in order to get incriminating data. The range of information is broad. Due to the principles of how computers and the Internet work,[155] there is always a massive amount of data and information involved. This information contains for instance data about an individual's online activities, such as sites visited, duration and time frames of visits, etc. Based on the fact that every person who enters the Internet leaves 'electronic footprints' behind which the computer stores indefinitely, (not only, but also) the police is able to track everyone's online activities. This principle, originally invented for the 'real world', is called

---

153 cf. Eoghan, Casey, Digital Evidence and Computer Crime – Forensic Science, Computers and the Internet (2000), p. 3.

154 cf. Eoghan (2000), p. 4.

155 When entering a webpage one is getting a copy of the data stored on a server, hence the view data such as images, text, sounds are copied from the host server to one own computer and stored there.

Locard's Exchange Principle[156] and applies now to the Internet as well. This provides the investigation authorities a wide pool of potential evidence. Hence, in order to be acknowledged before a criminal court, digital evidence has to be gathered and obtained in a certain legal way using specially formulated procedures.

Electronic information and data can be of great value for ongoing investigations and provide a huge amount of potential evidence. This data is mainly transmitted by and stored on a computer.[157] Despite its electromagnetic property, however, when used as evidence, this data has the same properties and value as ordinary, physical evidence. Electronic evidence is latent in the same sense that fingerprints or DNA evidence is latent. The only difference is that one cannot see physically the content of the computer. Therefore, further tools, both hardware as well as software applications are necessary to obtain all possible evidence.

The law enforcement agencies response to electronic evidence requires that its entire staff play a role. Throughout the whole investigation process, everybody involved has to do their due diligence and follow proper procedures so that the collected evidence will hold up in court. Starting with the recognition and collection of evidence to its preservation, transportation and storage, special proceedings and rules have to be followed in order to secure the evidence. Hence it is up most importance that all the staff of law enforcement agencies have to be trained and equipped adequately that they can handle electronic evidence properly. First of all, personnel have to be aware that, due to its very nature, electronic evidence is quite fragile. Data can be damaged, altered or even destroyed should the devices be handled inappropriately or if an examination was done in an improper manner. Therefore, it is necessary that there are special, universal standards – precautionary proceedings – in order to avoid these unwanted outcomes. There have to be rules of procedure to document,

---

156 Locard's Exchange Principle states that with contact between two items, there will be an exchange. cf. Thornton, John I, 'The General Assumptions And Rationale Of Forensic Identification,' in David L. Faigman, David H. Kaye, Michael J. Saks, & Joseph Sanders (eds), Modern Scientific Evidence: The Law And Science Of Expert Testimony (1997), 2nd edition.

157 For the ease, the author is just using the term computer – however firstly a computer consists of numerous physical components proceeding and storing information (CPUs – Central Processing Units or Memories) and secondly there are certainly more potential hardware components able to hold digital data. Such devices are e.g. Smart Cards, Dongles, Biometric Scanners, Answering Machines, Digital Cameras or diverse handheld devices such as Personal Digital Assistants (PDAs) or Electronic Organizers. For an exhaustive list cf. United States Department of Justice, National Institute of Justice, NJI 187736: Electronic Crime Scene Investigations: A Guide for First Responders, 2001, pp 12ff.

gather, preserve and investigate digital evidence. It should be kept in mind that any failure of following these rules may cause the evidence to be scrutinized in court. Furthermore, not only are these rules necessary to secure the usage of the evidence but also to avoid inaccurate conclusions.[158]

The following chapter is going to give a brief overview on the current rules and regulations regarding the handling of digital evidence and the soft- as well as hardware equipment required by the law enforcement agencies to fulfill their task.

2.4.2 Procedures established for Examinations

The European Network of Forensic Science Institutes (ENFSI) was established on 20 October 1995. The intention behind this network was for the directors of Western European governmental forensic laboratories to meet regularly in order to discuss topics of mutual interests. Another purpose of the ENFSI was to share knowledge, exchange experiences and come to common agreements in the field of forensic science. ENFSI is therefore recognized as an expert group in the field of forensic sciences. The number of members has increased steadily since the beginning, from 11 laboratories in 1993 to currently 56 laboratories in 32 European countries.[159] According to its homepage, ENFSI is recognized as a pre-eminent voice of forensic science worldwide by ensuring the quality of development and delivery of forensic science throughout Europe. One of the most important goals of this network is the encouragement of all ENFSI laboratories to comply with best practice and international standards for quality and competence assurance. These best practice manuals and glossaries of forensic terms are published regularly in several languages.[160] In order to handle a wide area of forensic science, ENFSI maintains 16 specialized groups dealing with different tasks and topics.

---

158 ACPO Good Practice Guide for Computer-Based Electronic Evidence (2005), Issue 4,p. 6.

159 Member states are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, the Netherlands, Norway, Poland, Portugal, Romania, Russia, Serbia, Slovenia, Slovakia, Spain, Sweden, Switzerland, Turkey, Ukraine and the United Kingdom; cf. further the homepage of ENFSI at <http://www.enfsi.eu/index.php> retrieved 28 July, 2009.

160 cf. further the homepage of ENFSI at <http://www.enfsi.eu/index.php> retrieved 28 July, 2009.

For this thesis, the interest of the, most relevant working group – the Forensic Information Technology (FIT) working group are '*[a]ll the sciences and technical disciplines combined to allow the examination of material that contain information (computers, networks, electronic devices etc…) to assist an investigation and, eventually, present evidence for a trial*.'[161] This means that the group analysis computer data, the technical aspects of Internet investigations and the examination and search of electronic devices. The main goals of the FIT working group are the development and promotion of the discipline of forensic information technology in ENFSI member laboratories and the establishment of quality in all aspects of forensic information technology.[162]

2.4.2.1 ENFSI Guidelines

Currently the 5th version of the Guidelines for the best Practice in the Forensic Examination of Digital Technology is available, which was finally completed in Istanbul, Turkey during the 3rd EAFS conference, in September 2003. This document was finally agreed upon at the ENFSI FIT working group meeting held in September 2005 at the Netherlands Forensic Institute. The document claims to be the 'Quality Assurance "core" document' and is intended *'to promote consistent and reliable evidence through the whole forensic process, from scene of crime to court. Amongst others, it is the policy of the Board that all member laboratories should achieve, or should be taking steps towards achieving, ISO Guide 25 compliant accreditation (e.g. EN 45001) for their laboratory testing activities'*[163] Furthermore, the guidelines contain requirements concerning qualifications, competence and experience of the personnel (points 3.3 and 3.4) and their training and assessment. Regarding the equipment used for the collection of evidence, the guidelines state that an equipment inventory needs to be established for all significant items used. Moreover, these tools have to be suitable for its purpose (point 3.7) in order to ensure the validation of the evidence. In regard to such a validation the guidelines state that:

- there is an agreed requirement for the technique or procedure;
- the critical aspects of the examination procedure have been identified and the limitations defined;

---

161 cf. <http://www.enfsi.eu/page.php?uid=62> retrieved 28 July, 2009.
162 cf. <http://www.enfsi.eu/page.php?uid=62> retrieved 28 July, 2009.
163 cf. point 3.1.1 of the Guidelines for the best Practice in the Forensic Examination of Digital Technology.

- the methods, materials and equipment used have been demonstrated to be fit for purpose in meeting the requirement;
- there are appropriate quality control and quality assurance procedures in place for monitoring performance;
- the technique or procedure is fully documented;
- the results obtained are reliable and reproducible.
- the technique or procedure has been subjected to independent assessment and, where novel, peer review;
- the individuals using the technique or procedure have demonstrated that they are competent to do so.[164]

2.4.2.2 IOCE Principles

The ENFSI guidelines refer mainly to a document set out by the International Organization on Computer Evidence[165] (IOCE), which was appointed by the G8 to do so. These principles[166] – the 'G8 Proposed Principles For The Procedures Relating To Digital Evidence' – were intended to ensure the harmonization of methods and practices among nations and guarantee the ability to use digital evidence collected by one country in the courts of another country:

- When dealing with digital evidence, all of the general forensic and procedural principles must be applied.

This rule speaks for itself and once again - the same regulations that apply for documentary or physical evidence are employed to digital as well. Since there is legally no difference between digital and physical information in the court of law, there is no difference in the gathering, usage and, finally, the presentation of it in court.

---

164 cf. point 3.8 of the Guidelines for the best Practice in the Forensic Examination of Digital Technology.

165 The IOCE is an NGO and provides an international forum for law enforcement agencies to exchange information concerning computer investigation and digital forensic issues.

166 cf. G8 Proposed Principles For The Procedures Relating To Digital Evidence at <http://www.ioce.org/fileadmin/user_upload/2002/G8%20Proposed%20principles%20for%20forensic%20evidence.pdf> or <http://www.ioce.org/core.php?ID=5> retrieved 5 August, 2009.

- Upon seizing digital evidence, actions taken should not change/alter that evidence.

Operating systems, such as Windows or Unix, as well as other programs frequently alter and/or add to the contents of electronic storage. This often happens in the form of automatic updates, often without the user's awareness. This is a very important fact because, in principal the onus is on the prosecution to show the court that the evidence produced had not been altered from the time when it was first taken into the possession of police to the time of presentation.[167] Hence, data held on a storage media, such as a computer, digital camera or external hard drive, must not be changed or tampered with, since the prosecution may rely on it in court.

- When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.

Generally, in compliance with the principles of computer based electronic evidence of the Association of Chief Police Officers (ACPO), image processing techniques should be applied wherever and whenever possible. This means that an image of the entire target device has to be made.[168] As an alternative, it is also possible to copy parts or just a certain selection of files onto a different hard drive. This may be done if the amount of data exceeds the storage capability of the device used for the image. However, in certain circumstances it may be necessary to access original data. This involves investigative work on the computer/storage device which is the object of a search, as for example, if the computer or storage device is in use, at the time. In such circumstances only a trained person is allowed to do so. Furthermore, this person is required to give evidence, explaining the relevance and the implication of his/her actions.

- All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.

All activities that involve digital evidence have to be done in accordance to the rules. They have to be objective in order to secure the integrity and continuity of the gathered evidence. Therefore, it is necessary that the investigative agency is able to demonstrate how evidence

167 ACPO (2005), p. 4.
168 For details please cf. below.

was gathered or recovered and that the search procedure the evidence underwent was clear. Hence, it is further mandatory that an audit trail is created for each digital device in order to record all the processes applied to the evidence. Furthermore, as it is with scientific writing and work in general, everything has to be objective, which means that a third person – a peer – comes to the same conclusions if they apply the same process. It is essential that information is replicable.[169]

- An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.

If an individual has acknowledged responsibility for an item by signing an access log they are responsible for all actions taken in respect of that item until such time as it is returned to store or formally transferred to another individual.[170] This means that evidence in the hand of any investigating individual becomes this person's solemn responsibility. These individuals are mainly the officers in charge of the investigation – the case officers.

- Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

This last regulation is mostly just the extension of the precedent one. It means that despite the huge responsibility for the individuals involved, their employers – i.e. the agency whom they are working for – play, nevertheless, important roles and are required to fulfill their obligations and duties.

As already mentioned earlier, the author tried to obtain information from the Austrian Ministry of the Interior on how customary searches of electronic devices are conducted and whether there is a good handbook for officers. The existence and the use of guidelines were confirmed by e-mail in August 2009. Unfortunately, these guidelines are only for the internal use, hence not publicly available.

169 ACPO (2005), p. 4.
170 cf. point 7.1.E of the Guidelines for the best Practice in the Forensic Examination of Digital Technology.

2.4.2.3 Recovery Process

Principles are good ways to standardize procedures. However, each procedure has its different stages within which certain steps have to be taken and methods have to be applied. The previously mentioned Association of Chief Police Officers divided the whole recovery process into four different stages while stating that these four may not be the limit. This 'Good Practice Guide for Computer-Based Electronic Evidence' points out that there has to be a collection phase, an examination process, an analysis phase and a reporting stage.[171]

2.4.2.3.1 Collection Phase

The collection phase includes the search for, recognition of, collection of and the documentation of computer-based electronic evidence. This can include real-time and stored information that may be lost unless precautionary steps are taken at the scene. In detail, digital evidence has to be secured in accordance with the internal guidelines of the law enforcement agency. All configurations of hard- as well as software have to be documented. First the diverse storage devices have to be identified, then physical access to them must be obtained, and finally the devices need to be disconnected appropriately to prevent the destruction, damage or alteration of data. Whenever it is possible the examiner's system should be used – thus, if possible the storage device should be removed in order to perform the acquisition. In cases where the examiners use their own storage device it has to be guaranteed that this device is forensically clean when acquiring the evidence. When collecting the evidence and transferring it to the examiner's storage device, appropriate hard- and software tools are required.[172]

2.4.2.3.2 Examination Processing

This phase is intended to turn collected digital evidence into 'physical' evidence – digital data is made visible in order to show its origin as well as its significance. Furthermore, the

---

171 cf. ACPO (2005), p. 24; further US National Institute of Justice, NCJ 187736 (2001), pp. 2-3.

172 For further details concerning the acquisition of evidence cf. United States Department of Justice, National Institute of Justice, NCJ 199404: Forensic Examination of Digital Evidence: A Guide for Law Enforcement (2004), pp. 11-15. Regarding the appropriate hardware and software cf. below.

evidence in its entirety is presented and it is possible to see the full content and state of the evidence. This gives the investigation authority the opportunity to discover all information and to reduce it to the relevant level. The latter is important as not the total load of data and information gathered in the collection phase is often necessary in regard to criminal proceeding. In general, it is to say that different types of cases and media may require different methods of examination.[173] A cornerstone of the investigation is the principle that examination should not be conducted on the original evidence whenever possible.

An examination consists generally of two different steps. Firstly, the preparation of working directories on separate storage devices or media to which the evidence can be extracted and secondly, the actual extraction of the evidence itself. Regarding the latter it is to mention that there are two different forms of extraction, namely physical and logical. While a physical extraction identifies and recovers data across the entire physical drive without any regard to the file system, the logical one does so based on the installed operating system(s), file system(s), and/or application(s).[174]

2.4.2.3.3 Analysis Phase

Analysis is the interpretation of the gathered and examined (extracted) data and its arrangement in a logical and useful format.[175] Thus, after examining the entire information and the potential reduction to the relevant content, the outcome is analyzed regarding its significance and value to the criminal case. The difference between an examination and an analysis is that the former is a technical task while the latter is rather a legal one. Thus, at both stages, experts trained for the particular work have to be employed. There are various different types of analysis, such as timeframe analysis, data hiding analysis, application and file analysis and ownership and possession analysis.[176]

---

173 US National Institute of Justice, NCJ 199404 (2004), p. 15.

174 Physical extraction includes keyword searching, file carving and extraction of the partition table and unused space on the physical drive; logical extraction includes e.g. the extraction of password-protected, encrypted or compressed files, unallocated space and the recovery of deleted files; for further details cf. US National Institute of Justice, NCJ 199404 (2004), pp. 15-16.

175 e.g.: where did it come from, how did it get there and what does it mean; cf. US National Institute of Justice, NCJ 199404 (2004), p. 15.

176 US National Institute of Justice, NCJ 199404 (2004), pp. 16-18.

2.4.2.3.4 Reporting Phase

In the final step, all acquired, relevant information has to be brought together and packed into a final report, which can be used later on for testimony purposes. Moreover, the seized material has to be secured and 1:1 copies (true copy) have to be made without altering the original data. Additionally, records of the steps undertaken have to be available in order to show that the investigation process was conducted in an appropriate, continuous manner and all principles were applied so that the integrity of the evidence is given. Furthermore, the origin of any evidence has to be documented. Therefore it is necessary to establish a registry for every object seized (hard drive, notebook, PDA etc) to establish an unbroken chain of evidence.[177]

2.4.3 Hardware and Software Tools

Today a broad range of different commercial as well as free tools and software exists, which are required in order to perform a forensic examination of a computer. These applications are assisted by certain hardware specifically designed for forensic purposes. The next chapter is dedicated to these tools, their usage and applications.

2.4.3.1 Imaging

As already stated earlier, it is always better not to examine the original evident rather than an exact copy of it. This principle is mainly due to cogency of proof – the original evidence was not altered or damaged in any way, data on it is still the original one. In order to make an exact 'copy' of the digital evidence, a procedure of imaging is applied. In order to improve the procedure applied when conducting a forensic image, special hardware is needed, i.e. cloning hardware. For instance, highly integrated solutions, such as the 'Solo-3 Forensic Kit' by Intelligent Computer Systems[178] are able to create a perfect duplicate at a high speed (up to 3 GB per min). These hardware devices clone the digital evidence to a storage device other than

---

177 Geschonneck (2006), p. 71.

178 cf. <http://www.icsforensic.com/index.cfm/action/catalog.browse/category/Solo-3%20Forensic/id_category/1442ada0-380f-483f-baa7-434305bb26e9> retrieved 10 August, 2009

the original. Thereby, the examiners of the law enforcement agency can do their investigative work on the clone and the original evidence does not get altered.

2.4.3.2 Disk Wipers

Before it is possible to create a forensic image it is mandatory to have clean – 'sterile' hard drives. As it can be easily imagined, that the demand for such 'disinfected' storage devices is quite high because of computers' increased storage space. The tools used to 'sterile' drives are called disk wipers. A disk wiping enables you to 'wipe' the content of a drive, which means that it is not possible to restore the data the drive contained at a later date. Hence, this process is not just used for the deleting of contents or the formatting of the hard drive – it goes far beyond that, because the data cannot even be recovered with the help of data recovery software. Disk wiping technology replaces all binary data – i.e. 0's and 1's – with simple 0's. More sophisticated algorithms, however, use a combination of 0's and 1's in order to fill up the storage device with random data. Wiping is necessary because the evidence later cloned on this storage device can be easily differentiated from the 'background' of the wiped disk.[179]

2.4.3.3 Additional Ways to Avoid Modifications

Avoiding unwanted modification of data is also possible through the use of read-only images. There are multiple ways to access a read-only mode, such as to mount the evidence volume in read-only mode. This form of investigation is often quite risky because if using the wrong options when mounting a storage device, data on it can be altered.[180] Furthermore, it is to mention that read-only mounting to achieve the stated outcome is only possible in Unix based operation systems – Windows is always altering the disk of the computer.[181] Hence, for Windows, the read-only mode is a rather useless way to avoid any unwanted alteration of data. The solution to this problem is write-blocking devices. These tools exist in the form of software as well as hardware. A software write blocker is something like a layer between the operation system and the device driver of the disk. Via such software applications all disk

---

179 cf. Böck, Benjamin, Computer-Forensik (2005), p. 102.
180 Solomon, Michael G. et al, Computer Forensics Jump Start (2005), p. 68.
181 cf. Böck (2005), p. 101.

access requests using standard operation systems calls are prevented from writing to the disk and thereby no alteration of a disk containing evidence is nearly 100% guaranteed.[182] The hardware version of a block writer operates in the same manner. This device is plugged in between the computer controller and the physical disk and can thereby block any write requests. The operating concept of both are the same, however, some think and argue that the hardware device is more secure because of the physical connection blocking commands to the disk.[183] There are currently different software and hardware writer blockers commercially available, covering a broad range of potential applications – from notebook drives to card readers. Software tools are for instance PDBlock[184] or EnCase,[185] hardware devices are for example DriveLock,[186] UltraKit or UltraBlock.[187]

2.4.3.4 Combinations – Tool Kits

Software tools are often used in combinations. Law enforcement agencies as well as private investigators hired for the reproduction of deleted data build up their own tool kits in order to be able to fulfill their agenda. There are a huge number of commercial as well as free tool kits available and thus only a few can be presented briefly:

2.4.3.4.1 EnCase

This Windows based application, is the leading commercial forensic software and offers a wide range of features. Inter alia it is capable to produce forensic images as well as import classical – via dd[188] - produced images. Due to this broad variety of usage option it is not surprising that EnCase is considered a standard tool for law enforcement agencies.[189]

---

182 cf. Solomon (2005), p. 69.
183 cf. Solomon (2005), p. 69.
184 By Digital Intelligence Inc, cf. <http://www.digitalintel.com> retrieved 11 August, 2009.
185 By Guidance Software, cf. <http://www.guidancesoftware.com> retrieved 11 August, 2009.
186 By Intelligent Computer Solutions, cf. <http://www.ics-iq.com/> retrieved 11 August, 2009.
187 By Digital Intelligence Inc, cf. <http://www.digitalintel.com> retrieved 11 August, 2009.
188 dd is a Unix tool originally intended to copy; in this context copy means to produce a clone; cf. further Geschonneck (2006), p. 124.
189 For a detailed description cf. Geschonneck (2006),pp. 120-124.

2.4.3.4.2 AccessData Forensic Toolkit[190]

AccessDate Forensic Toolkit is another commercial Windows based application for forensic examination of digital evidence. Besides the option of producing images, it offers some special features, such as a filter – the Known File Filter (KFF) – which is able to exclude unimportant files or a browser capable to analyze 270 different file formats at once,[191]

2.4.3.4.3 Freeware Tools

Freeware tools as well as tools based on open-source-software[192] initiatives and their features are very similar to each other. A good example for freeware is the toolkit F.I.R.E. - Forensic and Incident Response Environment.[193]

Further potential tools for forensic examinations of electronic storage devices can be found in Böck, Benjamin, Computer-Forensik (2005) which offers a comprehensive, but not exclusive overview on tools and their function on page 110-5.

2.5 Potential Procedures of RFI

As shown above, the described electronic tools can be applied to get access to data and information on an electronic (storage) device. Furthermore, they can be used in a variety of other ways, as for instance in the destruction of data on hard drives or to copy and send this information to somebody, or to even operate a computer from a remote location. In order to show the way these tools can be deployed by security agencies, a practicable distinction has to be made before going into further detail: namely the differentiation between obtaining access to a computer network and the use of this access thereafter.

---

190 By AccessData, cf. <http://www.accessdata.com> retrieved 11 August, 2009.

191 cf. Geschonneck (2006), pp. 128-129 as well as Böck (2005), pp. 104-105.

192 The term open-source software describes computer software for which there is no copyright holder; hence the source code and other rights are not reserved for copyright rather than they are a public domain. Thereby the public – the single user – is allowed to use, change, improve and redistribute the software.

193 cf. Geschonneck (2006), p. 111.

2.5.1 Obtaining Access

2.5.1.1 General Aspects

As already shown with the illustration of Trojan horses and other tools, there are numerous possibilities to get access to a computer system – thus to 'hack' into it. Regarding a potential use of key logging devices by law enforcement agencies it is to mention that, it is easier to install/remove and communicate[194] with software. This is especially true in situations where the computer is connected to the Internet. The easiest way to install RFS is to do it remotely where the software tool is uploaded to the target computer and installed afterwards. While this sounds quite simple in theory, it is rather hard in reality because somebody has to be tricked into doing so. This means that somebody needs to be encouraged – significantly the target person – to download and install the piece of software to the target computer, or to open a file received via e-mail. This can be a quite difficult task as criminals are aware of the potential dangers of such behavior. In order to obtain access to the target computer, various methods ranging from backdoors and the use of technical gaps to social engineering as well as physical attacks can be applied by security agencies.

First of all, and one of the most important tasks before access can be obtained is the identification of the target computer (system). This means that a certain computer has to be assigned to a specific person, i.e. the target person, or suspect etc. It is of utmost importance that one can proof without a reasonable doubt that the target person/suspect was/is using the RFI infiltrated computer system. Otherwise, any obtained evidence or information will be subject to objections and dismissal at a trial. Hence, the authenticity of the target person and the target computer has to be guaranteed in order to establish a powerful tool for the investigation authorities.[195]

Besides the various methods to install the spying device on a target computer, each of these approaches demands a detailed analysis of the computer system before it can be applied. This

---

194 The software key logger can copy files over the internet and send it to its originator via e-mail, ftp or wireless transmission; cf. Arends, Max, Surveillance in the Post 11 September, 2001 Era (2008), pp. 48-49.

195 This is especially important in cases where computers are sold or passed to other persons, as well as in cases where various person use a computer commonly. In such circumstances, there might be the requirement of further measures to be taken, in order to grant authencity; cf. as well BMJ/BMI (2008), pp. 10 and 12.

means that the security agency has to investigate which computer operating system the target person is using, which software applications are installed etc. Due to the fact that remote forensic software will be installed onto the target computer, causing an alteration of the entire computer system, it is necessary to know these things in advance in order to guarantee an authentic documentation of all system as well as security altering measures.[196] As a further consequence this implies that these alterations have to be documented repeatedly and that all consequence of an installation and use of an RFS to a computer system have to be known and calculable. The same is true for the removal of the software tools.[197]

2.5.1.2 Methods to Obtain Access

2.5.1.2.1 Backdoors[198]

Backdoors are a method to gain access to electronic data that have not been used to their full potential. Theoretically, legislators could mandate software producers to establish such gaps in their programs. Furthermore, the legislator could then delegate that the keys to these backdoors be made available to security agencies if required for any kind of criminal investigation. This would give security agencies easy access and knowledge about the data stored and processed on a computer if it is connected to a communication network, such as the Internet.

However, this promising approach assumes that software producers cooperate more or less with them. Not only the producers of computer operating system but also the various producers of antivirus/spying programs would be covert, and there is a certain risk that they won't all collaborate.[199] This is mainly due to the risk of bad reputation in the form of bad press which comes along with an even higher risk to get kicked out of the market by small startup companies, not collaborating and hence producing valuable, highly demanded anti spy products. Moreover, a circumvention of an obligation to cooperate is very likely, as anti spy

---

196 The reasons for this are similar to the already presented ones. There is an urgent need for authenticity and integrity as already presented in the context of decryption and encryption; cf. especially BMJ/BMI (2008), p. 10.

197 BMJ/BMI (2008), p. 11.

198 Please do not mix up this expression with backdoor Trojans as mentioned above although the idea behind their common name is the same.

199 cf. the article 'McAfee replies -- by denying any FBI contacts of any sort' at <http://www.politechbot.com/p-02839.html> retrieved 18 December, 2009.

programs can be easily up- as well as downloaded to/from the Internet. Besides this, there are a number of open source programs[200] intended to counter spying devices, so that an obligation to cooperate with the security authorities will be rather useless.

The use of backdoors in software applications would technically be the easiest but practically the most unlikely ones to work due to non-cooperation respectively easy ways to circumvent.

2.5.1.2.2 Technical Gaps

Technical gaps are a little bit more complicated than backdoors as they require more technical skill and knowledge to be put into usage. Gaps, on a very general basis, can be divided into host- and network based loopholes.

Host based gaps stem from errors of a software application of a computer system. This form of a technical gap is one of the most frequent security gaps and appears often in the form of a buffer overflow/overrun. This anomaly means that a massive amount of data is stored in a buffer outside the allocated memory. The outcome can be that the additional data overwrites bordering memory and can thereby result in a breach of system security. In order to trigger such an overflow, inputs have to done which are designed to execute code or to alter the way a specific program operates. As Feiler points out, a direct attack on the target (suspects) computer is possible if this data processor operates services which are accessible via the Internet (hence the suspect uses a HTTP server). However, this does not work without the active participation of the suspects themselves.[201]

Network-based gaps, on the other hand, are the results of network protocol errors. Unencrypted protocols are being used to carry out man-in-the-middle attacks on certain computers. This is possible as HTTP or FTP do not need any verification of the partners to the

---

200 cf. e.g. <http://de.clamwin.com/> retrieved 18 December, 2009.

201 cf. Feiler, Lukas, 'Technische Aspekte der Online-Durchsuchung' in Zankl, Wolfgang (ed), Auf dem Weg zum Überwachungsstaat? Neue Überwachungsmaßnahmen im Bereich der Informations- und Kommunikationstechnologie (2009), p. 175; as well as especially Elias, Levy (aka Aleph One), Smashing the Stack for Fun and Profit (2006) presenting a step-by-step introduction to exploiting stack-based buffer overflow vulnerabilities at <http://www.phrack.org/issues.html?issue=49&id=14#article> retrieved 18 December, 2009.

communication. Thus, the security agency, or any other third person could not only influence the authenticity of a communication but also impair its integrity. In order to achieve this, security agencies can even employ Internet service providers (ISP) in assisting with the process. This practice is intended to be established in Germany. All German ISP have to install a 'SINA Box'[202] in their network, allowing the police to monitor all communications that are taking place. As Birk shows in his article, these boxes could easily be modified at a low cost, so that it is possible to implement a remote forensic software (RFS) tool into any download. Hence, the content, as well as the source of the download do not matter. Shareware or test versions of new software, the update of the PDF reader, all of these downloads could be infected with an RFS. Users would install software that have RFS included in their programs.[203]

The application and use of technical gaps – especially that of network based gaps – would be a potential technical possibility to conduct remote forensic investigations. As illustrated, the advantages seem to be outweighing the disadvantages – the only thing missing now are legal provisions in order to apply them in real life in a legitimate manner.

2.5.1.2.3 Social Engineering

Social Engineering is a form of attacks, which uses human tendency to trust and help other people and attempts to obtain required, personal information in a very open way.[204] Remote forensic investigations have several options to use social engineering in order to obtain necessary information. As already shown with Trojan horses or similar spyware, the big challenge for the investigating authorities is to trick the target person to run a certain file or to install a certain software tool etc.

---

202 cf. for further details in German: <https://www.bsi.bund.de/cln_155/ContentBSI/Themen/sina/Systembeschreibung/sysbeschreibung.html> retrieved 12 August, 2009.

203 cf. Birk, Volker, Der Staat als Einbrecher: Heimliche Online-Durchsuchungen sind möglich (2007) at <http://www.heise.de/tp/r4/artikel/24/24766/1.html> retrieved 12 August, 2009.

204 cf. in this respect e.g. <http://www.microsoft.com/protect/terms/socialengineering.aspx> or <http://www.sicherheitskultur.at/social_engineering.htm> retrieved 18 December, 2009; Examples for social engineering attacks are e.g. when persons call a help desks, tells them that they would be a client of this company and have forgotten their password or they phone a person working for company X, tell them that they would be the person in charge for the IT application of the service provider of X and need the password of the person called, in order to install some new programs on their company desktop.

Similar to these methods are phishing attacks, consisting of e.g. e-mails pretending to be from a certain person or company and which demands the exposure of certain private information. If such common mass e-mails are sent to a specific group of people,[205] the attack is called spear phishing, which means that the attack is very target oriented and only meant to obtain information of this specific group.[206] However, the risk of being detected is quite high.[207]

In summary it can be said that social engineering works rather well for criminals trying to obtain other people's private information and thereby obtaining access to e-mail or banking accounts. However, the author doubts that it will be neither a useful, nor a successful device to counter criminal activities as felons are very well equipped and on constant alert in this respect.[208]

2.5.1.2.4 Physical Attacks

In situations where computers are not connected to the Internet, an installation procedure as described above is rather ineffective. Hence, security agencies have to come up with another way to gain access to the data processor. In these cases physical access to the computer is often the only solution to overcome the problem. The RFS or similar kind of hardware could be attached between the keyboard and the computer itself.[209] In other cases software programs could be installed by the police itself after having obtained physical access to the electronic device.[210]

In this context, special attention has to be drawn to the use of hardware devices in RFI's: One

---

205 e.g. the potential or known members of a criminal organization or a terrorist association.

206 cf. as well <http://www.microsoft.com/canada/athome/security/email/spear_phishing.mspx> retrieved 18 December, 2009.

207 cf. Feiler (2009), p. 174.

208 However, it could be argued that everybody – thus also criminals – know that fingerprints are used to convict criminals, hence most offenders wear hand gloves when committing burglar etc. On the other hand, fingerprints are still one of the most important source of evidence, meaning that not every criminal – even aware of this fact – does apply such conviction-preventive measures.

209 Note regarding this that, as mentioned prior key loggers can be transformed into Trojan horse programs by simply including a root kit.

210 After having passed the entrance door, it is regularly not really difficult to mount a computer and install a specific program on it. As Feiler points out, the big advantage for the investigating authority is that it knows exactly on which computer it is installed; cf. Feiler (2009), p. 174.

of the advantages of hardware devices are, that they cannot be detected by any anti-virus software. Having said that, it is already questionable whether – at this point in time - any anti-virus software would cause problems for law enforcement agencies. Virus scans, for example, recognize and delete only those malware programs already known publicly. In order to become commonly known, malware programs have to be spread regularly all over the Internet and thus all over the planet. However, this is exactly the opposite the special law enforcement RFS is supposed to do – 'malware' programs are only intended to be used in certain circumstances and in order to attack certain and specific target computers. Therefore, the hope that an anti-virus program might help with the detection of RFS is rather minor.[211] Furthermore, it is questionable whether the producers of these anti-virus programs had their customers' protection in mind. Some big, anti-virus producing companies already announced that they would not cooperate with government agencies in this matter, while others are still sitting on the fence.[212]

The major disadvantage of hardware devices in RFIs is that physical access to the computer has to be obtained in order to activate the RFS. Furthermore, in order to achieve the goal of the investigation, access should be obtained and installation should happen without the owner of the computer noticing. Not only is this a massive problem as to how-to handle this in praxi but also is it a legal issue in western countries.

2.5.2 Exploiting an Obtained Access

2.5.2.1 General Aspects

After access to a computer is obtained by the law enforcement agency, an RFI can be conducted. In principal, it is to say that as soon as the investigating authority has obtained access to a computer, it can virtually execute all functions of this particular computer. This means than the agency is able to install further software, browse through the directories, or simply just monitor the processes going on. Other options are, for instance, the use of already installed web cams or microphones in order to see and hear what is going on nearby the user or the computer.

---

211 cf. Birk (2007).
212 cf. for further details Arends (2008), p. 55

2.5.2.2 Encryption

The most important aspect of encryption is the investigating authority's ability to encrypt coded communication as well as to listen to decrypted phone calls over the Internet.[213] As illustrated above, decryption as well as encryption processes are conducted on the technical device used for sending the communication as well as for storing purposes. As soon as the communication is coded, there is no possibility to figure out its meaning. Not until it is decoded at the receivers', or reopened by the person with the right key, the intercepted communication/stored document does not make any sense. With the obtained access to a computer the investigation authorities have the ability to read decrypted written communication or listen to regularly decrypted phone calls. Another possibility would be to use a key logging device in order to figure out certain passwords or access or encrypting codes of the users.

2.5.2.3 Manual vs. Automatic

RFI can be conducted manually as well as automatically. Both methods offer some advantages as well as disadvantages: While the manual way seems to be more difficult and more expensive (due to the employment of more well trained people), it appears to be more effective. Officers observing computer activities or browsing through the directories and files of a computer are more flexible in doing so. However, they are slower doing so, than if this procedure would be conducted automatically. Another argument against manual conducting is that the risk of mistakes is higher due to human imperfection. An automatic search or surveillance done by specifically adapted software tools, on the other hand, can be conducted on a rather minimal budget with a smaller incentive to failures and oversights. The disadvantage, however, is, that software is not as flexible as humans and it operates strictly according to its code. Moreover, the gathered information has to still be evaluated afterward and while the officers employed in a manual RFI can separate the obvious important information from trash, software tools cannot do so and collect everything.

---

213 cf. in this respect inter alia as the report of the expert group on this topic at BMJ/BMI (2008), p. 49; furthermore Buermayer, Ulf, Die 'Online-Durchsuchung'. Verfassungsrechtliche Grenzen des versteckten hoheitlichen Zugriffs auf Computersysteme, HRRS 8/2007, p. 331; further Buermeyer, Technischer Hintergrund, p. 160

2.5.2.4 Integrity of Evidence

Besides the already mentioned authenticity of information that an RFI provides for law enforcement agencies, the integrity of the accumulated evidence is another essentialia for the reliable conduction of an RFI. This means that the risk of any alteration of the obtained data by the transmission process is non-existent. As the expert report points out, there is need for technical measures to ensure that RFS components cannot be substituted by other software tools by the target person. If it would be possible to exchange the RFS for any other tool in order to transmit only non relevant data to the authorities, the use of an RFI is more than just questionable. Hence, it is necessary to ensure that the applied RFS is unique, respectively personalized to a high degree.[214] As these requirements for an RFS seem reasonable and logical, it has to be kept in mind that they are also huge hurdles for any RFI. Due to the vast investigations and the, consequently, high costs prior to an RFI, its application is rather unlikely to happen frequently or extensively. Furthermore, an RFI does not only cost money but also time and it will take plenty of it to obtain all necessary information in order to guarantee all mentioned preconditions for reliable evidences.

2.5.2.5 Communication Channels

It is crucial that there are communication channels available, meaning that the investigating authority can either communicate with the target computer directly (remote use for search purposes) or receive the gathered data from the target computer. Without any communication channel, it is not possible – with the exception of a physical attack – to install RFS, thus the target computer has to be connected to a communication network such as the Internet.

2.6 Conclusion and Summary

The question, the author tried to answer in this chapter was, whether it was possible from a technical point of view to apply an RFI without the target person noticing it. Thus, it was analyzed whether this investigation method works in real life scenario. Therefore, the various technical aspects of a remote forensic investigation were illustrated, from the software tools to

[214] BMJ/BMI (2008), p. 13.

the technical principles telecommunication, encryption or anti-spyware programs are based on. In order to give a broad and a distinguished view on the entire issue of an RFI, the author divided the technical question into two parts, namely the obtaining of access to a computer and the exploitation of that access.

The conclusion of the conducted research was that obtaining (remote) access is the most difficult agenda for the security agencies due to a number of reasons. First of all, an identification of the target computer systems implies potentially extreme time consuming investigations prior to the actual 'attack' on that computer. Second of all, any technical information regarding the computer system (computer operating program, anti-spyware programs etc) has to be gathered as well. Not until the security agency has obtained this data it is possible to create a target customized software program in order to start an RFI. However, why it is important that the software tool of the security agency is customized? Why should it not be possible to use already existing tools in order to start efficiently an RFI? Besides the general problems with authenticity as already discussed above, problems related to the installation of that software tool on the target computer might occur. This is closely connected with the previously presented working methods of anti-spyware programs, i.e. signature based or heuristic detection:

In order to obtain access to a data processing device, different approaches can be applied. Due to the fact that they rely on a further (i.e. mainly the target) person to behave accordingly, backdoors and social engineering are rather unreliable methods.[215] A more dependable method for security agencies is the use of a direct physical attack on the target computer in order to attach hardware, such as a key logging device. However, as presented above, the most promising approach in this regard is the use of technical gaps, especially if an RFI is conducted as intended by Germany with its 'SINA Box'[216]. Via the application of such man-in-the-middle attacks, the security agencies could easily attach the RFS to any unencrypted message. When opening this message, generally the target person installs the RFS onto its computer and an RFI could be conducted.

---

[215] Regarding backdoors security agencies depend on the programmers of anti-spyware programs, while they depend on the target person itself when social engineering is applied, as the person is tricked into an installation of RFS.

[216] Note that in this instance the security agencies do rely on third persons as well, however, there are far less Internet service providers than provider for anti-spyware program; the remaining problem is still – and will always be – the target person itself !

However, even if the target person installs the RFS onto the intended computer, this does not guarantee a successful start of an RFI. Concerning the problematic factor of anti-spyware programs it is to point out that if the protection program on the target computer is signature based, customary available spyware is rather likely to be detected. Once spyware is identified as such, it is indexed into the databases of the various providers of protection programs. The signature of the spyware, thus its 'fingerprint', is used to find further related software. Instantly, the protection program issues a warning to the user of the attacked computer. Thus, when being notified that a certain program is infected with malware the 'RFS' will not be installed. Consequently, an RFI cannot be conducted. This indicates furthermore, that signature based detection is only working against already known mal- and spyware. On the contrary, it is rather ineffective against newly created and therefore unknown spyware.

Heuristic detection relies on typical behavior of spyware and is therefore quicker than detection by signature. An anti-spyware program using this method notifies the user if it identifies suspicious activities of a program. However, precisely because heuristic detection rests upon typical behavior, there is always some uncertainty in the notifications of the user of a computer. Suspicious behavior of a program letting the anti-spyware scan assuming that this program is spyware can lead to false alarms. As a consequence and if notifications happen frequently (even in connection with user reliable and trustful programs) the user could take these alarms not seriously enough.

From a technical point of view, this means that current anti-spyware programs are capable to firstly detect customary, already widely known spyware and secondly that spyware behaves according to its indented use. Hence, special computer programs customized to circumvent the principles of customary protection programs do have the potential to work properly for the security agencies. Thus, if such tools are employed in order to obtain access to a target computer, the likelihood of success (the secret installation of that tool) is quite high. Consequently the answer to the first question has to be that anti-spyware program only have a limited capacity to identify threats. For the author this is true with the understanding that security agencies work with customized software tools, taking into account the whole package of a target computer, i.e. software as well as hardware components a computer is working with respectively attached to a computer. However, it is not quite as simple as it sounds. Security agencies have to investigate certain criteria before they are able to create such a customized piece of spyware. All this investigative work includes a massive engagement of personnel, thus it is time-consuming and therefore also connected to high costs. Hence,

remote forensic investigations will not be on the daily agenda of security agencies and applications will be limited to mainly serious criminal activities.

As a finishing touch for the technical chapter of this thesis, the author wants to point out another, more general aspect of malicious software employed by security agencies:

Despite the fact that remote forensic tools and other surveillance devices operate like previously mentioned programs they are not malware. This improper connection from remote forensic software tools and surveillance devices is often made in public discussions and contributes immensely to the ongoing confusion in this matter. As these tools are intended to be employed by criminal investigation authorities, there has to be a legal basis for them in order to avoid massive complications.

To the contrary of malware RFSs do not attack a computer since the intentions behind them are completely different. Therefore there are neither offenders nor victims. In the case of malware it is the intention of an attacker to operate covert as long as possible and there are no real goals behind such an attack. Side effects are not important, they are just taken into account because there is no liability. Destruction is intended. The removal of the tool does not take place. Once the damaging effects are in force, it is irrelevant whether the victim becomes aware of an attack or not. Hence, the intention to keep it secret that these tools were installed on a computer are rather minor. Furthermore, it is completely unimportant who the victim is because malware does not focus on one single person. In addition, malware is not subject to correctness, scrutiny, or integrity. The attackers are not concerned whether they damage one certain computer or not because they are more interested in the widespread effects of their attack. The only goal is the general, malicious effect.

Furthermore, it is to say that provisions last regularly longer than technical possibilities, hence it is necessary to draft the corresponding legislation carefully and comprehensively. In order to do this successfully and avoid to be continuously ‘out of date’, it is essential to formulate broad general principles in a clear and unambiguous for on how remote forensic tools have to be handled and used.[217]

This brief technical part concerning RFIs offers a broad view of the whole matter and the reader needs to be well aware of the fact that everything mentioned above is essential and has

[217] cf. also Posch (2008), p. 40

to be kept in mind when dealing with RFI from a legal perspective.

3 Legal Aspects of RFI

This next part of this thesis provides an overview on the corresponding Austrian constitutional provision – including some fundamental rights and the question of proportionality, as well as the relationship between the Federation and the Federal States. It needs to be pointed out that this thesis only deals peripherally with human rights in regards to RFIs. Despite the fact that the thesis deals mainly with procedural provisions, a short section on substantive law is also included in order to illustrate the impact of criminal behavior, if an RFI would not be legalized for security agencies by the legal framework. Following the potential basic structure for an RFI as well as its possible implementation into the legal framework will be presented. In addition, the corresponding procedural provisions are illustrated in detail: On one hand, there will be an examination of specific regulations in the Austrian Code of Criminal Procedure and on the other hand, we will look at some of the potential provisions the Austrian Security Police Act has to offer.

3.1 Introduction

From a legal perspective, the Austrian Federal Ministers of Justice and of the Interior[218] pointed out that an RFI should be made legitimate but not for every instance. Restrictions are mainly due to the massive interference of an RFI and people's right of privacy. In concreto, the Ministers stated that an RFI should only be conducted in situations where it is necessary for the solution of

- a criminal act punishable by imprisonment for a minimum period of ten years, or of
- a criminal organization or a terrorist association according to sections 278a and 278b of the Austrian Criminal Code, or
- for the solution or prevention of a criminal act committed, or planed by such an organization or association.[219]

---

218 cf. Vortrag an den Ministerrat der Republik Österreich durch das Bundesministerium für Justiz und das Bundesministerium für Inneres hinsichtlich der Erweiterung des Ermittlungsinstrumentariums zur Bekämpfung schwerer, organisierter und terroristischer Kriminalitätsformen („Online-Durchsuchung'), 17 October, 2007.

219 cf. Vortrag an den Ministerrat der Republik Österreich, 17 October, 2007.

Furthermore, an RFI should be legally conducted if a person is strongly suspected of preparatory works in relation to a criminal organization or a terrorist association (sections 278a, 278b of the Austrian Criminal Code).[220]

Before going into any detail and identifying any potential legal basis for an RFI, an overview of the legal framework, starting with the Austrian Federal Constitution, is given.

3.2 RFI and the Austrian Constitution

3.2.1 State of Law

In Austria, the state of law develops from different regulations of the Austrian Federal Constitutional Law. Important in this context is that the Austrian Constitution handles this principle in its formal sense.[221] However, according to this perception, every country is its own state of law, because every country regulates and controls the behavior of its citizen by a coercive order, without the establishment of this order. Putting it differently, in its formal sense, a state of law means the exercising of state functions based on general provisions made known to the public and the possibility to guarantee these rules by a coercive order. No reference is made to the content of the provisions, indicating that it is imaginable that these rules contravene completely with the matters of fairness or humanity.[222] A state of law in its substantive sense is intended to overcome this 'unwanted' outcome of a state of law in its formal sense and to establish a just and fair-minded order. This is connected closely to the value concepts of the society, which was taken as point of critique, as it can be used by various ideologies as a basis for the establishment of totalitarian systems.[223]

---

220 These requirements are similar to those established for the conducting of an Optical and Acoustical Surveillance of Persons, according to section 136 para. 1 no. 3 of the Austrian Code of Criminal Procedure; cf. below.

221 cf. Walter, Mayer (2007), MN 165, p. 90; furthermore it is remarkable that this expression was coined especially by Hans Kelsen as quoted in Koja, Friedrich, Allgemeine Staatslehre (1993), p. 124.

222 cf. Funk, Bernd Christian, Einführung in das österreichische Verfassungsrecht (2007), 13th edition, MN 110, p. 99.

223 cf. Walter, Mayer (2007), MN 165, p. 91; as well as Funk, explaining the difference between the two concepts by the example of a National Socialist state; cf. Funk (2007), MN 110, p. 100

The formal aspect of a state of law is the basis for the principle that the entire public administration shall be based on law. In this respect, Art 18 para. 1 of the Austrian Federal Constitutional Law guarantees that for every single act of the Austrian Federation there has to be a legal basis,[224] thus that there is no legal vacuum.[225] Not only does each state authority need to have a legal foundation for his/her action but he/she is also obliged to not infringe other provisions higher in the hierarchy (according to their derogatory power).[226] This principle can also be summarized as the principle of the rule of law, which binds all federal as well as (provincial) authorities of the Laender (provinces) in the same way. Thus, if the act of an authority is against a more powerful provision in the hierarchy, it is unlawful. Furthermore, formal aspects can be found in the constitutional provisions dealing with the functions and organization of the judiciary, including the system of administrative courts, and constitutional jurisdiction. Concerning this, specific options of judicial control and review[227] have to be highlighted. The substantive aspect is put forward particularly by the provisions on fundamental rights, referring mainly to the principle of freedom and dignity.[228]

3.2.2 Fundamental and Human Rights

The hierarchy the sources of law are subjected to include one very vital and indispensable one: human rights. Within the Austrian legal system, fundamental rights can be found in

---

224 Note in this context that this explicit bondage to law means that the legislator has to determine administrative activities; however, since Austria became a Member State of the European Union, administrative activities can also be based on EU law. Hence the expression of law in Art 18 of the Austrian Constitutional Law was extended by European Community Law; cf. Jabloner, Clemens, Anwendungsvorrang des Gemeinschaftsrechts und Verwaltungsgerichtsbarkeit, in ÖJZ 1995, pp. 921 et seq.as well as VwSlg 15422 A/2000.

225 however, there are exceptions – Art. 130 para. 2 governs that no illegality exists where legislation forbears from the establishment of a binding rule on an administrative authority's conduct, leaving the determination of such conduct to the authority itself, and the authority has made use of this discretion in the spirit of the law. Moreover, there is also an exemption in foreign politics.

226 The hierarchy of the sources of law (structure of the legal system) in Austria is as follows (top-down): 1. Guiding principles of the federal constitution, 2. Primary and secondary Community law, 3. 'Ordinary' federal constitutional law, 4. Federal legislation, 5. Regulations, 6. Orders; The more difficult legislative procedure gives the constitutional law greater durability. A federal constitutional provision thus normally requires a majority of two thirds of the votes in the National Assembly, with at least half of the members being present. Additionally, the provision produced in this manner must be expressly designated as a 'constitutional law' or 'constitutional provision'. A valid resolution on federal legal provisions in the National Assembly, on the other hand, requires the presence of at least one third of the members and an absolute majority of the votes cast. For further details cf. <http://ec.europa.eu/civiljustice/legal_order/legal_order_aus_en.htm> retrieved 23 October, 2009.

227 according to Art 130 as well as Art 144 of the Austrian Federal Constitutional Law, the Constitutional as well as the Administration Court are empowered to review legislative as well as administrative acts.

228 cf. Funk (2007), MN 111, p. 101.

various forms. For instance, fundamental provisions were incorporated in the Basic Law of 21 December 1867 on the General Rights of Nationals in the Kingdoms and Laender, the Federal Act concerning the Protection of Personal Data or the Federal Constitutional Law. Further important sources of human rights are state treaties,[229] or international treaties and convention[230] ratified and thus applicable in Austria. In addition, Austria is a member of the Council of Europe and has signed the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) in 1957. Concerning this Convention it is to note that numerous provisions in the Austrian legal system refer directly to, or are interpreted in the light of this international convention. Moreover, there is already a wide and detailed constant jurisdiction of the European Court on Human Rights[231] which has to be taken into account as well.

In general, an RFI constitutes a serious interference with fundamental freedoms and rights, more specifically with the fundamental rights of data protection, the protection of privacy[232] as well as householder's rights.[233] Moreover, if an RFI is used for surveillance purposes there are also interferences with the telecommunications secrecy[234] and the freedom of communication.[235] Thus, fundamental procedural rights can be infringed, such as the right to a fair trial[236] etc, as well as an RFI can have proprietary outcomes, such as a damage of data and the corresponding right to the peaceful enjoyment of one's possessions.[237]

---

229 The Treaty of Peace between the Allied and Associated Powers and Austria 1920 or the Treaty for the re-establishment of an independent and democratic Austria 1955.

230 e.g. the Convention on the Elimination of All Forms of Racial Discrimination; the International Covenant on Civil and Political Rights; the International Covenant on Economic, Social and Cultural Rights; the Convention on the Elimination of All Forms of Discrimination Against Women; or the Convention on the Rights of the Child.

231 the court was established under the ECHR in order to monitor respect of human rights by states. For further information cf. the website of the court at <http://www.echr.coe.int/ECHR/EN/Header/The+Court/Introduction/Information+documents/> retrieved 23 October, 2009.

232 Art 8 Convention for the Protection of Human Rights and Fundamental Freedoms.

233 Law of 27 October, 1862 on Protection of the Rights of the Home, Federal Law Gazette No. 88/1862 as amended by: Federal Law Gazette No. 422/1974.

234 cf. as well BVerfG, 1 BvR 370/07, 1 BvR 595/07 of 27 February, 2008, maxim no. 3 referring to Art 10 para. 1 Basic Law for the Republic of Germany (German: Grundgesetz).

235 Art 10a Basic Law on the General Rights of Nationals in the Kingdoms and Laender 1867; note in this context that not until the case of Klass and others v. Germany of 6 September, 1978, the European Court of Human Rights did not acknowledge Art 8 Convention for the Protection of Human Rights and Fundamental Freedoms as basis of a human right telecommunication secrecy.

236 Art 6 Convention for the Protection of Human Rights and Fundamental Freedoms.

237 Art 1, Protocol 1 to the Convention for the Protection of Human Rights and Fundamental Freedoms.

Based on these fundamental, personal rights, the German Bundesverfassungsgerichtshof established a ruling guaranteeing cardinal rights to confidentiality and integrity of informational systems.[238] As the report of the expert group[239] concerning the matter of RFI points out precisely, this ruling and this view of the judges can neither be transferred directly into the Austrian legal system nor does this ruling have any implications on the Austrian legislation. However, the German ruling has provided Austria with more substance in the ongoing discussion on RFIs and it assists as an orientation due to the fact that the constitutional granted fundamental rights in Austria are established similar to those in Germany. Primarily, it is argued that a general right similar to the newly established one in Germany could also be justified by the current constitutional situation Austria,[240] as there are similarities in respect to an interference with fundamental/human rights and the correlating obligations of the State.[241]

There is a lot of literature[242] about the aspects of human/fundamental rights already available and therefore, this thesis will not go into any further details but just raise awareness in the respective chapters. There will be only references to the provision and some general statements regarding these rights. In addition, a short presentation on the reservation of statuary powers will be given subsequently.

---

238 cf. BVerfG, 1 BvR 370/07, 1 BvR 595/07 of 27 February, 2008, para. 201 referring to Art 2 para. 1 in conjunction with Art 1 para. 1 Basic Law for the Republic of Germany (German: Grundgesetz); Art 1 German Grundgesetz reads: 'Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority; whereas Art 2 para. 1 reads every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law. cf. official translation at <https://www.btg-bestellservice.de/pdf/80201000.pdf> retrieved 16 December, 2009.

239 BMJ/BMI (2008), p. 64.

240 BMJ/BMI (2008), p. 64.

241 BMJ/BMI (2008), p. 65.

242 cf. e.g. Rädler, Raphael, Die verdeckte Online-Durchsuchung als strafprozessuale Ermittlungsmaßnahme in Deutschland und Österreich (2009); Gudermann, Anne, Online-Durchsuchung im Lichte des Verfassungsrechts (2010); Buermayer, Ulf, Die „Online-Durchsuchung' Verfassungsrechtliche Grenzen des versteckten hoheitlichen Zugriffs auf Computersysteme, HRRS 8/2007; Schantz, Peter, Verfassungsrechtliche Probleme von „Online-Durchsuchungen", KritV 2007, 310, Sachs, Michael, Krings, Thomas, Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme", JuS 2008, 481; Rössel, Markus, Online-Durchsuchung vs. PC-Grundrecht, in ITRB, 2008, 75; Wilhelm, Georg, Online-Durchsuchung nur über richterlichen Befehl, ecolex 2008, 293 or Regenfelder, Wolfgang, Ermittlungsmaßnahmen bei neuen Informationstechnologien im Spannungsverhältnis zum Grundrechtsschutz (2008)

3.2.3 Reservation of Statuary Powers and the Principle of Proportionality

Generally speaking, an interference with fundamental freedoms caused by authorities is only possible under limited circumstances. This means nothing else than fundamental rights do not always prevail. In regard to the most constitutional granted rights there is a reservation of statuary powers, meaning that federal legislation (i.e. ordinary law) can – if it is empowered explicitly by the Constitution – modify or limit a certain fundamental right. This method gives the legislator a margin in dealing with rights of the individual and the interests of the general public, if these interests differ. However, this indistinctness is not intended to lead to an extension of interference possibilities rather than the authorities' competences to infringe legally human rights are to be interpreted principally in a tight way.[243] The main problem in this context is – not surprisingly – how far the empowerment of the legislator reaches, because only if the legislator exceeds the margin established by the reservation, the legitimacy of an interference with fundamental rights is against the Constitution.[244] As Walter/Mayer point out, there are two different forms of reservations, namely formal (general) reservations and substantive (special) reservations. The distinguishing aspect is that while the former does only look at the form of the legislative act (thus it has to be an ordinary law), the latter evaluates its content as well.[245]

In order to illustrate such reservations, the author is presenting a practical example of how this may work in the real world. Since the importance of the right to privacy and an interference of such for this thesis is of utmost importance, a brief summary will be given.

3.2.3.1 Example: Right to Privacy

According to Art 8 Convention for the Protection of Human Rights and Fundamental Freedoms [e]*veryone has the right to respect for his private and family life, his home and his correspondence.* These four different guarantees constitute the right to privacy and protect in this sense the private sphere of any citizen from illegal or arbitrary interferences of state

---

243 BMJ/BMI (2008), p. 65; note in this context that there are constitutional precepts in regard to specialty and a non-extension of coercive measures; furthermore the principles of legality and the prohibition of analogy in criminal law have to mentioned at this stage as well.

244 cf. Walter, Mayer (2007), MN 1339, p. 629.

245 cf. Walter, Mayer (2007), MN 1339, p. 629.

authorities. Art 8 Convention for the Protection of Human Rights and Fundamental Freedoms protects private life. The term of privacy is quite broad which makes it hard to define precisely and even causes overlapping of the different rights granted by Art 8. Despite the fact that all four guaranteed rights have to be distinguished clearly, even if their lines are often blurry, it does not mean that they have to be seen isolated from each other. Moreover, these four are already linked together by the common provision of Art 8 Convention for the Protection of Human Rights and Fundamental Freedoms and refer to each other contentiously as they are just different characteristics of the same – namely private life as such. Furthermore, this means that interferences can constitute a multiple interference with Art 8 so that the rights granted by it do not exclude each other. In addition it is to mention that some rights are only directed at human beings, while other rights are also granted to legal persons. For instance, only a human being does have the right to a family life by definition, whereas legal persons do also have a right to a private life[246] or enjoy protection of their correspondence.

Substantive reservations, such as that of the Convention for the Protection of Human Rights and Fundamental Freedoms, allow interferences of the state with fundamental or human rights. The precondition for this is that the interferences are in accordance with the law and necessary in a democratic society, in the interest of national security, public safety or the economic well-being of the country. Moreover, it is allowed when it is necessary for the prevention of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others.[247] This means that an interference with the right to privacy is legitimate if certain requirements are recognized.

Concerning Art 8 para. 2 Convention for the Protection of Human Rights and Fundamental Freedoms establishing this option of legitimate interference, it is to say that especially the term 'necessary' is of great importance. According to the European Court on Human Rights, '*the phrase 'necessary in a democratic society' means that, to be compatible with the Convention, the interference must, inter alia, correspond to a 'pressing social need' and be 'proportionate to the legitimate aim pursued'*.[248] Such measures could be legitimate if they

246 e.g. in respect to data protection etc.

247 Art 8 para. 2 Convention for the Protection of Human Rights and Fundamental Freedoms; but cf. as well in this respect Art 9 para. 2, Art 10 para. 2 etc Convention for the Protection of Human Rights and Fundamental Freedoms.

248 cf. Case of Silver and Others v. The United Kingdom, judgment of 25 March, 1983 (Application no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75), para. 97 (c).

are aimed to counter or prosecute serious forms of criminal activities constituting a major threat to the fundamentals of a State.[249]

Furthermore, the Court pointed out that the adjective 'necessary' involves the principle of proportionality.[250] This means that the intensity of interference is compared with the interest of the public – both are set into relation – in order to figure out whether interference is allowed or not. This means that the more serious the interference, the higher the requirements[251] that have to be fulfilled. Moreover, there is another condition which has to be taken into account when it comes to the principle of proportionality: The application of a coercive measure has to be optimized meaning that state authorities are only allowed to apply a method if there is no other less harsh method leading to the same results.[252]

As it can be seen, there is a strong focus on the principle of proportionality when it comes to coercive means. The principle of proportionality is essential for the constitutional legitimacy of interferences with fundamental rights. It plays a vital role, limiting and binding authorities exerting their competences on the one hand, and granting certain rights and strengthening the position of the affected person, on the other.

As a cornerstone of the Austrian Constitution, the principle emerged out of the jurisdiction and of doctrinal development. It is seen as general objectivity, as an element of equality before the law[253] and additionally it does have elements of the freedom from

---

249 BMJ/BMI (2008), p. 68.

250 cf. Case of Handyside v. The United Kingdom, judgment of 7 December, 1976 (Application no. 5493/72), para. 58.

251 This means nothing else than that the preconditions which have to be fulfilled are more strict – thus a serious interference requires a serious crime to be investigated, e.g. homicide etc; cf. in this respect as well the explanation in the chapter of this thesis on surveillance of data and communication.

252 In the context of an RFI it seems or at least it could be argued that a covert investigation constitutes as less harsh interference with the rights of the affected person, as nobody gets knowledge of the investigation, nothing is taken away, no physical items have to be secured/seized etc. However, as the report of the expert group points out precisely there is a different benchmark applied in these circumstances and a covert investigation is always seen as more intensive than an open investigation; cf. BMJ/BMI (2008), p. 69.

253 Art 7 para. 1 of the Austrian Federal Constitutional Law reads: All nationals (Austrian citizens) are equal before the law. Privileges based upon birth, sex, estate, class or religion are excluded. No one shall be discriminated against because of his disability; The Republic (Federation, Laender and municipalities) commits itself to ensuring the equal treatment of disabled and non-disabled persons in all spheres of every-day life; Similar to this the Universal Declaration of Human Rights and its Art 1: All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.

discrimination.[254] In this respect it is to note moreover, that, as the Austrian Constitutional Court ruled,[255] an evaluation of proportionality – thus to see whether the differences lay is a matter of fact – has to take into account the social development.[256] Proportionality is always accompanied by the principle of appropriateness,[257] indicating that acts, whether they are of legislative or executive nature,[258] firstly have to be justified objectively by the public interest. Secondly, they have to be capable to fulfill the intended aim, and thirdly, they have to be modest, which includes the prohibition of excess.

Illustrating a formula for the evaluation whether an interference with human rights is legal or not, it is to say that there has to be an examination of whether

- the actual activity fall into the protected area of the fundamental right
- there is an interference with this protected area of the fundamental right
- there is a legal basis for the interference
- there is a public interest in pursuit
- the activity is appropriate to protect this certain interest
- the coercive measure is proportional[259]

What does this mean for the legitimacy of a remote forensic investigation? Frankly, nothing

---

254 cf. Art 14 Convention for the Protection of Human Rights and Fundamental Freedoms stating that [t]he enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, color, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status; furthermore the attempts by the European Communities in Art 12 EC Treaty, Art 13 Treaty of Amsterdam, or the Council Directives no. 2000/43/EC implementing the principle of equal treatment between persons irrespective of racial or ethnic origin; no. 2000/78/EC establishing a general framework for equal treatment in employment and occupation; and no. 2004/113/EC implementing the principle of equal treatment between men and women in the access to and supply of goods and services; as well as Directive 2002/73/EC of the European Parliament and of the Council on the implementation of the principle of equal treatment for men and women as regards access to employment, vocational training and promotion, and working conditions.

255 cf. the ruling in regard to the entitlement to a pension of widowers in VfSlg 8871/1980 or the decision in respect to an unequal pensionable age in VfSlg 12567/1990.

256 Meaning that provisions seen originally as compliant with equality alter in a way so that they become inconsistent with the constitution (they become invalid); this is especially true in regard to the alteration of the social role model of men and women.

257 As Funk points out, these maxims were developed by the recent jurisdiction of the Austrian Constitutional Court and have limited to a large extend the frame for the Austrian legislator as well as they abolished numerous constraints; cf. Funk (2007), MN 412, p. 351; cf. furthermore, BMJ/BMI (2008), pp. 68-69 stating that appropriateness means the technical capability to conduct an RFI in an accurate way.

258 BMJ/BMI (2008), p. 65.

259 cf. Walter, Mayer (2007), MN 1343, p. 633; for further details in respect to the principle of proportionality please cf. below, the chapter of this thesis on the surveillance of data and communication.

much, as it is nothing else than a coercive means and has to simply fulfill the criteria mentioned above. Thus, from a general point of view, if public interest is prevailing over the interest of a suspect – i.e. the suspect's right to privacy – the method could be used in situations when all the other preconditions are also given.[260]

3.2.4 Federation vs. Federal States (Laender)

Due to the fact that an RFI can be established for the three different purposes and that it faces the requirements pointed out by the Ministers of Justice and of the Interior as illustrated above, the conducting of an RFI is primarily for the solution and only secondly for the prevention of criminal acts. According to the Austrian Federal Constitutional Law there are two possible basis for an RFI to be implemented successfully in order to empower the security agencies to conduct an RFI: the fields of criminal matters, dealing with the solution of a crime and security police, handling the maintenance of security.[261]

Due to the already mentioned federal structure of Austria involving a division of competences between the federal States (Laender) and the Federation as such, it is mandatory to have a look who is appointed to govern this matter. In general, the division of competences in Austria among the different players is regulated by Art 10 to Art 15 of the Austrian Federal Constitutional Law.[262]

- First of all there is Art 10 para. 1 no. 6 of the Austrian Federal Constitutional Law stating that the Federation has the power of legislation and execution in criminal law, meaning besides substantive also procedural matters in the field of criminal law.[263]
- Second of all, Art 10 para. 1 no. 7 of the Austrian Federal Constitutional Law deals with the maintenance of peace, order and security including the extension of primary assistance in general.

---

260 Hence only for the solution or prevention of certain serious crimes (punishable by imprisonment for a minimum period of ten years), or targeted against criminal organizations or terrorist associations.

261 Regarding the difference please cf. below.

262 In order to interpret these provisions several different 'theories' were established, such as the theory of fossilization the theory of point of view (German: Gesichtspunkttheorie), or the theory of allowance; cf. Walter, Mayer (2007), MN 295-9, pp. 173-177.

263 cf. for further clarification, the principle of adhesion concerning administrative proceedings and especially in respect to penal provision in administrative law, Walter, Mayer (2007), MN 259, pp. 151-152; as well as Mayer, Heinz, Das Österreichische Bundes-Verfassungsrecht, Kurzkommentar (2004), 4th edition, p. 32.

This means nothing else than the Federation is in charge for legislative acts, the performance in the field of criminal law and for the maintenance of inter alia security. However, that is not the whole truth because the Federation is not just competent in these fields, it is also liable for the functioning of criminal justice and the preservation of stability, order and security.

The Austrian legislator's intention is now to introduce into this framework of provisions the already described method of an RFI. Due to the fact that– the Federation is in charge for all legislative acts in this matter, the legislator could do one of two things: Firstly, it could amend federal codes, or secondly it could initiate a new Act in order to establish this new investigative method. Generally speaking, there is no difference in a qualitative sense between these two law-making procedures. The only thing the legislator has to do is to find and define the 'right' code into which the new provisions would fit the best. In regard to the actual intention of the Austrian government of implementing this method into the legal framework and due to the intended empowerment of law enforcement and police agencies, there are only two codes potentially qualified to host the new regulations, i.e. the Austrian Code of Criminal Procedure and the Austrian Security Police Act.

3.2.5 Criminal Police vs. Public Security Police

For comprehension purposes a clarification has to be made at this stage: before illustrating the mentioned legal documents, the Austrian system of security agencies aka police has to be explained in some detail.

The common use of the term 'police' can generally mean two different things, namely police in a functional or in an organizational sense. These two meanings refer in the first instance to the task of the averting of dangers through the exercise of direct administrative power and compulsion[264] and in the second instance to police as all agencies and officers occupied with this task and consequently labeled as police by the Austrian legislator.[265] Police, no matter which task it fulfills, is always carried out by the security agencies. This means that the

[264] according to Art 129a Austiran Federal Constitutional Law.
[265] Wiederin, Ewald, Einführung in das Sicherheitspolizeirecht (1998), MN 71-85, pp. 16-19.

security agencies are dealing with the tasks of the police in the respective area of law.[266]

When it comes to criminal law, criminal police, according to section 18 para. 1 of the Austrian Code of Criminal Procedure, is the authority exercising duties of criminal justice especially in regards to the investigation and prosecution of criminal acts. Section 18 para. 2 defines furthermore the criminal police in its organizational sense stating that the tasks of the criminal police are carried out by the security authorities.[267] Criminal police and its corresponding regional empowerment is governed by the Austrian Security Police Act. The specific empowerment and tasks delegated to the security agencies by the Austrian Code of Criminal Procedure are carried out by the officers of the security agencies. Finally, this provision states that the term criminal police does not simply cover certain functions but it also involves all security agencies as well as their officers (according to para. 2) in the function as criminal police.

In order to maintain public security and due to the rising awareness and grown sensitivity in regard to interferences with fundamental and human rights in the late 1980s, and driven by the fact that the Austrian legal system did not provide any regulation concerning the matter of public security police,[268] a corresponding legal Act was established in the early 1990s. This Act – the Austrian Security Police Act – came into force in May 1993 and has been amended several times so far.[269]

The Austrian Security Police Act regulates the organization of the police administration, and governs the exertion of the public security police according to section 3 of the Austrian Security Police Act. The exertion of public security police involves the maintenance of peace,

---

266 In this regard cf. as well the chapter on the relationship between criminal police and public security police below.

267 according to Art. 10 para. 1 no. 6 of the Austrian Federal Constitutional Law.

268 The Austrian Constitutions of 1918 and 1920 created rather a fragmentary system of regulations in respect to security police while the amendment of the Constitution in 1929 (Federal Law Gazetta 392) brought an empowerment of the States police function, as it transferred, inter alia, the competence in legislation and execution in this matter from the Laender to the Federation; cf. especially in this regard Art. 10 para. 1 no. 7 Federal Constitutional Law empowering the Federation to legislation and execution in the maintenance of peace, order and security (version 1929); cf. especially Adamovic, Ludwig, Grundriss des österreichischen Staatsrechtes (1927), p. 357; However, despite two attempts for codification (1968 and 1973), there were no sufficient regulations either in regard to the organization or the tasks of the security police; cf. Funk, Bernd-Christian, Das neue Sicherheitspolizeirecht – Kodifikation und Reform einer klassischen Verwaltungsmaterie, JBl 1994, footnote 11. as well as Hauer, Andreas, Keplinger, Rudolf, Sicherheitspolizeigesetz (2005), 3rd edition, pp. 35 et seq.and Wiederin (1998), MN 1-70, pp. 1-15.

269 For a brief but comprehensive overview please cf. Hauer, Keplinger (2005), pp. 35 et seq.

order and security, with the exception of the local public security police,[270] but includes the extension of primary assistance in general.[271] Police administration, in this context, refers to the general public security police, matters pertaining to personal status, including the registration of births, marriages and deaths, and change of name, aliens police and residence registration. Furthermore it deals with matters pertaining to weapons, ammunition and explosives, and the use of fire-arms, as well as press affairs and matters concerning the right of association and assembly.[272] Security agencies working within the framework of the Austrian Security Police Act are called public security police.

3.3 Substantive Criminal Law

Despite the fact that this thesis is primarily concerned with (criminal) procedural law, there are important substantive law provisions in the Austrian legal code related to this topic as well. Therefore, a brief survey of the related regulations and their significance in regard to the aim of this dissertation will be given. Not only do these provisions deal with computer related criminal acts but they also show basic principles concerning the handling of such criminal acts. This overview is given in order to show that everybody – thus even the security agencies – would commit a criminal act if they would conduct an RFI without legal empowerment to do so.

3.3.1 The Convention on Cybercrime

The most important (international) framework occupied with computer crime is the Convention on Cybercrime. The Convention can be signed by the member States of the Council of Europe and also by non-member States having participated in its elaboration. It went into force in July 2004. The related preparatory work until it was signed took already 12

---

270 German: lokale Sicherheitspolizei; According to Art 15 para. 2 Federal Constitutional Law local public security police is that part of public security police which exclusively or preponderantly affects the interests of the local community personified by the municipality and which, like preservation of public decency and defense against the improper creation of noise, can suitably be undertaken by the community within its local boundaries.

271 cf. already above and Art 10 para. 1 no. 7 of the Austrian Federal Constitutional Law.

272 according to section 2 para. 2 Security Police Act

years[273] and was characterized by massive objections of civil rights groups, especially when it came to human rights and data protection issues. This international treaty is the first one on crimes committed via the Internet and other computer networks and also contains a series of powers and procedures. The main intention behind it is to harmonize criminal policy in regard to cybercrime by adopting the appropriate legislation and to foster international cooperation between the member and non-member States of the Council of Europe.[274]

Chapter 1, Art 1 offers good and comprehensible definitions and use of terms of the convention's activities, whereas Chapter 2, section 1 covers criminal acts against the confidentiality, integrity and availability of computer data and systems (Art 2 – Art 6), computer-related offenses (Art 7 and 8), content-related offenses (Art 9) and offenses related to infringements of copyright and related rights (Art 10). Furthermore, it is to state that special emphasis was put on securing of evidence, in particularly on traffic data (Art 14 – Art 22). The Articles 23 to 35 are an attempted to fill potential gaps in the European Convention on Mutual Assistance in Criminal Matters[275] or other bilateral treaties. In this regard the efforts to improve the securing and transmitting of connection data should be mentioned.[276]

The Austrian way of handling computer related crime was based on this convention. With an amendment of the Criminal Code in 2002,[277] the Austrian Federal Council introduced inter alia the main substantial provisions in regard to cybercrime. Following these provisions are presented briefly:

---

273 Starting with recommendation No R (89) 9 on computer-related criminal acts which offered guidelines regarding the definition of certain computer crimes, the Council of Europe took several time the initiative for a harmonization in the field of IT-technology. However, it was not until 1996 when an international commission of experts was set up to elaborate a convention dealing with substantial criminal law concerning telecommunication and IT services. cf. further Schwarzenegger, Christian, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001, in Donatsch/Forster/Schwarzenegger (Hrsg), FS Trechsel (2002), p. 309.

274 Note, that the preparatory work for the harmonization was also joined by experts from the US, Canada and Japan.

275 cf. <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=030&CL=ENG> retrieved 8 October, 2009.

276 cf. Schwarzenegger (2002), p. 311.

277 Federal Law Gazette I No. 134/2002 (BGBl I 2002/134) - Bundesgesetz, mit dem das Strafgesetzbuch, die Strafprozessordnung 1975, das Strafvollzugsgesetz, das Suchtmittelgesetz, das Gerichtsorganisationsgesetz, das Waffengesetz 1996, das Fremdengesetz 1997 und das Telekommunikationsgesetz geändert werden (Strafrechtsänderungsgesetz 2002)

3.3.2 Penalized Behavior

3.3.2.1 Hacking and the Austrian Criminal Code
Illegal Access to a Computer System
Section 118a of the Austrian Criminal Code

There was a big discussion at governmental level regarding the relation between the harms and benefits of hacking attacks, especially regarding the question of whether hacking should be made a criminal offense. This is also true for the negotiation regarding the elaboration of the Convention on Cybercrime (CCC). In its Article 2, the final Convention deals with illegal access to computer systems. It is stated that the signing parties of this treaty (countries) shall adopt legislative measures to protect the confidentiality, integrity and availability[278] of computer systems and data. This criminal activity can be seen as the starting point for further, more dangerous forms of computer related offenses. Thus it was intended to cover already such preparatory acts under criminal law in order '[…] *to give additional protection to the system and the data at such an early stage* […].'[279]

Important to note in this context is the requirement of illegality; this means that the act in question has to be committed without any legal right. This seems prima facie consequently, however, this implements that a person who was hired by the owner of a computer system to break into this system would not commit a criminal act! For instance, it would not be illegal, if a 'hacker' hacked into a system with the aim of authorized testing or protection of the targeted computer system.[280] In addition, the Explanatory Report of the CCC declares that the experts who created this legal framework were aware of the problems that occurred due to the broad approach of Article 2 CCC. In paragraph 49 it is stated that a conviction may not always be appropriate[281] and that the various member countries had already developed a narrower approach, which required supplementary qualifying circumstances. Furthermore, it is mentioned that Parties to the CCC can implement any or all of the following qualifying elements:[282]

---

278 cf. Explanatory Report, Convention on Cybercrime, para. 44.
279 cf. Explanatory Report, Convention on Cybercrime, para. 45.
280 cf. Explanatory Report, Convention on Cybercrime, para. 47.
281 e.g. if there are circumstances […] where no dangers were created by the mere intrusion or where even acts of hacking have led to the detection of loopholes and weaknesses of the security of systems.
282 This means that in order to have a committed offence, all these circumstances (elements of an offence) have to be fulfilled.

- infringing security measures
- special intent to obtain computer data
- other dishonest intent that justifies criminal culpability or
- the requirement that the offense is committed in relation to a computer system that is connected remotely to another computer system[283]

Austria, as a signing member of this treaty, has implemented Article 2 into its Criminal Code under section 118a. When it came to defining a targeted computer system, Austrian legislator followed the wording of the CCC, stating in Art 1 lit a, that a '*computer system means any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*.' Austria implemented this definition in section 74 para. 1 no. 8 Austrian Criminal Code. Such devices can be hardware or software, thus processing units, video screens as well as programs and files, developed for automatic processing of digital data.[284] A person is already committing an illegal access if gaining only partly access to a computer system.[285]

With respect to computer data Austria's definition in section 74 para. 2 Criminal Code is in line with the CCC defining in its Art 1 lit b computer data as '*any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*'.[286] Thus, there are no restrictions to pure written data.[287]

Access gaining persons do not commit a criminal act if they have exclusive authority from the computer's owner/user to access a system. Hence, the act must therefore be committed without permission/approval.[288] Note that problems may arise in circumstances where computer systems are not operated by one single user, but rather by more people (shared desktop) or within the relationship of employers and their network administrators, for instance if the latter gain access to their boss' private e-mails. Hence, there is a difference between the power of disposition over a computer and the power of disposition over the data stored on it.

---

283 cf. Explanatory Report, Convention on Cybercrime, para. 50.
284 cf. Explanatory Report, Convention on Cybercrime, para. 23.
285 cf. as well Reindl-Krauskopf, Susanne, WK-StGB section 118a, MN 8 and 9.
286 cf. further Explanatory Report, Convention on Cybercrime, para. 25.
287 cf. Schwarzenegger (2002), p. 315.
288 cf. further Reindl-Krauskopf, WK-StGB, section 118a, MN 10.

Even though both powers may correlate that is not necessarily always the case.[289]

In order for an action to be a criminal offense, the suspect has to actively be gaining access to a system.[290] Thus, access means the actual entering of the whole or any part of it, such as hardware or stored data of the system installed, directories or content-related data. Access to a system is obtained as soon as the offender can operate actively within the computer system.[291] Thereby the offender has to overcome[292] special security[293] measures within the computer system. These security measures are only part of the computer system if they are in close relationship with the system. Examples for such measures are password detection when booting a computer or an installed firewall.[294] Important to note in this context is that measures which are in no direct relation to the access to a computer system, such as the locking of a room in which a system is located or an alarm system, are not a specific security measure.[295] To overcome security measures means that a person has to surmount or alter such a measure. In most cases this is done through the alteration of software, the removal of encryption or the installation of special software, such as Trojan horses etc. Unlawfully obtain passwords are also covered as a password scam – thus testing various passwords until the right is found – is regarded as overcoming of a security measure as well.[296] However, a person using failures of the system, as for instance failures of the operation system, constituting general failures or gaps in the system, is not be seen as such an overcoming. This is, on the other hand, only true as long as an offender does not use this systematic failure in order to alter or manipulate a specific security measure.[297]

---

289 cf. in this respect as well Reindl-Krauskopf, WK-StGB, section 118a, MN 10, 12; concerning the actual legal status of the holder of the right of disposal please cf. Reindl-Krauskopf, WK-StGB, section 118a, MN 14-8.

290 cf. further Reindl, Susanne, Computerstrafrecht im Überblick (2004), p. 14; as well as Reindl-Krauskopf, WK-StGB, section 118a, MN 20.

291 cf. Explanatory Report, Convention on Cybercrime, para. 46.

292 Note in this context that since the latest amendment of the Austrian Criminal Code it is not necessary anymore to infringe security measures rather than just to overcome them; cf. Reindl-Krauskopf, WK-StGB, section 118a, MN 26.

293 Note in this context that only safeguarded systems are protected by section 118a of the Austrian Criminal Code. Persons who did not protect their systems against any illegal access are not covered; cf. Reindl-Krauskopf, WK-StGB, section 118a, MN 22.

294 cf. further Reindl (2004), p. 15; in respect to password detection Reindl-Krauskopf, WK-StGB, section 118a, MN 23.

295 cf. Fabrizy, Ernst, Foregger, Egmont, StGB samt ausgewählten Nebengesetzen, Kurzkommentar (2006), 9th edition, section 118a, p. 373; EBRV 1166 BlgNR XXI GP, p. 24

296 cf. as well Reindl-Krauskopf, WK-StGB, section 118a, MN 27 and 28.

297 cf. as well above in the chapter of how to conduct an RFI; and Reindl-Krauskopf, WK-StGB, section 118a, MN 29.

Another important aspect of the Austrian solution regarding hacking is that section 118a Criminal Code states several special requirements regarding the offenders malice. The mental element of the criminal act entails that the offender acts with the intention (dolus directus specialis[298]) to spy (to gather knowledge),[299] to use the gathered data[300] and with the intent to receive profits or to harm somebody.[301] Moreover, it is to state that in Austria a hacker can only be prosecuted if the victim authorizes the law enforcement agency to do so. This regulation is mentioned under para. 2 and takes into account that hacking attacks can improve the security of computer systems through discovering gaps and backdoors.[302] Thus, section 118a of the Austrian Criminal Code does not represent a criminal act ex officio, which means public prosecutors are not able to prosecute the criminal acts by themselves alone. The authorization of at least a second person – in most cases one of the victims – is needed in order to prosecute a hacker. This means that the victim of a criminal act is not a victim per se, rather than the person who was the target of an attack decides whether it wants the offender to be prosecuted. It can be easily imagined that the owners of the computer system could appreciate the attack (as well as the subsequent suggestion and advice), which revealed the security vulnerability of their system and now they are able to improve it in an appropriate manner.

The establishment of section 118a of the Austrian Criminal Code was necessary since Austria had no corresponding 'hacking provision' in place. There have been attempts to criminalize such actions but the legislator always added some special requirements for the illegality. For instance, even prior to the introduction of the provision, it was already illegal to access a computer system[303] without permission, but additionally a special intention had to be present. Sections 148a and 126a of the Austrian Criminal Code claim that besides the illegal gained access, the intention of the offender to enrich themselves or to harm somebody make the

---

298 according to section 5 para. 2 of the Austrian Criminal Code.

299 cf. as well below the demanded intention for the prosecution according to section 119 of the Austrian Criminal Code.

300 This means the required intention to use the gathered data implies that criminals intend to use it by themselves, to forward the data or to make the data publicly available; cf. Reindl-Krauskopf, WK-StGB, section 118a, MN 36.

301 There is the need for the actual offenders' intention to enrich themselves or anybody else; cf. Reindl-Krauskopf, WK-StGB, section 118a, MN 37.

302 cf. Explanatory Report, Convention on Cybercrime, para. 49, stating […] that the broad approach of criminalization in the first sentence of Article 2 is not undisputed. Opposition stems from situations where no dangers were created by the mere intrusion or where even acts of hacking have led to the detection of loopholes and weaknesses of the security of systems.

303 cf. sections 148a and 126a of the Austrian Criminal Code.

action a capital offense. Furthermore, operating restrictions and business secrecy, data used for the commercial circle, of sections 122 – 124 Criminal Code were no real safeguard against hacking. This means that attacks of hackers lacking such intentions were not considered illegal until the adoption of this regulation.

3.3.2.2 Infringement of the Telecommunication Secrecy Section 119 of the Austrian Criminal Code

The old version of section 119 of the Austrian Criminal Code was devoted to old-fashioned telecommunication granting protection for information while it was being transmitted from one place to another. Section 119 is the corresponding criminal provision to the constitutional telecommunication secrecy[304] of Art 10a Basic Law on the General Rights of Nationals 1867, stating that '*Telecommunications secrecy may not be infringed*'. An amendment of this provision was necessary mainly due to advancing technologies and because of the standards emerging of the CCC.[305] The new version covers not only messages/communication transmitted via customary telecommunication but also the conveyance of information in computer systems.[306] The provision deals exclusively with content data, of a message.[307] The criminal act contains the use of devices connected or attached to a telecommunication facility or a computer system. Such devices do not have to be physical, even computer programs can be subsumed under this expression.[308] Any technical facility, capable to provide knowledge of the content of any communication transmitted via this telecommunication facility or this computer system to an outsider,[309] is covered by the expression.[310] It does only penalize the use of these devices, meaning that it is not necessary that the user of the device also installed it,[311] or that the simple use of such devices is already the actus reus. It is therefore not

304 cf. also Lewisch, Peter, WK-StGB section 119, MN 5a.
305 cf. Fabrizy, Foregger (2006), section 119, p. 374.
306 cf. Reindl (2004), p. 28.
307 Each content of a communication is covered, thus it is not necessary that there is a special character of secrecy involved. The intention of the offender has to be to gain unauthorized knowledge about the content of any message/communication transmitted via a telecommunication facility or computer system; cf. in this respect further more; cf. Lewisch, section 119, MN 9a, 9b.
308 Computer programs designed to send copies of all in- and outgoing e-mails to the offender are covered as well; cf. Reindl (2004), p. 29.
309 Meaning somebody not intended to gain unauthorized knowledge of the content of the communication. Thus, a person neither originator nor intended receiver of a communication.
310 cf. furthermore the comprehensive illustration – especially also in respect to WLANs – at Lewisch, section 119, MN 4 and 4a.
311 cf. Lewisch, section 119, MN 2, 3, 8.

necessary that the offender, or somebody else[312] actually gained knowledge about the content of the message in transmission[313] but in respect to the intention, it is necessary to have such purposes (dolus directus specialis). Remarkable in this context is also the fact that the use of devices is not limited to real time use, rather than even recording devices are covered as well, thus penalized by section 119 of the Austrian Criminal Code.[314] Contrary to the former wording of section 119, the simple attaching of, or the establishment of the recipient status of the device is not punishable anymore.[315]

3.3.2.3 Illegal Interception of Data
Section 119a of the Austrian Criminal Code

This provision deals with two different offenses:

In respect to the first offense, it is to say that if an act is not punishable according to section 119 of the Austrian Criminal Code it might be possible that one could at least be fined according to section 119a of the Austrian Criminal Code. The latter is therefore something like a backup for the first, as the first handles only messages and information whereas the latter deals with any types of data. Principally, the illustrations given in the context of an infringement of the telecommunication secrecy apply as well in this context. Thus, offenders have to use any spying devices,[316] enabling them to spy on communications before they can be punished. These spying devices have to be physically attached or connected to a foreign computer system[317]. The offenders criminal intend has to be dolus directus specialis. Moreover, they intentionally gain access to acquire unauthorized knowledge of the content of any data, or to provide such knowledge to somebody else, who is equally unauthorized. Unlike section 119 of the Austrian Criminal Code – which deals with verbal communication exclusively – section 119a of the Austrian Criminal Code handles spying attacks on any data.[318] Furthermore, it has to be established that any illegally obtained information is used to

---

312 Meaning that there has to be the intention to spy on the message in transmission. This implements the intention that either offenders themselves or somebody else gain knowledge of the message. From the quality of the offense there is no actual difference whether offenders themselves gain it or whether they want to grant this knowledge to somebody else; cf. in this respect as well Lewisch, section 119, MN 2.

313 cf. Reindl (2004), p. 29 as well as Lewisch, section 119, MN 7.

314 cf. Lewisch, section 119, MN 5.

315 cf. Fabrizy, Foregger (2006), section 119, p. 375.

316 cf. Reindl-Krauskopf, WK-StGB, section 119a, MN 4.

317 unlike section 119, section 119a of the Austrian Criminal Code deals only with computer systems and not like the former with both, telecommunication facilities and computer systems.

318 cf. Reindl-Krauskopf, WK-StGB, section 119a, MN 7, 8.

acquire monetary profits or harm somebody financially or personally.[319]

The second offense penalized by section 119a of the Austrian Criminal Code goes directly back to the CCC. The CCC in its Explanatory Report states under para. 57 that

> '*[t]he creation of an offense in relation to 'electromagnetic emissions' will ensure a more comprehensive scope. Electromagnetic emissions may be emitted by a computer during its operation. Such emissions are not considered as 'data' according to the definition provided in Article 1. However, data can be reconstructed from such emissions.*'

A computer system radiates electromagnetic waves while processing and it is easily possible to reconstruct this particular data. If there is no transmission of any kind of data, there is also no infringement of any transmission secrecy. However, such behavior constitutes an infringement with privacy and therefore it was necessary to criminalize such behavior as well. While, from a technical point of view, there are numerous ways to collect and gather electromagnetic emissions, this is unimportant in the legal context, meaning that the collection is penalized no matter how the data was collected.[320]

With regards to the intention (dolus directus specialis) of an offender committing this criminal act, the Austrian legislator governed, similar to the other provisions in this context, that the mental element consists of the aim to obtain knowledge and to receive a monetary gain, or cause a property loss of the attacked (or somebody else).[321] However, as Reindl-Krauskopf points out, there are some additional things to keep in mind. She argues that in respect to the spying intention of the offender, it is not sufficient that the offender simply gathers emissions in order to reconstruct data the victim types into its computer and saves it afterward. On the contrary, it is necessary that the offender tries to gather data intended to be or already being transmitted.[322]

---

319 cf. already the illustrations in this respect in the context of section 118a of the Austrian Criminal Code, above.

320 cf. in this respect and especially for the context of WLAN's Reindl-Krauskopf, WK-StGB, section 119a, MN 10.

321 cf. already above the illustrations in this respect in the context of section 118a of the Austrian Criminal Code.

322 Reindl-Krauskopf, WK-StGB, section 119a, MN 13.

In this respect and for the completeness of content, it is to say that besides section 119a there is another provision dealing with communication and data; section 120 (2a) of the Austrian Criminal Code is intended to protect the confidentiality of communications. It penalizes the recording of communications,[323] or the granting of access to the communication to unauthorized persons, or the making communication publicly available. Important in this context is that the communication is not intended to be received by the person committing the criminal act. Examples are situations where a person forwards or publishes a misguided e-mail, which he received unauthorized.[324]

3.3.3 Offenses Following Hacking Attacks

3.3.3.1 Damage of Data
Section 126a of the Austrian Criminal Code

The Austrian Criminal Code provides provision that deal with the potentially negative outflows of an attack. These are mainly criminal acts against property and were originally established to deal with criminal property damage. The newly created regulations, however, do not handle actual damages to physical objects but rather damage to electronic data. Thus, if an offender physically destroyed a disk or a CD – they would be prosecuted for criminal property damage. However, these disks may contain data that has a higher value than the actual media on which they are stored. In recognition of this value, the Austrian legislator implemented section 126a – damage of data – into its Criminal Code. Art 4 CCC – Data Interference deals with the same arguments.

The cause of damage to any electronic processed data,[325] already transmitted data [326] as well

[323] Note that a desultory recording of communications would not be covered; cf. Lewisch, Peter, Reindl-Krauskopf, Susanne, WK-StGB section 120, MN 31b.

[324] for a detailed overview on this provision, please cf. Lewisch, Reindl-Krauskopf, WK-StGB section 120, MN 31a-h; as well as Reindl (2004), p. 31.

[325] According to section 4 no. 9 of the Austrian Federal Act concerning the Protection of Personal Data the processing of data means the collection, recording, storing, sorting, comparing, modification, interlinkage, reproduction, consultation, output, utilization, committing, blocking, erasure or destruction or any other kind of operation with data of a data application by the controller or processor except the transmission of data.

[326] According to section 4 no. 11 of the Austrian Federal Act concerning the Protection of Personal Data, the committing of data means the transfer of data from the controller to a processor.

as committed[327] data is punishable by law. There is no difference whether this data is personal or not; even generic computer programs are covered by the Austrian Criminal Code as data.[328] Any data on a hard drive or any other storage device that is either processed, transmitted or committed,[329] is protected by this provisions. Data can only be damaged by people who do not have the authority to do so. Thus, if somebody does have a position similar to that of an owner of the data, they can not commit the criminal act.[330] In this respect the Explanatory Report under para. 62 mentions that an act is only punishable if committed 'without right'. However, it is necessary that this has to be interpreted quite carefully and that certain activities inherent in the design of networks or commonly operating or commercial practices authorized by the owner or operator are 'with right' and therefore shall not be criminalized.[331] This means that nobody can be liable for hacking into their own computer systems, and nobody can be charged for destroying their own, private data. This is reasonable because there is no public need to criminalize such behavior.

It is important to note that the damaged data must have some kind of monetary value,[332] otherwise we cannot speak of damage to data. In order to assess the value or damage of data one applies the same criterion as one would in the 'real', physical world.[333] There are two different kinds of punishable acts when it comes to the destruction of data: the actions, which make data useless[334] and activities concerning suppression of data. Thereby the owner of the data is impaired and has to bear a financial loss, constituted by the amount of money he has to expend in order to replace the damaged data.

The Austrian Criminal Code states that the offender has to have the intention (dolus

---

327 According to section 4 no. 11 of the Austrian Federal Act concerning the Protection of Personal Data, the transmission of data, the transfer of data of a data application to recipients other than the data subject, the controller or a processor, in particular publishing of such data as well as the use of data for another application purpose [Aufgabengebiet] of the controller.

328 cf. Reindl-Krauskopf, Susanne et al, WK-StGB section 74, MN 63-6.

329 Otherwise they would not be in existence; cf. Bertel, Christian, WK-StGB section 126a, MN 1.

330 cf. Reindl (2004), p. 19; as well as Bertel, WK-StGB, section 126a, MN 2.

331 for example: the testing or protection of the security of a computer system, or the reconfiguration of a computer's operating system that takes place when the operator of a system acquires new software (e.g., software permitting access to the Internet that disables similar, previously installed programs); cf. further Explanatory Report, Convention on Cybercrime, para. 62.

332 cf. for details Reindl (2004), pp. 20-23.

333 e.g. the exchangeable value (Tauschwert), utility value (Gebrauchswert), costs of restitution (Wiederherstellungskosten); cf. Reindl (2004), pp. 21-22.

334 Involving activities such as alteration or deletion.

eventualis)[335] to alter, delete, etc data in order for the offender to face conviction.

3.3.3.2 Interference of the Functionality of a Computer System Section 126b of the Austrian Criminal Code

This provision deals with the extension of a damage of data, as it evaluates the range of the damage. While the previously discussed provision is mainly concerned with attacks on a limited number of computers, this one deals with large scale attacks. It was not until the CCC was set up that Austria implemented such a regulation. Before that, there was just partial protection against such 'denial of service' attacks, through the Austrian Telecommunications Act.[336] A 'denial of service' (DoS) attack is an attack on a computer system that prevents or substantially slows the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system.[337] The Explanatory Report names spamming explicitly as a major threat to computer systems.[338]

Art 5 CCC criminalizes the intentional obstruction of the lawful use of computer systems. It protects the interest of operators and users of a computer or telecommunication system so it may be used accordingly. Furthermore, it punishes actions, which seriously prevent[339] the proper functioning of such systems. The term 'serious' is explained in further detail under para. 67 in the Explanatory Report and it is up to the signing parties on how they are going to define it. Section 126b of the Austrian Criminal Code regulates that an attack is seriously hindering, if a computer system collapses completely or if its speed is so substantially reduced that the practical value for the user is like a complete breakdown. Furthermore, the duration of the impediment can be used to calculate the seriousness of the attack.[340] Actual damage or the destruction of the computer system is not required.

---

335 according to section 5 para. 1 of the Austrian Criminal Code.

336 The Austrian public and administrative law provided some criminal regulations and via section 104 para. 3 no. 24 TKG (old version) it was possible to charge an attacker with ATS 500.000,-- if there has been a infringement against the prohibition of spam (section 101 TKG (old version); cf. further: Plöckinger, Oliver, Internet und materielles Strafecht – Die Convention on Cyber-Crime, in Plöckinger/Duursma/Helm (Hrsg), Aktuelle Entwicklungen im Internet-Recht (2002), p. 118.

337 cf. Explanatory Report, Convention on Cybercrime, para. 67.

338 cf. Explanatory Report, Convention on Cybercrime, para. 69.

339 Such hindering must take place by inputting, transmitting, damaging, deleting, altering or suppressing computer data; cf. Explanatory Report, Convention on Cybercrime, para. 66.

340 cf. Fabrizy, Foregger (2006), section 126b, pp. 392-393; in respect to the duration please cf. Reindl-Krauskopf, Susanne, WK-StGB section 126b, MN 9-13, 18.

The simple obstruction of the system is already punishable.[341] A person is considered breaking the law by simply entering data into, or transmitting data to a computer, no matter by what means.[342]

Concerning the mental element of the criminal act it is governed that the offender's intention (dolus eventualis) has to be focused on such hindering.

3.3.3.3 Misuse of Computer Programs or Access Data Section 126c of the Austrian Criminal Code

Not only was there the intention to punish actual hacking as a criminal activity but also there were ambitions to establish regulations concerning preparatory works for those acts. There was the intention to create a framework dealing with circumstances happening during the preliminary stages of the criminal act.

Art 6 CCC penalizes, under its heading 'misuse of devices', hacking tools, or better their production, sale, procurement for use, their import or distribution or the otherwise making available of such devices. According to the Explanatory Report, Art 6 focuses mainly on tools with the primary objective of hacking[343] and not dual-use devices. The latter are tools capable of conducting legal as well as illegal activities and neither their production nor their possession or (legal) use should be criminalized. This means that Art 6 CCC makes the distinction whether something is legal or not only on the basis of the criminal intentions of an unlawful act. The intention of the possessors or creators of these devices is the only 'thing', which makes the possession or creation of them illegal. There has been a long debate regarding this regulation and the final outcome is more or less a compromise and states that the possession or the creation of the devices has to be with the malice to commit a criminal act named in Art 2 – 5 of the Convention on Cybercrime.[344] Programs and tools created for the

---

341 However, short term delays are not covered; cf. Reindl-Krauskopf, WK-StGB, section 126b, MN 9.

342 cf. Reindl-Krauskopf, WK-StGB, section 126b, MN 14-6.

343 Tools objectively designed, or adapted, primarily for the purpose of committing an offence; cf. Explanatory Report, Convention on Cybercrime, para. 73; cf. as well Reindl-Krauskopf, WK-StGB, section 126c, MN 2.

344 Thus there has to be the intention to commit an Illegal Access (Art 2), an Illegal Interception (Art 3), a Data Interference (Art 4) or a System Interference (Art 5); cf. Explanatory Report, Convention on Cybercrime, para. 73 and 76.

authorized testing or the protection of a computer system are not covered by Art 6.[345]

When establishing section 126c of the Austrian Criminal Code, the Austrian legislator followed the standards of the CCC and implemented this preparatory criminal act, punishing in para. 1 no. 2 the production, import, sale, the distribution or the procurement of computer passwords, access codes or comparable data enabling the access to a computer system or a part of it.[346] Important in this context is that section 126c of the Austrian Criminal Code does not only constitute an ordinary offense to criminalize preparatory works, rather than its application is limited to preparatory works in regard to certain offenses. The computer programs[347] have to be capable and intended to be used to commit the criminal act indicated in section 118a, section 119, section 119a, section 126a and section 126c of the Austrian Criminal Code, thus Art 2 - 5 CCC or section 148a, thus computer fraud.

Once again, the Austria legislator demands a conviction for the misuse of computer programs or access data, at least dolus eventualis as mens rea.

3.4 Austrian Code of Criminal Procedure

3.4.1 Introduction

As presented in chapter 1, three different fields of application can be identified for an RFI. First of all, a remote access for search purposes, secondly surveillance of activities and thirdly surveillance of telecommunication. For each of these purposes, security agencies are provided with a broad range of investigative tools. This following chapter will look at these tools in detail in order to show whether an RFI could legally be conducted already. In this context it is to remark that the Austrian Code of Criminal Procedure offers various means of coercive. Not only do they differ in extend and intensity of interference with fundamental or human rights

345 e.g., test-devices (‘cracking-devices’) and network analysis devices designed by industry to control the reliability of their information technology products or to test system security are produced for legitimate purposes; cf. further Explanatory Report, Convention on Cybercrime, para. 77.

346 Note in this context that the penalize activity of a simple possession was introduced later on; cf. EBRV 309 BglNR XXII GP, p. 8.

347 Note that not only computer programs are cover. In addition section 126c of the Austrian Criminal Code governs that 'other comparable devices' or 'access data' are involved as well; cf. in this context Reindl-Krauskopf, WK-StGB, section 126c, MN 8-10.

but also in the puzzling variety of regulations they are obliged to.[348]

3.4.1.1 Criminal Investigation Proceedings

Generally it can be said that a penal proceeding starts when either the criminal police[349] or the public prosecution becomes aware of a criminal act and commences its investigation of this criminal act, which they are obliged to do according to section 2 para. 1 of the Austrian Code of Criminal Procedure.[350] This principle is called ex officio principle and it states that if somebody files a charge, it is not possible for this person to drop this charge. Sections 78 para. 1 and 80 of the Austrian Code of Criminal Procedure state that everybody has the right to file a charge if they have knowledge of a criminal act. This is usually done through the criminal police or it can also be done through the public prosecution itself.[351] The purpose of the investigation proceedings is to examine these charges and the evidence in detail in order to enable the public prosecution to decide whether it should charge the offender or stay the proceedings.[352]

Governed by the general principle of indictment in criminal proceedings,[353] the public prosecution is head of the criminal investigation proceedings.[354] This means that all doing during the investigation proceeding are supervised and directed by the public prosecution. However, public prosecution usually does not concern itself with the investigations very much until the criminal police hands over its final report. The criminal police itself has its own competences whereas the power to direct remains in the hands of the public prosecution.[355]

---

348 The Austrian legal system includes coercive measures conducted spontaneously by the criminal police, directed by the public prosecution and such directed by the public prosecution based on judicial approval; cf. for a brief overview, cf. Bertel, Christian, Venier, Andreas, Einführung in die neue StPO (2006), 2nd edition, MN 145, 146, p. 50.

349 Note in this context that in criminal proceedings the security agency is called criminal police – according to section 18 para. 1 of the Austrian Code of Criminal Procedure this is the authority exercising duties of criminal justice (Art. 10 para. 1 no. 6 of the Austrian Federal Constitutional Law), especially concerning the investigation and prosecution of criminal acts in the sense of this code.

350 Meaning that after either somebody filed a charge or the criminal police started investigations ex officio; cf. Seiler, Stefan, Strafprozessrecht (2009), 10th edition, MN 614 p. 168; furthermore section 1 para. 2 of the Austrian Code of Criminal Procedure.

351 cf. Seiler (2009), MN 615 p. 168.

352 cf. section 91 of the Austrian Code of Criminal Procedure.

353 cf. section 4 of the Austrian Code of Criminal Procedure and the related Art 90 para. 2 of the Austrian Federal Constitutional Law stating that in criminal proceedings the procedure is by indictment.

354 cf. sections 98 et seq. of the Austrian Code of Criminal Procedure.

355 cf. Seiler (2009), MN 623, p. 170.

This means that despite having its own competence to investigate, there is also the obligation to follow directions not only from the public prosecution but also from the court.[356] Section 99 para. 4 of the Austrian Code of Criminal Procedure governs that investigations may be postponed if necessary. It could be the case, for example, that a person involved in the criminal act needs to be tracked down before investigations can proceed. These delays must, however, not result in any serious danger of life, health, physical integrity or freedom of a third person.[357] Such circumstances are mainly given in situations where there are no actual victims – as for instance in respect to organized crime, illegal drug dealing, and smuggling of cigarettes. If, due to such instances, the criminal police decides to postpone its investigation, it is obliged to inform the public prosecution.[358] Furthermore, the criminal police is bound to document its investigations and deliver its final report to the public prosecution after concluding them.

The public prosecution, as head of the proceedings, does have the authority to direct investigations and also conduct investigations itself. The legal ramifications are mentioned in section 20 of the Austrian Code of Criminal Procedure and include the liability of the public prosecution for this stage of the criminal proceedings. Therefore the public prosecution has to decided how much freedom it will grant the criminal police for its investigation.

Nevertheless, it is up to the criminal police of when and how a direction is enforced.[359] While the criminal police is responsible for the conducting of a direction on site,[360] it is the competence of the public prosecution to decide on the appropriate steps (mainly but not always) of the potential end of criminal investigation proceedings. This means that the public prosecution can always close the proceedings, if the gathered information does not constitute a punishable matter of fact[361] or if it can bring charges against somebody because conviction is likely.[362] The decision for each of these steps involves a careful judgment of legal and

---

356 cf. section 99 para. 1 of the Austrian Code of Criminal Procedure.

357 Or without a postponement there would be such threats – cf. section 99 para. 4 no. 2 of the Austrian Code of Criminal Procedure.

358 cf. for further details Pilnacek, Christian, Pleischl, Werner, Das neue Vorverfahren – Leitfaden zum Strafprozessreformgesetz (2005), MN 402 et seq, pp. 79-81 and Vogl, Mathias, WK-StPO section 99, MN 9 et seq.

359 Note that that is not true if the direction of the public prosecution is based on a warrant – thus on the approval of the court. cf. furthermore below.

360 cf. Seiler (2009), MN 641, p. 173; however cf. further below.

361 cf. section 190 of the Austrian Code of Criminal Procedure.

362 cf. section 210 of the Austrian Code of Criminal Procedure.

factual circumstances by the public prosecution.[363]

The third entity in criminal investigation proceedings is a court (judge).[364] One of its main tasks is the approval of coercive. According to section 105 of the Austrian Code of Criminal Procedure, the court has to decide whether the public prosecution's request involving the interference of constitutional protected, subjective rights of an individual is granted. If an intended coercive is in conflict with one of these rights, the public prosecution needs the approval of a court to continue its investigation. Otherwise all taken action would be illegal.

This overview is a summary of the basic ideas behind the Austria way to handle investigation proceedings. However, it failed to state that since the amendment of the Austrian Code of Criminal Procedure,[365] the pre-trial proceedings have changed.[366] According to the new regulations, particularly the defendant was granted more procedural rights than previously. Thereby, Austria abolished a legal gap in the its legal system constituting a violation of Art 6 para. 3 lit c Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights).[367] Granting these defendants rights is the task of the public prosecution and furthermore, it has to ensure that the criminal police's work is according to regulations. The public prosecution can now also be called a relief agency,[368] which means that the management of the proceedings was intensified as well.[369]

To sum up, investigation proceedings involve three authorities: the public prosecution, which functions as head and partner of the criminal police. The court (judge) is occupied with questions of the investigation only on request, ex offico due to a judicial hearing of

---

363 cf. in this respect Bertel, Venier (2006), MN 168, p. 58.

364 e.g. the court is responsible for contradictory interrogations of victims and witnesses of criminal acts (section 165 of the Austrian Code of Criminal Procedure), the reconstruction of a criminal act (section 150 of the Austrian Code of Criminal Procedure) and for the judicial review of the investigation proceedings (sections 106 and 108 of the Austrian Code of Criminal Procedure)

365 In effect since 1 January, 2008.

366 Before the amendment of the Austrian Code of Criminal Procedure the investigation proceedings were generally dividing into criminal 'pre-investigations' (German: gerichtliche Vorerhebungen), ran and organized by the public prosecution; and judicial investigations before trial (German: gerichtliche Voruntersuchungen), ran and organized by the committing magistrate. However, 'pre-investigations' were conducted by the criminal police itself and the danger of suppression of evidence was used to refuse the defendant a contact with an attorney-at-law. This practice is now gone, meaning that defendants have the right to speak with a defending lawyer right from their detention. cf. concerning this special issue; cf. Bertel, Christian, Venier, Andreas, Strafprozessrecht (2004), 8th edition, MN 52 and 242, pp. 17, 63.

367 cf. especially Bertel, Venier (2004), MN 52, 242 and 317, pp. 17, 63, 83.

368 cf. section 106 para. 4 of the Austrian Code of Criminal Procedure.

369 cf. Bertel, Venier (2006), MN 153, p. 53.

evidence[370] and due to section 105 para. 2 of the Austrian Code of Criminal Procedure, and due to an appeal.[371]

3.4.1.2 Receipt of a Warrant

According to section 105 of the Austrian Code of Criminal Procedure, the court has to decide whether the public prosecution's request involving the interference of constitutionally protected, subjective rights of an individual is legitimate.[372] The court has to approve inter alia seizures (section 115 para. 2), or – due to the constitutionally granted right of banking confidentiality – requests concerning information of bank accounts (section 116 para. 3). In addition, the court has to approve requests in respect to searches of houses and locations (section 120 para. 1) and seizures of letters, information about data of a transformation of information, surveillance of messages and optical and acoustical surveillance of persons (sections 134 - 136 of the Austrian Code of Criminal Procedure).

In approving the request of the public prosecution, the court issues the search warrant. Not until then the public prosecution is allowed to give direction to the criminal police.[373] However, in this respect, Bertel/Venier argue that it is possible for the public prosecution to give direction regarding coercive measures with reservation to the court order.[374] Contrary to the legal situation, before the previously mentioned amendment of the Austrian Code of Criminal Procedure, the courts approval is not a writ of mandamus (German: 'Befehl') anymore, rather than an authorization to perform the requested action. The court does not have to consider tactical aspects of criminal procedures, hence the public prosecution is neither obliged to use this authorization actually nor to set a 'contrarius actus' if it abandons to use it.[375]

---

370 according to section 104 of the Austrian Code of Criminal Procedure.
371 cf. section 98 of the Austrian Code of Criminal Procedure.
372 cf. Fabrizy, Ernst, Die österreichische Strafprozessordnung – Kurzkommentar (2008), 10th edition, section 105, p. 232; furthermore cf. Pilnacek, Pleischl (2005), MN 428, p. 87.
373 Note the related critique regarding the double occupation with the direction of the public procedure in Bertel, Venier (2006), MN 165, p. 57.
374 cf. Bertel, Venier (2006), MN 166, p. 58.
375 cf. JAB 406 BlgNR XXII GP, p. 15.

According to sections 101 para. 2 and para. 3 of the Austrian Code of Criminal Procedure, the public prosecution has to request approval of a search etc, if this is needed. This means that the public prosecution and not the criminal police can forward requests to and is in contact with the court. Direct consultation between the court and the criminal police is not intended for criminal investigation proceedings.[376] This also includes that the court is not empowered to adopt coercive measures without a corresponding request from the public prosecution.[377] The written request for approval of a direction has to involve all documents and has to be justified. These obligations include that the public prosecution has to present relevant grounds on which the intended direction is and the corresponding approval has to be based.[378] Not only the request but also the warrant itself has to be justified. These requirements are the basis for some critique, as the Supreme Court ruled that a reference in the approval of the request (the warrant) to the justification in the request (direction to the criminal police) is sufficient.[379] Furthermore, Bertel/Venier argue that the direction can adopt the content of the court order.[380]

Closely related to this is the aspect that a warrant has to say explicitly what the public prosecution is allowed to do – i.e. which directions it is allowed to give. In the case of a search warrant, for instance, this includes a detailed description of what is searched for. [381] Moreover, it has to include a time limit,[382] forcing the public prosecution and the criminal police to conduct the warrant within the given time frame.

Section 101 para. 3 of the Austrian Code of Criminal Procedure further states that after the issuance of a warrant, it is the responsibility of the public prosecution to determine the actual requirement and the appropriate time for conducting the coercive measure.[383] Moreover, this provision states that if circumstances crucial to the approval of the request disappear or alter in a manner so that the establishment of a coercive measure would become illegal, disproportionally or in-expediently, the public prosecution has to abstain from it and inform the court about this new situation. This means that the public prosecution is not allowed to

---

376 Besides certain cases in which the court can use the criminal police in order to conduct further investigations in respect to a request of the public prosecution – cf. section 105 para. 2 of the Austrian Code of Criminal Procedure.

377 Pilnacek, Pleischl (2005), MN 412, p. 83.

378 cf. Fabrizy (2008), section 101, p. 226.

379 cf. Bertel, Christian, Venier, Andreas, Strafprozessrecht (2009), 3rd edition, MN 195, p. 62 and Seiler (2009), MN 644, pp. 174-175.

380 cf. Bertel, Venier (2006), MN 165 p. 57.

381 cf. regarding this requirement especially 13 Os 46/08a.

382 cf. section 105 para. 1 of the Austrian Code of Criminal Procedure – after expiring of the warrant it becomes inoperative; Regulary the judicial search warrant sets a limit between one to three days; cf. Bertel, Venier (2006), MN 237, pp. 84-85; furthermore cf. Fabrizy (2008), section 105, p. 232.

383 cf. regarding this and the corresponding problems between the public prosecution and the criminal police, EBRV 25 BlgNR XXII GP, p. 136.

postpone its directions correlating to the warrant . It would have to refrain from conducting a coercive and request a new approval. This means that a warrant is restricted by certain criteria. The Explanatory Report states objective criteria for such warrants, such as the manner of suspicion or the degree of difficulty of the investigations in general.[384]

As shown, crucial in regard to means of coercive is that they are judicial decisions. Moreover, they can only be implemented if requested by the public prosecution. Concerning this, it is further to note that the criminal police is only empowered to ask the public prosecution whether the public prosecution could request a coercive at the court.[385] The approval of the court – the warrant – establishes the basis for the coercive and defines its frame, border and target. In order to implement such a preventive judicial control of human rights, it is necessary that the court assesses the coercive and the related actual consequences.[386] Only in certain circumstances, if there is potential danger in a delay (periculum in mora), the criminal police is allowed – to use coercive measures without a direction or a corresponding warrant.[387]

3.4.1.3 Court Order

In principal it can be said that if means of coercive have to be based on judicial approval, a court order according to section 86 of the Austrian Code of Criminal Procedure is formally needed.[388]

From a general point of view there are three different decisions a court can issue, namely verdicts, orders and ordinances. This tripartite division (section 35 of the Austrian Code of Criminal Procedure) represents the forms of court decisions as well. While verdicts are decisions issued in an open or closed session in the 'Name of the Republic',[389] the other two forms are decisions issued not in such form. The only real difference between an order and an ordinance lies in the difference of the appeals proceedings, according to sections 87 – 89 of

384 cf. EBRV 25 BlgNR XXII GP, p. 136.
385 cf. section 93 para. 4, 105 of the Austrian Code of Criminal Procedure.
386 cf. EBRV 25 BlgNR XXII GP, p. 136.
387 cf. below.
388 Or at least it has to be justified afterwards by a court order, if the criminal police used it due to danger in delay; cf. furthermore below.
389 Art 82 para. 2 of the Austrian Federal Constitutional Law.

the Austrian Code of Criminal Procedure.[390]

Section 86 para. 1 of the Austrian Code of Criminal Procedure states that, a court order has to include the decision, the grounds of the decision and an explanation on rights of appeal. The decision itself has to involve the direction, the approval or the finding of the court as well as the correlated legal provisions. This means that the court has to clarify exactly what it decides and, in the case that there has been a request, to which extend it approves this request.[391] The explanation must state the actual findings and the legal considerations the decision is based on. In this context it is to remark that orders stating only the provision or reproducing only the legal text of the provision are illegal because they lack actual findings.[392] However, there is no general provision – according to section 270 para. 2 no.5 of the Austrian Code of Criminal Procedure – dealing with the questions of whether and how a court order has to be justified.[393] The explanation of the rights of appeal has to include whether such rights are given, which formalities apply, within which deadline and where the appeal has to be brought in. The proceedings furthermore regulate that an order has to be issued in writing and delivered to the persons entitled to an appeal.

Entitled to an appeal are the public prosecution, the defendants insofar as their interests are directly affected, as well as persons whose personal rights are affected.[394] In addition, if the court order states the proceedings, it has to be delivered inter alia to the criminal police. Concerning the right to appeal it is to mention that an objection against every court order is possible as long as the law does not explicitly revoke that right. The competent instance in this case would be the regional appeals court.[395] Above all, the public prosecution is entitled to appeal if its requests according to section 101 para. 2 of the Austrian Code of Criminal Procedure were not dealt with. This means that the public prosecution can appeal if a requested coercive was not approved by the court. A special right to appeal is granted to

---

390 cf. Fabrizy (2008), section 35, p. 85.

391 cf. Bertel, Venier (2006), MN 124, p. 42.

392 cf. Bertel, Venier (2006), MN 124, p. 42; cf. for the legal necessity of the explanation on rights of appeal EvBl 2008/183.

393 cf. Harbich, Herbert, Der Beschluss im Strafprozess und seine Begründung, in Österreichische Richterzeitung 1977, p. 142; section 270 para. 2 no. 5 of the Austrian Code of Criminal Procedure states regarding the grounds of the decision in a verdict that it shall be announced briefly but firmly, which facts the court accepted to be evident or not evident and due to which reasons the court did so. Furthermore, the court has to state which considerations have guided the solution of the specific legal issue. In the case of conviction the court has to name the found circumstances of aggravation (German: Erschwerungsumstände) and abatement (German: Milderungsumstände).

394 According to section 86 para. 3 of the Austrian Code of Criminal Procedure it is not necessary to issue and deliver the court order, if it was proclaimed orally and the beneficiaries (persons with the right of appeal) abandon their right of appeal.

395 section 87 para. 1 of the Austrian Code of Criminal Procedure.

persons claiming that their subjective rights have been violated by the court during a hearing of evidence.[396]

A warrant can only be issued by the court when requested by the public prosecution in form of a written court order. Both, the request as well as the approval – the actual warrant – have to be based on justifications and include the frame, the borders and the target of that specific warrant. In addition, it is always the public prosecution which is responsible for conducting and the court which is responsible for granting the subjective, personal rights of the affected person.

3.4.2 Search of Locations and Objects

3.4.2.1 General Aspects

According to section 119 para. 1 of the Austrian Code of Criminal Procedure it is admissible to search locations and objects, if it is assumed that there is a person suspected of a criminal act hiding, or that there are objects or traces present to be seized or to be analyzed. A search of objects in the sense of section 119 of the Austrian Code of Criminal Procedure can also be applied for the search of a computer, as a computer as a physical object that can be searched.[397] In this regard section 119 para. 1 refers further to the corresponding definition in section 117 no. 2 of the Austrian Code of Criminal Procedure defining the term search of locations and objects as the search of

a. premises, rooms, vehicles or vessels not publicly accessible, and

b. flats or other locations protected by householder's rights[398] and of objects located in such.

---

396 These appeals are called 'Säumnisbeschwerde' in the case of an appeal of the public prosecution, and 'Maßnahmenbeschwerde' in the latter case; cf. section 87 para. 2 of the Austrian Code of Criminal Procedure as well as Fabrizy (2008), section 87, p. 200.

397 cf. e.g. Buermeyer, Technischer Hintergrund, p. 158.

398 In general such locations mean premises directly used by landlords and their families, for living or even commercial purposes; the rights of the householder involve also parts of a house not occupied or inhabitable; cf. KH 834.

Important in this context is that publicly accessible locations like parks, streets or hallways do not fall under lit a and can be searched without any special documents.[399] IT facilities, thus hardware such as external hard drives, computers, laptops etc, are subsumed under the term 'objects'. This means that the search of a computer, the extract of the hard drive or the copying of the data stored on a computer is covered by the definition of search of locations and objects.[400] The provision of section 119 para. 1 of the Austrian Code of Criminal Procedure can be applied to data storage devices so that criminal police can search them. Evidence for this point of view can be found in the final report of an inter-ministerial working group where Kopetzky remarks in this context that the search of physical devices (personal computers, PDAs, servers, etc) can be conducted directly on site or in a well-equipped forensic laboratory.[401]

3.4.2.2 Different Locations – Different Requirements

Art 9 Basic Law on the General Rights of Nationals in the Kingdoms and Laender in accordance with Art 8 Convention for the Protection of Human Rights and Fundamental Freedoms provides a right for everyone that their private and family lives, as well as their homes and correspondences are protected.[402] Only in very specific situations, an interference of these rights can be accepted, which guarantees that only lawful searches shall be conducted.[403] According to the constant ruling of the Austrian Constitutional Court, householder's rights secure the dignity and the independence of the flat etc holder, especially in regard to circumstances and facts which are customary acknowledged to be protected from

399 cf. EBRV 25 BlgNR XXII GP, p. 165.

400 Lachinger, Edith, Die Online-Durchsuchung als Erweiterung des Ermittlungsinstrumentariums (2008), p. 28; cf. as well Tipold, Alexander, Zerbes, Ingeborg WK-StPO [2005], section 139, MN 10.

401 BMJ/BMI (2008), p. 14; for Germany cf. as well Buermeyer, Technischer Hintergrund, p. 158.

402 While Art 9 Basic Law on the General Rights of Nationals in the Kingdoms and Laender does only provide protection against random searches conducted by national authorities, Art 8 Convention for the Protection of Human Rights and Fundamental Freedoms grants protection against any interference with householder's rights. Hence, the latter provision is much broader than the former which is mainly due to the fact that while the former constitutes a formal reservation the latter is seen as a substantive reservation; cf. in this respect already the illustrations in the context of the Austrian Constitutional Law above; moreover cf. VfSlg 14864/1997.

403 If the affected person agrees with the coercive measure, meaning the entering of the criminal police is founded on the voluntary consent of the affected person (i.e. the search was allowed by them), the measure loses its coercive character. This implements even that the consent of one person out of more occupying a flat (e.g.: the wife consents in a search of a location occupied by herself and her husband) is sufficient, so that the measure looses this character; cf. in this respect especially VfSlg 5738 and 6696/1971. This fact implies that the measure is not an exercise of direct administrative power and compulsion; cf. VfSlg 10.850.

the insight of third persons.[404] This indicates that in order to conduct a legal search, a court order – thus a warrant – may be needed. 'May' because of a distinction between two different types of locations mentioned above has to be done:

- A search of flats or other locations protected by householder's rights[405] and of objects located in such (section 117 no. 2 lit b of the Austrian Code of Criminal Procedure), does not only need a direction of the public prosecution but also judicial approval by a court. Thus a warrant is needed.

- A search of premises, rooms, vehicles or vessels not publicly accessible (section 117 no. 2 lit a of the Austrian Code of Criminal Procedure) can be generally conducted by the criminal police without a warrant. However, a search according to lit a has also to be based on the same concrete suspicious circumstances as a search according to lit b.

The case of a search of premises, rooms, vehicles or vessels not publicly accessible[406], will be presented subsequently.

3.4.2.3 Locations Protected by Householder's Rights Section 117 no. 2 lit b of the Austrian Code of Criminal Procedure

3.4.2.3.1 Searching

The term 'search' in the context of a search of locations and objects means everything going beyond an ordinary active inspection.[407] By ordinary inspections we mean inter alia situations where an officer of the criminal police seeks for specific objects within specified locations

---

404 cf. KH 2285, cf. furthermore, Pilnacek, Pleischl (2005), MN 506, p. 105; they state furthermore that even a systematic inspection of at least a specific item (according to the Austrian Constitutional Court constant ruling, e.g. an armoire – cf. VfSlg 10897/1986, 11895/1988,) can be classified as a search of locations and objects.

405 Independent from their usage (private or for business purposes) gardens, subleased rooms and even hotel rooms, surgeries, stables and barns, chambers of notaries, lawyers, or offices as well as motor homes are covered by this terminology besides customary houses and flats; cf. especially Tipold, Zerbes, WK-StPO [2005], section 139, MN 2.

406 There are no householder's rights in regard to containers, cars or suitcases located outside protected areas (protected by householder's rights). However, as Tipold/Zerbes point out, a search of this objects would constitute an interference with privacy; cf. Tipold, Zerbes, WK-StPO [2005], section 139, MN 5.

407 cf. in this respect VfSlg 11650/1988 or 12122/1989.

and where it is not necessary that the officer opens containers or uncovers a concealment. If this happens in such an area (location protected by householders' rights), an official search is conducted.[408] The aim of a search is to find suspects, objects or traces related to a criminal offense.[409] While there is rather little need for further clarification in regard to the term 'offenders', there is such a need for objects or traces. First of all, objects could be used as evidence in the further investigation and later on in the main trial. The range of possible objects is quite broad and includes, for instance, guns used for committing a criminal act, preparatory tools such as maps, the stolen property but also objects which may include further clues to aid the investigation (for instance a directory of a computer).[410] Suspect or not, private persons as well as legal persons can become subjected to a search,[411] if this person constitutes the holder of the householder's rights of the target location.[412] The properties of a holder involve the actual control over the location, meaning that – for instance –legal owners of a house are not holders of a flat, even if they are in possession of a key to it, if this flat is hired out. This is an important fact to consider since certain rights as well as obligations are closely connected with the characteristic of being holder of a location.[413]

3.4.2.3.2 Reasonable Suspicion

In addition to the already presented general requirements for a warrant, there has to be reasonable suspicions concerning a committed criminal act. This suspicion has to be present before a warrant can be issued and the search can be conducted.[414] This means that a search can only be conducted if there is a concrete and reasonable assumption (based on evidence)

---

408 cf. in this respect, for further details and the related critique Tipold, Zerbes, WK-StPO [2005], section 139, MN 7-8; note in this context that a simple entering of such a location in order to determine whether a flat is occupied or not, does not constitute a search of locations; cf. in this respect VfSlg 14864/1997.

409 According to the Austrian Constitutional Court, a search of locations is only given, if a search is conducted in order to find persons or objects whose residence is not known. Simple entering of a flat during the search for a person, in order to interview the persons present in that flat regarding the residence of the suspect person, does not constitute a search of locations and objects as defined by sections 119 et seq.of the Austrian Code of Criminal Procedure; cf. in this respect VfSlg 5080/1965, 6528/1971, 9766/1983, 10547/1985, 11650/1988, 12056/1989, 12628/1991.

410 Tipold, Zerbes, WK-StPO [2005], section 139, MN 15.

411 cf. Lohsing, Ernst, Österreichisches Strafprozeßrecht, 4th edition (1952), p. 265.

412 Tipold, Zerbes, WK-StPO [2005], section 139, MN 24.

413 Please cf. as well below, the definition of a holder in respect to surveillance of data and communication, and the corresponding rights and obligations evolving from the position of a location's holder below; cf. furthermore Tipold, Zerbes, WK-StPO [2005], section 139, MN 24-9.

414 cf. Seiler (2009), MN 463 p. 130; however, this is also a legal requirement for an issued search warrant – cf. concerning this as well LG Klagenfurt 17.01.2008 7 Bl 8/08g stating that the command or authorization of a warrant requires the concrete suspicion of a committed criminal act; furthermore VwGH 8.9.1988, 88/16/0093.

that a person/object/trace is situated within an area protected by householder's rights.[415] Searches without such suspicion, hence searches conducted only on the basis of unspecified speculation or hope to gather suspicion thereby, are not allowed and will be dismissed at trial. This is also true for searches not indicating what is searched for.[416] Moreover, the mentioned assumption has to be in existence already in advance – thus prior to the actual search.

Out of section 119 para. 1 of the Austrian Code of Criminal Procedure special requirement of justification for an issued warrant can be drawn: it is necessary to name the essential circumstances on which the certain search warrant is based on. This includes especially matter of facts letting the criminal police assume that the item/person searched for is at the location, which should be searched.[417] In addition, there is the requirement that a warrant has to include an explanation, naming the object assumed in a flat etc. and how it anticipates to assist the solution of a criminal act.[418] This involves an illustration of the importance of the object for the investigation – hence a comprehensive clarification of the objects significance.[419] The court in its function as controlling authority is obligated to guarantee that the infringement is proportional to the investigated criminal act.[420] Proportional means that there has to be the right amount of balance between a coercive measure and the seriousness of a committed criminal act. The same word is used in regard to a committed criminal act and its punishment. The more serious the criminal act, the more serious is the correlating punishment. Hence, if the public prosecution requests a search concerning homicide, the court will approve a search but not if the public prosecution does so because of a minor theft.[421]

3.4.2.3.3 Rights of Affected Persons

Taking the principles of legality and proportionality into account, the Austrian Code of

---

415 cf. Schäfer, Karl in Löwe-Rosenberg, StPO, 25th edition, section 103 margin number (MN) 14; cf. furthermore, VfSlg 12267/1990.

416 cf. Tipold, Zerbes, WK-StPO [2005], section 139, MN 30.

417 cf. 14 Os 172/01.

418 cf. Fabrizy (2008), section 119, p. 266.

419 cf. Tipold, Zerbes, WK-StPO [2005], section 139, MN 32.

420 cf. Pilnacek, Pleischl (2005), MN 510, p. 106; this involves especially that interferences are not allowed in circumstances where there is a voluntary participation of the affected persons. However, this does not mean that the investigating authorities are obliged to use a search of locations and objects as last resort, meaning that only if other – less intrusive investigation methods are fruitless, it is allowed to conduct an enforceable search. cf. Mayerhofer, Christoph, Das österreichische Strafrecht, Strafprozessordnung §§ 1 – 270 (2004), p. 340.

421 In this respect cf. the further remarks in the chapter on surveillance of communication in this thesis.

Criminal Procedure states in section 121 para. 1 that the affected person[422] has to be informed about the reasons for the search and what is searched for. Then, either acceptance of the search will be requested, or the demanded items may be handed over voluntarily. This means that the criminal police is, by law ,obligated to inform the affected persons about the reason for search and what is search, as well as about their right to object to this measure. This is a general rule of criminal law, stated in section 6 para. 2 of the Austrian Code of Criminal Procedure and refers directly to the already mentioned European Convention on Human Rights and the right to a fair trial.[423] For instance, there is a provision concerning the reimbursement of expenses related to the compliance with the obligation.[424] Only if there is a possible periculum in mora (danger in delay), one can refrained from this request. The criminal police has to grant the person in possession of the location or object (i.e. the holder) the opportunity to hand over the items, or to rebut the grounds for the search.[425] In this context it is further to note that the criminal police – within the borders of proportionality – is even entitled to use force, in order to enforce the direction.[426]

Furthermore, in the case of the securing[427] of an item or data, the criminal police has to inform and confirm the affected person in writing about the search. This confirmation has to list all items secured by the criminal police, and to include legal instructions in regard to the affected person's right of appeal against the securing.[428] The criminal police is obliged to hand over this confirmation immediately or to inform the affected person within 24 hours.[429]

In addition, it is the fundamental right of the affected person to be present while a search of locations and objects is conducted and a personal confidant may be brought in,[430] as stated in section 121 para. 2 of the Austrian Code of Criminal Procedure. This is not just simply a right,

---

422 An affected person is the person whose rights are affected directly by the order or the conduct of any means of coercive; cf. for the definition section 48 para. 1 no. 3 of the Austrian Code of Criminal Procedure.

423 cf. Art 6 ECHR para. 3 determining civil minimum rights of an accused in criminal investigations.

424 Persons not suspected themselves of a specific criminal act do have the right to request reimbursement of the costs in regard to their expenditures; however suspects do not have such rights; cf. section 111 para. 3 of the Austrian Code of Criminal Procedure.

425 cf. Bertel, Venier (2009), MN 306, p. 91.

426 cf. section 93 para. 1 of the Austrian Code of Criminal Procedure; however, it is to note in this context that if the criminal police exceeds the warrant/court order, this can constitute an illegitimate interference of the constitutionally granted householder's right.

427 cf. below in 'Additional Empowerment by a Search Warrant'.

428 In respect to the term securing please cf. below; this right to appeal is stated in sections 106 and 115 para. 2 of the Austrian Code of Criminal Procedure; cf. EBRV 25 BlgNR XXII GP, p. 157.

429 cf. section 111 para. 4 of the Austrian Code of Criminal Procedure.

430 e.g. it is allowed to bring in an attorney-at-law; in this respect it is further to note that the affected person is free to leave the location of the search in order to contact an attorney-at-law (for example to have an undisturbed phone call with the attorney-at-law); cf. Seiler (2009), MN 469, p. 132.

the criminal police has to ensure the affected person can take advantage of this right. The holder, however, does not have to be present, if he chooses not to. Provision para. 2 states that, if there is a possible danger in delaying the search process, the right for a personal confidant may be omitted if it takes too long for them to be on scene. Furthermore, the criminal police can deny the participation of a personal confidant, if this person is suspected to be involved in the investigated criminal act.[431] Information about this right can be withheld in such cases. This does, however, not implement that the criminal police is not obliged to inform the affected person at all in case of danger in delay.[432] Section 121 para. 2 of the Austrian Code of Criminal Procedure further regulates that in circumstances where holders of the flat are not present, an adult flat mate is able to exercise these rights accordingly. In addition, when there is danger in delay it is possible to name two reliable, not involved persons in order to overcome the lack of presence of the affected person. The main reason for this is an indulgent conducting of the search.[433] Besides the holders of the location and their confidants (e.g. an attorney-at-law), the public prosecution is entitled to be present during a search. If the affected person is not suspected of the actual criminal act, the criminal police does not have to postpone the conducting until the confidant, such as a attorney-at-law arrives.[434]

One of the most important rights in this context is the right to avoid self incrimination. In the court of law nobody can be forced to testify against themselves or close relatives in criminal proceedings. This also applies to the compliance with court order and directions that suspects and their close relatives do not have to follow. The criminal police can, however, secure and seize objects from suspects. The principle of 'nemo tenetur se ipsum accusare' does not apply in this context.[435]

Section 122 para. 3 of the Austrian Code of Criminal Procedure states another fundamental right of affected persons: they have to be informed about the circumstance of a search, immediately or within the first 24 hours. This written confirmation has to include information that a search has been conducted, the corresponding results and – where applicable – directions of the public prosecution including the approval of the court. Issuing authority of

---

431 cf. section 160 para. 2 of the Austrian Code of Criminal Procedure.
432 In respect to danger in delay please cf. the illustration below.
433 cf. Tipold, Zerbes, WK-StPO [2005], section 142, MN 6.
434 cf. further Tipold, Zerbes, WK-StPO [2005], section 142, MN 7.
435 Nevertheless, as Pilnacek/Pleischl point out precisely, it is especially not allowed to use coercive detention against suspects; cf. Pilnacek, Pleischl (2005), MN 474, p. 99.

this confirmation can only be the criminal police, as they conduct a search. The confirmation has to include a directory of the secured and seized items and documents.[436]

Unlike the confirmation, an explanation on rights of appeal has to already be handed over at the time of the actual search on site.[437]

3.4.2.3.4 Excursus: Particular Professions and Confidentiality

For professionals who swore an oath of confidentiality, such as attorneys-at-law, notaries, repositories, physicians, media editors etc[438], this provision includes a special regulation. When the criminal police wants to search a location, which is used exclusively by such professionals, a representative of the legal entity representing the interests of that profession has to be present. This representative has to be brought in ex officio. These representatives are to ensure the confidential relationship between these certain professions and their clients remain intact. A professional's obligation of confidentiality towards his client cannot be breached by such search warrants.[439] Only in circumstances where these professionals themselves are suspected of having committed a criminal act, is it possible for the criminal police to (legally) search their premises.[440] section 60 of the Austrian Code of Criminal Procedure, further states that defense lawyers have to be excluded of the proceedings if they are inter alia suspected of the involvement of the same criminal act as their client.[441] It is illegal to search the office of defense lawyers as long as they are not yet excluded from the proceedings. Section 60 of the Austrian Code of Criminal Procedure provides the proceedings intended to clarify whether a defending lawyer is under suspicion or not.[442]

---

436 cf. below in 'Additional Empowerment by a Search Warrant'; and Bertel, Venier (2006), MN 247, p. 88.

437 cf. Pilnacek, Pleischl (2005), MN 522, p. 109.

438 cf. section 157 para. 1 no. 2 – no.4 of the Austrian Code of Criminal Procedure.

439 cf. section 144 para. 2 of the Austrian Code of Criminal Procedure; cf. furthermore Tipold, Zerbes, WK-StPO [2005], section 142, MN 8.

440 cf. section 144 para. 3 of the Austrian Code of Criminal Procedure and OGH 31.1.1992, 16 Os 15/91.

441 Another situation mentioned in section 60 of the Austrian Code of Criminal Procedure is where the defending lawyer uses the association with the detained suspected to commit criminal acts or to endanger the security and order of a penal institution, e.g. by transporting illegal items or messages. para. 2 offers the actual proceeding for the exclusion of a defending lawyer; further circumstances leading to an exclusion are provided by section 10 para. 1 of the Austrian Lawyer's Act.

442 cf. Bertel, Venier (2006), MN 246, pp. 87-88.

3.4.2.3.5 Additional Empowerment by a Search Warrant Securing and Seizure

The warrant empowers the criminal police to search all objects situated in the stated area. Hence, the investigators are allowed to search all furniture, bags, boxes etc.[443] In addition to this and according to section 110 para. 1 no. 1 of the Austrian Code of Criminal Procedure, a warrant empowers the conducting agency to secure all items searched for.[444] In order for these secured items to be seized, the public prosecution has to request the seizure at court. If the requirements for a seizure are not given, the securing has to be overturned and the item returned to the owner.[445] The difference between securing and seizure is that the actual securing of an item is the establishment of the authority to dispose of it and that securing is only a temporary/provisional measure intended to secure evidence. Contrary to this, seizure presumes already an actual securing and represents a judicial decision intended to establish and perpetuate legally the authority to dispose.[446]

3.4.2.3.6 Obligation to Comply with a Warrant?

While criminal police has the right to secure items during a search, the person in possession of an item of interest has the duty to hand it over if asked to do so. Items subject to securing have to either be handed to the criminal police or the access to these items has to be granted. This has to be done by the person who has the item at his/her disposal. In order to establish the duty to hand the item searched for to the criminal police, it is to say that the criminal police has only to assume that somebody has the item at his/her disposal. This person is obliged to hand it to the criminal police.[447] If the presumed person does not comply with his/her obligation,[448] this compliance can be enforced. These coercive means are listed in section 93 para. 4 of the Austrian Code of Criminal Procedure and include, amongst others, monetary penalties of up to Euro 10,000 and possible imprisonment for up to six weeks. Additionally, section 111 para. 1 of the Austrian Code of Criminal Procedure points explicitly

---

443 cf. Tipold, Zerbes, WK-StPO [2005], section 139, MN 32.
444 cf. in this respect the ruling of the Austrian Constitutional Court, VfSlg. 2990/1956, 7067/1973.
445 according to sections 113 para. 3, 115 para. 2 of the Austrian Code of Criminal Procedure.
446 cf. the definitions given in section 109 no. 1 and no. 2 of the Austrian Code of Criminal Procedure; further cf. Bertel, Venier, (2006), pp. 72-79; as well as Seiler (2009), pp. 126-128.
447 cf. Bertel, Venier (2006), MN 215, p. 77.
448 Concerning the actual obligations cf. section 93 para. 2 of the Austrian Code of Criminal Procedure.

to the provisions dealing with the search of locations and objects in this matter.

Another important aspect, mentioned in section 111 para. 2 of the Austrian Code of Criminal Procedure is that if data stored on data carriers have to be secured. This means that the holder of the data carrier[449] with access information has – on request – to grant criminal police access to this data. As electronic sets of data are immaterial objects, they need physical embodiment for their existence. A search for electronic data is therefore indivisible connected to the search for the related data carrier.[450] Access can be enabled by providing a password or a code.[451] The obligation to provide access includes moreover that the holder of the demanded data (carrier) has to hand over the electronic data carrier or a copy of it in a customary file format, or to produce such a file format. In addition, the person has to accept the production of a backup copy of the data stored on that data carrier.[452]

3.4.2.3.7 Accidental Discoveries

In this respect it is moreover to remark that if the criminal police finds items suspected to be of matter in other criminal cases than a warrant was issued, the criminal police is allowed to secure these items as well.[453] In this circumstance it is mandatory that the criminal police enters these findings into the records of the proceedings and informs the public prosecution. The public prosecution then evaluates whether it wants to request the seizure of these items at the criminal court. If the public prosecution comes to the solution that the securing was not legitimate – thus the circumstances under which a securing and thereafter a seizure can be conducted, are not given, or are cancelled – it has to suspend the securing process.[454] Moreover, the criminal police can secure items if danger in delay is given. At this juncture, the criminal police is obligated to request approval from the public prosecution (section 99

449 cf. Bertel, Venier (2006), MN 217, p. 77.

450 cf. Pilnacek, Pleischl (2005), MN 475, p. 99 who refer especially to the problems regarding huge computer networks and state that data could be hidden in such networks rather than be stored just on a computer. Hence it would be advantageous to know the 'architecture' of a network.

451 cf. Bertel, Venier, (2006), MN 217, p. 77.

452 According to the Explanatory Report to this provision (section 111 para. 2 of the Austrian Code of Criminal Procedure), its establishment is mainly due to Austria's signing of the Convention on Cybercrime; cf. EBRV 25 BlgNR XXII GP, p. 156; cf. in this regard as well the subchapter on encryption and decryption.

453 Accidental discoveries: e.g. a search warrant was issued in order to seize illegal drugs and the criminal police finds suspected stolen goods; cf. e.g. Seiler (2009), MN 468 p. 132.

454 cf. sections 113 para. 3, 122 para. 2 of the Austrian Code of Criminal Procedure.

para. 2 of the Austrian Code of Criminal Procedure) whereas the public prosecution has to request judicial seizure of the items (section 113 para. 3 of the Austrian Code of Criminal Procedure). However, there are no exact specification in the Austrian legal system stating the time frame for the public prosecution to evaluate the legitimacy of a securing.

3.4.2.3.8 Danger in Delay (periculum in mora)

A search of locations and objects is allowed even without a warrant if a periculum in mora (danger in delay) is present. This means that it was not possible for the criminal police to obtain directions from the public prosecution and the regular needed judicial approval without endangering the success of a search, or as Bertel/Venier put it, the taken action is so urgent that it is not even possible to receive an oral command from the public prosecution.[455] An evaluation whether danger in delay was present when the criminal police conducted the search is subject to a rigorous benchmark.[456] Such situations are given where even a slight delay would destroy an object searched for, or if it would enable the escape of a suspect.[457] The latter is especially true if, for example, the suspect was caught in the act of committing a crime or his involvement in the crime is evident.[458]

As mentioned previously, the criminal police has to inform the affected person and to request an acceptance of the search.[459] However, in situations of danger in delay, the criminal police can refrain from its obligation to inform and to request acceptance of the search. Note in this regard that, as Bertel/Venier point out, there can never be the danger of a rough delay, if the affected persons are informed about the main causes for the search and about their right to be present. On the contrary, only an informed person is able to contribute to the search and hand over the item searched for.[460]

---

455 cf. Bertel, Venier (2006), MN 211, p. 75; furthermore the rulings of the Austrian Constitutional Court VfSlg 9210/1981, 12513/1990 or 12657/1991.

456 cf. concerning this benchmark of danger in delay e.g. VfSlg 12701/1991 or 13043/1992 in the context of detentions.

457 cf. VfSlg 1890/1949, 1980, 2861/1955 or 5083/1965; however, Seiler argues that in respect to this aspect of danger in delay it is to remark that a simple, potential loss of evidence does not constitute such a situation; cf. Seiler (2009), MN 468 p. 132; contrary to this Tipold, Zerbes, WK-StPO [2005], section 141, MN 1.

458 In regard to obviousness it is to say that this can be if a person is trapped with the loot or the weapon used in a criminal activity by an organ of the security agency (and not by a 'private person').

459 cf. already above and section 121 para. 1 of the Austrian Code of Criminal Procedure.

460 cf. Bertel, Venier (2009), MN 306, p. 91.

According to section 122 para. 1 of the Austrian Code of Criminal Procedure, the criminal police is obliged to report immediately if it conducted a search of flats or other locations protected by householder's rights and of objects located in such (section 117 no. 2 lit b of the Austrian Code of Criminal Procedure) when there was danger in delay if there was no warrant for a conducted search at all. This special report is called 'Anlassbericht'[461] and has to include a detailed description of the circumstances leading to the urgency of a search in this specific case. This means that the criminal police has to justify the taken action in a formal report. Simple speculations, hypothetical considerations or even assumptions based on every day criminal investigation experience, regardless of the case, are therefore not sufficient as basis for danger in delay. Periculum in mora has to be founded on supporting evidences of the specific case.[462] The simple potential loss of evidence, for example, does not constitute a situation of danger in delay. Furthermore, the report has to include a justification why the notification of the public prosecution was not possible. The public prosecution has to get a well-founded report on which it can base their also well-justified request for approval of the search. If this approval is denied by the court, both the criminal police as well as the public prosecution are constrained to re-establish the appropriate legal situation. This means, that data and traces gathered during an illegal search have to be dismissed and secured items have to be returned.[463]

In every case of periculum in mora the affected person is entitled to be informed either immediately or within a 24-hour-time-span. This written confirmation has to include the information that a search has been conducted, the corresponding results and – where applicable – the direction of the public prosecution including the approval of the court.[464]

3.4.2.3.9 Accidental Discoveries vs. Danger in Delay

Periculum in mora and accidental discoveries deal with a somewhat similar issue. The main difference between this two regulations and the way situations of danger in delay are handled,

---

461 cf. section 100 para. 2 no. 2 of the Austrian Code of Criminal Procedure stating that such a report has to be conducted in circumstances where the criminal police considers a direction or an approval of the public prosecution or a decision of the court as necessary or suitable; or if the public prosecution requests a report.

462 cf. EBRV 25 BlgNR XXII GP, p. 169.

463 cf. EBRV 25 BlgNR XXII GP, p. 169.

464 cf. section 122 para. 3 of the Austrian Code of Criminal Procedure.

is that the former assumes an issued warrant while the latter expects that there is none while a search is taking place. Moreover, the former deals with accidental discoveries during a search approved by a specific warrant regarding another criminal act, while the latter deals with searches conducted completely without any warrant. Accidental discoveries do not only just involve the securing of an item but the infringement is also less serious due to the issued warrant for the search. Periculum in mora represent circumstances without any prior judicial control. However, both regulations provide fast and appropriate action and a broad and unrestrained a posteriori judicial control does not contravene.

In principle, both regulations deal with the problem of 'imperfect' warrants in the same way with the slight distinction that the public prosecution must not necessarily inform the court about the securing of items in danger in delay case. It is allowed to direct the criminal police to return items not believed to be of any concern in other criminal matters to the rightful owner. Only if the public prosecution comes to the conclusion that the secured items are needed in another criminal trial, it has to request judicial seizure of these things. In the latter case, where there is no warrant at all and the criminal police conducted a search due to periculum in mora, it is mandatory that judicial approval is requested afterward.[465]

Hence, any interference with householder's rights is always subject to judicial control.[466]

3.4.2.4 Search of Locations not Publicly Accessible Section 117 no. 2 lit a of the Austrian Code of Criminal Procedure

As mentioned above, there is a distinction between a search of locations and objects protected by householder's rights and a search of premises, rooms, vehicles or vessels not publicly accessible. While it is necessary for the former to be based on a warrant – or, as presented as well, to be justified by a corresponding judicial decision afterwards – the latter kind of search can be conducted without any special (formal) requirement or approval, either before or after

---

[465] Note in this context the critique of Bertel/Venier who argue that the search according to section 117 no. 2 lit b of the Austrian Code of Criminal Procedure in circumstances of danger in delay is unconstitutional because there is a clear dissent to section 2 HausRG (Art 9 Basic Law of 21 December, 1867 on the General Rights of Nationals in the Kingdoms and Laender, Art 8 Convention for the Protection of Human Rights and Fundamental Freedoms); cf. Bertel, Venier (2009), MN 305, p. 91.

[466] cf. Fabrizy (2008), section 120, p. 268; furthermore the extensive illustration in this respect in EBRV 25 BlgNR XXII GP, pp. 168-169.

a search.[467] However, this does not mean that there are no requirements at all for a search of these locations. First of all, and most importantly, is the precondition that the criminal police assumes a person suspected of a criminal act hiding at the specific location, or a certain object or trace of interest to criminal proceedings are located at this certain location. And second of all, these items (object or trace) need to be seized or analyzed due to their importance in criminal proceedings. The demanded assumptions are identical to those needed before a search according to lit b. Furthermore it is – again identical to lit b – required that this suspicion is based on facts and evidence, thus it has to be justified.

If such a situation is given, the criminal police is free to search the corresponding locations and does not need a special formal direction or approval from the prosecution/court. The criminal police is, however, still obligated to inform the affected person about the search and the reasons for it. Moreover, it has to request, for instance, the voluntary handing over of the searched items and it has to grant the affected person the same rights in regard to having a third party present, as shown in the presentation of lit b. The confirmation and the results of the search are formalities, identical to the one in the search of location protected by householder's rights.[468] Just like with other warrants, the criminal police is empowered – within the framework of a legal search – to secure found items. Similar to the proceeding under lit b, the criminal police has to inform the public prosecution about the securing.[469] Additionally, it is to mention that the affected person of such a search has the right to appeal against the acts of the criminal police.[470] Thereby, the control by the public prosecution and the judicial protection of human rights can be accomplished.[471]

3.4.3 Conclusion: Realization of an RFI

Having examined the procedural provisions governing the search of a computer, a new question arises: Can an RFI be conducted legitimately? Thus, can it be based soundly onto the

---

467 Publicly accessible locations like parks, streets or hallways do not fall under lit a and can be searched without any special requirements; cf. above.

468 cf. above and Bertel, Venier (2006), MN 251, p. 89.

469 Remarkable in this context is that section 122 para. 2 of the Austrian Code of Criminal Procedure concerning the handling of accidental discoveries is not applicable because this regulation is referring only to warrant based searches; cf. Bertel, Venier (2006), MN 252, p. 89.

470 section 106 of the Austrian Code of Criminal Procedure – cf. Fabrizy (2008), section 106, pp. 233-236.

471 cf. Pilnacek, Pleischl (2005), MN 519, p. 109.

presented and already existing provisions of a search of locations and objects? As already defined at the beginning of this thesis, the author is examining the legitimacy of an RFI in regard to its three purposes:

- Remote Access for Search Purposes
- Surveillance of Activities
- Surveillance of Telecommunication

Further requirements established by the Ministry of Justice and of the Interior[472] have to be taken into account. These preconditions involve that an RFI could be conducted in situations where it is necessary for the solution of a criminal act punishable by imprisonment for a minimum period of ten years, a criminal organization or a terrorist association according to sections 278a and 278b of the Austrian Criminal Code, the solution or prevention of a criminal act committed, or planed by such an organization or association. In addition, an RFI could be legally conducted if a person is strongly suspected for preparatory works in relation to a Criminal Organization or a Terrorist Association (section 278a, 278b of the Austrian Criminal Code). Hence, contrary to a customary search of locations and objects, these formal preconditions have to be given. If they are not, the court will not approve the request of the public prosecution and therefore not issue a warrant for an RFI. In such cases, however, the public prosecution could request a customary search of locations, thus the search cannot be conducted remotely.

Beforehand, it is to mention that due to the nature of a search of locations and Objects according to sections 119 et seq. of the Austrian Code of Criminal Procedure in this sense, this provision can only deal with one task, namely the implementation of an RFI for search purposes. The other two purposes are – already literally – rather illogical.

The question of whether a method could be subsumed under a certain provision of the Austrian Code of Criminal procedure has to be evaluated independently of the physical condition of the item searched for. This means that it does not make any difference whether

472 cf. Vortrag an den Ministerrat der Republik Österreich of 17 October, 2007.

the target object of a search is an electronic device respectively the data stored on it, or whether the criminal police is searching for any other physical objects. Moreover, as mentioned IT facilities are covered by the term objects and can therefore be searched as well.

Generally, a search of locations and objects is an open investigation method, meaning that the conducting officers of the criminal police are physically present on site. As shown in this context, the affected persons as well as the criminal police do have not only obligations but also rights when a search is conducted lawfully. For instance, the criminal police has to inform the affected person about the reasons for the search and what is searched for. The affected person itself has to be requested for acceptance of the search, or to hand over the demanded items voluntarily.[473] Moreover, the affected persons are entitled to be present or to bring in a personal confidant, while a search is conducted and they have to be informed about the circumstance of a search, immediately or within 24 hours.[474] The rights of the affected person are fundamental procedural rights guaranteed by Art 6 ECHR and can therefore not be ignored. This guarantee of a fair trial does, however, not comply with an RFI as this investigation method is intended to be done secretively, meaning that the affected person does not have any knowledge about the ongoing investigation. An application of sections 119 et seq. of the Austrian Code of Criminal Procedure in respect to an RFI would lead to an evasion of constitutional granted rights of the affected person.

Moreover, the principle of an openly conducted search is prevailing in order to limit the competences of undercover agents, leading thereby to an equalization of 'arms'[475] in a criminal trial.[476] Despite the fact that a computer can be subsumed under the term 'object', according to this provision[477], the actual search of a computer can only be conducted in an open and direct manner, meaning that the remote access to stored data on a computer is not granted by sections 119 et seq. of the Austrian Code of Criminal Procedure. The same is true for the securing (and the seizure afterwards) of items found on a computer prior to the

---

473 cf. already above and section 121 para. 1 Austrian Code of Criminal Procedure.

474 cf. already above and sections 121 para. 2, para. 3 Austrian Code of Criminal Procedure.

475 A principle emerging from the principle to a fair trial (Art 6 ECHR).

476 cf. in this respect Jahn, Matthias, Kudlich, Hans, Die strafprozessuale Zulässigkeit der Online-Durchsuchung, in JR 2/2007, pp. 57-61 furthermore, in respect to the German point of view cf. BGH Beschluss of 31 January, 2007, StB 18/08, in JZ 15/16/2007, pp. 796-800, including further remarks of Cornelius, Kai.

477 cf. above and Tipold, Zerbes, WK-StPO [2005], section 139, MN 10.

computer's official seizing. It is necessary that the investigation authorities conduct a search. Without a search, the criminal police is not entitled to secure evidence.[478]

This view is also supported by a report of an expert group, stating that a search of locations and objects, as well as the securing and seizure of items implies the physical contact with a physical location, thus the physical appearance of the investigation authorities at this location.[479] As it is exactly the intention of the investigation authorities to avoid physical presence on site, contentions stating that an RFI could be conducted legitimately via these procedural provision are not knock down arguments. Hence, an RFI in the form of a remote examination of a computer cannot be based on these provisions.

3.4.4 Surveillance of Communication

3.4.4.1 General Aspects

The amendment of the Austrian Code of Criminal Procedure in 2002,[480] which went into effect in 2008, brought some important alterations and extensions. It was clearly stated that the new regulations dealing with the surveillance of communication in chapter 5 involve every kind of communication, no matter how it is transmitted. While the former regulations were limited to communication transmitted via means of telecommunication, the new provisions include all means of transmission. Hence, surveillance in a wider sense – i.e. the seizure of letters,[481] the disclosure of transmission data, the surveillance of communication as well as the optical and acoustical surveillance of persons – are all included, independent of technology.[482] This also included now particularly communication conveyed via a computer system.[483]

---

478 There are, however, exceptions of this principle – cf. section 110 para. 3 Austrian Code of Criminal Procedure.

479 BMJ/BMI (2008), p. 33.

480 Federal Law Gazette 134/2002.

481 Note in this respect that a seizure of a letter cannot be involved as these a physical items and are not conveyed electronically rather than they are handed over physically from one person to another; cf. Tipold, Alexander, Zerbes, Ingeborg, WK-StPO section 134, MN 1 et seq.

482 cf. Pilnacek, Pleischl (2005), MN 584, p. 121.

483 The Explanatory Report states explicitly that this includes as well that a communication can be transferred via a customary telecommunication network before entering into a computer system and vice versa; cf. EBRV 25 BlgNR XXII GP, p. 187.

The procedure for every surveillance method is governed by sections 137 – 140 of the Austrian Code of Criminal Procedure. While sections 137 and 138 deal directly with the execution of surveillance, sections 139 and 140 handle the obligations of the investigating authorities and rights of the affected person after a conducted surveillance. As these regulations apply to all forms of surveillance, this chapter is going to commence with a brief presentation of these rules, which will be followed by an overview on further cornerstones and principles in this context. Thereafter, the actual surveillance methods will be illustrated in detail, including further information on procedural requirements and specifics.

3.4.4.2 Common Regulations according to Section 137 of the Austrian Code of Criminal Procedure and Section 138 of the Austrian Code of Criminal Procedure

According to these provisions, an optical and acoustical surveillance due to hostage-takings does not need the approval of the public prosecution or a court, rather than it can be conducted by criminal police itself. This is the only case where the criminal police is allowed to take actions without directions mainly due to the urgency in such circumstances. For all other investigation measures according to sections 135 and 136 of the Austrian Code of Criminal Procedure, the criminal police needs a direction from the public prosecution, which, for itself, needs judicial approval for every surveillance activity.[484] The entering of locations protected by householder's rights – according to section 136 para. 2 of the Austrian Code of Criminal Procedure – demands, in every single case, the explicit judicial approval.[485] For a temporal frame for surveillance measures,[486] section 137 para. 2 of the Austrian Code of Criminal Procedure governs that directions have to be made for future periods – only in the case of a disclosure of transmission data[487] past periods can be covered as well. A renewal of a direction is possible, if certain facts indicate– that a continued execution of surveillance would be fruitful. Important to note in this context is that an ongoing surveillance has to end, if the requirements, on which it was based, are no longer given.

---

484 cf. already above in the context of a search of locations and objects.
485 cf. below.
486 Measures according to sections 135 and 136 of the Austrian Code of Criminal Procedure.
487 section 135 para. 2 of the Austrian Code of Criminal Procedure.

3.4.4.2.1 Formal Requirements

From a formal point of view section 138 of the Austrian Code of Criminal Procedure sets out the requirements for the directions of the public prosecution as well as the judicial approvals (court orders). Each of them have to include

- the designation of the proceeding,
- the name of the defendant,
- the committed criminal act the defendant is suspected for, and its legal term, as well as
- the facts justifying the necessity and proportionality[488] of the measure for the solution of the specific criminal act.

Further, special requirements are mentioned relating to the disclosure of transmission data, the surveillance of communication as well as the optical and acoustical surveillance of persons. Directions as well as the corresponding court orders have to mention

- name or other identification criterion of the technical facility holder,[489] or the person to monitor,
- the relevant location,
- type of the communication conveyance, the technical facility and the terminal device or the type of technical device (potentially) used for an optical and acoustical surveillance,
- start and end time of a measure,
- rooms subject to legitimate entering,[490]
- facts stating possible danger for public security.[491]

---

488 cf. regarding the proportionality below.
489 cf. below concerning the surveillance of communication.
490 according to section 136 para. 2 of the Austrian Code of Criminal Procedure.
491 In the case of section 136 para. 4 of the Austrian Code of Criminal Procedure.

The further content of the written directions/approvals is governed by section 86 and section 105 para. 1 of the Austrian Code of Criminal Procedure – thus there has to be a justification (the grounds of the decision) and an explanation on rights of appeal.[492] Section 138 para. 2 of the Austrian Code of Criminal Procedure obliges the operators of mail as well as telecommunication services to assist in criminal investigations. For instance it is stated that providers (according to section 92 para. 1 no.3 of the Austrian Telecommunications Act 2003)[493] and other service providers (according to sections 13, 16 and 18 para. 2 of the Austrian E-Commerce Act – namely host, service, and access providers) have the obligation to provide specific information and to contribute to the investigation on request of the public prosecution. This obligation has to be stated explicitly via a separate direction mentioning the original direction (to the criminal police).[494]

3.4.4.2.2 Evaluation of Surveillance

It is the public prosecution's duty to evaluate the findings,[495] to organize the transformation of the relevant evidence into written form and to file it. In this respect, special attention has to be drawn to sections 140 para. 1,[496] 144[497] and 157 para. 2[498] of the Austrian Code of Criminal Procedure concerning the exclusionary rule. Moreover, at the end of surveillance measure, according to sections 135 para. 2 and para. 3, as well as 136 of the Austrian Code of Criminal Procedure, the public prosecution is bound to deliver its direction including the corresponding judicial approval to the defendant and any other affected person.[499] However, the delivery can be postponed if this is necessary and desirable not only for the ongoing but also for any other investigation proceedings.[500]

---

492 cf. already above the comments made in relation to the court order.

493 Stating that 'provider' means an operator of public communications services; However, obviously by mistake section 134 para. 5 of the Austrian Code of Criminal Procedure mentions section 92 para. 1 no. 3 of the Austrian Telecommunications Act 2003 meaning in fact section 92 para. 3 no. 1 of the Austrian Telecommunications Act 2003; cf. as well Reindl-Krauskopf, Susanne, WK-StPO sections 137, 138, MN 38.

494 cf. section 137 para. 3 of the Austrian Code of Criminal Procedure.

495 according to section 134 no. 5 of the Austrian Code of Criminal Procedure.

496 cf. below.

497 religious official secrecy and profession sworn to confidentiality.

498 denial of evidence.

499 Regarding the corresponding rights of the defendants and other affected persons please cf. below.

500 e.g. because there is an investigation going on in relating organized crime.

3.4.4.2.3 Principles of Surveillance

The principles of legality and proportionality, two of the main principles of law, are important in the context of coercive measures and all surveillance activities performed by investigation authorities. Based on this fact – stated explicitly in section 5 para. 1 of the Austrian Code of Criminal Procedure – the activities of the criminal police, the public prosecution and the courts shall be based on law.[501] No activities are allowed to interfere with the rights of persons, except in cases where there is explicitly a regulation and the interference is necessary for the criminal police to fulfill its tasks – i.e. the solution of crimes.[502] Every activity performed by investigation authorities has to be based on legal regulations. Prohibition of analogy[503] concerning interferences with human rights has to be taken into account. By implication this means, however, that measures dedicated to the fulfillment of the tasks which do not interfere with such rights, are always allowed.[504] Moreover, it is pointed out that each interference with the rights of persons has to be in an appropriate and reasonable[505] balance to the seriousness of the criminal act, to the level of suspicion and to the intended result. In circumstances where there are a number of target-aimed investigation methods of coercive measures, only the less effective[506] method or measure can be applied.[507] This includes that the investigating authorities have to exercise their competences in a preferably gentle, and the integrity of the affected person respecting manner.[508]

Legality and proportionality have to be taken into consideration and then pointed out explicitly. Furthermore, there has to be a system of decision making and judicial review, adjusted to the intensity of interference in order to point out that the ECHR is not just implemented theoretically but that these rights are concrete and enforceable. Moreover, on grounds of the principle of proportionality it can be concluded that there has to be judicial approval in regard to certain coercive as well as surveillance measures. This is particularly

---

501 cf. already above and Art. 18 para. 1 Federal Constitutional Law.

502 Thus a strict tie to its tasks – hence only measures taken in order to fulfill tasks are covered by the provisions of the Austrian Code of Criminal Procedure; cf. Fabrizy (2008), section 5, p. 36.

503 However, there is no such prohibition of analogy of criminal procedure provisions, if there is no explicit regulation of a question (cf. e.g. EvBl 1958/295); a corresponding prohibition like in substantive criminal law (ex post facto) does not exist; cf. Fabrizy (2008), section 5, p. 35.

504 cf. EBRV25 BlgNR XXII GP, p. 29 as well as Fabrizy (2008), section 5, p. 35.

505 cf. Fabrizy (2008), section 5, p. 36.

506 For the affected person; cf. section 48 para. 1 no. 3 of the Austrian Code of Criminal Procedure.

507 section 5 para. 2 of the Austrian Code of Criminal Procedure.

508 section 5 para. 2 of the Austrian Code of Criminal Procedure, cf. further Fabrizy (2008), section 5, p. 36.

true since the European Court of Human Rights sees the engagement of courts – thus of independent institutions – in regard to the approval of legitimacy of an activity, as a method capable to avoid misuse of authority.[509]

Coercive surveillance measures can pose a threat to the rights of innocent people due to the impact these investigations can have. Hence, prior to the surveillance measures, there has to be an evaluation to whether there is a balance between the interference and the seriousness of the criminal act, to even the suspicion and the intended result of this surveillance. This means that only in cases of serious criminal acts (for instance homicide) right of non-involved persons may legally be interfered with.[510]

In addition, the Austrian legislator brought about a relief commissioner under section 146 of the Austrian Code of Criminal Procedure who has to be involved in the investigations. The agendas of the commissioner include inter alia the evaluation and control of the direction, the approval and conducting of covert investigations, the optical and acoustical surveillance of persons, as well as the surveillance of data and communication and the disclosure of transmission data.[511] This position is intended to protect the legal interests of affected persons on behalf of these persons. Since human/fundamental rights or problems in respect to legal protection/relief are not part of this thesis, there will be no further analysis of this matter.[512]

3.4.5 Surveillance of Data and Communication

3.4.5.1 Introduction

Sections 135 para. 3 and 134 no. 3 of the Austrian Code of Criminal Procedure deal with communication and data transmitted between two or more persons, thus these provisions handle the surveillance of communication. This includes all forms of new technology as well as all standard types of communication.[513] In order to clarify the statement in the opening paragraph of this chapter it is necessary to present some of definitions concerning this

509 EBRV25 BlgNR XXII GP, p. 30; cf. as well Pilnacek, Pleischl (2005), MN 26, p. 6.
510 Reindl-Krauskopf, Susanne, WK-StPO section 135, MN 26.
511 section 147 para. 1 of the Austrian Code of Criminal Procedure.
512 Please cf. for a detailed illustration of the relief commissioner Vogl, Mathias, Der Rechtschutzbeauftragte in Österreich (2004).
513 Originally only the surveillance of the content of telecommunication – thus customary telephone conversations – were covered by the respective provision in the Austrian Code of Criminal Procedure (section 149 a-c); cf. further Reindl-Krauskopf, WK-StPO, section 134, MN 20.

context.

- ‘Surveillance of Communication’ means

  the determination of the content of communications transmitted or forwarded over a communications network or via an information society service.[514]

- ‘Communication’ means

  any information exchanged or conveyed between a finite numbers of parties by means of a publicly available communications service. This does not include any information conveyed as part of a broadcasting service to the public over a communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information.[515]

- ‘Communications Network’ means

  transmission systems and, where applicable, switching or routing equipment and other resources which permit the electronic conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.[516]

It is to mention, however, that due to the fact that communication is exchanged or conveyed by means of a publicly available communications service (cf. above), a communication conducted via a local area network (LAN) or via an intercom is not covered. This means that, for instance, e-mails sent within a LAN or phone calls via house telephone networks cannot be subject on surveillance, because this communication does not happen via a public network.[517]

---

514 section 134 no. 3 Austrian Code of Criminal Procedure

515 section 92 para. 3 no. 7 of the Austrian Telecommunications Act 2003.

516 section 3 no. 11 of the Austrian Telecommunications Act 2003.

517 Such 'non-public' communication could only be monitored via an optical and acoustical surveillance of persons according to sections 134 no. 4 in conjuction with 136 of the Austrian Code of Criminal Procedure; for that cf. below and Reindl-Krauskopf, WK-StPO, section 134, MN 43.

- ‘Information Society Service’ means

  any service, normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.[518]

Similar to communication networks, electronic transmissions can be conducted via wires, radio, optical or electromagnetic means. Examples for such services are inter alia various online services such as web shops, database services (access) and services of access and host providers, i.e. convey information over, granting of access to and storage of information in a network. The latter three are the most important out of a great variety of different services.[519]

Thus, surveillance of communication can be conducted in various forms, namely by listening, eavesdropping, recording, intercepting or any other surveillance of the content of a communication.[520] It is, however, not surveillance of communication if the communication is blocked, thus the communication does not pass the network and arrive at the receiver (no communication stop).[521] Important in this context is that this surveillance has to be conducted when communication is conveyed in the respective communication networks or via an information society service. Not only does this provision cover customary circuit-switched telephone calls, fax messages or wireless messages but also packet-switched communication such as e-mails, Internet phone calls or SMS. The aim of surveillance of communication is to determine the written or spoken content of a communication transmitted over a network.[522]

In this respect, and especially regarding the above presented search of locations and objects, a major question evolves, namely the question about the relationship between the surveillance of communication and the securing followed by the seizure of evidence (according to sections 109 no. 1 and no. 2 of the Austrian Code of Criminal Procedure). The former constitutes the gathering of potential evidence in real-time, while the latter secures stored, not live, communication. Such communication can exists in various forms, such as a SMS on a mobile phone, stored e-mails on a hard drive or on the e-mail account hosted by a provider. Due to

---

518 cf. section 1 para. 1 no. 2 des Notifications Act 1999.
519 Reindl-Krauskopf, WK-StPO, section 134, MN 44.
520 cf. Fabrizy (2008), section 134 no. 3, p. 302; furthermore Reindl-Krauskopf, WK-StPO, section 134, MN 47.
521 Reindl-Krauskopf, WK-StPO, section 134, MN 48.
522 cf. as well section 135 no. 5 of the Austrian Code of Criminal Procedure.

the fact that the former is conducted in real time an actual securing is not possible.[523] The line between these two investigation methods can be drawn at the point where a communication ends – thus the point of time when the receiver actually received and recognized the content. Before that point of time, there is a stronger requirement for protection, meaning that no securing is possible and special criteria have to be given in order to conduct surveillance of communication. This means that, if the investigation authorities want to get knowledge about the content of a communication, they can do so directly via the (secured or seized) cell phone (SMS) or computer of one of either the receiver or the sender of the communication. This requires that the communication is stored on a communication device. The other possibility would be to rely on a provider and gather the information there. Depending where the information is conducted, the different rules of the Austrian Code of Criminal Procedure apply, namely the provisions concerning a simple securing if data are gathered directly from the affected person, whereas the special provisions of surveillance of data and communication apply if data are gathered at the provider.[524]

Section 135 para. 3 of the Austrian Code of Criminal Procedure regulates situation where data and communication are monitored. Generally there are three different situations possible allowing the investigation authorities to monitor communication:

- surveillance with consent – section 135 para. 3 no. 2 of the Austrian Code of Criminal Procedure
- surveillance without consent – section 135 para. 3 no. 3 of the Austrian Code of Criminal Procedure
- surveillance due to hostage-takings – section 135 para. 3 no. 1 of the Austrian Code of Criminal Procedure

---

523 Recording would be the only potential solution, however, as this term is already covered by surveillance and as a record of surveillance is produced by the conducting agency, it does not have to be either secured or even seized afterwards. Furthermore, the agency is already in possession of the evidence which legally belongs to nobody else than the agency.

524 cf. in this context especially Reindl-Krauskopf, WK-StPO, section 134, MN 49 et seq.; regarding the question whether it does constitute already surveillance of communication when persons enable voluntarily the criminal police to listen to their phone calls, cf. ibid MN 56-8.

3.4.5.2 Surveillance with Consent

Section 135 para. 3 no. 2 of the Austrian Code of Criminal Procedure regulates that surveillance can be conducted in situations where this measure is anticipated to encourage the solution of a criminal act committed with criminal intent, punishable by a term of more than 6 month imprisonment and the holder of a technical facility having been, or intended to become the origin or destination of a communication agrees explicitly to this investigation. The most prominent reason for the consent to surveillance is to aid the police in investigating the creator of a message and to document the content of this message, to, for instance, capture the originator of a death threat etc.[525]

Anticipation in this context means that there is a high level of likeliness to obtain helpful evidence via surveillance in order to solve a potential criminal act and/or charge a suspect.[526] Nevertheless, there has to be real suspicion concerning a particular criminal act, comparable to the above presented suspicion concerning the search of locations and objects.[527] Committed criminal acts are not only subject to punishment according to the Austrian Criminal Code alone, but rather than to all penal provisions of the Austrian legal system, if these provisions are punishable by a term of more than 6 months imprisonment.[528]

The holder of a technical facility is the person who has the actual authority to decide who is allowed to use the facility, when, how, and under which circumstances, also referred to as the empowered person to dispose. Under normal circumstances, this person is in a contractual relationship with an operator of telecommunication services – such as host or access providers. The providers offer their services such as e-mail addresses or (mobile) phone numbers and a connection to a communication network. Thereby, they establish the possibility for the holder of the facility to communicate over the network, for instance via e-mail, Internet phone calls, SMS or MMS. This situation can cause a problem if the contractual partner of the provider and the actual holder of the technical facility are not the same person. For instance, there are several people living in one household sharing one land line, or a company equips his employees with cell phones or separate e-mail addresses. This means that

525 cf. Seiler (2009), MN 499, p. 139 or Pilnacek, Pleischl (2005), MN 591, p. 122.
526 cf. Fabrizy (2008), section 135, p. 306.
527 cf. above and especially LG Klagenfurt 17.01.2008 7 Bl 8/08g stating that the command or authorization of a warrant requires the concrete suspicion of a committed criminal act.
528 cf. Reindl-Krauskopf, WK-StPO, section 135, MN 24 referring to the Addictive Drug Act and the Financial Penal Act.

a) the holder is not the same person as the contractual relation to a provider, or b) no (single) holder exists, as numerous persons share the facility with the provider's contract partner.

However, the actual authority to dispose is needed in order to give an official declaration of consent. Therefore, the holder of the technical facility has to be verified and separated from contract partners.[529] This is particularly important since the demanded consent has to be expressed explicitly and conclusively. Presumed consents are not satisfactory nor are consents given after surveillance took place.[530]

If a partner to a communication agrees to a monitoring of this communication, the 'interference' is legitimate. Moreover, it does not constitute an illegal interference with human/fundamental rights either if an investigation authority gathers knowledge of any communication accessible publicly (e.g. online chats or verbal communication on the street).[531] This principle can be applied to all investigation methods to be examined.

3.4.5.3 Surveillance without Consent

According to section 135 para. 3 no. 3 of the Austrian Code of Criminal Procedure surveillance of data and communication can be conducted if this measure appears to be necessary

- *for the solution of criminal act committed with criminal intend, punishable by a term of more than one year imprisonment;*
- *or for the solution or prevention of a criminal act, planed or committed in the context of a Criminal Organization or a Terrorist Association according to sections 278a and 278b of the Austrian Criminal Code, or if this would be complicated otherwise, and*

  a) the holder of the technical facility, having been, or intended to become the origin or destination of a communication, is suspected urgently of a criminal

529 Furthermore and especially in regards to public accessible telecommunication facilities and pay phones cf. Reindl-Krauskopf, WK-StPO, section 135, MN 27-32.

530 cf. Fabrizy (2008), section 135, p. 306; further Reindl-Krauskopf, WK-StPO, section 135, MN 33.

531 cf. as well to BVerfG, 1 BvR 370/07, 1 BvR 595/07 of 27 February, 2008, maxim no. 4: Verschafft der Staat sich Kenntnis von Inhalten der Internetkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin nur dann ein Eingriff in Art. 10 Abs. 1 GG, wenn die staatliche Stelle nicht durch Kommunikationsbeteiligte zur Kenntnisnahme autorisiert ist. Nimmt der Staat im Internet öffentlich zugängliche Kommunikationsinhalte wahr oder beteiligt er sich an öffentlich zugänglichen Kommunikationsvorgängen, greift er grundsätzlich nicht in Grundrechte ein.

act committed with criminal intend, punishable by a term of more than one year imprisonment or of a criminal act according to sections 278a and 278b of the Austrian Criminal Code, or

b) due to certain facts it is anticipated that a person suspected of a criminal act according to lit a, will use this technical facility or establish a connection to it.

Surveillance procedures have generally two aims: Firstly, surveillance can be conducted in order to solve a criminal act and secondly it can be used to investigate criminal acts committed in the context of a criminal organization or a terrorist association. Since no consent at all is needed for such investigations, the requirements to monitor have to be consequently severer than in situation where there a consent is required.

3.4.5.3.1 Prosecution of a Criminal Act

In order for surveillance to be used to investigate, the particular criminal act has to be punishable by a term of more than one year imprisonment and carried out with criminal intend (dolus). Moreover, as stated in lit a, the holders of the technical facility has to be suspects themselves, or as stated in lit b, it is assumed that the suspects intend to use this technical facility or establish a connection to it.[532] Another important aspect in this context is the phrase: 'the appearance of necessity'; this means that surveillance is necessary in order to solve a criminal act, thus to establish the truth. In addition, if evidence can be gathered by less invasive measures than surveillance, these methods have to be implemented, because surveillance can only be used as a last resort (ultima ratio).[533]

In order to conduct surveillance of data and communication, the law enforcement agencies must have strong suspicions about the affected person. This strong suspicion has to be based on both, the objective (actus reus) and subjective (mens rea) matters of fact of the actual criminal act.[534] Strong suspicion is given in particular, if there is a high level of probability that the suspected person is the offender of a certain criminal act. This corresponds to the

---

532 cf. for more clarification of the term holder and the range of penal acts above under chapter 'Surveillance with Consent'.

533 Reindl-Krauskopf, WK-StPO, section 135, MN 36.

534 cf. Fuchs, Helmut, Festschrift für Winfried Platzgummer (1995), p. 434.

suspicion needed to remand a person in custody.[535]

If, according to lit b, the investigating authority assumes that the suspected offender will use or establish a connection to the technical facility, there has to be corresponding evidence to back up these assumptions. In this respect it is to say that the terms 'use or establish a connection to the technical facility' implies an active act of the suspect. The main questions in this context is, whether it is allowed to monitor data and communication of not suspected persons, if it is assumed that the suspect will contact them[536]

3.4.5.3.2 Surveillance and Organized Crime

Section 135 para. 3 no. 3 Austrian Code of Criminal Procedure empowers the investigation authorities to conduct surveillance if there would be complications in regard to the solution or prevention of criminal acts intended to or committed in the context of the organized crime (sections 278 - 278b of the Austrian Criminal Code). As mentioned above, the holder of a technical facility has to be strongly suspicious, or the use or the establishment of a connection to the facility by a strongly suspected person has to be present. Contrary to the use of surveillance for the solution of a criminal act, it is not necessary that this investigating method is ultima ratio (the last resort). It can be implemented if other methods would be harder to conduct, cause delays, or higher financial costs.[537] Furthermore, in comparison to the above presented surveillance situation, it is to note that it is not necessary that the committed criminal act is punishable by a term of more than one year imprisonment and carried out with criminal intend. Due to the fact that this provision deals with organized crime, suspicion in regard to the formation of a criminal organization or a terrorist association alone is sufficient for conducting surveillance. This can be seen as an extension of criminal investigation methods, as even criminal acts punishable by a term of less than one year imprisonment can be investigated by surveillance of data and communication.[538] In circumstances where there is already suspicion regarding the foundation of a criminal organization, the criminal police is allowed to postpone its investigation in order to solve or prevent criminal acts about to be

---

535 cf. Reindl-Krauskopf, WK-StPO, section 135, MN 37.

536 cf. as well the practical example and the critique in Reindl-Krauskopf, WK-StPO, section 135, MN 39-40, referring to 12 Os 152/00.

537 cf. Reindl-Krauskopf, WK-StPO, section 135, MN 42.

538 cf. the extensive examination of this problem in Reindl-Krauskopf, WK-StPO, section 135, MN 43.

committed by the organization. This possibility in the Austrian Code of Criminal Procedure, as mentioned above, involves another extension of the surveillance. However, as Reindl-Krauskopf argues, there are two limitations to that: firstly there has to be strong suspicion in regard to the organizational aspect and secondly there has to be suspicion concerning the organization's committed or planned criminal acts.[539]

3.4.5.3.3 Surveillance due to Hostage-Takings

Section 135 para. 3 no. 1 of the Austrian Code of Criminal Procedure provides the criminal police with an important tool in regard to investigations of hostage-takings. As this provision deals with a variety (of different methods, which have to presented first, the detailed description of surveillance due to hostage takings will be illustrated subsequently afterwards.[540]

3.4.6 Conclusion: Realization of an RFI

Contrary to a search of locations and objects, Surveillance of Data and Communication according to sections 135 para. 3 in conjunction with 134 no. 3 of the Austrian Code of Criminal Procedure is capable to deal with the latter two task of an RFI, the surveillance of activities and the surveillance of telecommunication. This is especially true since these provisions are not dealing with data stored in a communication system, but they rather govern the handling of communication.[541]

Due to the very nature of an RFI as a covert investigation method, the surveillance of data and communication seems to be more appropriate in this case, since this method is also a covert investigation. Moreover, the physical as well as mental elements of the criminal act for the conduction of surveillance are similar to that put forward by the Austria Federal Ministry of

---

539 cf. Reindl-Krauskopf, WK-StPO, section 135, MN 44; cf. furthermore below in the context of a major electronic eavesdropping operation.

540 cf. the presentation in the chapter on surveillance of persons; however, cf. as well the critique of Reindl-Krauskopf, WK-StPO, section 135, MN 46.

541 cf. below.

Justice and of the Interior.[542] The elements of the criminal activity require certain seriousness as well as there has to be a certain level of criminal intend. This is important, especially in view of the principle of proportionality, which has to always be kept in mind when dealing with covert investigations. Furthermore, as already stated above, surveillance of communication involves every kind of communication, no matter how it is transmitted. Hence, there are no specific technological requirements, meaning that it applies to communication conveyed via a computer system as well.[543]

The surveillance of data and communication regulates the handling of communication and deal thereby on the on hand with the outer communication data – thus who communicated with whom and when – and on the other hand with the surveillance of the communication's content, as long as this specific communication is transmitted. There is, however, no extension to data stored in a communication system.[544] Only if communication or data is conveyed or exchanged over a communication system, the criminal police is allowed to intercept and use it. Surveillance of communication constitutes the gathering of information in real-time. At the point where a communication ends, meaning the point when the receiver recognizes the content, the monitoring of the communication ends as well. Hence, from that point in time on, only a disclosure of transmission data can be conducted.[545] Important to note in this context is that stored communications on electronic storage devices etc. is not covered by this provision.

3.4.6.1 Surveillance of Telecommunication

When it comes to surveillance of data and communication, an RFI, in the sense of surveillance of telecommunication, is not possible. Hence it cannot be subsumed under sections 135 para. 3 in conjunction with 134 no. 3 of the Austrian Code of Criminal Procedure, surveillance of data and communication. Due to the fact that these provisions deal with an interception of communication, there is need for clarification of the term 'interception'. Interception, in this context, refers to the points in time when a communication is sent out and when it is received. Only between these two points in time is it possible to intercept – everything else would legally not constitute an interception. As already mentioned

542 cf. Vortrag an den Ministerrat der Republik Österreich, of 17 October, 2007.
543 cf. EBRV 25 BlgNR XXII GP, p. 187.
544 BMJ/BMI (2008), p. 38.
545 cf. below.

above, it is not difficult to define when a communication is received, i.e. the point of time when the receiver actually recognizes the content. However, it is more complex to define when a communication is sent:

First of all, it is necessary that a statement is made in either oral or written form, because it is only possible to monitor observable things. Thus, the monitored persons have to express their thoughts willingly, as mind control in the sense of reading someone's thoughts is not possible, or legally viable.[546]

Second of all, depending on the form of communication, there are different limitations. When writing a letter, e-mail, SMS or an instant message, the originator express him/herself indirectly, as they have the power to refrain from sending the communication to the receiver. For instance, the originator wants to confess his love to his beloved neighbor via a letter – not until he posts it, any communication happened between the two. Before posting a letter or pressing the corresponding button to send the message, the designated sender just transformed his/her inner intellectual world into electronic data. However, until the information is sent, these thoughts are still highly intimate.[547] Only after the communication has left the originators sphere of influence, is it transmitted – thus ready to become intercepted.

An oral communication, in this context, is somewhat different since the originator of a communication does not have to press a certain button for it to be sent and received. It is transmitted on the spot to the receiver. However, there does not seem to be an unequal treatment of both means of communication by the Austrian Code of Criminal Procedure. Why should an oral conversation be treated differently than a written one? Is the former less worth being protected? Further problem can occur in one way communication where the message is not immediately received by the person it is directed to, i.e. message on an answering machine etc.

However, in both cases – the oral and the written communication – there is the need for

546 cf. as well BMJ/BMI (2008), pp. 26 and 96-97.

547 In this respect just think about the question whether it is loud if you are alone shouting in a deep forest and nobody can hear you …???

something additional in order to have a communication sent. In the first case, the send button has to be pushed; and in the second case, a connection to the communication partner has to be established, thus a number has to be dialed. Problems might occur in situations where a computer or a mobile phone is not logged onto a communication network, such as the Internet or there is a signal-free zone with no connection at all. In these circumstances it is not possible to communicate at all, meaning furthermore that an interception cannot be conducted.

An interception, by definition, cannot be conducted on a technical device.[548] The use of any bugs, Trojan horses, key loggers etc. on communication devices does not constitute an interception of a communication rather than a search of an electronic device, thereby interfering massively with the most private and intimate affairs of a person. The usage of such devices is more or less similar to a remote access for search purposes – the shared characteristics are evident. There is, however, no difference between the surveillance of data and communication done in this way and the remote access to a digital diary on a computer.[549]

3.4.6.2 Surveillance of Activities

In respect to the second potential task of an RFI – the surveillance of activities – it can be argued that when a user browses, a different form of communication is present. The electronic device sends requests to specific homepages/servers and receives, as reply, a copy of the demanded information, which are then stored on a server. The viewed data, such as images, text, sounds, are then copied from the host server to the user's own computer and stored there. Hence, there is communication when 'surfing the web'. However, as just presented above – this information can only be gathered via an interception and as the use of any technical device on a computer does not constitute an interception, surveillance of activities cannot be based on surveillance of communication and data according to sections 135 para. 3 in conjunction with 134 no. 3 of the Austrian Code of Criminal Procedure.

---

548 Note in this context that, as already presented in the chapter of this thesis on the technical aspects of a RFI, due to the modus operandi of modern communication networks, an interception is rather unlike fruitful because of its digital packet-switched transmission; cf. already above.

549 A non-communication or message related data processing does not constitute a expression in the wider sense as stated in BMJ/BMI (2008), p. 26.

In addition, for both tasks of an RFI the criminal polices depends on the assistance of providers. In this respect there is no provision empowering the criminal police to store or monitor communication on their own, meaning that the investigation authorities and the providers have to cooperate in order to conduct surveillance of data and communication.[550] This is reasonable since providers have a contractual relationship with their clients, i.e. the user whose communications the criminal police wants to monitor, and thus all communication related information is accessible by the provider.

3.4.7 Disclosure of Transmission Data

3.4.7.1 Introduction

A disclosure of transmission data is, according to section 134 no. 2 of the Austrian Code of Criminal Procedure, a disclosure of traffic date, access data and location data of a telecommunication service or an information society service.[551] The definitions of these different kinds of data can be found in the Austrian Telecommunications Act 2003 stating that

- 'Traffic data' means

  any data processed for the purpose of the conveyance of a communication on a communications network or for the billing thereof.

This definition originates from the Directive 2002/58/EC of the European Parliament and of the Council.[552] As the Explanatory Memorandum to the Telecommunications Act 2003 points out, traffic data […]'*consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network.*'[553] In respect to criminal proceedings, especially the active and passive participants of a telecommunication (respectively their numbers) and

---

550 Regenfelder (2008). p. 106.

551 section 134 no. 2 of the Austrian Code of Criminal Procedure.

552 Directive 2002/58/EC of the European Parliament and of the Council of 12 July, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

553 cf. (15) of Explanatory Memorandum of Directive 2002/58 EC.

the time and duration are of great interest.[554]

- 'Access data' means

  the traffic data created at the operator during access by a subscriber to a public communications network and required for assignment to the subscriber of the network addresses used for a communication at a specific point of time.

This type of data describes the part of traffic data necessary for the identification of a participant of an Internet communication. Hence, as such access data are only a subarea of traffic data.[555]

- 'Location data' means

  any data processed within a communications network, indicating the geographic location of the telecommunications terminal equipment of a user of a publicly available communications service.

This definition goes back to the above mentioned EC Directive and […]'*refers to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.*'[556] This refers at least data arising during a communication.[557] However, even data from outside a conducted communication is covered by the definition. Such data arises, for instance, when a mobile phone is switched on and logged into a network.[558]

As previously mentioned, the term information society service refers to any service, normally provided for remuneration, at a distance, by electronic means and at the individual request of

---

554 cf. Reindl-Krauskopf, WK-StPO, section 134, MN 32.
555 cf. AB 184 BglNR XX GP, p. 3 as well as Singer, Christian, in Stratil, Alfred (ed), TKG – Telekommunikationsgesetz (2003), 3rd edition, section 92, p. 292.
556 cf. (14) of Explanatory Memorandum of Directive 2002/58 EC.
557 cf. Reindl-Krauskopf, WK-StPO, section 134, MN 34.
558 In this respect, please cf. Reindl-Krauskopf, WK-StPO, section 134, MN 35.

a recipient of services.[559]

Section 134 no. 2 of the Austrian Code of Criminal Procedure states which data has to be disclosed in specific circumstances. Providers are obligated to disclose particular data bound to a telecommunication (traffic data) or independent of a telecommunication (location data).[560] The disclosure of transmission can be used to capture call data and for a location analysis. While the capturing of call data deals with the detection of terminals that are or were the origin and destination of a telecommunication, the assessment of location deals with the definition of the local area the terminal device is or was situated.[561]

Important to note in this context is that phone numbers are double functional – as the personal number of a user it is 'master data' according to section 92 para. 3 no. 3 of the Austrian Telecommunications Act 2003, and in case of a telecommunications it is considered traffic data as well. This circumstance raises the question to whether data may be disclosed by the investigating authorities.[562] Moreover, there is a difference between the disclosure by a provider – thus the contractual partner of a user – and the securing (and later seizure) of mobile phones of computers directly from their users. As modern electronic devices store a massive amount of data, both methods (disclosure or seizure of the device) would be equally fruitful. However, there are different provisions applicable for the two methods.[563]

Similar to the surveillance of data and communication[564] the disclosure of transmission data is allowed in circumstances where there is

- disclosure with consent – section 135 para. 2 no. 2 of the Austrian Code of Criminal Procedure

---

559 cf. section 1 para. 1 no. 2 des Notifications Act 1999 and above concerning surveillance of data and communication.

560 cf. EBRV 25 BlgNR XXII GP, p. 187.

561 Fabrizy (2008), section 134, p. 301.

562 cf. for further details Reindl-Krauskopf, WK-StPO, section 134, MN 38.

563 i.e. a search of locations or objects (cf. above) and a disclosure of transmission data; cf. furthermore cf. for further details Reindl-Krauskopf, WK-StPO, section 134, MN 40.

564 This is mainly due to the fact that surveillance of data and communication is historically seen the prototype of an interference with the content of a communication; cf. Reindl-Krauskopf, WK-StPO, section 135, MN 21.

- disclosure without consent – section 135 para. 2 no. 3 of the Austrian Code of Criminal Procedure
- disclosure due to hostage-takings – section 135 para. 2 no. 1 of the Austrian Code of Criminal Procedure

3.4.7.2 Disclosure with Consent

Section 135 para. 2 no. 2 of the Austrian Code of Criminal Procedure governs that surveillance can be conducted in situations where this measure is anticipated to encourage the solution of a criminal act committed with criminal intent, punishable by a term of more than 6 month imprisonment and if the holder of a technical facility, who has been, or intends to become the origin or destination of a communication, agrees explicitly to this surveillance.

The solution of a criminal act is of utmost importance in these cases, meaning that it has to be highly likely that a disclosure will provide the necessary evidence needed to solve a criminal act and/or to charge a suspect.[565] A limitation to the Austrian Criminal Code is not given.

3.4.7.3 Disclosure without Consent

According to section 135 para. 2 no. 3 of the Austrian Code of Criminal Procedure, a disclosure of transmission data can take place if it is anticipated that the solution of a criminal act committed with criminal intend, punishable by a term of more than one year imprisonment is encouraged. In addition, it may be expected that data of the defendant can be detected. In comparison to a disclosure with consent, the requirements for a disclosure without consent have to be consequently severer. However, both methods have the aim to encourage the solution of a criminal act in the sense already stated above.

Again, this provision of disclosure without consent is quite similar to the surveillance without

[565] cf. Fabrizy (2008), section 135, p. 306.

consent. The main difference is that the disclosure is only allowed for the solution of a criminal act punishable by a term of more than one year imprisonment and not, as in the above presented case of surveillance, also explicitly in regard to organized crime. The similarities of surveillance of data a communication without consent and a disclosure of transmission data without consent are evident. However, there are also some differences. While a disclosure has to simply encourage the solution of a criminal act,[566] the conducting of surveillance has to be the last resort (ultima ratio) for a criminal investigation.[567] Furthermore, a simple suspicion of a criminal act is enough for a disclosure, whereas there has to be strong suspicion before surveillance can be conducted. The different requirements for both investigation methods are mainly due to the less invasive character of a disclosure in comparison to surveillance without consent.[568]

The gathering of a defendant's data is to be anticipated. For instance, a defendant's telephone number can be disclosed if it is assumed that a specific person of interest has phoned the defendant. This means that out of a known person's data, data, such as a telephone number, of a defendant is gathered. However, as Reindl-Krauskopf points out, 'data of the defendant' is a rather broad term and can involve numerous things and situations.[569] For instance, it is allowed to conduct a disclosure of the victim's transmission data (e.g. of homicide), if it is anticipated that he/she has or was contacted his/her by the murderer.[570]

3.4.7.4 Disclosure due to Hostage-Takings

Section 135 para. 2 no. 1 of the Austrian Code of Criminal Procedure provides the criminal police with an important tool for investigations in hostage-takings. A disclosure is allowed *if and as long as there is strong suspicion in regard to a hostage-taking, and a disclosure is*

---

566 Meaning that there is a certain presumption that a disclosure will result in useful evidence; cf. Reindl-Krauskopf, WK-StPO, section 135, MN 61.

567 Meaning that if evidence thought to be gathered via a disclosure could be gathered by other (less invasive) investigation methods, its conducting is not allowed; cf. already above and Reindl-Krauskopf, WK-StPO, section 135, MN 36.

568 Note that a disclosure presents only isolated and temporal limited data of conducted communications, whereas surveillance includes the content of these communications; cf. in this context especially the critique in Reindl-Krauskopf, WK-StPO, section 135, MN 61.

569 For an extensive examination of the borderline and the related problems cf. Reindl-Krauskopf, WK-StPO, section 135, MN 62.

570 cf. OGH 18.1.2001, 12 Os 152/00 and 12 Os 153/00 regarding a disclosure of data of pay phones in the context of homicide.

limited to instances and statements accomplished at the time and location of the deprivation of liberty.

Similar to the below presented surveillance of persons in a hostage-taking, there are limitations for the disclosure of transmission data. Strong suspicions[571] and the limitation to the time and the location of the deprivation of liberty, according to section 99 of the Austrian Criminal Code are needed.

3.4.8 Conclusion: Realization of an RFI

Similar to surveillance of data and communication, a disclosure of transmission data according to sections 134 no. 2 in conjunction with 135 para. 2 of the Austrian Code of Criminal Procedure seems to be potentially able to deal with the latter two task of an RFI, the surveillance of activities and the surveillance of telecommunication. However, due to the reasons already presented in the context of the surveillance of data and communication it is not working. The reasons for this are the same as just presented in the context of surveillance of data and communication (according to sections 135 para. 3 in conjunction with 134 no. 3 of the Austrian Code of Criminal Procedure). The fact that there is cooperation between providers and the criminal police is a strong argument against an application of a RFI based on a disclosure of transmission data. Apart from that, investigation authorities are rather interested in content data than in other things.[572]

---

571 Regarding the requirement of strong suspicion please cf. above in the chapter about surveillance of data and communication without the consent; further Fuchs (1995), p. 434;and Reindl-Krauskopf, WK-StPO, section 136, MN 4,5.

572 cf. BMJ/BMI (2008), p. 4.

3.4.9 Surveillance of Persons

3.4.9.1 Introduction

Section 134 no. 4 of the Austrian Code of Criminal Procedure defines the phrase of 'optical and acoustic surveillance of persons' as surveillance of

- the conduct of persons – by interference with their right to privacy – and
- the statements of persons – privileged information

by the use of technical means for an image and audio transmission, and for an image and audio recording, without the affected person's noticing .[573]

As it is with all coercive measures, surveillance of persons interferes with the rights of the affected person. However, in this case the provision states precisely which right it infringes, namely Art 8 ECHR – the right to privacy. Furthermore, other infringements, such as with the right to data protection or the householder's rights, are also highly likely.

Since surveillance is carried out without the knowledge of the affected person – surveillance of data and communication is a pure covert investigation. In fact, the main intention behind a covert investigation is that observed persons continue to do everything as they normally would and not change their behavior because they know they are being monitored.[574]

The Austrian Code of Criminal Procedure distinguishes between pure optical operations, using only technical means to transmit or record images, and electronic eavesdropping operations. The latter can be divided into two different options of surveillance: First of all it is possible that nobody but the monitoring person knows of this particular surveillance. This means that only technical tools are use in order to observe the conduct or statements of persons. This special form of surveillance is called a major electronic eavesdropping

---

573 section 134 no. 4 of the Austrian Code of Criminal Procedure.

574 cf. Reindl-Krauskopf, WK-StPO, section 134, MN 109; in this respect it has to be mentioned that the relation between section 134 no. 4 and section 131 of the Austrian Code of Criminal Procedure is that the former deals with an electronic 'observation' while the latter constitutes only the work of undercover agents leaving technical means aside; cf. furthermore below and ibid MN 113.

operation. On the contrary to this, a minor electronic eavesdropping operation involves also technical facilities for monitoring, but in addition a well-informed person – such as an undercover agent – is present on site.

The main difference between these two forms is that while the former in conducted with the means of technical equipment only, such as bugs established in private rooms – the latter involves, besides technical equipment, a person that is physically present. A detailed presentation follows.

3.4.9.2 Conduct of Persons

Privacy means everything not intended to be known by a larger undefined group of persons. Thus an interference with the right to privacy is given when the affected person is monitored unknowingly – as for instance when they are at home. However, this does not constitute that privacy is only given if a certain location is not publicly accessible, as for example in the case of a publicly accessible toilet.[575]

3.4.9.3 Statements of Persons

Besides the conduct of persons, the second goal of surveillance is the monitoring of people's verbal statements. Here, only statements not directly intended for the public or a third person are covered. Hence, there is not explicitly an interference with the right to privacy involved. Overall the two aims of surveillance of persons are similar: in both cases a monitored person trusts that nobody else than the persons directly present knows about statements made or behavior brought forth. Generally, these statements are made in self-contained locations, familiar to the monitored persons (in their flats, in their cars, etc). The only difference when it comes to the conduct of persons is, that statements are made in publicly accessible places, which does not necessarily constitute that the persons expect to be monitored or over-heard by a third party.[576]

---

[575] cf. Reindl-Krauskopf, WK-StPO, section 134, MN 110; regarding this, special attention has to be drawn to an observation according to section 130 of the Austrian Code of Criminal Procedure; cf. ibid MN 110

[576] e.g., persons may reckon that their conduct can be monitored when having a chat in a cafe; however the discussing they are having with somebody else in this cafe is not intended to be noticed by third person – thus it is conducted in an appropriate manner; cf. ibid MN 112.

3.4.9.4 Use of Technical Means

Only if technical facilities are used for surveillance is it regulated by sections 134 et seq. of the Austrian Code of Criminal Procedure.[577] Generally, any technical devices capable to convey or store images and sounds are included and can be used for monitoring purposes. According to the government bill introducing this provision, it means any technical device capable to intensify and transfer impressions or audios, or to record impressions or audios.[578] Examples for such devices are cassette tape or video recorders, listening devices, mini microphones, or bugs but also digital devices such as CD- or DVD burners.[579]

Section 136 of the Austrian Code of Criminal Procedure defines the requirements under which an optical and acoustical surveillance can be (legally) conducted. Overall there are five different options of surveillance laid out in this provision, each with different requirements for its execution:

Para. 1 states the three main situations in which optical and acoustical surveillance may be applied: no. 1 includes surveillance in hostage-taking situations, no. 2 deals with the minor electronic eavesdropping operation, and major electronic eavesdropping operation are summarized in no. 3. Furthermore, para. 3 mentions two situations limited to optical surveillance only, namely surveillance outside of flats or other locations protected by householder's rights in no. 1 and surveillance inside of such locations in no. 2.

3.4.9.5 Surveillance due to Hostage-Takings

Para. 1 no. 1*: if and as long as there is strong suspicion in regard to a hostage-taking, and surveillance is limited to instances and statements accomplished at the time and location of the deprivation of liberty;*

Section 136 para. 1 no. 1 of the Austrian Code of Criminal Procedure provides the possibility

---

577 Surveillance without the use of nearly any technical means constitutes an observation according to section 130 of the Austrian Code of Criminal Procedure; only technical means for the assignment of a person's position are allowed in this respect; cf. ibid MN 113.

578 cf. EBRV49 BlgNR XX GP, p. 16; Hence binoculars or similar tools are not covered as they establish or guarantee only actual impressions, rather than installing a transmission; the same is true for tracking devices or for devices used for wiretapping.

579 cf. Leukauf, Otto, Steininger, Herbert, Kommentar zum Strafgesetzbuch, (1992), 3rd edition, MN 4 et seq, p.714; furthermore Reindl-Krauskopf, WK-StPO, section 134, MN 113.

for the investigating authorities to conduct an optical and acoustical surveillance if and as long as there is strong suspicion[580] that a person – subject to this surveillance – abducted and confines another person. Furthermore, it is to note that such surveillance is limited to the time and the location of the deprivation of liberty, according to section 99 of the Austrian Criminal Code.

Regarding the temporary limitation in such cases, it is to say that whenever surveillance is conducted, there has to be strong suspicion concerning a hostage-taking. As soon as this suspicion is gone (for instance – it becomes apparent that there is/was no hostage-taking, or the hostage was released), the corresponding surveillance has to be abandoned. This also means that law enforcement is not allowed to keep on monitoring in order to investigate whether there were backers or partners in crime. Thus, strong suspicion in respect to a hostage-taking has to be given throughout the whole surveillance in order for it to continue.[581] Local limitation in hostage situations indicate that only the actual location of the hostages – respectively their assumed location – can be monitored, meaning once again that there is no possibility to observe (potential) backers etc.

Due to these strong limitations, it is, however, not necessary for the criminal police to obtain a warrant prior to exercising surveillance. This is stated explicitly in section 137 para. 1 of the Austrian Code of Criminal Procedure.

3.4.9.6 Minor Electronic Eavesdropping Operation

Para. 1 no. 2: *if surveillance is limited to instances and statements intended to be noticed by an undercover agent (or alike), or if these things* could *be noticed directly by an undercover agent, and this evidence appears to be necessary for the solution of a crime according to section 17 para. 1 of the Austrian Criminal Code;*[582]

---

580 Regarding the requirement of strong suspicion please cf. above in the chapter about surveillance of data and communication without the consent; further Fuchs (1995), p. 434; and Reindl-Krauskopf, WK-StPO, section 136, MN 4,5.

581 cf. Reindl-Krauskopf, WK-StPO, section 136, MN 6.

582 Note in this context that the difference between an offense and a crime is that the latter is punishable by a term of more than three year imprisonment.

Section 136 para. 1 no. 2 of the Austrian Code of Criminal Procedure provides the regulations of a minor electronic eavesdropping operation. This surveillance method is limited to processes and statements either meant to be noticed by a person involved with the surveillance, or accessible to this person. Hence, this form requires the employment of an undercover agent or alike.[583] The undercover agent tries to win the trust of the unsuspecting affected person in order to gather evidence. Thereby the agent is subject to a certain risk of detection

There are two different ways to gather evidence in minor electronic eavesdropping operations: On the one hand, the undercover agent gets involved or informed directly by the affected person who is known to the undercover agents,[584] or on the other hand the undercover agent can observe statements or processes not addressed directly to him.[585] Surveillance conducted in this manner constitutes only a minor interference, since the well-informed person gathers information based on what he would have noticed or heard anyway.[586] It is only a reliable way to secure evidence in order to solve a crime.[587]

A minor electronic eavesdropping operation is only permitted if necessary and conducted in relation to the solution of a crime according to section 17 para. 1 of the Austrian Criminal Code, meaning criminal acts punishable by a term of more than three year imprisonment. Please refer to the previous chapter of the surveillance of data and communication.[588] Here again necessity (‘appears to be necessary’) is the key to an approved surveillance, meaning that surveillance has to be necessary in order to solve a criminal act. In addition, the requirement of surveillance is ultima ratio, meaning that if evidence could be gathered by less invasive investigation methods, a minor electronic eavesdropping operation is prohibited.

---

583 As Reindl-Krauskopf points out, such surveillance can be conducted by an undercover agent or other well-informed person – thus a minor electronic eavesdropping operation can be conducted by a staff of the criminal police or other personnel, cf. Reindl-Krauskopf, WK-StPO, section 136, MN 12.

584 Such statements are e.g. messages, information and alike directly addressed to the undercover agent, meaning that the affected person is intended to tell etc the undercover these things explicitly.

585 This means e.g. that the undercover agent achieves knowledge of something said to a third person while the agent was nearby a conversation; cf. Reindl-Krauskopf, WK-StPO, section 136, MN 11.

586 cf. EBRV49 BlgNR XX GP, p. 17.

587 cf. Seiler (2009), MN 506, p. 141.

588 cf. above as well as EBRV49 BlgNR XX GP, p. 17.

The concrete suspicion against a person needed for the execution of surveillance does not have to be explicit. For surveillance to be permitted, it has to assist the solution of a crime. Suspicion similar to that required for the search of locations and objects is needed in order for one to be warranted. The only things necessary are a suspicion that a crime has been committed and that a person capable to give relevant information can be monitored. Otherwise surveillance would not be relevant for the solution of that crime.[589]

3.4.9.7 Major Electronic Eavesdropping Operation

Para. 1 no. 3: *if the solution of a criminal act punishable by imprisonment for a minimum period of ten years, or of a Criminal Organization or a Terrorist Association according to sections 278a and 278b of the Austrian Criminal Code, or for the solution or prevention of a criminal act committed, or planed by such an organization or* association*; or if the investigation regarding the residence of a person suspected of such crimes would be desperate or complicated otherwise and*

> *a) the affected person is strongly suspected of having committed one of the mentioned crimes or*
>
> *b) due to facts it is assumed that the affected person will established a connection which such a person*

Section 136 para. 1 no. 3 of the Austrian Code of Criminal Procedure deals with major electronic eavesdropping operations. The main difference between a minor and a major operation is that while the former involves at least one well-informed, involved person, the latter is conducted entirely electronically, meaning that none of the monitored persons knows about the surveillance. Hence, the barriers for an execution are higher. Moreover, major electronic eavesdropping operations have three different goals: the solution of a crime, prevention of a criminal act of a criminal organization or terrorist association, and the investigation of a suspect's residence.

---

589 cf. Reindl-Krauskopf, WK-StPO, section 136, MN 14.

3.4.9.7.1 Solution of a Crime

The limitations for a major electronic eavesdropping operation require that a person is strongly suspicious of having committed a serious felony, one that is punishable by an imprisonment for a minimum of 10 years.[590] In addition, further aspects have to be taken into consideration when it comes to criminal organizations or a terrorist association. When it comes to organized crime, for example, strong suspicion in regard to the organizing aspect of it has to be present. Hence, there needs to be suspicion against long run establishments of a business-like cooperation operated by a number of people for the purpose of committing certain criminal acts, gather influence or to corrupt other person etc. In addition, strong suspicion must be given that the suspect has founded the organization or participates in it.[591] As Reindl points out in this respect, an occasional participation in criminal acts is too little to justify surveillance, there has to be a direct involvement in the organization as such.[592] The same is true – with the relating modifications[593] – for a terrorist association. If these requirements are given, investigators are allowed to conduct surveillance – either of the strongly suspected person (lit a), or of a person assumed to be contacted by the strongly suspected person (lit b) – thus of a contact person.[594]

3.4.9.7.2 Prevention or Solution of a Crime

As already stated in the context of the surveillance of communication, due to the fact that this provision deals with organized crime, suspicion in regard to the formation of a criminal organization or a terrorist association alone is sufficient for conducting a major electronic eavesdropping operation.

Most importantly, there has to be suspicion in regard to the organizational aspect – thus suspicion that a criminal organization or a terrorist association is established.[595] Furthermore, the target person of such surveillance has to be, according to lit a, suspicious of a crime, that is punishable by imprisonment for a minimum period of ten years, or of having committed or

---

590 cf. above and Fuchs (1995), p. 434.
591 cf. section 278a para. 1 of the Austrian Criminal Code.
592 cf. Reindl-Krauskopf, WK-StPO, section 136, MN 16.
593 according to section 278b of the Austrian Criminal Code.
594 e.g. it is allowed to monitor the flat of the strongly suspected person's girlfriend, if there are reasons to believe that this person is going to visit her and evidence could be gathered by this surveillance; cf. Reindl-Krauskopf, WK-StPO, section 136, MN 18.
595 cf. as well the illustrations subsequently.

planned criminal acts within such organizations, or according to lit b, a contact person of such a suspect. This means that in both cases it is necessary that surveillance is directed against the specific person directly. Note in this context that the suspicion of a membership in a criminal organization is sufficient for the conduction of surveillance, if it is assumed that surveillance is enough to prevent or solve criminal acts committed by the organization or association, and this goal could otherwise only be achieved with substantially greater effort.[596] This indicates that a major electronic eavesdropping operation is only legal if dual suspicion is present: for one there has to be a strong suspicion that a specific crime (even below a maximum imprisonment of then years) was or is being committed, and second of all this crime was/is committed by a criminal organization.

3.4.9.7.3 Residence of a Suspect

If a person is suspected for the criminal acts mentioned in section 136 para. 1 no. 3 of the Austrian Code of Criminal Procedure, it is possible to conduct a major electronic eavesdropping operation in the residence of the suspect, if all other requirements are fulfilled as well. Once again, strong suspicion is needed before the suspects themselves (lit a) or their contact partners (lit b) can be monitored.

A major electronic eavesdropping operation can, furthermore, only be conducted if certain requirements regarding its necessity and proportionality are met. First of all, this method of surveillance has to be necessary in order to solve or prevent crimes stated in the provision. The provision governs that it is allowed a) if the solution or prevention of the crimes would be despairing, and b) if the solution or prevention of the crimes, or the investigation concerning the residence of a person would be complicated otherwise. The latter requirement somewhat softens the demands for a conduct because it means that a major electronic eavesdropping operation can be allowed even if there are other measures at disposal. This method is not the last resort (ultima ratio).[597] In addition to this, section 136 para. 4 2nd sentence of the Austrian Code of Criminal Procedure states that there has to be the assumption that the planned criminal acts constitute a great danger for public security. This threat is given, if planned

[596] cf. EBRV49 BlgNR XX GP, p. 18.
[597] cf. Reindl-Krauskopf, WK-StPO, section 136, MN 21.

crimes are every different to regular, ordinary crimes. The simple suspicion concerning the application of a major electronic eavesdropping operation cannot be justified by a simple hunch that it may be prevented.[598]

Section 136 para. 2 of the Austrian Code of Criminal Procedure offers another, not less significant possibility for the investigating authorities. It states that to *the extent that surveillance is unavoidable according to para. 1 no. 3, it is allowed to invade a flat or another location protected by householder's rights, if due to facts it is assumed that a suspected person will use the affected location.*

Hence, this provision allows in circumstances where a legal (judicial approved) major electronic eavesdropping operation cannot be conducted successfully without the installation of technical devices in flats or other locations protected by householder's rights, the entering of such premises can be allowed as well. However, there has to be reasonable suspicion in regard to the use of the location by the suspected person.[599] The installation or de-installation of surveillance devices (e.g. bugs etc) has to be granted by a separate judicial approval (thus a second warrant) because this action constitutes an autonomous interference with fundamental rights.[600] The same principles as in the search of location and objects apply in this context as well – hence, only if the location is protected by householder's rights, judicial approval is necessary. Other locations (for instance vehicles etc) can be entered in order to install surveillance devices without a second, separate and explicit warrant. Nevertheless, the rights of affected persons are restrained because there is an interference with their privacy according to Art 8 ECHR.[601]

3.4.9.8 Optical Surveillance[602]

Section 136 para. 3 of the Austrian Code of Criminal Procedure regulates pure optical surveillance. As already mentioned, there are two possible forms:

An optical surveillance of persons in order to solve a criminal act is allowed

---

598 cf. ibid MN 20, 22 and JAB 812 BlgNR XX GP 6.
599 cf. Reindl-Krauskopf, WK-StPO, section 136, MN 19.
600 cf. section 137 para. 1 of the Austrian Code of Criminal Procedure.
601 cf. concerning further information in this context Reindl-Krauskopf, WK-StPO, section 136, MN 19.
602 cf. e.g. Fabrizy (2008), section 136, p. 310 or Pilnacek, Pleischl (2005), MN 593 et seq, p. 123.

- *if it is limited to processes outside homes or other locations protected by householder's rights and if it is intended to observe items or locations in order to monitor the conduct of persons having contact with these items or visiting these locations, or*

- *with consent of the holder, if it is solely for the purpose mentioned in no. 1, in a flat or other locations protected by householder's rights, intended to solve a criminal act punishable by imprisonment for a minimum period of one year and if the solution would be complicated otherwise.*

As with a search of locations and objects, there is a division between locations protected by householder's rights and such which are not. In the latter case surveillance can be conducted in order to solve any criminal act. The only requirements are suspicion in regard to a committed criminal act and that surveillance is only intended to monitor objects or locations in order to gather information about persons entering. In addition, an evaluation according to section 5 of the Austrian Code of Criminal Procedure has to be conducted – thus proportionality has to be given. Regarding the phrase 'outside areas protected by householder's rights', a distinction has to be made: on the one hand there are premises, rooms, vehicles or vessels not publicly accessible[603] and on the other hand there are locations publicly accessible, such as parks, streets or hallways.[604]

A pure optical surveillance of locations protected by householder's rights demands further and more difficult criteria before it can be conducted. First of all, it has to have the intention to solve a criminal act punishable by imprisonment for a minimum period of one year. Second of all, the solving of that specific criminal act would be complicated otherwise, meaning that an optical surveillance is allowed even if there are other investigation methods available. However, the other methods have to require substantial greater effort to achieve the same result. Third of all, proportionality has to be evaluated and lastly the most important requirement, the consent of the location's holder is needed. The consent has to be expressed explicitly and has to be declared before the actual surveillance takes place.[605]

---

603 cf. the comments regarding a search of locations and objects.

604 cf. regarding this difference especially Reindl-Krauskopf, WK-StPO, section 136, MN 26-9.

605 cf. concerning the consent the comments made in regard to surveillance of data and communication – surveillance with consent.

As it is with other procedural provisions, the public prosecution has to report its intended direction (after a judicial approval) to the agency of the public prosecution.[606] However, there is an exception to this, namely in the case of surveillance due to hostage-takings. In such situations, where an actual dangerous situation is present, no such requirement has to be met. Concerning the temporary frame of an optical and an acoustical surveillance it is to say that it depends on necessity, better, the length of time it takes to accomplish the task.[607] Both the public prosecution's direction and the judicial approval have to include all relevant data mentioned above.[608]

3.4.9.9 Rights and Obligations

As mentioned above, sections 139 and 140 of the Austrian Code of Criminal Procedure handle the investigating authorities' obligations towards the affected person, as well as the affected persons' rights after a conducted surveillance/disclosure. These regulations apply for all three of the above illustrated methods, namely for the disclosure of transmission data, the surveillance of communication as well as the optical and acoustical surveillance of persons and will be presented hereafter. Before going into any detail it is to mention that while section 139 deals with the procedural rights of the affected person, section 140 treats procedural question in regard to the use of gathered evidence in a criminal trial. Thus, both regulations deal simultaneously on the one hand with the rights of the affected person and on the other hand with the obligations of the (three) criminal investigation authorities.

Section 139 of the Austrian Code of Criminal Procedure states clearly that defendants are allowed to have insight to all corresponding results, meaning that the right to inspect collected evidence has to be granted. This is not only true during the main trial, but also during trial

606 according to section 10a Public Prosecution Act.

607 cf. Reindl-Krauskopf, WK-StPO, sections 137, 138, MN 54-5 especially in regard to the former (monthly) time limit which was not implemented in the new Code rather than the legislator established a simple evaluation of proportionality.

608 Thus the designation of the proceeding, the name of the defendant, the committed criminal act the defendant is suspected for, and its legal term, as well as the facts justifying the necessity and proportionality of the measure for the solution of the specific criminal act; the name or other identification criterion of the technical facility holder, or the person to monitor, where a measure is applied (the relevant location), type of the communication conveyance, the technical facility and the terminal device or the type of technical device (potentially) used for an optical and acoustical surveillance, time of a measure's begin and ending, rooms subject to legal entering, facts stating the danger for public security; However, not every information is mandatory as it is possible, e.g., that the name of the defendant is not yet known – cf. as well EBRV49 BlgNR XX GP, p. 20.

preparation.[609] However, the public prosecution is allowed to withhold (parts of the) results, if there is legitimate interest of any third person in them and these (parts of) results are of no concern in the main trial. Information cannot be withheld if is being used in the main trial because the defendant has the right to have insight into all evidence against him. This right of the defendant does not require any justification.[610] Besides the right to have access to all information, defendants are entitled to request the transformation of results into written form respectively image format. Again, there is the requirement that the results are of concern and this is not violating the exclusionary rules of sections 140 para. 1, 144[611] and 157 para. 2[612] of the Austrian Code of Criminal Procedure. This opportunity for the defendant means a safe guard against claims for the prosecution (in the main trial) stating that relevant, exculpatory documents etc have been destroyed etc.[613] Furthermore, it is to note that results of no concern or irrelevant for the main trial have to be destroyed on request of the defendant or ex officio. However, this request does only constitute a suggestion[614] of the defendant. If the public prosecution, in its function as head of the proceedings, does not comply, an appeal to the court can be made (according to section 106 of the Austrian Code of Criminal Procedure).[615]

Defendants also have the right to request the discontinuation of any measures against their person whenever they learn about any surveillance activities against themselves.[616] As Reindl-Krauskopf points out precisely, the reason for this right – which is not stated explicitly in the Austrian Code of Criminal Procedure – is the secrecy of these measures.[617] As already stated above in the context of an optical and acoustical surveillance of person, the investigation methods are pure covert ones. A covert investigation is characterized by the fact that the affected persons are not aware of a conducted surveillance – they behave as if they were unobserved. Consequently, if these people find out that they are being monitored, they would change their behavior accordingly. In addition, defendants are entitled to object to the judicial

609 cf. JAB 812 BlgNR XX GP 8; further OGH 24.6.2004, 15 Os 13/04.

610 In respect to an optical and acoustical surveillance of person as well as an surveillance of data and communication, cf. OGH 21.11.2000, 11Os 108/00 and OGH 11 Os 109/00.

611 Religious official secrecy and profession sworn to confidentiality.

612 Denial of evidence.

613 cf. Fabrizy (2008), section 135, p. 316-7.

614 according to Bertel, Venier (2006), MN 322, p. 113.

615 cf. ibid MN 322, p. 113.

616 Regularly the suspected – later the defendant or affected – persons should get informed about the conducting of surveillance method after the end of it. However, if they figure it out earlier there has to be a right to request the ending of such privacy affecting activities; according to section 137 para. 3 of the Austrian Code of Criminal Procedure the public prosecution has to terminate surveillance if the correlating requirements disappear (cf. already above); cf. further Reindl-Krauskopf, WK-StPO, section 139, MN 4.

617 cf. ibid, MN 4.

approval empowering the investigation measure at the regional appeal court,[618] and furthermore, they are allowed to appeal against the direction of the public prosecution and the actual conduction by the criminal police at the court.[619]

Due to the public prosecution's obligation to deliver its direction including the corresponding judicial approval to the defendant and any other affected person as stated in section 138 para. 5 of the Austrian Code of Criminal Procedure, it can be concluded that the latter group of persons do have similar rights as the defendant. This is true, as according to section 139 para. 2 of the Austrian Code of Criminal Procedure affected persons[620] are in general entitled to have insight into the results of surveillance, since their privacy was interfered with. Furthermore, affected persons can request the destruction of documents etc concerning them, similar to the rights of defendants as illustrated above. Important in this respect is further that the public prosecution is obliged to inform all affected persons if their identities are known or they are identifiable without special effort.[621] The rights to appeal and to raise an objection are similar to the rights of the defendant mentioned above.

Section 140 of the Austrian Code of Criminal Procedure deals with procedural question in regard to the use of gathered information. This provision governs the utilization of the results[622] of a disclosure of transmission data, surveillance of data and communication as well as an optical and acoustical surveillance of persons.[623] Thereby the provision divides the gathered information into three possible findings, namely para. 1 the use of evidence in respect to the specific criminal act the warrant was issued for (the original criminal act), para. 2 the use of accidental discoveries, and para. 3 the legal use of these results in other, unrelated proceedings. Important in this context is that, irrespective of the investigation method, utilization is only allowed in accordance with the following rules – otherwise the results are invalid.

---

618 section 87 para. 1 of the Austrian Code of Criminal Procedure; cf. already above.

619 according to section 106 of the Austrian Code of Criminal Procedure.

620 Affected person are entitled for insight as far as their data of a communication, communication intended for them or steaming from them, conversations conducted by them, or images with their picture on it, are concerned.

621 Without special effort (German: ohne besonderen Verfahrensaufwand) means further, easily conducted inquiries; the effort depends on the seriousness of interference with the affected person's privacy; cf. Reindl-Krauskopf, WK-StPO, section 139, MN 8.

622 according to section 134 para. 5 of the Austrian Code of Criminal Procedure.

623 Note in this respect, as already mentioned above, that a seizure of a letter cannot be involved as this is a physical item and not conveyed electronically; cf. Tipold, Zerbes, WK-StPO , section 134, MN 1 et seq.

3.4.9.10 Rights and Obligations In Respect to Surveillance of Data and Communication, Disclosure of Transmission Data

Usage of information gathered by these two investigation methods in respect to the original criminal act it the same. The use is allowed if the public prosecution gave legal direction, which was followed by a corresponding judicial approval. This is pointed out explicitly by section 140 para. 1 no. 2 of the Austrian Code of Criminal Procedure. In addition to these formal requirements, there are for sure substantial ones. Hence, it is necessary that the preconditions mentioned in sections 135 para. 2 and para. 3 of the Austrian Code of Criminal Procedure are given, which include: Actual or strong suspicion, the necessary consent for conducted surveillance or disclosures which was also directed and approved. Only if both, the formal as well as the substantial requirements are fulfilled, the gathered information is allowed as evidence in trial.

Notable in this context are the provisions in regard to confessional secrets, profession sworn to confidentiality[624] and the regulations concerning a denial of evidence.[625] There can either be a legitimate direction or a legitimate judicial approval, if theses protection mechanisms are being invaded by surveillance of data and communication/disclosure of transmission data. This implicates that even if the direction and the approval were legitimate, and information infringing with these principles are gathered, the information cannot be used.[626] Problems such as these occur regularly, for instance, in situations where there is surveillance of data and communication and facilities of a third person are monitored because it is believed that a strongly suspected person will contact this person.[627] Note in this context the right to a fair trial (access to legal representation) as guaranteed by the ECHR.

Accidental discoveries are treated almost identical as the circumstances described in the context of a search of location and objects. These discoveries may be used in other criminal proceedings if the following conditions apply. First of all, this information has to emerge from a legitimately directed and approved investigation measure. Second of all, the results can only

---

624 according to section 144 of the Austrian Code of Criminal Procedure; cf. in this respect already the illustration to an exclusion of a lawyer in section 60 of the Austrian Code of Criminal Procedure.

625 according to section 157 para. 2 of the Austrian Code of Criminal Procedure.

626 cf. in this respect further Reindl-Krauskopf, WK-StPO, section 140, MN 9.

627 according to section 135 para. 3 no. 3 lit b of the Austrian Code of Criminal Procedure; cf. already above and Reindl-Krauskopf, WK-StPO, section 140, MN 10.

be used as evidence for other criminal activities, if the investigation of those criminal acts surveillance of data and communication, respectively a disclosure of transmission data would have been implemented.[628] Only if the other criminal act (i.e. not the initial criminal act causing the investigation) is punishable by imprisonment of a minimum period of one year, the use of accidental discoveries is legitimate.[629] This limitation arises due to the fact that in the case of accidental discoveries the affected person does not know anything of surveillance/disclosure. Hence, the same requirements as for surveillance/disclosure without consent have to apply for the use of accidental discoveries. Again, the provisions in regard to confessional secrets and professions sworn to confidentiality as well as the regulations concerning a denial of evidence have also to be notified at this stage.[630]

Different treatment is given to results originating from surveillance/disclosure due to hostage-takings. Despite the fact that there has to be in accordance with the above mentioned regulations, a legitimate direction and approval and the special regard to the specific regulations of sections 144 and 157 para. 2 of the Austrian Code of Criminal Procedure there are no further limitations imposed on to the use of surveillance results.[631]

3.4.9.11 Rights and Obligations in Respect to Optical and Acoustical Surveillance of Persons

The results of both, a major as well as a minor electronic eavesdropping operation, can only be used if there were legal directions set forth by the public prosecution and corresponding judicial approvals. Furthermore, as mentioned above, it is mandatory that the use of the results is limited to the solution of a crime, thus a criminal act punishable by a term of more than three years of imprisonment. There are, however, special regulations to deal with possible problems with this investigation method and profession sworn to confidentiality, especially if these persons are suspects in the crime.[632]

Accidental discoveries during an optical and acoustical surveillance of persons have to be

---

628 according to section 140 para. 1 no. 4 of the Austrian Code of Criminal Procedure.
629 cf. Reindl [2005], section 149c, MN 16; as well OGH 27.5.2004, 12 Os 44/04, SSt 2004/39.
630 cf. in this respect further Reindl-Krauskopf, WK-StPO, section 140, MN 13-5.
631 cf. regarding this and the related critique ibid MN 16.
632 cf. in this respect ibid MN 18 et seq.

documented separately from all other findings.[633] Once again, if it is intended to evade the protective purposes of section 144 of the Austrian Code of Criminal Procedure, the gathered information cannot be used in the main trial, meaning that the results are invalid.[634] The use of accidental discoveries in trial proceedings is limited to the solving of a crime as illustrated above. Legal directions from the public prosecution's office as well as the corresponding judicial approval are mandatory.

The same is true when it comes to a pure optical surveillance, according to section 136 para. 3 of the Austrian Code of Criminal Procedure. However, there is one fundamental difference since accidental discoveries from an optical surveillance can be used for the solution of any criminal act, not only just for crimes.[635] But, as Reindl-Krauskopf points out correctly, there has been an editorial mistake and the legislator created a legal gap when legalizing these principle/or similar. She argues that there has to be an analogy to section 140 para. 1 no. 4 of the Austrian Code of Criminal Procedure in order to close this particular legal gap. Hence, this means that accidental discoveries gathered by a pure optical surveillance outside flats or other locations protected by householder's rights, can be used to solve any criminal act, while discoveries achieved by an optical surveillance conducted within flats etc can only be used to solve criminal acts punishable by imprisonment of a minimum period of one year.[636]

Accidental discoveries obtained during an optical and acoustical surveillance of persons due to hostage-takings are treated similar. The mentioned principles concerning the prohibition of evasions apply as well as since all requirements are cited in the substantial provisions. However, due to section 137 para. 1 of the Austrian Code of Criminal Procedure, stating that there is no need to obtain a warrant (i.e. no direction or judicial approval prior to the hostage-taking),[637] this requirement does not apply. This implements – not unopposed – that there are no limitations in respect to the use of accidental discoveries.[638]

---

633 with respect to the exclusionary rules of sections 140 para. 1, 144 and 157 para. 2 of the Austrian Code of Criminal Procedure; cf. furthermore already above.

634 Note in this context that the difference between an offense and a crime is that the latter is punishable by a term of more than three year imprisonment; cf. already above and Reindl-Krauskopf, WK-StPO, section 140, MN 21; in respect to profession sworn to confidentiality please cf. ibid, MN 23-4.

635 at least according to the wording of section 140 of the Austrian Code of Criminal Procedure.

636 cf. further Reindl-Krauskopf, WK-StPO, section 140, MN 25.

637 in regard to the strong limitations cf. already above.

638 cf. further Reindl-Krauskopf, WK-StPO, section 140, MN 26.

3.4.9.12 Usage of Result in Other Proceedings

According to section 140 para. 3 of the Austrian Code of Criminal Procedure, the use of results gathered by the above illustrated investigation methods is also allowed in other judicial and administrative proceedings, if their use in criminal proceedings was or would have been legitimate.[639]

3.4.10 Conclusion: Realization of an RFI

The optical and acoustical surveillance of a person according to sections 136 in conjunction with 134 no. 4 of the Austrian Code of Criminal Procedure appears to be the most likely possibility to be the basis for an RFI. This is especially true since the requirements for an RFI set out by the Ministry of Justice and of the Interior[640] are equal to that of the optical and acoustical surveillance of persons.

By definition it is not possible to conduct surveillance of a person in order to get remote access to a computer for search purposes as a task of an RFI. Sections 136 in conjunction with 134 no. 4 of the Austrian Code of Criminal Procedure are just concerned with the surveillance and not with any search purposes, meaning that the aim is to gather information about a person by monitoring his/her behavior and oral statements. However, a distinction has to be made when it comes to the other two task of an RFI, namely surveillance of activities and surveillance of telecommunication, in order to examine any potential applications:

3.4.10.1 Minor Electronic Eavesdropping Operation

A minor electronic eavesdropping operation can never be a foundation for an RFI. The minor 'case' of an optical and acoustical surveillance of persons deals with the listing and recording of privately made statements while an undercover agent is present. This agent or any other person informed about the surveillance – is the crucial requirement. In the case of an RFI, the only thing present would be a technical device in the form of a Trojan horse etc. Thus an application of a minor electronic eavesdropping operation as surveillance of activities (RFI) is not working due to the absence of a well-informed person. Not surprising, this is also true for

639 cf. the extensive illustration at Reindl-Krauskopf, WK-StPO, section 140, MN 28-36.
640 cf. Vortrag an den Ministerrat der Republik Österreich of 17 October, 2007.

the surveillance of telecommunication.

3.4.10.2 Major Electronic Eavesdropping Operation

During a major electronic eavesdropping operation the presence of an undercover agent is not required. However, an RFI is not intended to monitor a specific person, but it is rather used for the surveillance of the conduct of programs and how they are applied by a (specific) user. Contrary to this, the optical and acoustical surveillance of persons is directed to the optical surveillance of the person itself and the statements this person has made with the use of technical devices. This is done with the assistance of video cameras, mini microphones and similar, thus tools to transmit and record images and audio files. Surveillance of persons constitutes surveillance of the conduct and behavior of persons and not just the performance of a computer program.[641] Hence, surveillance of activities cannot be based on a major electronic eavesdropping operation. Concerning the surveillance of telecommunication Reindl-Krauskopf argues that this would be possible and covered by an optical and acoustical surveillance.[642] However, from the author's point of view a major electronic eavesdropping operation does not legitimate an RFI because communication does always involve an expression to the external world. Only after the communication has left the originators sphere of influence, is it transmitted – thus ready to become intercepted and monitored.[643]

Despite these circumstances, the optical and acoustical surveillance of persons in their private rooms in order to listen to telephone calls conducted via the Internet (Voice over IP) and/or to monitor keystrokes with a video camera, are, from a criminal procedural, thus legal point of view, allowed[644] and can be quite successful as well. Such handling,[645] however, shows that

641 cf. Reindl-Krauskopf, WK-StPO, section 134, MN 115; as well as BMJ/BMI (2008), p. 26.

642 cf. Reindl-Krauskopf, WK-StPO, section 134, MN 116.

643 cf. already above in the context of surveillance of data and communication; Note concerning this that the report of an expert group support the view that there is currently no legal basis for a covert electronic surveillance of a computer; cf. BMJ/BMI (2008), p. 33.

644 BMJ/BMI (2008), p. 26.

645 During investigations concerning an online published video constituting a menace for Austria in 2007, the criminal police (Federal Departement for the Protection of the Constitution and the Combat of Terrorism – BVT) conducted surveillance of data and communication. According to the officers, the BVT contacted the provider of the suspect and arranged that data of this person, before it enter the internet are copied and sent to surveillance device (what ever this may mean?). In the following, experts examined the content of the data. Due to the fact that the suspect used a proxy server in Malaysia and decoded this data, it was not possible to gather knowledge of about 35 % of the data. Therefore a major electronic eavesdropping operation was conducted legally. Bugs as well as two cameras were installed in order to monitor the conduct and the statements made by the suspect (especially during Internet phone calls); cf. report at <http://futurezone.orf.at/stories/261511/> retrieved 4 December, 2009.

there is still a gray area within the Austrian legal system, as the investigation authority used, because an optical surveillance within the suspect's flat was not possible, a technical device to send screen shots established on the suspect's computer. According to the conducting officers, every 60 seconds a picture of the screen was sent to an officer sitting next door. With these images and with the assistance of the recorded keystrokes[646] the police was able to reconstruct what happen within this minute.

In accordance with the already above stated, the author does not consider these proceeding as a legitimate use of electronic devices. From his point of view, there is no real and legal problem with the bugging of the suspect's flat or to listen to telephone calls or other conversations. However, the use of screen shots and video cameras in order to monitor a screen and what is written on it does not constitute a communication and can therefore not be intercepted. A similar problem would occur if bugs were used as acoustical key logging devices. There has to be a clear differentiation between a verbal communication and a simple written form of communication,[647] illustration of purely internal thoughts and the most private and intimate affairs of a person.[648]

3.5 Security Police Law

3.5.1 Introduction

Task and Competences of the Public Security Police

A complete list of all three tasks of the public security police can be found in part two of the Austrian Security Police Act (i.e. sections 19 to 27a). Part three of the same Act, i.e. sections 28 to 50 handles the capacities of the public security police. According to section 28a para. 2 and para. 3 of the Austrian Security Police Act the public security police is allowed, in order to fulfill its tasks, to use all legitimate resources not interfering with any rights of persons. Only if the legitimacy of a provision evolves or if there is no less intrusive method available,

646 The article does not say which kind of key logging devices was used.
647 private video files, 'oral diary', photos ...
648 BMJ/BMI (2008), p. 26.

the empowerment to interfere with the rights of persons is given.[649] Important in the context of the capacities is furthermore section 29 of the Austrian Security Police Act, stating that the public security police has to bear in mind the principle of proportionality at all times. This means – similar to the requirement of proportionality in the context of the Austrian Code of Criminal Procedure and in general in that of the Austrian Constitution – that every action of the public security police has to be balanced in respect to its outcome.[650] For instance, an action is not allowed if it can cause more damage than the danger they try to avoid with this action.[651] Furthermore, an action does not only have to be proportional but also it is required that it is necessary, suitable and appropriate.[652]

According to the sections 28 and 29 of the Austrian Security Police Act, the public security police is only allowed to interfere with the rights of persons if

- the Austrian Security Act provides a competence,
- there is no other (i.e. milder and suitable) method for the accomplishment of the task (principle of ultima-ration), and
- the relation between occasion (the actual task) and the intended aim is proportional.

---

649 Remark in this context that the Austrian Security Police Act does not only grant competences to the security agencies but also it establishes procedural rights for the affected persons of a public security police activity. The rights are similar to that set out by the Austrian Code of Criminal Procedure however they are not stated in a clear and proper manner. Due to this fact, section 30 para. 1 of the Austrian Security Police Act introduced a minimum standard of rights: on request, the affected person has to be informed about the reason and aim of the activity as well as about the personal number (German: Dienstnummer) of the officer; moreover, an affected person does have the right to bring in a confidant and to submit important facts and demand their treatment as findings. However, as long as the aim of the activity – i.e. to achieve a certain goal – is endangered, these rights are not guaranteed, according to section 30 para. 2 of the Austrian Security Police Act. Please note in this respect that the Federal Ministry of the Interior has to issue a regulation including guidelines for the activities of the security agencies' officers (section 31 of the Austrian Security Police Act). This competence of the Ministry of the Interior is based on Art 10 para. 1 no. 14 of the Austrian Federal Constitutional Law.

650 Demmelbauer/Hauer explain it as a principle of prudence or rationality, meaning that the use of excessive measures to achieve the same aims (public security, public order, etc) is not allowed. They argue that there is the obligation for the security agency to weight all possible measures in situations where there are more than just one. This evaluation must be conducted in a prudent, rational, non-random, hasty or excessive manner. cf. Demmelbauer, Josef, Hauer Andreas, Grundriss des österreichischen Sicherheitsrechts unter besonderer Berücksichtigung der Sicherheitsverwaltung (2002), MN 66, p. 31.

651 Similar to the above presented evaluation in regard to proportionality, there has to be an evaluation of the capability, the necessity and the appropriateness of the interference. As Pürstl/Zirnsack point out, the public security police has to choose – if possible – a method directed against the originator of the threat (dangerous aggression, etc), the most flexible competence to handle and it is only allowed to apply its competences as short as possible. Furthermore, only the least intrusive method of more than one is allowed to be applied. Pürstl, Gerhard, Zirnsack, Manfred, Sicherheitspolizeigesetz (2005), pp. 116-117.

652 cf. in respect to the principle of proportionality the chapter on the Austrian Constitution, the Austrian Code of Criminal Procedure as well as Hauer, Keplinger (2005), pp. 305-308; Lepuschitz, Michael, Schindler, Thomas, Das österreichischen Sicherheitspolizeigesetz (2008), 5th edition, pp. 80-81; cf. Demmelbauer, Hauer (2002), MN 66-8, pp. 31-32.

3.5.2 Tasks

The various tasks can be subdivided into

- maintenance of public order
- primary assistance, and
- maintenance of public security

3.5.2.1 Maintenance of Public Order

According to the rulings of the Austrian Administration Court, public order is the entirety of unwritten rules of behavior in public, whose compliance is seen as an essential requirement for a harmonious social coexistence of human beings.[653] This means that the task of maintaining public order is based on no legal (hence only social) provisions, which help to enforce these rules. Furthermore, it is to remark that while maintaining public order, the interest of every single individual to exercise his/her fundamental rights and freedoms has to be kept in mind by the public security police.[654] This indicates that disturbances of the public order affecting other people in their exercising of fundamental rights and freedoms, have to be prevented. This is also true if the disturbance itself is the exercise of a fundamental right, such as the right to the freedom of association.[655]

Overall, it can be said that two social preconditions are required before an intervention by public security police is possible. Firstly, the required social provision has to be recognized by the society, meaning that a simple acceptance (of this provision) by a majority is not sufficient. This requirement can be further explained by the restriction to the exercise of fundamental rights and freedoms. Secondly, the required recognition is based on the overall belief that the compliance with the social provision is necessary for an established order to be maintained.

---

653 cf. VwSlg 543 A/1948; or the judgments of 13 February, 1984 Z 82/10/0178 respectively of 9 July, 1984 Z 84/10/0080)

654 cf. section 27 para. 1 of the Austrian Security Police Act, second sentence.

655 cf. Art 11 Convention for the Protection of Human Rights and Fundamental Freedoms as well as Art 12 Basic Law of 21 December, 1867 on the General Rights of Nationals in the Kingdoms and Laender; in this respect especially the decision of the Austrian Constitutional Court VfSlg 16054/2000.

The task of maintaining public order is intended to create the conditions for a peaceful social coexistence in circumstances where there is no threat of a harmful aggression,[656] as presented in the chapter on the averting of danger and as illustrated subsequently.

3.5.2.2 Primary Assistance
Section 19 of the Austrian Security Police Act

In a high number of cases, primary assistance is the start for the activities of the public security police.[657] By law, the police has an obligation to assistance if an actual threat to life, health, liberty or property of persons exists, or such threat is imminent.[658] It is therefore the duty of the public security police to verify whether such a threat is given, and to take appropriate steps, if necessary. These actions can be qualified as simple provisional and subsidiary tasks.[659] Important to note in this context is that a simple task – such as primary assistance – does not constitute any competences. Such competences can be found in sections 32 et seq. of the Austrian Security Police Act[660] and will be presented subsequently.

3.5.2.3 Maintenance of Public Security

Chapter 2 of Part 2 of the Austrian Security Police Act starting with section 20 deals with the maintenance of public security. This chapter includes the tasks of averting of danger,[661] the precautionary protection of legally protected interests,[662] tracing and search activities,[663] consultations by the criminal police[664] and dispute settlements.[665] These tasks show that there

656 e.g. a threat arising from a massive gathering of people etc.
657 Hauer, Keplinger (2005), p. 239.
658 cf. in this respect as well Art 78a para. 2 of the Austrian Federal Constitutional Law.
659 Hauer, Keplinger (2005), p. 239; as well as BMJ/BMI (2008), p. 39; note furthermore that primary assistance of security agencies is therefore a subsidiary emergency competence for all cases of administration police as well as the local public security police which try to protect the mentioned legally protected goods (German: Schutzgüter) or life health, liberty and property of persons – cf. in this respect Art 15 para. 2 of the Austrian Federal Constitutional Law; moreover, it is to state that primary assistance means the averting of danger not limited to a certain administrative region rather than the danger is not connected to a certain branch of administration; cf. in this respect especially Mayer (2004), p. 36.
660 Part 3, Chapter 2 of the Austrian Security Police Act.
661 according to section 21 of the Austrian Security Police Act.
662 according to section 22 of the Austrian Security Police Act.
663 according to section 24 of the Austrian Security Police Act.
664 according to section 25 of the Austrian Security Police Act.
665 according to section 26 of the Austrian Security Police Act.

is a strong focus of the combat of judicial punishable activities, i.e. criminal activities.[666] In this context and especially in connection with this thesis, the averting of danger is of great importance. Hence, a detailed illustration of this special task performed by the public security police will be given.

3.5.2.4 Averting of Danger
Section 21 of the Austrian Security Police Act

Generally speaking, the averting of danger is one of the key tasks of the public security police,[667] according to section 16 para. 1 of the Austrian Security Police Act. A dangerous situation constitutes a situation, which is most likely leading – according to the customary experiences – to a harmful outcome. If after evaluation of the whole situation no intervening steps are taken, the likelihood of a harmful outcome (damage) is objectively given.[668] Hence, there has to be an ex ante evaluation of the situation in order to assess the potentiality of danger.[669]

A general danger is the umbrella term putting together two narrower terms. Namely, danger is given

- in the case of a dangerous aggression according to no. 1, and
- in the case of criminal associations according to no. 2.

3.5.2.4.1 Dangerous Aggression

A dangerous aggression is, according to sections 16 para. 2 and para. 3 of the Austrian Security Police Act, typically given when a criminal activity is conducted and it is carried out with criminal intend, hence, in situations where there is already a dangerous aggression or

---

666 cf. in this respect Hauer, Keplinger (2005), p. 240, stating that there is a difference between the definition of public security in the Austrian Security Police Act and the corresponding definition in public administration provisions.

667 Next to primary assistance; cf. as well Hauer, Keplinger (2005), p. 241.

668 Wiederin (1998), MN 203, p. 51.

669 This has to be taken into account if there is a review of the public security police's activities; cf. in this respect the explanation of Leo, Andreas, Prävention und Repression im Rahmen der Sicherheitspolizei (2005), p. 83-86.

where such an aggression is imminent.[670] In this respect, the definition of general dangers includes the actual threatening of legally protected interests through executing of certain criminal activity[671] as well as the threatening of these interests by preparatory works.[672] The second case refers, as stated, to activities of criminal associations, or as section 16 para. 1 no. 2 of the Austrian Security Police Act puts it, if there are three or more persons associate with the criminal intent to exercise criminal activities.[673] In this respect it is to mention that – unlike the shown preconditions in the case of a dangerous aggression – no specific criminal activity is required. This means that a criminal association as such is already a criminal activity and therefore punishable. Properties of an association are, for instance, a consolidated structure, which is based on the specific division of labor. Furthermore, the association's intent has to be directed towards to commit criminal activities in a continued way. This is done by an use of its 'personnel' and funds[674] However, as Wiederin points out, there are no real essentialia; on the contrary, a coalition of several persons bound together by the intend to commit undefined criminal acts is sufficient to be branded as criminal association.[675]

General danger, which is generally counteracted by the public security police is closely connected with criminal activities[676] and can be seen as defined accessory to criminal law.[677] The main difference between these two areas of law – i.e. criminal law and public security

---

670 section 16 para. 1, para. 2 and para. 3 of the Austrian Security Police Act.

671 These offenses and crimes include all acts punishable according to the Austrian Criminal Code with the exception of sections 278, 278a, 278b, and any acts committed by carelessness or criminal acts for whose prosecution the consent of the affected person is needed or in instances where the affected person has to claim punishment itself; furthermore offenses and crimes include acts punishable according to Prohibition Act 1947, acts punishable according to the Aliens Police Act 2005 and acts punishable according to the Illegal Drug Act.

672 Funk, Bernd-Christian, Das neue Sicherheitspolizeirecht – Kodifikation und Reform einer klassischen Verwaltungsmaterie, JBl 1994, foot note 5.

673 Note in this context that the definition of section 16 para. 1 no. 2 of the Austrian Security Police Act was cloned of the old version of section 278 of the Austrian Criminal Code dealing with the foundation of gangs (German: Bandenbildung); the current version of sections 278a et seq.of the Austrian Criminal Code do not correlate with that of a criminal association according to the Austrian Security Police Act; cf. in this respect especially Hauer, Keplinger (2005), p. 213; and EBRV 81 BlgNR XXI GP, pp. 5 et seq.

674 cf. Brenner, Franz, et al, Kriminalpolizei und Strafprozessreform – Konzept der Arbeitsgruppe StPO-Reform des Bundesministeriums für Inneres zu einem sicherheitsbehördlichen Ermittlungsverfahren (1995), p. 62.

675 Wiederin (1998), MN 282, pp. 66-7.

676 cf. in this respect especially section 16 of the Austrian Security Police Act and its definitions of averting of danger, dangerous aggression and danger investigation; furthermore Wiederin (1998), MN 203-40, pp. 51-58; in addition, these tasks reside generally with the security agencies as Hauer/Keplinger point out precisely – cf. Hauer, Keplinger (2005), p. 241.

677 cf. e.g. Hauer, Keplinger (2005), p. 215; Wiederin (1998), MN 272, p. 65; or Fanari, Linda, Befugnisse der Sicherheitsorgane nach dem Strafprozessreformgesetz im Verhältnis zu jenen des Sicherheitspolizeigesetzes (2005), p. 49.

police law – is that the latter does not demand any culpability[678] of the activity. This is due to the fact that the public security police is obliged to protect the legally protected interests of the victims, whereas in criminal law cases the focus of interest lies on the person who committed a criminal act.[679] For a closer examination of the difference between both, please cf. the corresponding chapter subsequently.

3.5.2.4.2 Danger Investigation

In addition to the presented definitions of general danger, section 16 para. 4 of the Austrian Security Police Act regulates the so-called 'danger investigation', stating that this means the detection of a source of danger and matters of fact in regard to a potential danger. Such detections, and in a wider sense, verifications of such dangers, are essential before any competence can be used by the public security police. This principle can also be drawn out of the principle of proportionality and means that before the public security police is using any of its competences, it is mandated to evaluate the actual (dangerous) situation and to make its decision to act based on the criterion of necessity and appropriateness. Hence, any averting of danger is always preceded by a corresponding evaluation of the situation.[680]

Section 21 of the Austrian Security Police Act states that the security agencies are engaged with the task of averting of general dangers (thus dangerous aggression and criminal associations).[681.] Moreover, it is to say at this stage that it is the obligation of the public security police to put immediately[682] an end to a dangerous aggression,[683] implicating that the public security police is not allowed to wait until danger becomes real, rather than it is forced to intervene already in the – regularly not subject to prosecution – preparatory stages of a criminal activity.[684] This rule applies also, if there is already a person suspected of this criminal activity, meaning that the Austrian Security Police Act is still applicable and the

---

678 cf. e.g. Leo (2005), p. 93.

679 cf. Dearing, Albin, Sicherheitspolizei und Strafrechtspflege – Versuch einer Bestimmung des Verhältnisses zweier benachbarter Rechtsgebiete, in Festschrift Platzgummer (1995), p. 231.

680 cf. ibid p. 236; this principle is also mentioned explicitly in section 21 para. 3 of the Austrian Security Police Act.

681 section 21 para. 1 of the Austrian Security Police Act.

682 However, there is the possibility for the public security police to postpone this if another criminal activity could be solved so; cf. Hauer, Keplinger (2005), 3rd edition, pp. 243-244.

683 section 21 para. 2 of the Austrian Security Police Act is therefore illustrating para. 1 in a further sense.

684 cf. EBRV 148 BlgNR XVIII GP, p. 36; as well as section 22 para. 2 of the Austrian Security Police Act.

further proceeding is not governed by the Austrian Code of Criminal Procedure.[685] Furthermore, the public security police is entitled by para. 3 to an extended danger investigation, meaning an averting of danger in the context of serious threats. It is governed that the security agencies has the task of monitoring groups which – due to their structure and the ongoing development in their environment – are expected to represent a serious threat to public security, especially in the context of ideological and religious motivated aggression.[686] This provision was intended to allow the observation of extremist groups already in a point of time when they have not yet committed any criminal activities but when it is assumed that they will do so in the near future. The legislator pointed out that experiences have shown that tendencies towards radicalism establish over time. This is especially true if foreign developments and experiences are taken into account of the analysis.[687]

3.5.3 Competence Regarding Averting of Danger

Similar to the already above stated, the task of averting of danger does not come with any competences. The competences concerning the averting of danger are the same as those in respect to primary assistance and can be found in sections 32 et seq. of the Austrian Security Police Act. As not all of these competences are of concern in the context of this thesis, only the key competences of the public security police in regard to an RFI will be presented:

3.5.3.1 Competence to Enter and Search of Premises, Rooms and Vehicles Section 39 of the Austrian Security Police Act

In order to get access to a communication system, it may be necessary to enter premises or other locations. Section 39 para. 1 of the Austrian Security Police Act constitutes a competence of the public security police, within the scope of its task of primary assistance or averting of a dangerous aggression. The public security police does have the competence to

685 In respect to the relationship between these two legal acts, please cf. below.
686 Lepuschitz, Schindler (2008), pp. 67-68.
687 cf. for further details concerning the intention behind the establishment of that provision EBRV 81 BlgNR XXI GP, p. 5.

enter premises, rooms and vehicles.[688] In addition to the authorization of entry, the public security police can also search[689] these locations if this has to be done:

- in order to find a person whose life or health is threatened immediately,[690]
- in order to find a person initiating an actual dangerous aggression,[691]
- in order to find an object intended to be used for a dangerous aggression.[692]

The public security police's competence includes also the opening of containers located in rooms if the preconditions of para. 1 are fulfilled and the search is conducted for one of the purposes expressed explicitly by section 39 para. 5 of the Austrian Security Police Act. A general reference to the well-known principles of proportionality in section 29 of the Austrian Security Police Act and to the principles in regard to confessional secrets and profession sworn to confidentiality.[693] Furthermore, it is to mention that para. 7 governs that the provisions of sections 121, 122 para. 2 and para. 3 as well as section 96 of the Austrian Code of Criminal Procedure apply mutatis mutandis.[694]

In this context it is to remark that after the end of a dangerous aggression, a search of premises, rooms, vehicles and containers cannot be based on the Austrian Security Police Act,

---

688 cf. section 39 para. 1 of the Austrian Security Police Act; this means nothing else that an entry is only allowed for legitimate purposes; however, it is to note that – as already remarked above – danger investigations according to section 16 para. 4 of the Austrian Security Police Act can be conducted as well; cf. already above and especially (Einführungs-) Erlass des BMI of 19 April, 1993, 94.762/15-GD/93.

689 cf. section 39 para. 3 of the Austrian Security Police Act; note in this context that an inspection granted voluntary by the holder of the premise etc is qualified as a non-interfering method according to section 28a para. 2 of the Austrian Security Police Act and is allowed even if the preconditions of an entry and search of premises, rooms and vehicles are not given. However, if these preconditions are present, a conducting by force (as a coercive measure) is allowed; cf. Hauer, Keplinger (2005), p. 448; furthermore, please note that according to the Austrian Constitutional Court, a search of locations is only given, if a search is conducted in order to find persons or objects whose residence is not known. Simple entering of a flat during the search for a person, in order to interview the persons present in that flat regarding the residence of the suspect person, does not constitute a search of locations and objects as defined by sections 119 et seq.of the Austrian Code of Criminal Procedure; cf. in this respect VfSlg 5080/1965, 6528/1971, 9766/1983, 10547/1985, 11650/1988, 12056/1989, 12628/1991; cf. already the illustrations in regard to a search of locations and objects in the Austrian Code of Criminal Procedure above.

690 e.g. the victim of hostage-takings, or a person announced to commit suicide; cf. furthermore Hauer, Keplinger (2005), pp. 448-449.

691 e.g. a sniper, cf. furthermore Hauer, Keplinger (2005), p. 449.

692 e.g. explosives hidden in a building etc, cf. Hauer, Keplinger (2005), p. 449.

693 cf. section 39 para. 7 of the Austrian Security Police Act; cf. moreover the illustrations in the chapter of this thesis on the Austrian Code of Criminal Procedure.

694 Concerning the procedures rights of an affected person respectively the obligation of the conducting authority; e.g. the issuance of a confirmation etc.; however, as Lepuschitz/Schindler argue the public security police has to comply with these formalities only and in so far as this is possible, cf. Lepuschitz, Schindler (2008), p.117-118; cf. moreover, already above and the mentioned provisions.

but a search of locations and objects according to the Austrian Code of Criminal Procedure has to be conducted.[695]

Part 4 of the Austrian Security Police Act deals with the handling of personal data by the public security police. Again there are some provisions included which might be relevant in the context to be used as basis of a RFI. There will be a short illustration focusing on these provisions.

3.5.3.2 Legitimacy of Processing of Personal Data Section 53 of the Austrian Security Police Act

Before going into details of this provision, it is important to note that surveillance of communication, or better the content of a communication, is not possible under section 53 of the Austrian Security Police Act, as there is a constitutional manifested obligation for the investigating authorities to obtain judicial approval. Such an approval is only provided by the Austrian Code of Criminal Procedure and not by the Austrian Security Police Act.[696] Hence, the regulation in the Austrian Security Police Act can only deal with data other than content data.[697]

Section 53 para. 3a of the Austrian Security Police Act governs that the security agencies are entitled to request certain information from telecommunication providers[698] (according to section 92 para. 3 no. 1 of the Austrian Telecommunications Act 2003) or service providers[699] (according to section 3 no. 2 of the Austrian E-Commerce Act). They are obliged to provide the following information as soon as possible and free of charge:

- No. 1 – the name, address and participants number of a specified termination,

---

695 cf. section 39 para. 8 Austrian Security Police Act.

696 cf. Reindl-Krauskopf, WK-StPO, section 134, MN 60.

697 Despite the fact that there is the possibility to use an IMSI catcher (cf. below) for the interception of communication and to obtain thereby the content of the communication, it is not allowed for the public security police to do so; cf. Reindl-Krauskopf, WK-StPO, section 134, MN 67.

698 provider means an operator of public communications services

699 Service provider means a natural or legal person or other institution with legal capacity which provides an information society service; cf. already above in this thesis in the chapter on surveillance of communication and data.

- No. 2 – the Internet protocol address (IP address) belonging to a certain communication and its time of transmission, as well as
- No. 3 – the name and address of the user whom a certain IP address was assigned to at a specific time,

if there is – due to certain facts – an assumption of a concrete dangerous situation and the security police needs this information in order to fulfill its tasks.[700] The information of no. 1 can be requested for primary assistance purposes as well as for the averting of a dangerous aggression,[701] and the passive number of a participant.[702] This means that telecommunication providers are obliged to provide the public security policy with demanded information in case of a concrete dangerous situation when the public security police is in need of this information in order to be capable to fulfill its tasks according to the Austrian Security Police Act.[703] Regularly, this provision is used in order to obtain master data (no. 1), which are in a reciprocal correlation to each other, meaning that if the telephone number is known, the name and address of the participant can be requested.[704] Despite the fact that the provisions sound like they would only deal with telephone numbers and customary telecommunication, as Reindl-Krauskopf points out precisely, it can be used for IP addresses as well. Depending on the actual circumstances, it might be possible to draw conclusions from master data directly to an IP address of the user, or vice versa. However, if there has to be an inquiry regarding a dynamic IP address beforehand, than a request for master data is not given, according to section 53 para. 3a no. 1 of the Austrian Security Police Act.[705] In this respect, it is further to note that both, dynamic (no. 3) as well as static (no. 2) IP addresses are covered by this provision.

In this context, one could criticize that the legitimacy of a request depends on the precondition

---

700 Not only is it mandatory that this information has to be essential for the fulfilling of the tasks of the public security police, but also is there the legal requirement of a justification, meaning that there is the assumption – based on certain facts – of a concrete dangerous situation; cf. Reindl-Krauskopf, WK-StPO, section 134, MN 66.

701 cf. the example of a phone call of a few minutes taking place at around 11:00am and the time frame would be from 11:00 to 11:15am: cf. regarding the requirement of accuracy and the implications Reindl-Krauskopf, WK-StPO, section 134, MN 63.

702 meaning that the public security police is empowered to ask the name, address and participants number by providing a time frame and the number of the communication's participant who was contacted; cf. Hauer, Keplinger (2005), 3rd edition, p. 601.

703 cf. Regenfelder, Wolfgang, Ermittlungsmaßnahmen bei neuen Informationstechnologien im Spannungsverhältnis zum Grundrechtsschutz (2008), p. 78.

704 cf. Reindl-Krauskopf, WK-StPO, section 134, MN 61.

705 cf. ibid MN 61.

of a concrete dangerous situation, meaning nothing else than periculum in mora – danger in delay – in connection with the absence of any judicial approval. Since a concrete dangerous situation or periculum in mora leave a broad margin for interpretation, huge criticism in respect to fundamental rights may arise.[706] Due to the fact that it is possible to conduct a complete evaluation of connection data within the scope of the Austrian Security Police Act without any judicial approval, any judicial control after the investigation is of great importance for a potential criminal trial.[707]

Section 53 para. 3b of the Austrian Security Police Act[708] grants the public security police the option to obtain the location data of a terminal device, if there are reasons to assume that there is a contemporary danger to life or health of a person[709]. In this respect it is to note that the providers are obliged, not only to provide information concerning the location of a certain terminal device to the public security police immediately, but they also have to provide information about the IMSI.[710] The position of a terminal device can then be conducted via a IMSI catcher and is directed to mobile phones, respectively their SIM cards. Via such IMSI catchers it is possible to track – depending on the quality of the network – an accident victim more or less precisely. However, this provision does not mandate the releasing of any further information by the providers. Especially are they not obliged to provide the IMSI catchers themselves.[711] The public security police is accountable for the legitimacy of the request and has to obtain documentation for the request within 24 hours. In the context of para. 3b it is further to note that contrary to para. 3a the telecommunication providers are entitled to reimbursement of arisen costs, according to the Surveillance Cost Ordinance 2004.[712] Reindl-Krauskopf raised the question whether such a regulation should also apply to para. 3a. The

---

706 cf. e.g. as danger in delay was stressed in January 2008 in order to obtain an IP address of July 2007; cf. Moechel, Erich, Wirtschaft: „Misstrauen gegen SPG bleibt' in <http://futurezone.orf.at/stories/256683> retrieved 2 December, 2009; furthermore please cf. <http://www.bigbrotherawards.at/2008/Preistraeger> retrieved 2 December, 2009.

707 cf. in this respect especially section 140 of the Austrian Code of Criminal Procedure and Reindl-Krauskopf, WK-StPO, section 134, MN 64.

708 The interesting topic of IMSI catchers and their use by police was highly debated in Austria and there is still some discussion going on; cf. e.g. the references in Regenfelder (2008), pp. 46 et seq.and pp. 75 et seq; furthermore Fox, Dirk, Der IMSI-Catcher, in Datenschutz und Datensicherheit (2002), p. 212; and Reindl-Krauskopf, WK-StPO, section 134, MN 75.

709 e.g. the, in Austria, often stressed lost or injured backcountry skier; however such a danger could also be given in situations of a dangerous aggression (e.g. in the case of a hostage-taking) as Reindl-Krauskopf points out precisely; cf. Reindl-Krauskopf, WK-StPO, section 134, MN 69.

710 IMSI stands for International Mobile Subscriber Identification and means a number of identification corresponding to a SIM (Subscriber Identity Module) card.

711 cf. Reindl-Krauskopf, WK-StPO, section 134, MN 70.

712 Federal Law Gazetta II 322/2004.

argument is that the public security police has to provide certain information concerning its request to the providers in order to enable the latter to provide the requested data. Furthermore, there is the requirement for the security agency to state, in detail, the concrete dangerous situation, the legal basis of its request etc. Overall, there is no real difference between para. 3a and para. 3b except that para. 3b demands a formal documentation of the request to be forwarded to the providers within 24 hours.[713]

3.5.3.3 Special Regulations for Investigation Section 54 Austrian Security Police Act

Section 53 para. 4 of the Austrian Security Police Act states that the public security police is principally entitled – within the Austrian legal framework – to gather information and personal data via all appropriate means and process it.[714] Not surprisingly, out of this provision, a broad range of methods evolve that can be used by the public security police. However, section 54 of the Austrian Security Police Act provides the corresponding limitations, which are special regulations concerning the investigation of personal data, its limitations and boundaries. Certain aspects of paragraph 54, such as para. 2, para. 4 and para. 4a are of general interest to this thesis since they deal with items applicable to an RFI.

Section 54 para. 2 of the Austrian Security Police Act handles the investigation of personal data through observations[715] - thus with a covert investigation method – and governs that this method is only allowed in the following instances:

- No. 1 to conduct an extended danger investigation,[716]

---

713 cf. Reindl-Krauskopf, WK-StPO, section 134, MN 73.

714 Hauer, Keplinger (2005), p. 608.

715 Observation in this context means more than just simple accidental watching of a person, it is rather a structured, systematical awareness of optical or acoustical information (i.e. a specified person), over a longer (not specified in advance) period of time, which is connected with a specific dedicated personal and impersonal effort. This means nothing else than the accidental awareness during patrolling cannot be qualified as an observation; cf. in this regard especially Hauer, Keplinger (2005), p. 610; as well as Wiederin, Ewald, Privatsphäre und Überwachungsstaat - Sicherheitspolizeiliche und Nachrichtendienstliche Datenermittlungen im Lichte des Art 8 EMRK und der Art 9-10a StGG (2003), pp. 110 et seq; moreover, Pürstl, Zirnsack (2005), p. 211.

716 according to section 21 para. 3 of the Austrian Security Police Act.

- No. 2 to be able to prevent a punishable activity of a certain person against life, health, morality, freedom, assets of a third person, or the environment[717]
- No. 3 if the averting of dangerous aggressions or criminal associations[718] would be endangered or complicated otherwise.

According to Hauer/Keplinger it is unclear why the legislator used the expression 'punishable activities' in this section, especially since throughout the whole Act it is normally referred as dangerous aggressions. A simple literal construction would consequently lead to the conclusion that even regulatory offenses would be covered. It is argued that this cannot have been the intention of the legislator; hence they are in favor of a reduction to judicial punishable criminal activities.[719]

An observation can be conducted as soon as the public security police gets knowledge about a certain person's plan to commit a penal activity. It is not necessary for the security authority to have enough information on that criminal activity that it can undertake preventive steps.[720] As Pürstl/Zirnsack point out, the public security police has to evaluate whether it is better to prevent a criminal activity by observation or by confronting the (not yet chargeable) 'offender'.[721]

Section 54 para. 4 of the Austrian Security Police Act deals with the investigation of data of persons conducted with visual and audio recording devices. These types of investigations are only allowed in connection with the averting of a dangerous aggression or a criminal association, or in the context of an extended investigation of danger. Furthermore, this can be done undercover; if an averting of a dangerous aggression or a criminal association would be endangered or complicated otherwise.[722] However, there are also some limitations to the gathering of personal data. First of all, according to no. 1, the use of audio recording devices

---

717 Meaning that the criminal activity is still on the preparatory level and the penal outcome is not yet present; this has to be seen in the light of section 16 para. 3 of the Austrian Security Police Act.
718 according to section 21 para. 1 of the Austrian Security Police Act.
719 Hauer, Keplinger (2005), pp. 610-611.
720 Such as warning the potential victims, etc.
721 cf. Pürstl, Zirnsack (2005), p. 211.
722 according to section 54 para. 4 of the Austrian Security Police Act referring to para. 3.

in order to record private[723] statements where there is not at least one undercover agent present is illegal,[724] and second of all, according to no. 2, it is equally not allowed to use image recording devices in order to record the private conduct of person if there is not at least one informed person present.[725] However, entire public conduct/behavior or statements can be recorded, and the recording of situations where an undercover agent, is present, is also permitted.[726] The telecommunication secrecy[727] is not affected by this provision.

Section 54 para. 4a of the Austrian Security Police Act handles the use of image and audio recording devices in connection with an averting of criminal associations. It governs that the public security police is only allowed to use such techniques, if there is the assumption that a crime[728] will be committed and that special attention has to be put on the principle of proportionality, as stated in section 29 Austrian Security Police Act.[729]

3.5.4 Conclusion: Realization of an RFI

The public security police's task of maintaining public order, can never constitute a sound basis for an RFI. This is due to the fact that this agency only deals with rules for public behavior whose compliance is essential for a peacefully existing society that embraces morality, customs and civility. However, there are some other competences, which are capable to handle this matter.

---

723 private is seen as the opposite of publicly – thus everything spoken and done which is not intended to be noticed by a larger undefined group of persons; cf. already the chapter on surveillance of persons.

724 This constitutes a prohibition of a major electronic eavesdropping operation; cf. already the illustration concerning this in the corresponding chapter of this thesis on surveillance of persons; cf. moreover Hauer, Keplinger, (2005), p. 612.

725 This constitutes the prohibition of a major optical surveillance; cf. already the illustration concerning this in the corresponding chapter of this thesis on surveillance of persons; cf. moreover Hauer, Keplinger (2005), 3rd edition, p. 612; and Leo (2005), pp. 156-157.

726 Hence, a minor electronic eavesdropping operation can be conducted; cf. already the illustration concerning this in the corresponding chapter of this thesis on surveillance of persons; cf. moreover Hauer, Keplinger (2005), 3rd edition, p. 613.

727 according to Art 10a Basic Law of 21 December, 1867 on the General Rights of Nationals in the Kingdoms and Laender; stating that the 'telecommunications secrecy may not be infringed'.

728 Note in this context that according to section 17 para. 1 of the Austrian Criminal Code the difference between an offense and a crime is that the latter is punishable by a term of more than three year imprisonment.

729 cf. already above.

3.5.4.1 Primary Assistance and Maintenance of Public Security Section 19 and 21 of the Austrian Security Police Act

Due to the fact that it is the obligation of the public security police to assist in the case of an actual threat to life, health, liberty or property of person or an imminent threat thereof, an RFI can be conducted under these provisions. The same is true for the maintenance of public security in the form of an averting of danger. Both tasks involve several competences, as illustrated in the corresponding chapters of this thesis.

3.5.4.1.1 Remote Access for Search Purposes

According to section 39 of the Austrian Security Police Act the public security police is only allowed to enter and search premises, rooms and vehicles if there is an actual or imminent threat to life, health etc.[730] Here, the wording of the provisions for primary assistance contradicts the potential use of an RFI. The same is true in respect to an averting of a danger, as the competence to enter and search potential locations is limited to the search for objects/persons constituting the basis/originator of a dangerous aggression.[731]

3.5.4.1.2 Surveillance of Activities

As presented above, section 54 para. 2 of the Austrian Security Police Act deals with special regulations concerning the investigation of personal data and sets out the limits in regard to observations made by the public security police. However, this provision does not mention anything in regard to the use of electronic devices. This means that it handles customary observations where officers of the public security police follow a suspect from one place to another, thereby gathering information about the person.[732] Therefore, this provision cannot be used as a sound basis for an RFI.

---

730 cf. section 39 para. 3 no. 1 Austrian Security Police Act.

731 cf. sections 39 para. 3 no. 2, no. 3 Austrian Security Police Act; note in this context, as it was already illustrated that after the end of a dangerous aggression or an actual/imminent threat to life etc. a search can only be conducted in accordance with the regulations set out by the Austrian Code of Criminal Procedure; cf. already above and section 39 para. 8 Austrian Security Police Act.

732 cf. in this regard especially Hauer, Keplinger (2005), p. 610

Besides classical police work in the form of an observation, section 54 para. 4 of the Austrian Security Police Act covers the use of image and audio recording devices and the corresponding limitations, prohibiting not only a major electronic eavesdropping operation, but also a major optical surveillance by the public security police. The Austrian Security Police Act restricts preventive measures[733] to minor electronic eavesdropping operations or minor optical surveillances.

In conclusion, it can be said that the inclusion of a minor electronic eavesdropping operation into an RFI is not possible under, either the Austrian Code of Criminal Procedure or under the Austrian Security Police Act.

3.5.4.1.3 Surveillance of Telecommunication

Section 53 of the Austrian Security Police Act constitutes an equal situation as the one illustrated above in the context of surveillance of data and communication, and a disclosure of transmission data. Besides the fact that the possibilities of this provision can constitute a (more or less) important piece of a jigsaw puzzle in an RFI,[734] they would both[735] not be used legitimately as there is again the requirement of a dangerous aggression or a primary assistance. Furthermore, in conformity with the provisions in the Austrian Code of Criminal Procedure, the public security police depends on the assistance of providers and the fact that content data is covered by these provisions. Hence, there is no provision empowering the criminal police to store or monitor communication on their own.

In summary it can be said that in the Austrian Security Police Act no legal basis for surveillance of telecommunication as a task of an RFI can be found. Considering that all investigations, preventive tasks and competences are similar to the regulations dealing with criminal procedures, it should not come as a surprise that the Austrian Security Police Act cannot be used as a basis for conducting an RFI.

---

733 cf. section 54 para. 4 Austrian Security Police Act governs that such devices can only be legally use in order to an averting of a dangerous aggression or a criminal association, or in the context of an extended danger investigation.

734 BMJ/BMI (2008), p. 43.

735 Disclosure of certain data and the option for the use of an IMSI catcher; cf. already above and sections 53 para. 3a and para. 3b Austrian Security Police Act.

Denying the application of an RFI under one of the above illustrated procedural provisions of the Austrian legal order implements that currently no RFI can be legally conducted, consequently, it is necessary to establish new provisions in order to empower the security agencies to apply such investigation methods. This can either be done in the form of new provisions incorporated into one of the two legal Acts – i.e. the Austrian Code of Criminal Procedure, or the Security Police Act – or by setting up a new legal Act handling remote forensic investigations. Generally, there are no qualitative differences between these options. However, due to the preventive character of the investigation method, certain issues have to be kept in mind. Constitutional and structural problems occur, as do questions in regard to prevention and procedural law in principal.

This brings us the fourth and last chapter of this thesis, which deals with the prevention of crime and criminal procedural law. Included in this chapter are the main difficulties that arise when the RFI provision would be established either in the Austrian Code of Criminal Procedure or in the Austrian Security Police Act.

4 Prevention and Criminal (Procedural) Law

The Austrian legislator's intentions behind the establishment of an RFI are not only focused on the solution of already committed criminal acts but also for the prevention of such.[736] Hence, an RFI has to be conducted legitimately in order to prevent a criminal act from happening.

True, prevention is better than cure and to hinder somebody from hurting anybody else should be a maxim to act on. Therefore, the Austrian legislator provides already different tasks and competences for the security agencies: for instance, as presented above public security police is entitled to the averting of danger in the cases of a dangerous aggression or of criminal associations. Hence, it is possible (within the limits of the law) to prevent criminal incidents. This means, however, that the security agencies are allowed to interfere at a very early stage of a (potential) criminal act. That is the crucial point: while repressive measures generally start after a criminal activity happened preventive measures are taken already before such direct criminal activities are even conducted. The critiques regarding an RFI are all about the aspect of prevention. The Austrian legislator fully aware of this delicate situation therefore created certain minimum standards. These standards were established within the framework of procedural law. On the one hand, the competences of the security agencies are limited and on the other hand, citizens are guaranteed certain freedoms as the authorities have to have a certain degree of suspicion based on facts.[737] However, there are further points of critique in the context of prevention via RFIs and the potential incorporation of this investigation method into the Austrian legal framework.

In the following chapter on RFI and the prevention of criminal activities, especially the prevention of terrorist attacks, the problematic relationship between criminal procedural law and the frustration of incidents will be analyzed. In order to give a comprehensive impression on the whole matter, this chapter starts with a brief historic overview on the development of states and their philosophical basis. Understanding this development is important in this context as it shows the evolution from a state of nature to a state of law and in a further step to

---

736 The Austria Federal Ministers of Justice and of the Interior pointed out that an RFI should be conducted in situations where it is necessary for the solution or prevention of a criminal act committed, or planed by a criminal organization or a terrorist association; cf. Vortrag an den Ministerrat der Republik Österreich of 17 October, 2007.

737 cf. already above in the chapter on Criminal Procedural Law and on Security Police Law.

a potential state of prevention. While the principles of these three ‘states’ are not alike they are linked and refer to each other to a certain extend. The author points out the key principles a state of law is based on and why the concept of a state of prevention is diametrically opposed. Furthermore, it will be illustrated how and why states of law did emerge and how states of law try to handle terrorist threats and are thereby moving towards a state of prevention. Subsequently, the main issues accompanying the question of prevention within the regime of criminal law are presented.

The challenges for the Austrian legal order when dealing with RFIs include especially the confronting tasks between the public security police and the criminal police: The entire Austrian legal order does not provide any provisions authorizing anything like an RFI. Hence, the relationship between the tasks is essential to decide whether a provision establishing that investigation method has to be based in the Austrian Code of Criminal Procedure or in the Austrian Security Police Act. For the author of this thesis, the conclusions drawn out of this relationship (i.e. how the ‘task of prevention’ could be handled) lead consequently to a notorious systematic failure within the Austrian legal order.

Another challenge is a problematic provision within the Austrian Criminal Code, thus it is of substantive criminal law origin. This provision implies already some tricky preventive aspects and is therefore highly debatable, as it deals inter alia with the membership in a criminal organization or a terrorist association. The provision constitutes a shift of the boundary of penal relevant behavior into the direction of prevention.

Fundamental and human rights are the last challenge the author will examine. The principle of proportionality as a cornerstone of the Austrian Constitution contains elements of the freedom from discrimination. In order to maintain the freedom from discrimination, the legislator has established some benchmarks: for each investigation method, certain and predefined levels of suspicion have to be given. Whether and how these levels can be taken into account is the subject of the latter subchapter.

4.1 General Aspects of Prevention

4.1.1 From A State of Nature to a State of Prevention

Historically, the emergence of national states as well as the development of its tasks is closely connected to the relationship between security and freedom. Prevailing at the beginning of this evolution was security. The creation of nation states as warrantors for peace and security was in fact the answer to the (mostly confessional induced) civil wars. The social contract theory, established by Thomas Hobbes (1588 – 1679) in his famous book 'Leviathan' is the main basis for Western political philosophy. For Hobbes, a political philosopher, in a state of nature, there is a war of all against all (bellum omnium contra omnes), where man is a wolf to man (homo homini lupus). A supreme political authority does not exist. Therefore an authority of absolute power has to be established, i.e. by a contract. This contract is an agreement between individuals who renounce the individual right to govern themselves and transfer this right to the sovereign. However, contrary to the system of absolutism claiming its absolute power directly from god, the concept of Hobbes is based on a rational solution. For Hobbes it is a rational solution for all parties, because (civil) society submits itself under the power of the sovereign who in exchange establishes security and peace as well as it ends the situation of uncertainty in a state of nature. Despite the fact that the 'Leviathan' was published 1651, this point of view is still present in modern days, as for instance the German Constitutional Court underlines.[738] However, due to the absolutist rulers (governments) following this conception the situation for the civil society was rather unsatisfactory, as absolutist power was not restricted to anything.

In a further evolutionary step the power of the sovereign was not only based on law but also was limited by law. The law set out the framework within the sovereign was able to reign. The concept of a state of law binds sovereign activities in a formal (to the provisions established by the civil society) and in a substantive (to the freedom of the individual) sense. The relationship between freedom and security is clearly defined and involves that an interference with the freedom of an individual is only permitted when and insofar as it is mandatory to maintain security and peace. A state of law is therefore a model based on the assumptions that

738 cf. BVerfG, 1 BvR 256/08 of 2.3.2010, MN 318: Dementsprechend hat das Bundesverfassungsgericht den Staat als verfasste Friedens- und Ordnungsmacht beschrieben und die von ihm zu gewährleistende Sicherheit seiner Bürger als Verfassungswert anerkannt, der mit anderen im gleichen Rang steht und unverzichtbar ist, weil die Institution Staat auch davon ihre Rechtfertigung herleitet.

the sovereign is only responsible for countering violent attacks from the outer and within society. On the other hand, society governs itself more or less alone. Laissez-faire was the credo, meaning let them alone. However, this model became also unsatisfying, due to the impressions of social behavior in the years of the starting industrialization. Due to the harsh working conditions, including inappropriate supply with basics such as nutrition, sanitary or medical care, the danger of riots and social unrest or revolutions was quite high. Hence, it became more and more obvious that the sovereign had to take up social tasks in order to guarantee internal stability and social security. The concept of a welfare state as the main consequence of this development widened the tasks and competence of the sovereign enormously. The sovereign – the state – is somehow an omnipresent state occupied with a wide range of agendas. Due to these facts, the interdependency of the state and its citizen is quite strong.[739]

So far the last step in the described development seems to be a step towards prevention. The increase of the states' responsibilities in security issues reaches new heights in the highly complex and globalized industrial societies which tend to be more receptive to malfunctions, as Huster and Rudolph, two professors of the University in Bochum/Germany, have put it.[740] Due to the potential dimension of damages, even the slightest malfunction can cause serious losses – of financial capital as well as human lives. Hence, in industrialized societies the sovereign has to take action before problems even arise in order to prevent serious damages. In such environments, as they argue, it is not enough to react on existing or obvious dangers, rather than (at the best) to avoid an incident to happen. Thus, prevention is better than cure. In modern society, the main concept is based on risk (assessment) while in security issues the term prevention is used. A state of prevention, as the authors call it, was observed for the first time in the domain of environmental and technical law. Two areas of law whose complexity and tendency towards danger are obvious. Hence, it is not surprising that when these fields of law developed the potential dangers were discussed. The civil society is in demand for information regarding the potential dangers connected to technological achievements and innovations. Especially, the eventual influence on the environment as the main basis of live is of great interest. Hence, the constructors of, for instance, nuclear power plants etc. have to proof that they have a profound risk management. Risk management in regard to scientific assessment of the consequences and a strict control of them from the sovereign are vital in the

---

739 Note in this context that the possibility of intervention by the state and therefore the dependency of the people on their sovereign is quite high.

740 Huster, Stefan, Rudolph, Karsten (ed.), Vom Rechtsstaat zum Präventionsstaat (2008), p. 14.

course of the official approval and technical admission.

It is often argued that the structure of threats emerging from terrorist activities does not have any similarities with that of ordinary criminal law, rather than it is similar to those of the just described technical and environmental issues. Huster/Rudolph hold five arguments in favor of this point of view. Firstly, the threat cannot be individualized – hence, everybody could be hit by an attack. Secondly, the threat is not applicable to a specific location – hence an incident could happen nearly everywhere. Thirdly, the dimension of potential damage can be compared with that of potential incidences in the technical or environmental field. Fourthly, the general preventive aspects of ordinary criminal law are not working, as terrorists cannot be impressed by measures of general deterrence, such as sovereign punishment in the form of imprisonment etc. And finally, a terrorist threat does not only have a systematic character due to its potential network structure. It is also this character making it special, as its activities are directed against a political system as such.[741] It has to be noted at this stage that Huster/Rudolph assume terrorism in its new form targeting nothing less than political order/stability and the entire lifestyle of the western world. They noted that terrorism is (not necessarily) directed against any important political leaders or elites, taking at least some collateral damage in the form of dead bystanders into account. The goals are large-scale attacks hitting potentially everybody. Hence, the current form of terrorism is a global threat in which suspects and locations for attacks are not identifiable. The dimension of damage caused by it does have an extent not known until recently and the characteristics of this threat are rather vague and diffuse. Therefore, it shares some important qualities with technical or environmental issues and it should be dealt with on the basis of the same principles.

4.1.2 Issues Challenging A State of Law

As a general rule, a state of law consists of laws set by the lawmaker. These rules are intended to guarantee a peaceful coexistence in civil society. The sovereign punishes behavior against these rules and maintains thereby peace and security. Thus, behavior in conformity with the law does not provoke the sovereign to step in and take any action against a person. This implements that the sovereign is content with behavior in conformity with the law. Thus, the sovereign does not interfere with the attitude or morals of its citizen. A state of law is

741 cf. Huster, Rudolph (2008), pp. 14-15.

characterized by an equal treatment of all its citizens regardless of sex, age, political or confessional views. Closely related to this is the principle that the sovereign respects privacy and guarantees data protection when handling personal data of its citizens. Equal treatment and the respect of privacy are principles set out inter alia in international treaties and declarations and can be seen – with other fundamental principles – as the very basis of western society, thus of western states as such.

The big challenge out of this non terminal list of principles of a state of law is that they are partly diametrically opposed to prevention and precaution. Prevention by its nature and common sense is forcing the security agencies to gather information about potential terrorist targets and when these incidents could happen. Furthermore, information about potential terrorist activists is needed in order to identify the 'enemy'. Data is collected directly by security agencies, or other entities are obliged to do so and disclose the demanded information to the security agencies when needed. Hence, as it can be easily imagined, infringements with privacy or problems with data protection law may occur.

The second and probably most challenging issue in the context of terrorism and its prevention is the principle of proportionality. As already aforementioned,[742] in a state of law an interference with fundamental rights caused by authorities is only possible under limited circumstances. The relationship between security and freedom is handled via the principle of proportionality. It limits and binds the sovereign and its competences on the one hand, and strengthens the position of the citizens on the other. According to the principle of proportionality, interferences of the sovereign with fundamental and human rights of its citizen are only allowed if and in so far as these interferences are firstly, capable to counter threats. Secondly, interferences have to be necessary in the sense that there is a pressing social need[743] and thirdly, interferences have to be appropriate in the sense of modest, excluding any form of excess. In order to conduct an evaluation whether the principle of proportionality is complied with, it is required that the legally protected interest/good and the corresponding threat are described in detail. This is set into relation with the intended interference. Without any naming or description of the legally protected good and the threat it is facing, it is not possible for the court (who has to issue a corresponding warrant) to evaluate the relationship of the intended interference and the legally protected good. However, as security agencies

742 cf. point 3.2.3 of this thesis.

743 cf. already above and the case of Silver and Others v. The United Kingdom, judgment of 25 March, 1983 (Application no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75), para. 97 (c).

have to handle threats to the legally protected interest ‘security’, this system of evaluation leads to a dead end:

A modern day terrorist threat is not a concrete threat, but rather, the dealing with a certain level of risk. In most cases, this risk can neither be individualized nor described but the potential dimension of damage is considered to be quite extensive. Thus, the well-established system to evaluate proportional interferences does not work properly in this context. What is missing is a benchmark, a guideline to conduct an assessment in the matter of terrorism.

After illustrating the fundamental (constitutional) principles western societies are commonly based on, the next part of this thesis evaluates further constitutional issues in the context of prevention and criminal law: the relationship between the aforementioned tasks[744] of the public security police and that of the criminal police.

4.2 Public Security Police vs. Criminal Police

When it comes to the implementation of RFIs, one of the main questions is into which legal framework they can be incorporated. The Austrian security agencies have to either apply the Code of Criminal Procedure or the Security Police Act in order to deal with criminal activities. As shown, neither the Code of Criminal Procedure nor the Security Police Act does provide currently a legal basis for any investigation method similar to an RFI. Hence, in order to evaluate which is the best to host an RFI, the differences between the two acts as well as their relationship has to be examined. Therefore, the relationships between the activities of the public security police on the one, and the criminal police on the other hand have to be presented. Not only are there different prerequisites for who deals with what but there may also be diverse outcomes and consequences for the implementation of an RFI.

Overall, it can be said that there is a fine line between the tasks of the security police and the criminal police. Generally speaking, the averting of danger – as the main task of the public security police – has to be legally separated from the tasks of the criminal prosecution. Theoretically, the relationship between the two forces and thus the difference is clear and

744 As determinate by Austrian constitutional law.

depends on the anticipated outcome of an investigation on who will conduct it.[745] While the Austrian Security Police Act deals with an averting of danger, the Austrian Code of Criminal Procedure is concerned with the solution and conviction of already occurred happened criminal activities. Thus, criminal prosecution handles committed crimes by solving them, governing the solution for these criminal activities and serving repressive purposes. The task of the public security police – i.e. the averting of danger – is future oriented. Hence, the tasks are not repressive but rather preventive. The task of the public security police tries to avoid future criminal acts or harmful outcomes to happen.[746] The clarifying tasks of the public security police are only intended to 'solve' dangerous aggression and are not directed to any other judicial punishable activities.

Despite this relatively concrete distinction between the delegated jobs of the public security and criminal police, it is possible that their goals and tasks overlap. Especially in the course of time, the question emerges as to when the security agencies operate as public security police and at which stage criminal police 'takes over'. Thus, at which stage does prevention turn into repression.

In this respect section 22 para. 3 of the Austrian Security Police Act offers an answer: As soon as a specific person is suspected of having committed a criminal activity, the criminal police is empowered to investigate, meaning only the Austrian Code of Criminal Procedure is applicable. Nevertheless, as long as a threat exists or as long as there is danger that the offender will repeat the criminal act, the provisions of the Austrian Security Police Act are applicable. Hence, the public security police has to investigate the significant matters of fact[747] of a dangerous aggression. So it is able to evaluate whether there is the threat of further dangerous aggressions and perform steps to prevent such aggressions.[748] This task exists regardless of the tasks according to criminal proceedings. Thus, even after the end of an aggression, investigations can be based on the Austrian Security Police Act until a specific person is under suspicion.[749] After that, a clarification based on legal aspects of the criminal

---

745 However, this is not always that clear as VwSlg 13084 A/1989 points out in stating that even though the security agency applies Art V EGVG in accordance with (the old) section 24 Austrian Code of Criminal Procedure, the activity falls under the expression of public security police according to Art 10 para. 1 no. 7 Austrian Constutional Law.

746 cf. for further remarks in this regard Wiederin (1998), MN 291-5, pp. 68-69.

747 Thus the course of events as well as the actor(s).

748 cf. Pürstl, Zirnsack (2005), pp. 99-100.

749 cf. in this respect especially Wiederin (1998), MN 294-5, p. 69; Hauer, Keplinger (2005), p. 256, as well as Fuchs, Helmut, Zerbes, Ingeborg WK-StPO [2006] section 24 MN 38–40.

act is needed, to decide who continues work on the case, because once a specific person[750] is suspected[751] of having committed the criminal activity, the provisions of the Austrian Code of Criminal Procedure apply exclusively.

However, it is possible that both laws (Act as well as Code) are applicable at the same time, as the Administration Court ruled.[752] Such situations can emerge when there is not yet a specific person suspected of a crime. As the explanatory materials of the Austrian Security Police Act state, there is a general danger (of repetition) as long as the offender's perpetration is not proven, thus the criminal act remains unsolved.[753] Hence, the security agency fulfills a double function – public security police as well as criminal police.[754] In any case, this parallel application of both laws ends when the identity of a suspected person is clarified and the preventive aim recedes that of the criminal law. This shows that the averting of danger is always the main priority.[755] Until the offender is known the Austrian Security Police Act, and from there on only the Austrian Code of Criminal Procedure is applicable.[756] However, there is one limitation to this as the provisions on the handling of data of the Austrian Security Police Act are still valid.[757]

As shown, the main difference between the Austrian Security Police Act and the Austrian Code of Criminal Procedure is that the clarifying task of the public security police of a criminal case ends earlier than that of the criminal police. This involves also the principle that the public security police deals to a large extend with the immediate prevention of criminal activities, while the tasks of the criminal police are characterized mainly by their repressive nature.[758] This form of division of agendas has various reasons. The most important one for this thesis is that the restriction for the public security police to investigate until a specific

---

750 A specific person is a person individualized, even it is not yet known by name; e.g. if somebody points at a person shouting: 'He did it'; cf. as well VwGH, 17 December, 1997, 97/01/0139. Note in this context that if the suspicion against a certain person disappears, the task of the public security police reestablishes.

751 In this respect it is to mention that the suspicion has to be based on facts (similar to the requirements for a search etc – an assumption); cf. furthermore especially Hauer, Keplinger (2005), pp. 298 et seq.

752 VwGH, 16 February, 2000, 99/01/0399.

753 EBRV 148 BlgNR XVIII GP, p. 29.

754 Dearing, Albin, in Dearing, Albin, Haller, Birgitt, Das Österreichische Gewaltschutzpaket (2000), p. 105 et seq.

755 Some even speak of a precedence of the averting of a danger over the solution and conviction of happened criminal activities; cf. Fuchs, Zerbes, WK-StPO [2006], section 24 MN 36; as well as Funk, JBl 1994, footnote 63.

756 VwGH, 16 February, 2000, 99/01/0399.

757 cf. Funk, JBl 1994, footnote 71.

758 cf. for a comprehensive overview and critique of the Austrian Security Police Act draft, Davy, Benjamin, Davy, Ulrike, Gezähmte Polizeigewalt? Aufgaben und Neuordnung der Sicherheitspolizei in Österreich (1991), pp. 72 et seq.

person is suspected of a criminal act is mainly due to the fact that the suspected person does have certain procedural rights – such as those set out by Art 6 Convention for the Protection of Human Rights and Fundamental Freedoms. These rights, or better their protection, lie entirely in the hand of the Austrian Code of Criminal Procedure, meaning that the provisions of the Austrian Code of Criminal Procedure are responsible for the protection of human/fundamental rights.[759] This is taken into account mainly by the principle of proportionality. Hence, every interference with human/fundamental rights has to be evaluated whether it is proportional (in regard to the committed criminal act).

The division of the tasks is reasonable and comprehensive. However, recent developments in this field, especially in the context of surveillance and other investigation methods interfering seriously with fundamental rights of the affected person, are the subject of some critique to be presented briefly.

4.2.1. Diminishing Separation

Due to the fact that an RFI is intended to be established in the same way as a major electronic eavesdropping operations according to section 136 para. 1 no. 3 of the Austrian Code of Criminal Procedure,[760] thus not only for crime solution but also for crime preventive purposes, the separation of the various tasks of the security agencies becomes more and more blurred. The actual functional dissociation of the two task forces, as intended originally by the Austrian Constitutional Law, is diminishing and prevention, as the key task of the public security police are mixed with the tasks of the criminal police. The repressive nature of the criminal police is decreasing and its tasks are taking on a more and more preventive nature. This can be clearly observed by the establishment of certain substantive criminal law provisions.[761] Whether this is a good thing or not, is a completely different question, however, from a formal point of view there should be a clear cut distinction in order to fulfill the requirements of the Austrian Constitutional Law. Not only from a procedural perspective, but also from the perspective of the person applying these regulations, it appears to be more

---

759 cf. EBRV 272 BlgNR XXIII GP, p. 5 as well as Dearing, Albin, in Dearing, Albin, Haller, Birgitt, Das Österreichische Gewaltschutzpaket (2000), p. 106; cf. furthermore below.

760 cf. already the critique at Fuchs, Helmut, 'Zum Entwurf eines Bundesgesetzes über besondere Ermittlungsmaßnahmen zur Bekämpfung Organisierter Kriminalität' in Strafrechtliche Probleme der Gegenwart (1997), pp. 263-299.

761 cf. in this regard to the sub-chapter on substantive criminal law below.

desirable to have clear and distinct boundaries between the tasks. Uncertainties do not constitute a sound and proper basis for the well being of a state and for the confidence and loyalty its citizen should bare for it. It is especially important that trust can be placed in the national authorities, otherwise a peaceful and save coexistence becomes unrealistic.

4.2.2. Protection of Human Rights

Human rights have to always be minded when dealing with coercive measures. In Austria, the protection of fundamental rights is in the hand of the Code of Criminal Procedure. This is due to the fact that the Austrian Security Police Act empowers the security agencies to investigations until a specific person is under suspect. Therefore, the use of coercive measures is rather limited. The coercive measures of the public security police are weaker and in general less intrusive than those used by the criminal police. On the one hand, this can be explained by the fact that public security police does only deal with circumstances where it comes to an averting of danger[762] thus if there is an immediate need for an interference by the security agency. There is no question whether there is culpability in play or not. Even if there is vis major, the provisions of the Austrian Security Police Act apply. Moreover, coercive measures do not need approval if conducted in the context of an averting of danger.[763] On the other hand, if a specific person is already identified as a suspect by the security agency, this person is subject to investigations by the criminal police and therefore, does have certain procedural rights, i.e. rights granted inter alia by the Convention for the Protection of Human Rights and Fundamental Freedoms. At this point, there is less urgency[764] and the criminal police can evaluate everything in detail before conducting, for instance, a search or apply any other coercive measures. Moreover, the steps taken by the criminal police have to be directed and approved by two further entities, namely the public prosecution and the court. Especially the latter fact legitimates a higher degree of intrusion of a suspect's human and fundamental rights, and later on of potential affected persons.

---

762 Involving also the threat of a repetition of e.g. a dangerous aggression; cf. already above.

763 However, this does not mean that there is any legal vacuum – all acts of the security agencies are subject to (at least) subsequent judicial control and approval; cf. e.g. in the context of the public security police section 88 para. 1 Austrian Security Police Act stating that the Independent Administrative Tribunals (Art 129a Austrian Constitutional Law) pronounce judgment after exhaustion of the administrative appeal stages, in so far as such come into consideration on complaints by persons who allege infringement of their rights through the exercise of direct administrative power and compulsion.

764 Although there might be situation of danger in delay; cf. already above.

Coercive measures, as used in the context of the criminal police, can greatly interfere with human rights. Therefore, these measures have to fulfill certain criteria to become legitimate. Substantive reservations[765] allow interferences of the state with the fundamental or human rights, if these acts are in accordance with the law and '*[…] necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*'[766] An interference with fundamental and human rights – in our specific case the right to privacy – could be legitimate if certain requirements and boundaries are recognized. Since only the Austrian Code of Criminal Procedure is capable to deal with the protection of human rights, serious interferences with these rights have to be dealt with by this code and not by the Austrian Security Police Act. In addition, the latter is not even capable to deal with serious interferences as it does not provide any procedural provisions to do so. In this respect, also the German Bundesverfassungsgerichtshof in its ruling regarding the confidentiality and integrity of informational systems holds as one of the maxims that the secretly infiltration of informational systems has to be based on judicial approval.[767]

The illustration of the relationship between the Austrian Code of Criminal Procedure and the Security Police Act shows that none of them is capable to host the intended RFI provision. While the former is intended to handle serious interferences with fundamental/human rights after a criminal incident happened, the latter was established inter alia to counter ongoing or hinder approaching criminal attacks. An RFI, however, tries to combine these two tasks. Whether such a provision can be introduced properly into the legal system of Austria or whether an introduction of the proposed provision would constitute a systematic failure is examined in the next chapter.

---

765 cf. already above in the chapter on constitutional law.

766 Art 8 para. 2 Convention for the Protection of Human Rights and Fundamental Freedoms; but cf. as well in this respect Art 9 para. 2, Art 10 para. 2 etc Convention for the Protection of Human Rights and Fundamental Freedoms.

767 cf. BVerfG, 1 BvR 370/07, 1 BvR 595/07 of 27 February, 2008, maxim no. 2: German: Die heimliche Infiltration eines informationstechnischen Systems ist grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Das Gesetz, das zu einem solchen Eingriff ermächtigt, muss Vorkehrungen enthalten, um den Kernbereich privater Lebensgestaltung zu schützen.

4.3 Systematic Failures

By law, the public security police has to conduct an evaluation of the whole situations prior to the use of any of its competences, whereas there are no such requirements for the criminal police. The reason for this different treatment is that the public security police does not need any approval by a higher authority as it mainly deals with urgent situations. This means that the time constraint of the public security police requires a special evaluation of the situation:

A minimum amount and a sound basis of facts are required before the public security police can assume that an averting of danger is needed. These facts have to constitute an individual and isolated case. Based on these facts, it is possible to draw conclusions of what is going to happen, should the public security police not use its competences. The actual threat can be concluded out of a scenario or a situation likely to lead to a harmful outcome – according to the customary experiences. This prognosis has to be concrete and comprehensive in all its aspects. Thus, the likelihood of a harmful outcome (damage) is objectively given, i.e. foreseeable. Furthermore, there has to be a temporal connection between the actual threat and the proposed damage, meaning that the actual danger would soon cause damage to legally protected goods.[768] Only if all preconditions are fulfilled, the public security police is allowed to use its competences in order to avert the danger.

Due to the fact that the criminal police is not bound to any similar preconditions, the extension of its application towards prevention is highly problematic. Especially, the requirements of predictability and the temporal aspect have to be questioned. True, there are threats emerging from criminal organizations and terrorist associations but to which extend, or which legally protected goods will be affected is rather doubtful. Moreover, it is quite uncertain if or where, for instance, a terrorist attack will happen as well as it can be questioned who, out of a big group of persons, will commit the criminal activity.[769] The requirements according to the Austrian Code of Criminal Procedure are wage, leaving much room for interpretation. Neither do they ask for any clarification and ascertainment of the concrete suspicion. In addition, it is to state that the criminal activities of criminal organizations and terrorist associations are, according to the Austrian Criminal Code, quite

---

768 cf. also BVerfG, 1 BvR 370/07, 1 BvR 595/07 of 27 February, 2008, para. 251-252.

769 In respect to the culpability of a membership in a criminal organization or a terrorist association, please refer below to the chapter on prevetntion and substantive criminal law.

broad and do not oblige the criminal police to evaluate the kind of damage or harmful outcome of the activity. The proposed provision constitutes only vagueness to a great extend. From the point of view of the thesis' author, this range is far too broad and if the Austrian legislator wants to introduce such an intrusive investigation method into the legal framework, there have to be stricter, more specific standards. Otherwise, it is rather unlikely that a correct application of the provision can be guaranteed.

An introduction could, for example, provoke problems with Art 18 of the Federal Constitutional Law ensuring that every act of the administration has to have its legal basis. Furthermore, it is to say that, if there is no defined scenario of threat, both the investigating and the prevention authorities have a far too wide scope of action. An extension of empowerment – even if limited to the prevention of serious crime – leads to confusion on the part of the investigation authorities as well as to indisposition on the part of any citizen. This is especially applicable if citizens do not know in which situations they have to envisage being monitored.[770]

The author has to admit that a solution for this difficulty could not be found. Every potential approach led to a dead end. Repression does not get along well with prevention and vice versa, so it is with the Austrian Code of Criminal Procedure and the Security Police Act. Both are oriented not only in different but also conflicting directions Thus, at the end of the day it will be the criminal courts and at the very end the Austrian Constitutional Court deciding whether and how the method of an RFI can be established within the Austrian legal system.

4.4 Substantive Criminal Law

Not only can prevention be handled via procedural provisions but it could also be dealt with in substantive provisions. Contrary to procedural issues, the latter are not as obviously:

Due to the important requirement of proportionality, serious interferences with fundamental and human rights by covert investigations, an RFI can only be conducted if there is a serious crime to be investigated and solved. Furthermore, a higher degree of suspicion has to be

[770] The author is aware of the fact that the similar provision (section 136 para. 1 no. 3 Austrian Code of Criminal Procedure) is already in force; however, the problems are equal and to question as well in this context.

given, meaning that the assumption of the security agency that a person might be an offender is not enough. Hence, strong suspicion in regard to the committed crime as well in regard to a specific person (group of persons) have to be given to make a serious interference with privacy legitimate. A linkage between the seriousness of the crime investigated, the degree of suspicion and the used coercive measures is widely used and appears to be a reliable concept in order to guarantee that proportionality is retained. This problem is rather minor, if the security agencies investigate a serious crime. Due to the fact that the Austrian legislator intends to establish the same requirements for an RFI as for a major electronic eavesdropping operation according to section 136 para. 1 no. 3 of the Austrian Code of Criminal Procedure, there are – besides the already above presented (current) legal as well as technical problems, and leaving the questionable preventive aspects aside – no further barriers in this respect. From the perspective of proportionality, an RFI could be conducted for the solution of a crime.

The establishment of an RFI is intended in order to prevent criminal acts committed, or planed by a criminal organization or a terrorist association (according to sections 278a, 278b Austrian Criminal Code).[771] However, these provisions dealing with such organizations/associations constitute already preventive aspects to some extent. Further questions arise in this context since the extension of the tasks of the criminal police in the direction of prevention is a duplex one.[772] First of all, the law mentions explicitly that an RFI can be conducted in order to prevent criminal activities, and second of all, the substantive provisions of sections 278a and 278b of the Austrian Criminal Code do have another far reaching preventive facet. While the former is rather unproblematic and does not raise any difficulties, the latter is a bit trickier and therefore has to be illustrated in further detail.

4.4.1 Criminal Organizations and Terrorist Associations

The definitions of criminal organizations and terrorist associations involve a longer lasting aspect, meaning that both groups have to be established for a longer period of time. While a

771 cf. Vortrag an den Ministerrat der Republik Österreich of 17 October, 2007.

772 Note in this context that this is not only true for a RFI but also in respect to major electronic eavesdropping operations, as these can be conducted under the same circumstances; cf. in this respect especially Fuchs (1997), pp. 263-299.

criminal organization has to be structured business alike,[773] its terrorist counterpart does not have such a requirement.[774] A criminal organization is defined by a greater count of members,[775] whereas its terrorist counterpart is already given when at least two persons cooperate. Both provisions (i.e. sections 278a and 278b of the Austrian Criminal Code) require that the groups have to be formed with the goal of committing certain criminal activities, mentioned in the provisions itself, involving mainly serious crime.[776]

To become liable for the criminal activities of a criminal organization or a terrorist association means to either be a founder of the group or to be one of its members.[777] The latter requires that offenders participate in a criminal activity according to the common will of the group or that they provide any kind of information or means to the common will of the group, such as financial assets. Furthermore, it is required that the offenders are operating intentionally in accordance with the common will of the group in every instance.[778] This means that they act knowingly that thereby the organization/association or its penal activities are fostered. However, a simple commitment does not constitute the status as member, since the 'offenders' have the possibility to step away from their intention. Furthermore, a simple passive member of such groups is not subject to any prosecution, according to the report of the judiciary committee.[779]

The fact that the membership to such groups alone is punishable by terms of imprisonment between six months and five years (criminal organization) respectively between five and fifteen years (for leaders of terrorist association)[780] is highly problematic as it shifts the boundary of penal relevant behavior extremely into the direction of prevention.[781] Despite the linkage to a criminal activity – needed inter alia in order to apply coercive measures – this connection is a rather formal one. By referring to the simple membership to one of the

---

773 German: unternehmensähnlich; meaning that the organization does have several characteristics of an ordinary business such as a division of labor between the members, a hierarchic structure as well as a certain degree of infrastructure; cf. JAB 409 BlgNR XX GP, p. 11.

774 The degree of organization is that of a criminal organization according to section 278 Austrian Criminal Code.

775 Regularly this means ten persons; cf. in this regard e.g. 15Os116/08k.

776 Important in this context is moreover that section 278a as well as section 278b Austrian Criminal Code punish members not only for the crimes conducted by themselves, but also for their membership; meaning that the actual criminal activity is in conjunction with the provision on organized crime; cf. e.g. 11 Os 62/97 or 11 Os 58/02.

777 As defined in section 278 para. 3 Austrian Criminal Code.

778 according to section 5 para. 3 Austrian Criminal Code; cf. EBRV 1166 BlgNR XXI GP, p. 36.

779 cf. JAB 409 BlgNR XX GP, p. 12.

780 Certainly some further preconditions have to be fulfilled, especially the definition of a criminal organization/terrorist association must be given.

781 Note at this stage that it is not the intention of the author to relieve the culpability of founding and active members of one of these groups, rather than the author wants to raise awareness for something else.

mentioned groups, the field of application is massively extended in the direction of preparatory works.[782] Furthermore, the principle that suspicion has to be based on objective criterion becomes void as there are no real objective circumstances to which the suspect can be tied to. Only the mental elements of a crime are taken as reference point of suspicion, or putting it differently, there are no real objective circumstance to which the suspicious can be tied to.[783] This is especially true in circumstances where the criminal organization or terrorist association has not yet set 'classical' criminal activities. Despite the fact that there are exceptions to the context of liability of members, as mentioned above, there can be massive interferences with their privacy which are solely based on the reason that these people are connected, related or befriended with the wrong persons.[784]

In order to use coercive measures, the security agencies do need suspects, i.e. persons suspected of having done something criminal or suspected for doing something alike in the future. Without suspects it is hard to justify any investigation method. Hence, if the security agencies do want to investigate whether a person or a group of persons has done (or will do) something illegal, these persons have to be known. At least they have to be identifiable. This is true for the tasks of the security police and the criminal police. Certainly, not always are there concrete persons under suspicion at the beginning of each investigation. The procedural principle that there has to be an identifiable person in order to apply coercive measures such as an RFI is overruled somehow by the vagueness of the two provision of sections 278a and 278b of the Austrian Criminal Code. By the wording of substantive criminal law the criminal police is explicitly empowered to take preventive actions against a more or less precisely defined group of persons. If the group is not identifiable, thus if the security agencies do not know a single member of a group who should be monitor? However, if a member of a potential criminal group is known, the (assumed) intention of a group of person to cooperate and to commit certain criminal acts is taken as the basis for a coercive measure. In addition, there are no strict and clear preconditions for the criminal police for when it should be allowed to conduct any coercive.

---

782 Zerbes, Ingeborg, 'Das Urteil des deutschen Bundesverfassungsgerichts zur Online-Durchsuchung und Online -Überwachung – Grundrechtlicher Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme – auch in Österreich', in ÖJZ (2008), p. 845.

783 e.g. a simple membership in a criminal organization or terrorist association – which is itself more or less entirely defined by intentionality; this is especially true before the member has either participated in criminal activities or provided any means or information.

784 cf. in this regard furthermore below.

With the possible implementation of an RFI provision the criminal police, in order to prevent criminal activities, will be explicitly empowered by the wording of the proposed RFI provision[785] and partly by the vague wording of the mentioned substantive criminal law provisions.

Not only has there to be a certain person who is going to commit a crime, but also there has to be a certain level of suspicion that this will happen. The Austrian legislator has established different levels of suspicion in order to address the principle of proportionality. As a cornerstone of the Austrian Constitution, this principle contains elements of the freedom from discrimination. The next chapter is dedicated to strong suspicion and will examine whether and how strong suspicion is able to maintain the freedom from discrimination.

4.5 Strong Suspicion

In regards to fundamental and human rights, RFIs appear to be highly controversial, since the principle of proportionality emerging out of jurisdiction and doctrinal development forms a cornerstone of the Austrian Constitution. It is regarded as the basis for general objectivity, as an element of equality before the law[786] and in addition, it contains elements of the freedom from discrimination.[787]

In order to evaluate these aspects, it is necessary to point out that generally the Austrian Code

---

785 as well as in regard to section 136 para. 1 no. 3 Austrian Code of Criminal Procedure

786 cf. Art 7 para. 1 Austrian Federal Constitutional Law reads: All nationals (Austrian citizens) are equal before the law. Privileges based upon birth, sex, estate, class or religion are excluded. No one shall be discriminated against because of his disability; The Republic (Federation, Laender and municipalities) commits itself to ensuring the equal treatment of disabled and non-disabled persons in all spheres of every-day life; Similar to this the Universal Declaration of Human Rights and its Art 1: All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.

787 cf. Art 14 Convention for the Protection of Human Rights and Fundamental Freedoms stating that [t]he enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, color, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status; furthermore the attempts by the European Communities in Art 12 EC Treaty, Art 13 Treaty of Amsterdam, or the Council Directives no. 2000/43/EC implementing the principle of equal treatment between persons irrespective of racial or ethnic origin; no. 2000/78/EC establishing a general framework for equal treatment in employment and occupation; and no. 2004/113/EC implementing the principle of equal treatment between men and women in the access to and supply of goods and services; as well as Directive 2002/73/EC of the European Parliament and of the Council on the implementation of the principle of equal treatment for men and women as regards access to employment, vocational training and promotion, and working conditions.

of Criminal Procedure deals with criminal activities that have already been committed. It handles the investigations of classical crimes, such as homicide, fraud or theft. The penal outcome – a dead person or a loss in monetary means – is an important point of reference that a criminal activity was carried through. It is the obligation of the investigation authorities to figure out thereafter, whether the outcome is the result of an indictable activity, thus whether it was achieved in a chargeable manner and with the corresponding malicious intentions. Hence, the authorities have to investigate whether both, the physical elements of an offense as well as the mental elements of an offense are present.[788]

Prevention deals with situations that lay outside the realm of regular criminal activities. Not every criminal activity is carried out effectively, rather than criminals or terrorists spend a lot of time on planning coups and attacks. This planning phase can take place long before the actual crime and is characterized by inconspicuous activities, normal and ordinary preparatory works. Social adequate activities, such as the purchase of a kitchen knife do not provoke any suspicion, as such items are sold zillion times a day. On the other hand, the purchase of a kitchen knife could be as well a criminal activity, as this tool could be used to commit a felony. The purchase of the knife could be the first step leading to homicide or a robbery. The same is true for the purchase of any data carrier, a laptop, a modem or a coaxial cable. With the help of such tools/devices a hacker can potentially start a hacking attack on networks; denial of service attacks on governmental servers could be conducted and many more corruptive things[789] are possible with simple, ordinary and non-suspicious tools. Despite the fact that preparatory works are already punishable by law, nobody would ever argue that the sale of kitchen knives or any other item mentioned should become prohibited. This shows that besides the physical elements, mental elements have to be present for a conviction as well. Not until a person uses a tool in the wrong, socially inadequate manner there is no reason for the investigation authorities to become active. If something happens, the repressive character of the Austrian Code of Criminal Procedure offers a broad range of different coercive measures in order to solve the criminal activity. And before that point in time? Nothing – it is simply not possible to prevent somebody from buying or using a knife.

This describes the characteristic of the mental elements of an offense. It cannot be seen, heard or monitored. The only option is to wait until either something happens or the potential

788 Rather logically given in the case of homicide, as the death penalty was abandoned in Austria.
789 Also cf. to the section on substantive criminal law of this thesis.

criminals unveil their intentions. Suspicion, at the stages prior to the actual commitment of the crime, is, by its very nature, indefinite. As already mentioned above, the security agency has to have a sound basis of facts leading to the conclusion that a harmful outcome is inevitable. Contrary to the public security police, the criminal police has to take culpability into account. Thus, the criminal police deals in addition to the physical elements of a crime, mainly with the mental elements of a crime. The physical (thus the rather obvious) elements of an offense generally pose a minor problem, as the interpretation of even social adequate behavior gives ample scope.[790] Every single activity can be explained by the way it fits the predetermined conclusion. One can always find enough 'evidence' to prove one's point of view.[791]

This is true for all preventive measures; however it is intensified when it comes to criminal organizations or terrorist associations. In both instances, the mental element outweighs the physical elements of the offense. The fact that members of such a group are subject to prosecution for their simple membership, even if no criminal activity – besides the foundation of a group – was realized, appears to be questionable. Certainly, it is easier for the 'prevention' authorities to focus on a group and to see every single activities of one of its members as an activity of the group. By looking at all group activities, however, the possibility to gain knowledge of the potential intentions behind these activities is higher, than by just focusing on the doings of a single member. The security agencies could gather important evidence in regard to the common will of the group by summarizing all group activities, which is not necessarily that obvious in every instance. Even these conclusions are sometimes a matter of misinterpretation and misjudgments. A cluster of various activities of diverse persons does not necessarily indicate whether these people do act in accordance with the group's common will, nor does it put forth the common will. Moreover, there is also a problem with the 'timely' distance between the preparatory works and the actual committal of the criminal activities. Without the knowledge of a person's intention,[792] or at least the strong suspicion that somebody intends to commit a crime, coercive measures have to be questioned. Prevention in the Austrian Code of Criminal Procedure does not work without this

---

790 Note in this context that both kinds of elements are important and necessary to be present for the conviction of a criminal act.

791 Note in this context that even contradicting activities can be interpreted in such way, as it can be argued that the criminal tries to lay a false trail. Remark furthermore that the author does not try to discredit the work of the security agencies; it is only intended to raise awareness for these facts. To err is human, thus everybody – so as the police forces – has to be aware of this problem and behave correspondingly.

792 e.g. the explicitly expressed intention of a person to commit a crime or to cooperate with others in order to commit crimes; or any other hard facts in this direction.

knowledge.[793]

The problem of discrimination plays an important role when it comes to knowledge of intention. Concerning the use of a data screening – a specific profiling method[794] – the use of certain criterion was made illegal. In Austria,[795] as well as throughout Europe,[796] big discussions arose on, whether such profiling methods in the context with terrorist activities are in conflict with fundamental rights. Especially after the 9/11 attacks in the United States of America, governments all over the world focused their intelligence service investigations on a certain group of people. Germany, for instance, collected sensitive personal data from various databases relating to approximately 8.3 million persons. The data for this profile was based on traits of the 'Hamburg cell', members of the 9/11 hijackers, around Mohammed Atta. The main intention behind this profiling was to identify and, at a further stage, to monitor 'sleepers', i.e. terrorists not yet active. Due to a claim of a Moroccan national, the German Federal Constitutional Court in 2006, had to decide whether this form of (pre)investigation was legitimate or not. The court ruled that the following characteristics used in the data screening in order to identify potential terrorists was unconstitutional:[797]

- Male
- aged 18 to 40

---

793 Even the report of the expert group recognizes this great problem stating that: German: Denn dann lässt man den Verdacht der Planung eines Delikts oder den Verdacht einer Vorbereitungshandlung genügen, also den bloßen Verdacht eines Geschehens (wenn überhaupt ein konkretes „Geschehen' ausgemacht werden kann), das weit ins Vorfeld der eigentlichen Rechtsgutsschädigung vorverlagert ist. Außer (vermutete) Absichten des „Verdächtigen' und seinen Gedanken hat man kaum ein reales Substrat zur Hand, an das man die Verdachtsprüfung anknüpfen könnte; cf. BMJ/BMI (2008), pp. 35-36; the argument that the mental elements leave traces (in the form of notes, e-mails stored on a computer) that can be detected by an RFI is a bit shortsighted. As all these traces can be obtained easily via an ordinary house search, the criminal police can do so. However, it is not intended to conduct such physical house searches and RFIs cannot be subsumed under any form of a search of location and objects; cf. already above in the corresponding subchapter.

794 An investigation method using computer and various databases to match human parameter to specific person in order to find an offender.

795 cf. e.g. Novak, Manfred at <http://diepresse.com/home/panorama/oesterreich/524410/index.do?from=suche.intern.portal> retrieved 11 January, 2010.

796 cf. especially the corresponding report of the EU Network of Independent Experts on Fundamental Rights, Ethnic Profiling (2006), at <http://ec.europa.eu/justice_home/cfr_cdf/doc/avis/2006_4_en.pdf> retrieved 11 January, 2010.

797 The judgment denied data screening due to the right of informational self-determination (cf. MN 154-162 of the judgment). Moreover, the German Federal Constitutional Court ruled that data screening could only be considered admissible where the public authorities are acting in response to a 'specific endangerment' to public order and/or individual rights; cf. in this respect the ruling 1 BvR 518/02 of 4 April, 2006 and Neue Juristische Wochenschrift 2006, No. 27, page 1939.

- (ex-)student
- Islamic religious affiliation
- native country or nationality of certain countries, named in detail, with predominantly Islamic population.[798]

This shows clearly the problem of the very human tendency of stereotyping. The hijackers were Muslim, thus all Muslim are terrorists. True, Islamic terrorist activities are a threat to the western societies, but does a vague threat allow massive interferences with the fundamental and human rights of all Muslims? Once again, the answer is that interferences with fundamental and human rights should only be allowed in situations where there is already a specific danger and were the intentions of a suspicious group are certain to a high degree. This is not only true in regard to the mental elements of an offense, but also in the light of the security agencies' human resources. Imagine that the above presented profile is taken as the basis for surveillance without any further evidence of a potential common will or any further evidence concerning a future terrorist attack. This would mean that a massive amount of data would have to be processed (unfeasible financially and manpower wise) and most importantly, the desired outcome, i.e. to find a sleeper,[799] is not guaranteed.[800]

This profile is also highly problematic in respect to ethnic or racial discrimination and therefore unconstitutional not only in Germany, but also in Austria and the rest of Europe. Proportionality as the main principle of objectivity is not given if – without concrete suspicion – data of citizen are proceeded. Thereby the principle of equality before the law is violated because only male Muslims aged 18 to 40 etc. are under suspicion without having committed

---

798 cf. Kett-Straub, Gabriele, 'Data Screening of Muslim Sleepers Unconstitutional' in German Law Journal, [Vol. 07 No. 11] p. 970.

799 The author assumes that the security agencies want to find sleepers; however, it could be desired to find not any sleepers, meaning that Austria is a safe country; cf. as well the next footnote.

800 Remark in this context that due to the massive amount of data, the risk that a sleeper is not identified is quite high. The grid is broad in the beginning and tightens in the course of the investigation. This is especially important to achieve a manageable, i.e. proceedable and monitorable number of persons. Therefore, every more additional characteristics are added, e.g. whether the persons do have a pilots' license etc. Once a person does not fulfill a criterion, it is out and not covered anymore. Moreover, it is to mention that all the criterion are widely known or at least easily to guess nowadays, so that it is not hard for terrorists to hide and 'fall through the grid.' A comprehensive overview on how the German authorities handled their investigations after 9/11 gives Haverkamp, Hauke, 'Präventive Rasterfahndung: Ein effektives Instrument der Terrorismusbekämpfung?' in HFR 2009, pp. 106-107.

a crime or any other objective evidence, other than pure assumptions or stereotyping.[801] Besides the fact that the decision of the German Federal Constitutional Court deals with a different investigation method, the principles can also be applied for an RFI. Especially in the context of criminal organizations and terrorist associations, the danger of unjustified investigations[802] is omnipresent. An innocent weekly gathering of male Muslim students in a private flat can be seen as a terrorist association, even if they are just studying together for their midterm exams etc.[803]

In Austria, the Federal Ministers of Justice and of the Interior signaled their awareness of the problematic relationship between prevention, in the context of criminal procedure, and the general requirements for coercive measures. Therefore, it was decided that an RFI should only be legitimate in situations where there are some additional formal preconditions given.[804] Concerning an application for an RFI for prevention purposes, the expert group followed the view of the two Federal Ministers and proposed to add some further requirements,[805] which have to be implemented before an RFI can be conducted. Thereby, legal relief, as well as proportionality, should be consolidated and the possibilities for a review should be granted. Furthermore, the expert group argued that after an RFI is finished, all corresponding documents should have to be published anonymously and made accessible to the public. This would be a signal and would allow an evaluation and discussion by scholarship.[806]

The German Bundesverfassungsgerichtshof handled the problematic relationship between

---

801 cf. in this respect e.g. De Schutter, Olivier and Ringelheim, Julie, 'Ethnic Profiling: A Rising Challenge for European Human Rights Law' in Modern Law Review, Volume 71, Issue 3 (2008), pp. 358-384.

802 i.e. not based on strong suspicions due to hard facts.

803 Another quite controversial and highly political case is that of some animal rights activists which are now subject to prosecution because of having committed the criminal activity of a criminal organization according to section 278a Austrian Criminal Code; for further details please cf. <http://derstandard.at/1259281991089/Monsterprozess-gegen-Tierschuetzer-startet-im-Maerz> retrieved 12 January, 2010; furthermore, a 'civil right' organization of fathers came under suspicion of having established a criminal organization; cf. <http://diepresse.com/home/panorama/oesterreich/541649/index.do?direct=542213&_vl_backlink=/home/panorama/oesterreich/542213/index.do&selChannel=> retrieved 1 March, 2010.

804 cf. Vortrag an den Ministerrat der Republik Österreich of 17 October, 2007.

805 As these further requirements are quite broad and bear massive political implications it is not the intention of the author to go into any further details in this respect. However, for the interested reader some reference will be presented: for an comprehensive overview on the tasks of the relief commissioner please cf. Vogl (2004); in respect to the requirement for a council of judges instead of a single judge deciding about the conducting of a RFI, please cf. Pressl, Bettina, Die Bedeutung der Ratskammer im Strafprozess (1992); cf. as well BMJ/BMI (2008), p. 36.

806 cf. BMJ/BMI (2008), p. 36.

prevention and coercive measures in a different way. In its ruling regarding the confidentiality and integrity of informational systems the court pointed out that the secretly infiltration of informational systems for the purpose of monitoring of, or searching for information could only be legitimated if there are de facto points of reference that a definite danger to a superior important legally protected interest is given. Superior important legally protected interests are life, limb and liberty of person or interests of the general public. A threat to the interests of the general public concerns the foundations or the existence of the state, or the basis of the existence of the affected human beings.[807] However, the courts states furthermore that an interference may be justified, as long as there are determined matters of fact indicating imminence to the superior important legally protected interest, even it is not entirely certain that the threat will arise.[808] The court refers to a risk based approach (danger prognosis) stating that it is obvious that assumptions and general empirical judgments are not capable to justify any interference via an RFI.[809] The main reference point for such prognosis is the emergence of a concrete danger.

For the German Bundesverfassungsgerichtshof a concrete danger is defined by three criterions: firstly, it is an isolated/individual case; secondly, there is certain proximity of time between the danger and the harmful outcome; and thirdly, there is a close connection to an individual perpetrator or a group of perpetrators.[810] The more concrete the actual danger, i.e. the more details known about it and the more foreseeable the danger, the more likely an RFI could be applied legitimately. Thus, putting it differently, the seriousness of interference with fundamental and human rights by an RFI would not be taken into account appropriately in cases where RFIs are conducted without connection to an individual, concrete and foreseeable danger for legally protected interests.[811]

As mentioned in the chapter on general aspects of prevention, a modern day terrorist threat is

---

807 cf. BVerfG, 1 BvR 370/07, 1 BvR 595/07 of 27 February, 2008, maxim no. 2 stating: Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

808 cf. BVerfG, 1 BvR 370/07, 1 BvR 595/07 of 27 February, 2008, maxim no. 2 stating: Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.

809 cf. BVerfG, 1 BvR 370/07, 1 BvR 595/07 of 27 February, 2008, MN 250.

810 cf. BVerfG, 1 BvR 370/07, 1 BvR 595/07 of 27 February, 2008, MN 251.

811 cf. BVerfG, 1 BvR 370/07, 1 BvR 595/07 of 27 February, 2008, MN 252.

not a concrete threat. Handling terrorist threats is rather a handling of a certain level of risk. Risk management as defined as '*the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events*'[812] could be the solution to handle the prevention of serious criminal acts. Despite the fact that risk management deals mainly with risks coming from uncertainties in the financial context (project failures, credit risks, etc), it can be applied to natural disasters or alike as well.[813] The scientific assessment of risks along with the calculus of probabilities could be a way out of the dilemma. There are several reasons why the author favors the scientific approach. This approach could possibly offer

- a clear benchmarks for the authorities regarding the application of RFIs,
- therefore, a low level of arbitrariness in using RFIs. Therefore,
- the affected person could trust in an objective application of an RFI, as
- every RFI (or the precondition leading to an RFI) would be reasonable and replicable. Thereby,
- objectivity would also be given in a potential review process.

Besides this potential solution to the question of strong suspicion, the author wants to add that the presented additional preconditions recommended by the Federal Ministers of Justice and of the Interior for an RFI are only some good steps in the right direction. It is to point out that we are dealing with highly political issues and therefore objectivity should be the highest criterion and the benchmark in every investigation. The author is aware that this is hard to achieve. However, as RFIs are seen quite controversially an objective application of this investigation method is of great importance. Especially, as regularly uncertainty and vagueness is surrounding this gray area of covered investigations, creating ambiguous situations constantly.[814]

---

812 cf. Hubbard, Douglas, The Failure of Risk Management: Why It's Broken and How to Fix It (2009), p. 10.

813 In order to evaluate risks and thereby to counter threats, scientific standards have been developed: cf. for instance the standards oft he Project Management Institute or the International Organization for Standardization. ISO/IEC Guide 73:2009, Risk management — Vocabulary (2009) and ISO/DIS 31000, Risk management — Principles and guidelines on implementation (2009).

814 cf. in this respect as well Zerbes (2008), p. 845.

Conclusion

The main intension of this thesis was to answer these following three questions dealing with the application of remote forensic investigations within the Austrian legal system:

- Firstly, from a technical point of view, is it possible to apply an RFI without the target person noticing it, thus, does this investigation method even work in praxi?
- Secondly, from a pure legal point of view would it currently be legal for the Austrian security agencies to conduct an RFI? and
- Thirdly, could the prevention of a criminal incident even be legally conducted within the framework of the Austrian Code of Criminal Procedure (something the author disputes)?

While there were rather clear answers to the two former questions, the third question proves to be more difficult and uncertain to answer:

Technically it is possible to apply an RFI if certain preconditions are fulfilled. An RFI works if the security agencies follow a certain code of procedure and use customized software tools. Whether it is successful in every instance and whether it would be applied often, is a completely different thing. Due to its high costs the author assumes that the security agencies would apply this method only in a limited number of cases. Hence, remote forensic investigations will not be on the daily agenda of security agencies and applications will be limited to mainly serious offenses.

From the legal point of view, the author came to the conclusion that neither the Austrian Code of Criminal Procedure, nor the Austrian Security Police Act contains a sound basis for an RFI. Every investigation method lacks some vital components, thus an RFI cannot be subsumed under any of the illustrated methods. The potential legitimacy of an RFI was examined in regard to its three different purposes, namely the remote access for a) search purposes, b) surveillance of activities or c) surveillance of telecommunication.

a) Search Purposes

The search of locations and objects appeared be to be the best to host an RFI for search purposes. First of all, a search of location and objects is the only provision within the Austrian Code of Criminal Procedure dealing with search purposes. Second of all, this provision can be applied independently of the physical condition of the item searched for. Hence, it does not make any difference whether the target object of a search is an electronic device respectively the data stored on it, or whether the criminal police is searching for any other physical objects. In addition IT facilities are also covered by the term objects. However, the biggest handicap for an application of this provision in the form an RFI is that the provision constitutes an open investigation method. Thus, the conducting officers of the criminal police have to be physically present on site. Further problems occur in regard to the rights of the affected person respectively to the obligations of the criminal police (e.g. the affected person is entitled to be present or to bring in a personal confidant; the duty of the criminal police to inform the affected person about the reasons for the search, etc). The affected person's rights are guaranteed by Art 6 ECHR and can therefore not be suspended. Thus, a fair trial is not guaranteed if a search is conducted secretively. As it is the intention of the investigation authorities to avoid physical presence on site, contentions stating that an RFI could be conducted legitimately via this procedural provision are not knock down arguments. Hence, an RFI in the form of a remote examination of a computer cannot be based on a search of locations and objects.

The same is true for the corresponding procedural provision in the Austrian Security Police Act as the public security police is only allowed to enter and search premises, rooms and vehicles if there is an actual or imminent threat to life, health etc. The competence to enter and search locations is limited to the search for objects/persons constituting the basis/originator of a dangerous aggression.

b) Surveillance of Activities and

c) Surveillance of Telecommunication

The investigation methods of surveillance of data and communication, disclosure of transmission data and surveillance of persons appeared to be capable to handle the two latter intended task of an RFI: surveillance of activities and telecommunication. This is especially

true since all of them are covert investigation methods. Contrary to an image of a hard drive as conducted via an RFI for search purposes, continued surveillance of the activities would be prolonged information on what happened in the course of time. Each alteration, manipulation etc. of data is recorded, trusting that sooner or later, suspects will use passwords in order to decipher their files. Hence, the activities of a target person could be monitored and thereby a copy of the hard drive might be created. Communication over the Internet is a special form of telecommunication – hence the legal regulations concerning the surveillance of customary telecommunication are applicable as well. Surveillance of telecommunication over a longer period of time enables the collection of data on conducted information flow. The common basis for all procedural provision in the Austrian legal order to monitor data and communication or persons is communication. In every instance, the legislator refers to an ongoing or conducted communication. Hence, in order to monitor online activities or telecommunication a communication process must take place. Communication in this respect involves every kind of communication, no matter how it is transmitted and so there are no specific technological requirements.

Due to the fact that the procedural provisions deal nearly in every instance with the interception of communication (apart from a disclosure of communication data – i.e. stored outer communication data of who communicated when with whom), an application of an RFI cannot be subsumed under these provisions. Interception refers to two points in time, i.e. when a communication is sent out and when it is received. By definition it is only possible to intercept between these two points. Everything else does not constitute (legally) an interception. As the author made clear, it is rather complex to define when a communication is sent. Firstly, only observable things can be monitored, i.e. the monitored person has to express their thoughts willingly. Secondly, depending on the form of communication further limitations apply. Not until the sender pushes the send bottom, a written communication is sent. Thus, the originator of an e-mail has the power to refrain from sending the communication to the receiver. Before this point in time, the e-mail does not constitute a piece of communication and can therefore not be intercepted. In order to gather knowledge of this data it is necessary to conduct a search of location and objects, thus an open investigation. Furthermore, it is not possible – already by definition – to conduct an interception on a technical device. Hence, for the author the use of software devices on communication equipment is not an interception but a search of an electronic device.

Surveillance of persons in the form of a minor, or a major electronic eavesdropping operation

is not capable either to host an RFI. In the former case optical and acoustical surveillance of persons deals with the listing and recording of privately made statements while an undercover agent is present. This person is the crucial requirement – the person cannot be replaced by a technical devices. In respect to the latter case a technical device is used in order to monitor a target person itself and the statements this person makes. In both cases the target is the person conduct and communication and not just the performance of a computer program.

The Austrian Security Police Act handles the processing of personal data and sets out the limits in regard to observations made by the public security police. The provisions, however, do not handle the use of electronic devices. Within the mentioned Act only the treatment of data gathered via customary observations are governed. The collection of information by interviews of person or request to certain other authorities is dealt within the Act. There are no indications that the use of special technical devices would be legitimate. In addition, when collecting information – even such of location data – the security police depends on the cooperation of internet service/access providers or providers of telecommunication services. Besides the requirement of a dangerous aggression or a primary assistance, the security police is not allowed to store or even monitor communication on their own.

Furthermore, it is to note that also the German Bundesverfassungsgerichtshof in its ruling regarding the confidentiality and integrity of informational systems holds that the secretly infiltration of informational systems has to be based on judicial approval. Thus, such provisions cannot be hosted by the Austrian Security Police Act.

Prevention has a special and interesting relationship to criminal law. In fact, that was the reason for the author to have a closer look at it. The problem with RFIs within the Austrian legal system is the difficult terrain the law makers are maneuvering through when intending to create provisions dealing with prevention in criminal law matters. The range of issues related to this question is intensive, thus the author was only able to give a general overview. Secondly, the author pointed out some problematic cases within the Austrian legal order, starting from constitutional to substantive criminal law and ending with criminal procedural law. In sum, no definite answer can be given. It is especially the great vagueness surrounding the matter of crime prevention that makes it rather challenging to say whether it can be legally conducted within the framework of the Austrian Code of Criminal Procedure. In particular one finding is crucial in this respect:

The shown lack of determination by the law makers in the context of the evaluation of proportionality is a serious issue causing even more severe problems. However, in the perspective of modern day terrorism this dilemma is even worse. This becomes obvious when having a closer look on the intentions behind modern day terrorism, confessional motivated terror. The intention of modern day terrorism is to point out, firstly, that the Western (political) system is not working and cannot provide any security to any of its citizens, and secondly, that its own ideology/religion etc. is prevailing. Modern day terrorism tries to point out the helplessness of the entire Western society. Especially in the cases of suicidal bombing attacks this intention can be seen clearly. A person is killing himself – for – what he thinks is - the bigger common good. Obviously the Western world has no common understanding for these senseless actions in which no direct political message is communicated. Comprehensibly, people in the Western world are asking for effective counter attacks, as they do not want to be intimidated. They rather want the leaders to show resoluteness and strength against a common enemy. The war on terror, as it was proclaimed by the United States, involves not only general – commonly known – warfare. Further legislative action has been taken.[885] The Western world felt and still feels that it finds itself in an exceptional situation if not even in a situation similar to a state of emergency. However, exactly at this point of time history repeats itself. Thomas Hobbes and his arguments are omnipresent in these discussions for ever more competences for the sovereign.

The solution to the dilemma of prevention within the Austrian Code of Criminal Procedure could be the application of risk management tools, as known from the economic world. The author beliefs a potential solution to this highly political and controversial issue can be found by the application of scientific methods. Thereby clear benchmarks for the authorities and a low level of arbitrariness in the use of RFIs could be established. Hence, a high level of objectivity in the application of RFIs could be assured.

[885] cf. in this regard, especially the USA PATRIOT Act (abbreviation for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001).

Sources

• Internet Sources

- AccessData Forensic Toolkit

  <http://www.accessdata.com> retrieved 11 August, 2009

- What is a Computer Worm?

  <http://articles.winferno.com/antivirus/computer-worms/> retrieved 19 May, 2008

- Big Brother Award Preisträger 2008

  <http://www.bigbrotherawards.at/2008/Preistraeger> retrieved 2 December, 2009

- Kriminalprävention und Opferhilfe

  <http://www.bmi.gv.at/cms/BK/praevention_neu/wir_ueber_uns.aspx> retrieved 22 October, 2009

- SINA-Systembeschreibung

  <https://www.bsi.bund.de/cln_155/ContentBSI/Themen/sina/Systembeschreibung/sysbeschreibung.html> retrieved 12 August, 2009

- Basic Law for the Federal Republic of Germany

  <https://www.btg-bestellservice.de/pdf/80201000.pdf> retrieved 16 December, 2009

- An Explanation of Computer Forensics

  <http://www.computerforensics.net/forensics.htm> retrieved 12 August, 2009

- European Convention on Mutual Assistance in Criminal Matters, CETS No.: 030

  <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=030&CL=ENG> retrieved 8 October, 2009

- Robert Morris biography at

  <http://pdos.csail.mit.edu/~rtm/> retrieved 14 May, 2008

- Clamwin – Open Source Security

- <http://de.clamwin.com/> retrieved 18 December, 2009

- Monsterprozess gegen Tierschützer startet im März

  <http://derstandard.at/1259281991089/Monsterprozess-gegen-Tierschuetzer-startet-im-Maerz> retrieved 12 January, 2010

- Gezielte Fahndung nach Ausländern "gesetzeswidrig"

  <http://diepresse.com/home/panorama/oesterreich/524410/index.do?from=suche.intern.portal> retrieved 11 January, 2010

- "Terror": Dubioser Vorwurf gegen Scheidungsväter-Aktivisten

  <http://diepresse.com/home/panorama/oesterreich/541649/index.do?direct=542213&_vl_backlink=/home/panorama/oesterreich/542213/index.do&selChannel=> retrieved 1 March, 2010

- Computer Forensics – Digital Intelligence

  <http://www.digitalintel.com> retrieved 11 August, 2009

- Schriftliche Fragen mit den in der Woche vom 30. Oktober 2006 eingegangenen Antworten der Bundesregierung

  <http://dip21.bundestag.de/dip21/btd/16/032/1603231.pdf> retrieved 21 October, 2009

- Legal order – Austria

  <http://ec.europa.eu/civiljustice/legal_order/legal_order_aus_en.htm> retrieved 23 October, 2009

- EU Network of Independent Experts on Fundamental Rights, Ethnic Profiling

  <http://ec.europa.eu/justice_home/cfr_cdf/doc/avis/2006_4_en.pdf> > retrieved 11 January, 2010

- European Court of Human Rights

  <http://www.echr.coe.int/ECHR/EN/Header/The+Court/Introduction/Information+documents/> 23 October, 2009

- European Network of Forensic Science Institutes

  <http://www.enfsi.eu/index.php> retrieved 28 July, 2009

- Forensic Information Technology

  <http://www.enfsi.eu/page.php?uid=62> retrieved 28 July, 2009

- Misstrauen gegen SPG bleibt

- <http://futurezone.orf.at/stories/256683> retrieved 2 December, 2009

- Guidance Software

  <http://www.guidancesoftware.com> retrieved 11 August, 2009

- Der Staat als Einbrecher: Heimliche Online-Durchsuchungen sind möglich

  <http://www.heise.de/tp/r4/artikel/24/24766/1.html> retrieved 12 August, 2009

- Solo-3 Forensic Kit

  <http://www.icsforensic.com/index.cfm/action/catalog.browse/category/Solo-3%20Forensic/id_category/1442ada0-380f-483f-baa7-434305bb26e9> retrieved 10 August, 2009

- Intelligent Computer Solutions

  <http://www.ics-iq.com/> retrieved 11 August, 2009

- G8 Proposed Principles For The Procedures Relating To Digital Evidence

  <http://www.ioce.org/fileadmin/user_upload/2002/G8%20Proposed%20principles%20for%20forensic%20evidence.pdf> retrieved 5 August, 2009

- G8 Proposed Principles For The Procedures Relating To Digital Evidence

  <http://www.ioce.org/core.php?ID=5> retrieved 5 August, 2009

- From Viruses to Cybercrime

  <http://www.kaspersky.com/virusinfo> retrieved 15 May, 2008

- What is spear phishing? Help prevent identity theft from new, targeted phishing scams

  <http://www.microsoft.com/canada/athome/security/email/spear_phishing.mspx> retrieved 18 December, 2009

- What is social engineering?

  <http://www.microsoft.com/protect/terms/socialengineering.aspx> retrieved 18 December, 2009

- Smashing The Stack For Fun And Profit

  <http://www.phrack.org/issues.html?issue=49&id=14#article> retrieved 18 December, 2009

- McAfee replies -- by denying any FBI contacts of any sort

  <http://www.politechbot.com/p-02839.html> retrieved 18 December, 2009

- Introduction to Spyware Keyloggers

  <http://www.securityfocus.com/infocus/1829> retrieved 11 June, 2008

- Schutz gegen Social Engineering - neue psychologische Ansätze

  <http://www.sicherheitskultur.at/social_engineering.htm> retrieved 18 December, 2009

- Keyloggers: How they work and how to detect them

  <http://www.viruslist.com/en/analysis?pubid=204791931> retrieved 10 June, 2008

Literature

- ACPO Good Practice Guide for Computer-Based Electronic Evidence (2005), Issue 4
- Adamovic, Ludwig, Grundriss des österreichischen Staatsrechtes (1927)
- Arends, Max, Surveillance in the Post 11 September 2001 Era (2008)
- Bertel, Christian, Venier, Andreas, Strafprozessrecht (2004), 8th edition
- Bertel, Christian, Venier, Andreas, Strafprozessrecht (2009), 3rd edition
- Bertel, Christian, Venier, Andreas, Einführung in die neue StPO (2006), 2nd edition
- Beutelspacher, Albrecht et al, Kryptografie in Theorie und Praxis – Mathematischen Grundlagen für Elektronisches Geld, Internetsicherheit und Mobilfunk (2005)
- Beutelspacher, Albrecht et al, Moderne Verfahren der Kryptographie (2006), 6th edition
- BMJ/BMI, Erweiterung des Ermittlungsinstrumentarium zur Bekämpfung schwerer, organisierter und terroristischer Kriminalitätsformen („Online-Durchsuchung') (2008)
- Böck, Benjamin, Computer-Forensik (2005)
- Brenner, Franz, et al, Kriminalpolizei und Strafprozessreform – Konzept der Arbeitsgruppe StPO-Reform des Bundesministeriums für Inneres zu einem sicherheitsbehördlichen Ermittlungsverfahren (1995)
- Brandl Margit, Voice over IP – Rechtliche, regulatorische und technische Aspekte der Internettelefonie (2001)
- Buchmann, Johannes, Einführung in die Kryptographie (2003), 3rd edition
- Buchmann, Johannes A., Introduction to Cryptography (2003), 2nd edition
- Buermeyer, Ulf, Die „Online-Durchsuchung'. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 4/2007

- Buermayer, Ulf, Die „Online-Durchsuchung'. Verfassungsrechtliche Grenzen des versteckten hoheitlichen Zugriffs auf Computersysteme, HRRS 8/2007
- B.P., Lathi, Modern Digital and Analog Commuication Systems (1998), 3rd edtion
- Chirillo John, Der Hacker-Angriff (2004)
- Curtin, Matt, Brute Force – Cracking the Data Encryption Standard (2005)
- Davy, Benjamin, Davy, Ulrike, Gezähmte Polizeigewalt? Aufgaben und Neuordnung der Sicherheitspolizei in Österreich (1991)
- Dearing, Albin, Sicherheitspolizei und Strafrechtspflege – Versuch einer Bestimmung des Verhältnisses zweier benachbarter Rechtsgebiete, in Festschrift für Winfried Platzgummer (1995)
- Dearing, Albin, in Dearing, Albin, Haller, Birgitt, Das Österreichische Gewaltschutzpaket (2000)
- Demmelbauer, Josef, Hauer Andreas, Grundriss des österreichischen Sicherheitsrechts unter besonderer Berücksichtigung der Sicherheitsverwaltung (2002)
- De Schutter, Olivier and Ringelheim, Julie, 'Ethnic Profiling: A Rising Challenge for European Human Rights Law' in Modern Law Review, Volume 71, Issue 3 (2008)
- Diffie, W. and Hellmann M. E.New Directions in Cryptography, IEEE Transactions of Information Theory, 6 November, 1976
- Ebner, Gerhard, Voice Over IP – Grundlagen, Einrichtungen und Konfiguration (2006)
- (Einführungs-) Erlass des BMI of April 19, 1993, 94.762/15-GD/93
- ElGamal, T., A Public Key Cryptosystem and a Signature Scheme based on Diskrete Logarithms. IEEE Transactions on Information Theory, Vol. IT-31 (1985)
- Elias, Levy (aka Aleph One), Smashing the Stack for Fun and Profit (2006)
- Eoghan, Casey, Digital Evidence and Computer Crime – Forensic Science, Computers and the Internet (2000)
- Fabrizy, Ernst, Die österreichische Strafprozessordnung – Kurzkommentar (2008), 10th edition
- Fabrizy, Ernst, Foregger, Egmont, StGB samt ausgewählten Nebengesetzen, Kurzkommentar (2006), 9th edition
- Fanari, Linda, Befugnisse der Sicherheitsorgane nach dem Strafprozessreformgesetz im Verhältnis zu jenen des Sicherheitspolizeigesetzes (2005)
- Feiler, Lukas, 'Technische Aspekte der Online-Durchsuchung' in Zankl, Wolfgang (ed), Auf dem Weg zum Überwachungsstaat? Neue Überwachungsmaßnahmen im Bereich der Informations- und Kommunikationstechnologie (2009)

- Fox, Dirk, Der IMSI-Catcher, in Datenschutz und Datensicherheit (2002)
- Friedman, Thomas L., 'It's a Flat World, After All', New York Times 3 April, 2005
- Fuchs, Helmut, 'Grundsatzgedanken und Zweckrationalität in der aktuellen kriminalpolitischen Diskussion', Festschrift für Winfried Platzgummer (1995), p 425-450.
- Fuchs, Helmut, 'Zum Entwurf eines Bundesgesetzes über besondere Ermittlungsmaßnahmen zur Bekämpfung Organisierter Kriminalität' in Strafrechtliche Probleme der Gegenwart (1997)
- Funk, Bernd-Christian, Das neue Sicherheitspolizeirecht – Kodifikation und Reform einer klassischen Verwaltungsmaterie, JBl 1994
- Funk, Bernd Christian, Einführung in das österreichische Verfassungsrecht (2007), 13th edition
- Geschonneck, Alexander, Computer Forensik – Systemeinbrüche erkennen, ermitteln, aufklären (2006), 2nd edition
- Gibson, Wiliam, Burning Chrome (1982)
- Gudermann, Anne, Online-Durchsuchung im Lichte des Verfassungsrechts (2010)
- Harbich, Herbert, Der Beschluss im Strafprozess und seine Begründung, in Österreichische Richterzeitung (1977)
- Hauer, Andreas, Keplinger, Rudolf, Sicherheitspolizeigesetz (2005), 3rd edition
- Haverkamp, Hauke, 'Präventive Rasterfahndung: Ein effektives Instrument der Terrorismusbekämpfung?' in HFR (2009)
- Horak, Ray, Telecommunication and Data Communications Handbook (2007)
- Hubbard, Douglas, The Failure of Risk Management: Why It's Broken and How to Fix It (2009)
- Huster, Stefan, Rudolph, Karsten (ed.), Vom Rechtsstaat zum Präventionsstaat (2008)
- International Organization for Standardization: ISO/IEC Guide 73:2009, Risk management — Vocabulary (2009)
- International Organization for Standardization: ISO/DIS 31000, Risk management — Principles and guidelines on implementation (2009)
- Jabloner, Clemens, Anwendungsvorrang des Gemeinschaftsrechts und Verwaltungsgerichtsbarkeit, in ÖJZ (1995)
- Jahn, Matthias, Kudlich, Hans, Die strafprozessuale Zulässigkeit der Online-Durchsuchung, in JR 2/2007
- Kaspersky Eugene, Malware (2008)

- Kett-Straub, Gabriele, 'Data Screening of Muslim Sleepers Unconstitutional' in German Law Journal, Vol 07, No. 11
- Klaeren Herbert, Viren, Würmer und Trojaner (2006)
- Koja, Friedrich, Allgemeine Staatslehre (1993)
- Lachinger, Edith, Die Online-Durchsuchung als Erweiterung des Ermittlungsinstrumentariums (2008)
- Leo, Andreas, Prävention und Repression im Rahmen der Sicherheitspolizei (2005)
- Lepuschitz, Michael, Schindler, Thomas, Das österreichische Sicherheitspolizeigesetz (2008), 5th edition
- Leukauf, Otto, Steininger, Herbert, Kommentar zum Strafgesetzbuch (1992), 3rd edition
- Lohsing, Ernst, Österreichisches Strafprozessrecht (1952), 4th edition
- Mayer, Heinz, Das Österreichische Bundes-Verfassungsrecht, Kurzkommentar (2004), 4th edition
- Mayerhofer, Christoph, Das österreichische Strafrecht, Strafprozessordnung §§ 1 – 270 (2004), 5th edition
- Neue Juristische Wochenschrift (2006), No. 27, Rechtsprechung - BVerfG - 4.4.06 - 1 BvR 518/02 - Verfassungsmässigkeit der präventiven polizeilichen Rasterfahndung
- New Oxford American Dictionary (2005), 2nd edition
- Nölle, Jochen, Voice Over IP - Grundlagen, Protokolle, Migration (2005), 2rd edition
- Pilnacek, Christian, Pleischl, Werner, Das neue Vorverfahren – Leitfaden zum Strafprozessreformgesetz (2005)
- Posch, Reinhard, 'Technische Aspekte zur Online-Durchsuchung ' in Online-Durchsuchung (2008)
- Pressl, Bettina, Die Bedeutung der Ratskammer im Strafprozess (1992)
- Pürstl, Gerhard, Zirnsack, Manfred, Sicherheitspolizeigesetz (2005)
- Rädler, Raphael, Die verdeckte Online-Durchsuchung als strafprozessuale Ermittlungsmaßnahme in Deutschland und Österreich (2009)
- Regenfelder, Wolfgang, Ermittlungsmaßnahmen bei neuen Informationstechnologien im Spannungsverhältnis zum Grundrechtsschutz (2008)
- Reindl, Susanne, Computerstrafrecht im Überblick (2004)
- Robens Daniel, Internet-Spionage – der Sicherheitsratgeber für Ihren PC (2000)

- Rössel, Markus, Online-Durchsuchung vs. PC-Grundrecht, in ITRB, 2008, 75
- Rux, Johannes, Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden, in JZ 6/2007
- Sachs, Michael, Krings, Thomas, Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“, JuS 2008, 481
- Salomon, David, Data Privacy and Security (2003)
- Schäfer, Karl in Löwe-Rosenberg, StPO, 25th edition
- Schantz, Peter, Verfassungsrechtliche Probleme von „Online-Durchsuchungen“, KritV 2007, 310
- Schwarzenegger, Christian, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001, in Donatsch/Forster/Schwarzenegger (Hrsg), FS Trechsel (2002)
- Schwenk, Jörg, Sicherheit und Kryptographie im Internet – Von sicherer E-mail bis zu IP-Verschlüsselung (2005), 2nd edition
- Seiler, Stefan, Strafprozessrecht (2009), 10th edition
- Singer, Christian, in Stratil, Alfred (ed), TKG – Telekommunikationsgesetz (2003), 3rd edition
- Solomon, Michael G. et al, Computer Forensics Jump Start (2005)
- Thornton, John I, ‘The General Assumptions And Rationale Of Forensic Identification,’ in David L. Faigman, David H. Kaye, Michael J. Saks, & Joseph Sanders (eds) Modern Scientific Evidence: The Law And Science Of Expert Testimony (1997), 2nd edition
- United States Department of Justice, National Institute of Justice, NJI 187736: Electronic Crime Scene Investigations: A Guide for First Responders (2001)
- United States Department of Justice, National Institute of Justice, NCJ 199404: Forensic Examination of Digital Evidence: A Guide for Law Enforcement (2004
- Vogl, Mathias, Der Rechtschutzbeauftragte in Österreich (2004)
- Vortrag an den Ministerrat der Republik Österreich durch das Bundesministerium für Justiz und das Bundesministerium für Inneres hinsichtlich der Erweiterung des Ermittlungsinstrumentariums zur Bekämpfung schwerer, organisierter und terroristischer Kriminalitätsformen („Online-Durchsuchung’), 17 October 2007
- Walter, Robert, Mayer, Heinz, Grundriss des österreichischen Bundesverfassungsrechts (2007), 10th edition
- Wätjen, Dietmar, Kryptographie – Grundlagen, Algorithmen, Protokolle (2008), 2nd edition

- Wiederin, Ewald, Einführung in das Sicherheitspolizeirecht (1998)
- Wiederin, Ewald, Privatsphäre und Überwachungsstaat - Sicherheitspolizeiliche und Nachrichtendienstliche Datenermittlungen im Lichte des Art 8 EMRK und der Art 9-10a StGG (2003)
- Wilhelm, Georg, Online-Durchsuchung nur über richterlichen Befehl, ecolex 2008, 293
- Zerbes, Ingeborg, 'Das Urteil des deutschen Bundesverfassungsgerichts zur Online-Durchsuchung und Online -Überwachung – Grundrechtlicher Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme – auch in Österreich', in ÖJZ (2008), p. 834

• Judgements

Germany:

- 1 BvR 518/02 of 4 April, 2006
- BGH Beschluss of January 31, 2007, StB 18/08, in JZ 15/16/2007
- BVerfG, 1 BvR 370/07, 1 BvR 595/07 of 27 February, 2008
- BVerfG, 1 BvR 256/08 of 2 March, 2010

Europe:

- Case of Handyside v. The United Kingdom, judgment of 7 December, 1976 (Application no. 5493/72)
- Case of Silver and Others v. The United Kingdom, judgment of 25 March, 1983 (Application no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75)

Austria:

- KH 834
- KH 2285
- LG Klagenfurt 17 January, 2008 7 Bl 8/08g

Austrian Constitutional Court:

- VfSlg 1890/1949
- VfSlg 1980/1950

- VfSlg 2861/1955
- VfSlg 2990/1956
- VfSlg 5080/1965
- VfSlg 5083/1965
- VfSlg 6528/1971
- VfSlg 6696/1971
- VfSlg 7067/1973
- VfSlg 8871/1980
- VfSlg 9210/1981
- VfSlg 9766/1983
- VfSlg 10547/1985
- VfSlg 10897/1986
- VfSlg 11650/1988
- VfSlg 11895/1988
- VfSlg 12056/1989
- VfSlg 12122/1989
- VfSlg 12267/1990
- VfSlg 12513/1990
- VfSlg 12567/1990
- VfSlg 12628/1991
- VfSlg 12657/1991
- VfSlg 12701/1991
- VfSlg 13043/1992
- VfSlg 14864/1997
- VfSlg 16054/2000

Austrian Administration Court:

- VwSlg 543 A/1948
- VwGH judgment of 13 February, 1984, Z 82/10/0178
- VwGH judgment of 9 July, 1984, Z 84/10/0080
- VwGH judgment of 8 September,1988, 88/16/0093
- VwSlg 13084 A/1989
- VwGH judgment of 17 December, 1997, 97/01/0139
- VwGH judgment of 16 February, 2000, 99/01/0399
- VwSlg 15422 A/2000

Austrian Supreme Court

- EvBl 1958/295
- 16 Os 15/91
- 11 Os 62/97
- 11 Os 108/00
- 11 Os 109/00
- 12 Os 152/00
- 12 Os 153/00
- 14 Os 172/01
- 11 Os 58/02
- 12 Os 44/04
- 15 Os 13/04
- SSt 2004/39
- 13 Os 46/08a
- 15 Os 116/08k
- EvBl 2008/183

- **Legislative Materials**

  - EBRV 148 BlgNR XVIII GP
  - AB 184 BglNR XX GP
  - EBRV 49 BlgNR XX GP
  - JAB 812 BlgNR XX GP
  - JAB 409 BlgNR XX GP
  - EBRV 81 BlgNR XXI GP
  - EBRV 1166 BlgNR XXI GP
  - EBRV 25 BlgNR XXII GP
  - EBRV 309 BglNR XXII GP
  - JAB 406 BlgNR XXII GP
  - EBRV 272 BlgNR XXIII GP

- **Commentaries**

  - Bertel, Christian, WK-StGB
  - Lewisch, Peter, WK-StGB
  - Lewisch, Peter, Reindl-Krauskopf, Susanne, WK-StGB
  - Reindl-Krauskopf, Susanne, WK-StGB

  - Fuchs, Helmut, Zerbes, Ingeborg, WK-StPO [2006]
  - Reindl-Krauskopf, Susanne, WK-StPO
  - Tipold, Alexander, Zerbes, Ingeborg, WK-StPO [2005]
  - Tipold, Alexander, Zerbes, Ingeborg, WK-StPO
  - Vogl, Mathias, WK-StPO

Abstract

The purpose of this thesis is to provide an introduction and general overview of the newly developed method of remote forensic investigations. It intends to present RFIs in a rather broad and general way with a special focus on the relationship between technology and law. T

The technical part of this thesis involves presentations of software programs potentially capable to be applied in RIFs. The terms of ‘malware’ and ‘viruses’ are also clarified, as are the expressions ‘spyware’ and the various forms of ‘Trojan horses’. Special attention is given to the technical issues and properties of telecommunication as well as to that of decryption and encryption. In order to show how a computer has to be searched physically by law enforcement agencies, the author gives a brief introduction into computer forensics. The illustration includes a description of the established procedures for the investigation authorities and the various principles the process is based on. Furthermore, a brief overview of the special hardware as well as software tools is given. Thereafter, a presentation of the potential application of a remote forensic investigation in regards to its two main purposes, i.e. obtaining access to a computer and the exploitation of that access.

The legal part of this thesis starts with an overview on the relevant provisions in the Austrian constitutional law and one of its cornerstones - the principle of proportionality. Despite the fact that this thesis is mainly dedicated to procedural law, the author gives a summary of important substantive law provisions. This is necessary in order to show that the security agencies would – without empowerment to conduct a remote forensic investigation – commit a criminal act and would therefore be liable for it as well. After an introduction into criminal procedures law, involving an illustration of general principles – such as the principle of indictment, or the system of warrants – the relationship between the criminal police, the public prosecution and the court as well as their special tasks and competences, the provisions in regard to remote forensic investigations are pointed out extensively. Especially the following provisions of the Austrian Code of Criminal Procedure are examined in detail including an extensive effort to subsume an RFI under them:

- Search of Locations and Objects
  according to section 117 no. 2 in conjunction with section 119 para. 1 of the Austrian Code of Criminal Procedure
- Surveillance of Data and Communication

according to section 135 para. 3 in conjunction with section 134 no. 3 of the Austrian Code of Criminal Procedure

- Disclosure of Transmission Data
  according to section 134 no. 2 in conjunction with section 135 para. 2 of the Austrian Code of Criminal Procedure
- Surveillance of Persons
  according to section 136 in conjunction with section 134 no. 4 of the Austrian Code of Criminal Procedure

Following this, a similar approach is used in order to present the Austrian Security Police Act. Special focus is put on the tasks of maintaining public order, primary assistance and maintaining public security. Consequently, the competences of the public security police will be illustrated in the same manner as the competences of the criminal police:

- Competence to Enter and Search of Premises, Rooms and Vehicles
  according to section 39 of the Austrian Security Police Act
- Legitimacy of Processing of Personal Data
  according to section 53 of the Austrian Security Police Act
- Special Regulations for Investigation
  according to section 54 Austrian Security Police Act

The final part of this thesis is dedicated to the relationship between the prevention of criminal incidents and criminal procedural law. Starting with rather general considerations to prevention and a historic overview on the development from a state of nature, to a state of law and finally to a state of prevention, following five aspects are examined in depth:

- General aspects of prevention,
- Relationship between the criminal police and the public security police,
- Systematic questions regarding an incorporation of RFIs into the Austrian legal order,
- Preventive aspects within the regime of substantive criminal law, and
- Demanded degree of suspicion.

Summarizing, it is to state that the intention for this thesis is to give a broad and general overview on RFIs, from a technological as well as a legal point of view. The focus is – unlike other publications in this respect – not directed on fundamental/human rights issues, rather than on issues related to a potential incorporation of RFIs into the Austrian legal order. The Austrian Code of Criminal Procedure and the Austria Security Police Act are the points of reference and the standard of comparison.

Abstract German

Diese Arbeit setzt sich zur Aufgabe, die neue Ermittlungsmethode der Online Durchsuchung zu erörtern und in einer breiten und allgemeinen Art zu präsentieren. Ein besonderer Fokus wird dabei auf das Verhältnis von Technik und Recht gelegt.

Dem Leser wird vorab ein weit gefasster technischer Teil präsentiert, der die Darstellung der verschiedenen, im Zuge einer Online Durchsuchung angewendeten, Software-Programme involviert, wobei besonderes Augenmerk auf die technischen Aspekte der Telekommunikation sowie der Verschlüsselungstechnik gelegt wird. Darüber hinaus beinhaltet die, in einem Abschnitt konzentrierte, technische Aufarbeitung des Dissertationsthemas eine kurze Einführung in die Computer-Forensik, also die Vorgehensweise einer „Computerdurchsuchung“ durch die Strafverfolgungsbehörden. Neben einer Beschreibung der festgelegten Verfahren und Prinzipien einer derartigen „Computerdurchsuchung“ wird überblicksmäßig auch auf die speziellen Hard- und Software-Tools eingegangen. Diesen technischen Teil abschließend werden sodann auch die angedachten Einsatzgebiete der Online-Durchsuchung aufgezeigt und einer faktisch-technischen Begutachtung unterzogen.

Der auf die technische Erörterung folgende Rechtsteil der Arbeit enthält neben einem Überblick über die verfassungsrechtlichen Bestimmungen, insbesondere eine Auseinandersetzung mit der in punkto Online-Durchsuchung wesentlichen Frage der Verhältnismäßigkeit. Trotz des Umstandes, dass sich die vorliegende Dissertation vor allem mit dem Verfahrensrecht befasst, erfolgt eine kurze Darstellung von wichtigen materiell-rechtliche Bestimmungen. Nach einer Einführung in die Strafprozessordnung und ihrer Grundsätze – wobei insbesondere das Kräfteverhältnis zwischen Kriminalpolizei, Staatsanwaltschaft und Gerichten sowie das System zur Durchsetzung von Zwangsmaßnahmen erläutert wird – konzentriert sich die Darstellung auf einzelne Bestimmungen der StPO, die auf den ersten Blick gerechtfertigt erscheinen, eine Online-Durchsuchung durchzuführen. Die dabei eingehend beleuchteten verfahrensrechtlichen Paragraphen betreffen:

- Durchsuchung von Orten und Gegenständen (§§ 117 Z2 iVm 119 Abs 1 StPO),

- Überwachung von Nachrichten (§§ 135 Abs 3 iVm 134 Z3 StPO),
- Auskunft über Daten einer Nachrichtenübermittlung (§§ 134 Z2 iVm 135 Abs 2 StPO),
- Großer bzw. kleiner Lauschangriff (§§ 136 iVm 134 Z4 StPO).

Im Anschluss widmet sich die Dissertation dem Sicherheitspolizeigesetz.

Die Aufarbeitung des SPG erfolgt in gleicher Art und Weise wie die zuvor erörterten Thematiken, wobei die darin normierten Aufgaben des Rechtsträgers, i.e. die erste allgemeine Hilfeleistungspflicht sowie die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung und die damit einhergehenden Kompetenzen der Sicherheitspolizei, einer näheren Begutachtung unterzogen werden. Im Speziellen werden folgende Bestimmungen untersucht:

- Betreten und Durchsuchen von Grundstücken, Räumen und Fahrzeugen (§ 39 SPG),
- Zulässigkeit der Verarbeitung von personenbezogenen Daten (§ 53 SPG),
- Besondere Bestimmungen für die Ermittlung (§ 54 SPG).

Die betreffenden Unterkapiteln des rechtlichen Teils dieser Dissertation endet mit dem Versuch, die Online-Durchsuchung als modernes Ermittlungs- und Beweissicherungsinstrument die besprochenen verfahrensrechtlichen Bestimmungen zu subsumieren.

Im abschließenden Teil beschäftigt sich die vorliegende Arbeit mit dem Verhältnis von Prävention und (Straf-)Verfahrensrecht. Ausgehend von generellen Überlegungen zu Prävention und einem historischen Abriss der Entwicklung vom Naturrecht zum Rechts- und schließlich zum Präventionsstaat, beleuchtet der Autor die problematische Wechselbeziehung anhand von fünf Punkte näher:

- Generelle Überlegungen zur Prävention,
- Verhältnis der Kompetenzen von Kriminal- und Sicherheitspolizei,

- Systematische Problem der Eingliederung der Online Durchsuchung im Rechtssystem Österreichs,
- Präventive Aspekte im materiellen Strafrecht,
- Verdachtslage vor Durchführung einer Online Durchsuchung.

Zusammenfassend ist festzuhalten, dass nach Intention der vorliegenden Dissertation der geschätzte Leser einen generellen Überblick über das Thema „Online Durchsuchung“ erhalten soll. Darüber hinaus wird der Versuch unternommen, sowohl die in der Maßnahme involvierten technischen als auch rechtlichen Aspekte gleichermaßen zu erläutern und einander gegenüber zu stellen. Der Fokus soll dabei jedoch nicht wie in anderen, bereits verfügbaren Schriften auf grund- und menschenrechtlicher Basis liegen, sondern wird vielmehr die problematische Eingliederung dieser Ermittlungsmethode in das österreichische (Verfahrens-)Rechtsystem aufgezeigt. Dabei dienen insbesondere die Strafprozessordnung und das Sicherheitspolizeigesetz als Vergleichsmaßstab.

Curriculum Vitae Autoris

Education:

10/2008 – 06/2009 **Diploma Programme**
Diplomatic Academy of Vienna (with scholarship)
Multidisciplinary and multilingual postgraduate programme with focus on international economics, international relations, international politics and international law

09/2007 – 01/2008 **Bond University, QLD, Australia**
Faculties of Law, Humanities and Social Science
Research semester for PhD in jurisprudence

03/2008 to date **Vienna University of Economics and Business**
Bachelor studies of Economics and Social science

11/2006 to 03/2011 **Faculty of Law, University of Vienna**
PhD in jurisprudence
conducted and presented research papers:

- Conflicting Dispute Settlement Outcomes
- The Austrian System of the Protection of Financial Data in Criminal Investigations
- Electronic Equipment and Criminal Law - an overview on the Australian way of handling electronic devices in criminal investigations
- Criminal Profiling and Cyber-Evidences
- Privacy in Criminal Investigation

10/2002 – 11/2006 **Faculty of Law, University of Vienna**
Magister Iuris (equivalent to MA)
conducted and presented research papers:

- Private International Law vs. E-Commerce
- The European Convention on Cybercrime
- The Directive on the Retention of Data
- Voice over Internet Protocol (VoIP)
- Legal Interactions between Decisions of International Organizations and European Law, especially concerning the Legal Order of Austria
- The EU Legislation Procedures especially concerning the Tasks and Role of the Commission and its internal Process

01/2006 – 06/2006 **Faculty of Law, University of Lapland, Rovaniemi, Finland**
Erasmus exchange semester with focus on European Law

Scientific Work Experience:

10/2009 – 10/2010 **Faculty of Law, University of Vienna**
Section for International Law and International Relations Project assistant**:** CARE Consular Assistance Regulation in Europe