Dr. Farsam Salimi

19th International AIDP-Congress – "Information Society and Penal Law"

Section 3

National Report for Austria[*]

A. General Questions

1) *Are there current (legal or socio-legal) definitions for applications of IT and ICT within the context of criminal procedure (including forensics)? How are such conceptual definitions reflected in the literature, legislation, court decisions and relevant practices within the context of criminal procedure?*

There is **no general definition** for applications of IT and ICT within the context of Austrian criminal procedure, e.g. within the Austrian Code of Criminal Procedure (CCP). As far as the transmission and processing of data is concerned, there is the term "automationsunterstützte Datenverarbeitung" which means **automatically processed data** in Art. 100 CCP (reports of the Criminal Police ["Kriminalpolizei"] to the Public Prosecution Service ["Staatsanwaltschaft"]) and Art. 102 CCP (order or permission of the Public Prosecution Service) and Art. 116 CCP (monitoring bank transactions). The definition of "computer system" in Art. 74 par 1 fig 8 of the Austrian Criminal Code (CC) and the offence "Betrügerischer Datenverarbeitungsmissbrauch" (computer-related fraud) in Art. 148a CC contain the same term (a similar wording can be found in the offence "Datenbeschädigung" (data interference) in Art. 126a CC). "Automationsunterstützte Datenverarbeitung" includes all forms of digital data processing, so this term comes as close as possible to a general definition of IT-applications. This wording is basically derived from Art. 1 lit a Cyber Crime Convention of the Council of Europe. A similar definition can be found in the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

Furthermore, the title of the Articles 74 et seq CCP "**Application of Information Technology**" has to be mentioned. Despite the title, these articles do not contain rules about the requirements and extent of the application of IT but rather rules of procession, correction, erasure and inhibition of personal data. These terms are derived from the Federal Act on the Protection of Personal Data (Datenschutzgesetz 2000).
The CCP contains aspects of IT in the **sections concerning specific investigation measures**, such as Monitoring of Telecommunication Traffic Data ("Auskunft über Daten einer Nachrichtenübermittlung" and "Auskunft über Vorratsdaten", Art. 134 fig 2 and 2a CCP), the Interception of the Contents of

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

Revue électronique de l'AIDP / Electronic Review of the IAPL / Revista electrónica de la AIDP
(ISSN - 1993-2995), 2014, RA-2:1

Telecommunication ("Überwachung von Nachrichten", Art. 134 fig 3 CCP), optical and acoustic surveillance ("Optische und akustische Überwachung", Art. 134 fig 4 CCP) and the rules on data mining ("Automationsunterstützter Datenabgleich", Art. 141 CCP).

In the same way **specific rules concerning the main proceeding** contain provisions on the application of special forms of IT and ICT, e.g. video-supported interrogations. One has to arrive at the conclusion that, in fact, there is no *general* definition for applications of IT and ICT within the context of criminal procedure, but single provisions, however, contain specific forms of applications of IT and ICT.

The **discussion in doctrine and practice** during the last years has focussed on the question, which forms of criminality should be seen as forms of "Cyber Crime" as there is no general definition of this type of criminality within the Austrian legal system. A discussion on the definition of applications of IT and ICT within the criminal procedure law could not be detected.

2) *Are there specific institutions and/or task forces involved in the implementation of ICT within the criminal justice system?*

The **Criminal Police** lead the criminal investigation under the control and supervision of the Public Prosecution Service. In addition to the criminal investigation the preventive fight against crime by the **Security Police** is to be mentioned. Although the Austrian legal system draws a distinction between the criminal procedure (based on the CCP) and security police measures (based on the Act on Security Police, "Sicherheitspolizeigesetz", SPA), in practice there is much of overlapping. Generally, the Austrian Police play a double role, as there is no organizational or personal difference between Criminal Police and Security Police. Although the internal organisation the law enforcement authorities of the Federal Ministry of the Interior is divided into special units with special tasks, this division is normally not predetermined by law.

According to Art. 6 of the **Special Unit Act** ("Sondereinheitenverordnung", Federal Law Gazette No II 207/1998) optical and acoustic surveillance which is aimed at special professional groups such as defence counsels, attorneys-at-law, patent attorneys, notaries public, economic trustees, psychotherapists, psychologists, probation officers, media owners, media staff members etc (Art. 157 par 1 fig 2 – 4 CCP) and large bugging operations ("Großer Lauschangriff", Art. 136 par 1 fig 3 CCP) are conducted by the SEO (special unit for observation, "Spezialeinheit für Observation"), which is directly responsible to the General Direction for Public Security ("Generaldirektion für die öffentliche Sicherheit") within the Federal Ministry of the Interior.

Moreover, the department 4 of the Austrian Criminal Intelligence Service ("Bundeskriminalamt", BK), "Criminal Analysis", plays an important role in the implementation of IT within the criminal procedure by applying both operational and strategic criminal analysis. The department 5 of the BK, called "Criminal Police Support Services", deals with observation, undercover investigation and especially all questions related to cyber- and network crime. The department 6 of the BK, "forensics", deals inter alia with the "Central Identification Service" ("Zentraler Erkennungsdienst"). Within the Federal Ministry of the Interior, Group IV/B is responsible for the applications of IT and ICT.

In the same way **other operational units of the police authorities** (officials of the regional criminal investigation offices [Landeskriminalämter], the Federal Bureau of Anti-Corruption [BAK, "Bundesamt für Korruptionsprävention und Korruptionsbekämpfung"], or the Federal Bureau for Protection of the Constitution and Fight against Terrorism [BVT, "Bundesamt für Verfassungsschutz und Terrorismusbekämpfung"]) apply automatic data processing in their daily work (electronic file system of the police: "PAD", see question E. 5) as well as during interrogations, communication or special investigation measures.

Within the **judicial authorities** the Department 5 of the presidential section ("Legal data processing/E-Justice") in the Federal Ministry of Justice is responsible for the application of IT and ICT within the Austrian Justice. The "VJ" ("Verfahrensautomation Justiz", Procedure Automatisation Justice), run by the "Bundesrechenzentrum" (Federal Computer Centre Ltd.) as a special tool, is applied to register all forms of judicial procedure. Nevertheless, the criminal file system is not run entirely electronically at Court yet (see question E. 5).

3) *Are there private (commercial) organisations (companies) that offer ICT related services to the criminal justice system? If so, can you give examples? What limits have to be observed?*

Private organisations only play a role as **Experts** which have to be appointed in investigations by the Public Prosecution Service, when investigations or taking of evidence requires specific expert knowledge. This can be the case during the investigations as well as during the main proceeding. Related to IT and ICT experts are often appointed for analyzing confiscated data (Art. 126 CCP).

Private telecommunication companies and internet providers are obliged to cooperate with the law enforcement authorities. They have to provide information data of a message transmission that is retained due to billing purposes (billing data) or due to the obligations arising from the data retention directive of the EU (see question B. 5) and to cooperate in the surveillance of messages (Art. 138 par 2 CCP, Art. 76a CCP).

Apart from this, private companies are not directly involved in the criminal investigation and prosecution. The results of private investigations, such as interior (forensic) investigation of companies by compliance or forensics departments, can be used in the criminal proceeding if they do not interfere with professional secrets (see Art. 112 CCP).
Generally spoken private persons are bound to the limits of the Act on the Protection of Personal Data (Datenschutzgesetz 2000). As far as criminal law is concerned they cannot be empowered to act with public authority as it is – in some cases – possible within the administrative law.

As to the mere technical support also private companies offer **services to the justice system**, such as the "Bundesrechenzentrum" (Federal Computer Centre Ltd.) supporting special tools such as the "VJ", or other private companies providing software for special IT-applications and programs.

B. Information and Intelligence: building information positions for law enforcement

1) *Which ICT-related techniques are used for building information positions for law enforcement agencies?*

In the Austrian legal system **building information positions** as a part of the preventive fight against crime is mainly regulated in the Act on Security Police (SPA, Sicherheitspolizeigesetz). The compilation of information in order to build information positions is particularly a task of the "BVT" (see question A. 2). According to Art. 21 par 3 SPA the security police, in practice the BVT, are assigned to the task "erweiterte Gefahrenerforschung", which means **"extended potential danger identification".** For this purpose the observation of groupings is admissible, if, in view of the existing structures and expectable developments in the surroundings of these groupings, it has to be expected that criminal offences will be committed causing severe danger to public security, in particular, violence motivated by ideologies or religious beliefs. Since 2012 this special task has been opened – under special requirements – towards the observation of single potential perpetrators. Therefore – besides regular observation (Art. 54 par 2 SPA) and undercover investigation (Art. 54 par 3 SPA) – special IT-related investigation measures are admissible for the BVT: The optical and acoustic surveillance outside private rooms and processing image data, compiled by private persons (Art. 54 par 4 SPA and Art. 53 par 5 SPA).

These measures, taken by the BVT for purposes of Art. 21 par 3 SPA, need to be **authorized in advance** by the legal protection attorney within the Federal Ministry of the Interior ("Rechtsschutzbeauftragter beim Bundesministerium für Inneres"). As there is no judicial control of security police measures in general, these intelligence measures are not controlled by court either (see also question B. 7).

Building information positions is **not included in the criminal proceedings** in the narrower sense, according to the CCP. Nevertheless, some investigation measures that were implemented in 1999 such as the optical and acoustic surveillance and data mining according to the Articles 136 and 141 CCP do contain **some preventive aspects,** especially in fighting terrorism and organized crime.

Building information positions by police authorities is also supported by the **criminal analysis** according to **Art. 53a SPA**, applied by the department 4 of the Criminal Intelligence Service (see question A. 2). The combination of different data sources of the police authorities can help to uncover complex criminal structures and organized criminal groups, offer a new basis for further investigations and thus to build a general information position concerning special risk groups and potential perpetrators.

2) *To which type of public (e.g. DNA databases) and private (PNR or financial data such as SWIFT data) databases do law enforcement agencies have access?*

First, the law enforcement authorities have access to **Identification Registers** ("erkennungsdienstliche Evidenz"). According to Art. 65 SPA (Erkennungsdienstliche Behandlung, identification measures) the compilation of identity data of suspects is permitted, if the crime is committed in the framework of a criminal association ("kriminelle Verbindung", three or more people collaborating with the intent to continue to commit punishable acts) or the measure is necessary for hindering further criminal attacks (Art. 65 par 1 SPA) regarding the type of the crime or the way of committing the crime or the personality of the suspect. The Central Identification Register ("Zentrale erkennungsdienstliche Evidenz", section 75 SPA) is a database that is conducted by the police authorities containing also fingerprint data and DNA-data both personal-related and DNA-data related to unknown subjects ("offene Spuren"). Besides there is the Criminal Police File Index ("Kriminalpolizeilicher Aktenindex", KPA) according to section 57 par 1 fig 6 SPA and the "Criminal Record" ("Strafregister") according to the Act on Criminal Record ("Strafregistergesetz") which is led by the Federal Police Headquarters Vienna ("Bundespolizeidirektion Wien"). These data bases only contain specific data of suspects and perpetrators for security police and criminal police purposes.

Furthermore, the police authorities have access to all **other public databases** such as the Central Population Register ("Zentrales Melderegister") of the municipality, the Central Vehicle Register ("Zentrales KFZ-Register") according to section 47 Act on Vehicles ("Kraftfahrgesetz") or the Land Register ("Grundbuch") and the Commercial Register ("Firmenbuch"). As far as a database is concerned that is not conducted by the police authorities, access to these contents has to fulfil the requirements of compilation of data according to section 53 SPA.

Data which has been **compiled by private persons** (e.g. SWIFT-Codes, PNR-data) is admissible through the measures of seizure and confiscation (Art. 110 CCP). A data seizure and confiscation is only legally allowed for the clearing of a concrete crime but not for preventive purposes such as building information positions. A direct access to these private databases by the law enforcement authorities without the requirements of Art. 110 CCP is not admissible.

3) *Can techniques labelled as data mining and data matching be applied? If so, can these techniques be used to create profiles of potential perpetrators or risk groups? If so, have special tools been developed for law enforcement agencies?*

Data mining ("Automationsunterstützter Datenabgleich") is admissible, if there is a simple suspicion regarding a crime (Art. 17 CC) and the clarification of this crime otherwise will be significantly hindered (small data mining operations). In this case only certain data compiled in criminal proceedings or for other public purposes may be included. In cases of a suspicion of a crime for which a custodial sentence of more than 10 years or of a crime committed in the framework of a criminal or terrorist organisation (large data mining operations) is stipulated, it is allowed to include a wider range of governmental data and private data (Art. 141 CCP). Art. 141 par 4 CCP stipulates that certain sensitive data, like data relating to natural persons concerning their racial or ethnic origin, political opinion, religious beliefs and health or sex life, must not be included in any data mining operation.

According to Art. 143 par 1 CCP, each contracting entity ("Auftraggeber") of a data application, whose data shall be included in a data mining process, is obliged to search the data application for the relevant criteria and to communicate all data, which contain those criteria. According to Art. 142 par 1 CCP, the Public Prosecutor shall order a data mining operation on the basis of a court authorisation.

The **operational criminal analysis** that is based on Art. **53a SPA** can also be counted to a type of data mining. This measure is admissible without judicial control.

Apart from these special provisions data mining operations are not admissible as far as data from different sources shall be included. Searching for special data (data-matching) within the different files of the electronic file system of the police ("PAD") by entering the name and the date of birth of a person is illicit (Art. 13 par 2 SPA). Although this restriction will be dispensed on January 1st 2014 searching for special data in the entire PAD-database will not be allowed after this date either, as the separation of criminal police data and other data has to be observed (see Art. 13a SPA, coming into effect on 1st January 2014).

Above all the **principles of the Act on the Protection of Personal Data** (Datenschutzgesetz) every retention and processing of personal data, such as the

processing for analysing purposes, has to be carried out on a legal basis. This also applies to the transmission of data between different contracting entities ("Auftraggeber") and between different tasks of the same entity.

Therefore there is **no general admissibility of data mining and data matching** processes that exceed the special measures mentioned before as far as data from different sources is to be included. The systematic search within the data in single file is not subject to any restrictions. For this purpose law enforcement authorities (Police, Public Prosecution Service, the Court) can use any possible techniques and IT-applications.

4) *Can coercive measures (e.g. interception of telecommunications) be used for building up information positions?*

For preventive purposes **in the framework of the extended potential danger identification** (Art. 21 par 3 SPA) the optical and acoustic surveillance (Art. 21 par 3 and Art. 54 par 4 SPA), observations (Art. 54 par 2 SPA) and undercover investigations (Art. 54 par 3 SPA) are admissible. In this precautionary stage of investigations no other coercive measures such as the investigation of telecommunication traffic data or the interception of telecommunication are permitted (except for the investigation of master data ("Stammdaten") according to Art. 53 par 3a fig 1 SPA).

As far as the preventive **fight against criminal associations** ("kriminelle Verbindung") is concerned, IT-traffic data (IP address, corresponding name and address to a dynamic IP address) can be requested from telecommunication companies and internet providers (Art. 53 par 3a fig 2 and 3 SPA).

If **criminal investigations against criminal and terrorist organizations** are considered to have a preventive effect (see question B. 1), the investigation measures of Art. 136 and 141 (optical and acoustic surveillance and data mining, both based on the CCP) are to be mentioned.

5) *Which private actors (e.g. internet providers or telecom companies) retain or are obliged to retain information for law enforcement agencies?*

As mentioned before (question A. 3) **providers of public communication services** according to Art. 92 par 3 fig 1 Act on Telecommunication ("Telekommunikationsgesetz") are **obliged to provide information about data of a message transmission** (traffic data) that has been retained for billing purposes (Art. 134 fig 2 CCP) or according to the data retention obligations based on the data retention directive (Art. 134 fig 2a CCP). The providers also have to cooperate in the **surveillance of messages** (content data). This measure shall be

ordered by the Public Prosecution Service based on a court authorization. Moreover, providers of communication services are obliged to comply with requests of the criminal police, the public prosecution service or the courts on standing data (Art. 76a par 1 CCP) and name and address corresponding to a dynamic IP address and other e-mail-related data (Art. 76a par 2 CCP). IT- and telecommunication data has also to be provided to the security police for preventive purposes (Art. 53 3a and 3b SPA).

The **obligation of the providers to retain** this data can be found in the Art. 90 par 7, 99 par 2 and 5 and 102a fig 2 -4 Act on Telecommunication. These obligations of retention or authorization of data processing affect both telecommunication and internet data.

Credit or financial institutes are obliged to provide information about banking accounts and banking transactions. Nevertheless there are no specific duties of data retention as the data on accounts and transactions is retained anyway for other purposes.

Besides these special provisions **every private person** is bound to comply with requests of law enforcement authorities (seizure, Art. 110 CCP). This obligation does not apply to the same extent to persons holding a professional privilege (see Art. 112 CCP).

6) *Which private actors can provide or are obliged to provide information to law enforcement agencies?*

Telecommunication companies, IT-providers and credit and financial institutes were already mentioned before (see Question 5.)
Besides these private actors **every private person** can provide information to the law enforcement agencies, such as pictures and videos. According to Art. 53 par 5 SPA the security police are allowed to process private video material, that is provided by private actors, for preventive and tracking and tracing purposes.

Furthermore, every person who has in his/her disposing power **objects or property items** that are to be seized, is obliged to release them, when requested so by the criminal police or the Public Prosecution Service, or to facilitate the seizure in any other way (**Art. 110 CCP**). Although Art. 110 primarily deals with the seizure of objects it is also applicable on the seizure of IT-related evidence and data. This derives from Art. 112 and 115 CCP: They say that data on a storage medium may be seized, confiscated and evaluated.

7) Is there judicial control on building information positions?

As the investigations and data processing is based on the SPA there is no judicial control. Most of these measures are controlled by the independent **Legal Protection Attorney in the Federal Ministry of the Interior** ("Rechtsschutzbeauftragter beim Bundesministerium für Inneres"). The Legal Protection Attorney is not bound by any directions and subject to observe official secrecy in the exercise of his tasks arising from the SPA. There are three different modes of supervision by the Legal Protection Attorney:

1. Investigation measures in the framework of the extended potential danger identification ("erweiterte Gefahrenerforschung", Art. 21 par 3 SPA) have to **be authorized** in advance. Therefore, Security authorities faced with a task arising from Art. 21 par 3 SPA, prior to the performance of such a task, shall obtain authorization from the Legal Protection Attorney. The same shall apply, if it is intended to take special compiling measures such as optical or acoustic surveillance (Art. 54 par 6 SPA) within the framework of extended potential danger identification.
2. Security authorities intending to put public places under long-term surveillance by means of image and sound recording devices under Art. 54 par 6 and 7 SPA, the implementation of a criminal analysis database (Art. 53a SPA) or the compilation of data for the analysis and evaluation of the probability of dangers of constitutional institutions (Art. 53 par 1 fig 7) shall inform the Legal Protection Attorney who has the **opportunity to comment** thereon within three days.
3. Security authorities shall **notify** the Legal Protection Attorney of any compiling of personal data by requests on telecommunication traffic data (Art. 53 par 3a), by undercover investigations (Art. 54 par 3), by undercover use of image or sound recording devices (Art. 54 par 4) or processing of data compiled and transmitted by others using image and sound recording devices (Art. 53 par 5 SPA) stating the essential reasons for the compiling.

If the Legal Protection Attorney notices any illicit secret investigation measure or data compilation he has to inform the person concerned or – if this is not possible – appeal to the Data Protection Commission ("Datenschutzkommission") instead of the person concerned. The Data Protection Commission decides on the legality of the data compiling.

C. ICT in the criminal investigation

1) Can law enforcement agencies carry out interception real time of a) e-traffic data; b) content data?

a) E-Traffic Data

To carry out monitoring of telecommunication traffic data (Art. 134 fig 2 CCP) the law enforcement agencies have to involve telecommunication providers. Data retained for billing or technical purposes or due to the data retention obligation (Art. 134 fig 2a CCP) have to be transmitted to law enforcement agencies if the

preconditions of Art. 135 par 2 CCP are fulfilled. Even though in most cases the law enforcement authorities receive retained data, real-time-interception of traffic data (especially location data) is admissible as well.

b) Content Data

As far as content data is concerned both real-time interception and retention of the content data and following transmission is admissible (see Art. 134 fig 3 CCP). In practice – just as for traffic data monitoring – telecom providers are involved. The law enforcement agencies use to request the interception and the companies addressed are obliged to cooperate (Art. 138 par 2 CCP). There is a question in dispute, whether the law enforcement authorities are *obliged* to involve telecommunication companies or may carry out content data interceptions on their own. The wording of Art. 134 fig 3 CCP seems to allow an interception without involving telecom companies, whereas the historic background of the provision seems to contradict this interpretation.

2) *Can law enforcement agencies have access to/freeze/search/seize information systems for a) e-traffic data; b) content data?*

As mentioned before law enforcement authorities, according to the wording of Art. 134 fig 3 CCP, are allowed to freeze, search and seize **content data** by surveillance of messages. An interception of content data in the framework of the SPA is not admissible.

As far as **traffic data** is concerned, the telecommunication companies and internet providers are obliged to cooperate and comply with the requests of law enforcement authorities. This applies to criminal investigations (CCP) and the security police measures (SPA).

According to Art. 110 seq CCP it is permitted for law enforcement authorities to **search and seize information systems** (hard disks, data media) for content and traffic data. For example, a mobile phone can be seized by the police according to Art. 110 CCP and searched for the numbers dialled or the content of messages which have been sent or received. Art 110 CCP, however, does not allow the access to messages that are stored on the voice mailbox.

For the **digital access to computers** in order to search for saved data, and for the continuously digital monitoring of the use of a computer, **rules in Austria are still missing**. However, the Vienne Regional Criminal Court regarded it as allowed for the purposes of evidence that the police clandestinely installed a special software on a computer of a suspect, which transferred screenshots and key log data to the law enforcement authorities. The Court applied the rules on the surveillance of the content of telecommunication (Art. 134 fig 3 CCP) and on optical and acoustic surveillance (Art. 134 fig 4 CCP) to these investigative measures. The admissibility of such investigative measures without an explicit provision in the CCP is a question of intensive dispute within the doctrine.

3) Can telecom companies or service providers be obliged to share data with law enforcement agencies? In case of non-compliance, are there any coercive measures or sanctions?

Telecom Companies and internet providers are **obliged to comply** with the requests of law enforcement authorities according to CCP and SPA. They have to transfer retained traffic data and cooperate in the interception of telecommunication data (see questions B. 6). The obligation to cooperate arises from Art. 138 par 2 CCP. For data mining processes according to Art. 141 CCP the obligation arises from Art. 143 CCP.

Within the CCP these obligations are confirmed by coercive measures and sanctions. If the telecom company concerned refuses to comply with the requests of the law enforcement authorities a penalty of € 10.000 or not more than six weeks of imprisonment is provided (Art. 93 par 4 CCP).

As security police measures are concerned telecom companies and service providers are obliged to cooperate either, though there are no specific coercive measures or sanctions for the case of illicit non-compliance.

4) May law enforcement agencies apply video surveillance? Can they oblige natural or legal persons to cooperate?

The application of video surveillance is covered both by the **CCP** (criminal police) and the **SPA** (security police).

The definition **of video surveillance** within criminal investigations can be found in Art. 134 fig 4 CCP. This article contains the application of image and sound recording devices. The optical and acoustic surveillance of persons is the surveillance of the behavior and statements of persons by the use of technical means for the transmission of pictures or sound and for picture or sound recording. Art 136 CCP differentiates between

a) optical and acoustic surveillance in the case of **kidnapping** (Art. 136 par 1 fig 1 CCP)

b) **small bugging operations** ("Kleiner Lauschangriff", Art. 136 par 1 fig 2 CCP), where an undercover agent conducts the surveillance or where at least one of the dialogue partners is informed of the surveillance. In this case a general and simple suspicion regarding a crime ("Verbrechen", According to Art. 17 CC "Verbrechen" is defined as an offence for which imprisonment of more than three years is stipulated).

c) **large bugging operations** ("Großer Lauschangriff", Art. 136 par 1 fig 3 CCP) without knowledge of the involved parties require a person who is strongly suspected to have committed a crime, for which imprisonment of more than 10 years is stipulated, the crime "criminal organization" (Art. 278a CC, membership or founding of such an organization) the crime "terrorist organization" (Art. 278b CC membership or leading of such an organization) or a crime within the framework of a criminal or terrorist organization.

d) **visual surveillances** ("Spähangriff", Art. 136 par 1 3 CCP). The surveillance is only visual and is restricted to processes outside of a home, a simple suspicion that any punishable act – regardless of the threatened punishment – has been committed is sufficient. If it is performed in a dwelling, an intentional punishable act, for which imprisonment of more than one year is provided for, is required. For this purpose it is admissible to enter a certain dwelling if the accused person is likely to stay in the rooms in future (Art. 136 par 2 CCP). This entering needs a separate authorization by the Court (Art. 137 par 1 CCP).

Moreover, the application of tracking devices is admissible in the framework of an **Observation** (Art. 130 par 2 CCP).

In the framework of the CCP every image data compiled by private persons can be **seized, confiscated** (Articles 110 and 115 CCP) and used in trial as evidence by the investigation authorities. Privates, though, are not obliged by rules of criminal or security police law to use recording devices or retain data. They only have to provide data that is already available.

According to **Art. 54 par 4 SPA** the security police are allowed to use image and sound recording devices for the aversion of dangerous attacks or combating criminal associations and for purposes of extended potential danger identification (Art. 21 par 3 SPA). In this case it shall be inadmissible to compile personal data with sound recording devices to record non-public statements made in the absence of a person compiling or with image recording devices to record non-public conduct not taking place in the scope of perception of the person compiling. The Legal Protection Attorney has to be notified with this surveillance measures.

If, based on certain facts, in particular due to previous dangerous attacks, it is to be feared that in **public places** dangerous attacks against life, health or property of people will occur, security authorities, to prevent such attacks, may compile personal data of people present with image or sound recording devices (**Art. 54 par 6 SPA**). However, they shall announce this in advance in such a way that it becomes known to a circle of persons potentially concerned as wide as possible. Data compiled in such manner may also be processed for purposes of the aversion and clarification of dangerous attacks occurring in these public places, as well as for

purposes of the search for wanted or missing persons. If these records are not required for further prosecution based on suspected punishable acts they shall be deleted not later than after 48 hours.

According to **Art. 53 par 5 SPA** for purposes of averting dangerous attacks and combating criminal associations, if certain facts imply severe danger to public security, for purposes of extended potential danger identification (Art. 21 par 3 SPA) and for purposes of searching for wanted or missing persons, security authorities shall be empowered to use personal image data which were lawfully compiled by legal entities of the public and private sector using image and sound recording devices and were transmitted by them to security authorities.

5) May or must law enforcement agencies apply audio-visual recording of interrogations (suspects, witnesses)?

Audio-visual recording of interrogations is **admissible** (Art. 97 par 1 CCP) and used in practice very often. Nevertheless, the recording is not obligatory. This applies to interrogations conducted by the criminal police as well as for those conducted by the Public Prosecutor or by the Court, both for interrogations of suspects and witnesses. If recording devices are applied the statement has to be recorded completely. Witnesses may object to recording their interrogation.

D. ICT and evidence

1) Are there any rules on evidence that are specific for ICT-related information?
2) Are there any rules on integrity (e.g. tampering with or improper processing) and security (e.g. hacking) of ICT-related evidence?

In general, **Art. 74 par 2 CCP** covers the **handling of personal data** concerning both IT and ICT data and conventional personal data. According to Art. 74 par 2 the criminal police, the Public Prosecution Service and the Court have to comply with the principle of proportionality and – as far as sensitive categories of data or criminal law-related data is concerned – make provisions to preserve the interest of confidentiality of the person concerned. Art. 75 CCP provides the data protection principle of obligatory correction or erasure of inaccurate personal data or data compiled unlawfully. Moreover Art. 75 par 2, 3 and 4 CCP provide deadlines for the erasure of specific categories of data. According to Art. 75 par 5 data that has been compiled through interception of telecommunication content data, by optical or acoustic surveillance or by data mining processes may be introduced and used in a civil law or administrative law proceeding connected to the actual criminal law proceeding or for the aversion of serious attacks (Art. 17 SPA).

The handling of IT-related evidence which has been compiled by large bugging operations ("großer Lauschangriff", Art. 136 par 1 fig 3 CCP) and data mining processes ("automationsunterstützter Datenabgleich, Art. 141 CCP) within the police authorities is regulated in a **general direction issued by the Federal Minister of the Interior** ("Geheimschutzordnung", see Art. 55c SPA). This direction contains a general code of conduct for handling information gained by such surveillance measures, in particular, relating to their copying and saving as well as measures to guarantee, that any access to such information is recorded. The direction, for example, stipulates that the personal data has to be kept secret and appropriate security measures (according to Art. 14 Act on Data Protection) have to be taken. The access to this data shall be reserved to the number of persons necessary to fulfil the tasks. This direction is not open to public.

As for the handling of IT-related data arising from large bugging operations ("großer Lauschangriff", Art. 136 par 1 fig 3 CCP) by the Public Prosecution Service and the Court, there is an **ordinance issued by the Federal Ministry of Justice** ("Verschlusssachenordnung für die Durchführung einer optischen oder akustischen Überwachung", BGBl II 256/1998). This direction contains rules on the access to this data, the saving and the transmission of such categories of IT-related data.

Apart from these special provisions, the **general data security principles of Art. 14 Data Protection Act** are to be considered. According to Art. 14 DPA the law enforcement authorities as contracting entities ("Auftraggeber") have to make provisions to maintain data security.

Besides these provisions, there may be further **internal directives** on the handling of IT-related evidence that are not open to the scientific public.

3) Are there any rules on admissibility (incl. the principle of procedural legality) of evidence that are specific for ICT-related information?

There are **no specific rules** on admissibility of *ICT-related* evidence. According to Art. 74 par 1 the principles of the Data Protection Act apply to the criminal law proceedings and Art. 75 par 1 CCP provides that inaccurate or unlawfully compiled personal data has to be erased. These rules apply to both IT-related and conventional personal data. Above all, the entire criminal procedure is based on the principle of procedural legality. The criminal police, the Public Prosecution Service and the Courts shall only interfere in personal rights if there is a sufficient and explicit legal permission. The interference must not be more invasive than necessary to fulfil the task. Therefore, interferences in the right on data protection (Art. 1 Data protection Act) for purposes of criminal investigations have to be based on an explicit provision in the CCP (Art. 5 CCP). That's why most members of the doctrine deny the admissibility of online access to computers (see question C. 2).

According to Art. 140 par 1 fig 1 CCP the results of traffic or content data monitoring and optical or acoustic surveillance (see Art. 134 fig 5 CCP) may only be used in the criminal proceeding if the investigative measure was legally ordered by the Public Prosecution Service and authorized by the Court. The results may also be used in other judicial or administrative proceedings as evidence if their introduction into the criminal proceeding was (or would be) admissible (Art. 140 par 3 CCP).

As far as the **security police** are concerned Art. 28a par 2 SPA stipulates that any interference in personal rights has to aim at fulfilling a special task of security police and using a special permission that is admissible for this special task.

4) Are there any specific rules on discovery and disclosure for ICT-related evidence?

Each accused person has the right **of access to the files** ("Akteneinsicht", Art. 51 CCP). This right includes all evidences available to the criminal police, the Public Prosecutor or the Court. If the evidence contains the identity or personal circumstances of somebody who could be endangered by the inspection of files, it is admissible to provide partly censored files to the accused (Art. 51 par 2 CCP). Further restrictions of the access to the files at the investigation stage are allowed to maintain the investigation purpose. The inspection of the records can be permitted – as far as technically possible – by using a display screen or through electronic data transmission (Art. 53 par 2 CCP).

Art. 145 par 2 CCP provides, that the orders and permissions of certain investigation measures (among them: monitoring of telecommunication data, optical and acoustic surveillance and data mining), the authorizations by Court and the results have to be **kept separated** from the remaining file until the order becomes legally valid.

The accused person has the right to **receive copies** at his/her cost (Art. 52 CCP). Until 13.12.2012 the accused person had no right to receive copies of image and sound recordings. This evidence could only be inspected at the Court. The Constitutional Court of Austria ("Verfassungsgerichtshof", VfGH) abolished this restriction in Art. 52 CCP as it did not comply with the Austrian constitution (Decision G 137/11 from Dec 13th 2012).

The publication of information obtained through an inspection of files containing personal data of other persons that has not been introduced in a public trial or been otherwise disclosed to the public is forbidden, if this would effect a violation of predominant justified interests of confidentiality of others (Art. 54 CCP).

Besides these general provisions, **Art. 139 CCP** provides the accused person's right to examine the results of ICT-related investigation measures defined in Art. 134 fig 1-3 CCP (Art. 134 fig 5 CCP). Parts of the files can be censored by the Public Prosecution Service if necessary to protect the rights of other persons.

5) Are there any special rules for evaluating (probative value) ICT-related evidence?

There are **no special rules** for evaluating ICT-related evidence. The general principle of free appraisal of evidence is also applicable on ICT-related evidence: According to Art. 14 CCP the Court shall, on the basis of the available evidence, decide in its free opinion whether the relevant facts are considered proven. In case of doubt the Court always has to decide in favour of the accused or other persons concerned. This provision is applicable on both IT-related evidence and conventional evidence.

E. ICT in the trial stage

1) How can or must ICT-related evidence be introduced in the trial?

According to the **principle of immediacy** (**Art. 258 par 1 CCP**) ICT-related evidence, just as conventional evidence, has to be introduced in the trial hearing ("Hauptverhandlung", Art. 246 par 1 CCP). Audio-visual recordings and audio tapes are played during the trial, written reports, such as written results of an interception of telecommunication and optical or acoustic surveillance (Art. 134 fig 5 CCP) have to be read in the trial or presented by the presiding judge.
Audio-visual recordings or protocols of interrogations of other accused persons or witnesses shall only be introduced under special conditions: According to Art. 252 par 1 CCP they shall be played or read if the

- interviewed person is not available anymore (She died, her residence is unknown, her personal appearance is not possible due to important reasons),
- if the statement of the person questioned in the trial differs from his statement in the investigations in essential points;
- if the witness legitimately refuses to give evidence and the Public Prosecutor and the accused person had the opportunity to take part in the interrogation by the Court during the investigations (adversarial interrogation);
- if the witness refuses to testify without being entitled to do so,
- if the accused person and the Public Prosecutor agree to the reading of the protocol or the introduction of the tape.

Protocols and audio-visual tapes of former interrogations of the accused may be read or played in trial, if the accused does not want to make a statement in the trial hearing or if his statement differs from former statements (Art. 245 CCP).

2) *Can distant interrogations (e.g. by satellite connections) be applied?*

Art. 247a CCP provides, that witnesses, whose personal appearance in court is not possible due to their age, an illness, frailty or other important grounds, may be interrogated by **video conference**.

Moreover, if the residence of witnesses or accused persons is situated outside the district of the competent Public Prosecution Service or the Court they may be interrogated by video conference at the Public Prosecution Service or the Court of their residence. In this case the Public Prosecutor and the defence-counsel have to agree to this form of interrogation (Art. 247a CCP and Art. 153 par 4 CCP).

Furthermore, an interrogation by video-conference is admissible for witnesses who stay abroad if the state concerned provides legal assistance upon request (Art. 247a par 2 CCP). According to Art. 10 of the "Convention established by the Council in accordance with Art. 34 of the Treaty on the European Union, on Mutual Assistance in Criminal Matters between the Member States of The European Union" this form of legal assistance should be possible in every member state of the European Union.

3) *Can digital and virtual techniques be used for the reconstruction of events (killings, traffic accidents)?*

Art. 149 CCP provides the **reconstruction of punishable acts** ("Tatrekonstruktion"): The probable circumstances of an offence may be re-enacted at the scene of crime or another place connected to the punishable act and recorded by audio and visual recording devices. This form of evidence has to be introduced in the trial as well (see question E. 2). Art. 150 CCP provides the special procedure of the reconstruction.
Besides this provision there are no restrictions for the Public Prosecution Service and the defence-counsel in applying video and IT-techniques for the presentation of evidence at the trial hearing.

4) Can audio-visual techniques be used to present evidence at trial (in its simplest form: pictures and sound)?

Audio-visual recordings must be introduced into the trial by using audio-visual displays (see question E. 2). Beside these recordings, the application of audio-visual techniques within the trial hearing is no subject to restrictions as long as the

conditions of Art. 246 CCP are maintained: In recent cases of extensive economic offences, for example, including a large number of accused persons and other parties video techniques are used. In a spectacular case in the city of Klagenfurt, video-beamer, document cameras and widescreen displays were used to show documents to the accused person or – generally spoken – present evidence at trial. By using a video switch the judge could decide whether the accused was able to see the screen or not. Moreover, an audio and video broadcast of the entire proceeding to an assembly hall next to the courtroom was provided, in order to enable a larger number of persons to participate in the trial. This very special trial proves that using audio visual devices aiming to support acts of procedure that are legally admissible, is not bound to restrictions. The possibility of using the techniques is just a question of logistics and technical and financial capabilities.

5) Can criminal "paper" case files be replaced by "electronic ones"? Are there any developments towards digitalising of the trial proceedings?

The **police authorities** have already replaced the "paper" case files by **electronic files**. According to **Art. 13 par 2 SPA** they are authorised to use computer-assisted data processing in performing tasks conferred by law for the documentation of official acts and administration of official files. For such purposes, they may use data on natural or legal persons as well as objects to which the procedure to be documented is related, such as, in particular, date, time and place, vehicle data, reference and file number, including processing and filing remarks, as well as names, role of the person concerned, sex, previous names, aliases, nationality, date of birth, place of birth, residential address and other data serving to reach the person concerned. If required, also sensitive data (Art. 4 fig 2 of the Data Protection Act) and data as defined in Art. 8 par 4 of the Data Protection Act shall be used. Selection of data from the total amount of data stored only according to name and sensitive data shall be excluded, for selection another date relating to the facts documented has to be entered instead. The technical application is called **"PAD"** ("Polizeiliches Aktenprotokollierungs- und Dokumentationssystem"). In this application security police acts and criminal police acts as well as every administrative law act conducted by the police authorities is processed.

Whereas the police already use electronic files the **judicial authorities** (Court, Public Prosecution service) still use **paper case files**, though it is admissible to add data media to the file. A specific applicable legal authorization of data processing for the Austrian judicial authorities, such as Art. 13 par 2 SPA for the police authorities, does not exist yet. Nevertheless, the **trend** within the Austrian criminal Justice system – as for other areas of the Austrian Administration ("Elektronischer Akt – "ELAK", electronic file) – seems to go to the **implementation of electronic files** (compare the electronic legal relations according to Art. 89a Act on the Organization of Courts, E-Government). For example, the Austrian Constitutional Court – as the first Court in Austria – has recently replaced the paper case files by electronic files.

This development also becomes apparent, for example, regarding the implementation of a special department in the Federal Ministry of Justice (Department 5 of the presidential section called “Legal data processing/E-Justice”) responsible for the application of IT and ICT within the Austrian Justice System. The “VJ” (“Verfahrensautomation Justiz”, Automatisation Procedure Justice; Art. 80 Act on Organization of Courts [“Gerichtsorganisationsgesetz”]), run by the “Bundesrechenzentrum” (Federal Computer Centre Ltd.) as a special tool is applied to register all forms of judicial procedure. Nevertheless, the criminal files are not run entirely electronically at Court. The paper files are still necessary.

There are reports of the Austrian Court of Audit (“Österreichischer Rechnungshof”, ACA) recommending the reorganization and digitalization of the case file system within the Austrian Justice System. A short term change of the status quo seems to be unlikely due to organizational and financial reasons.

Dr. Farsam Salimi
Institute of Criminal Law and Criminology, University of Vienna
farsam.salimi@univie.ac.at