Preparatory Colloquium
24 – 27 September 2013, Antalya (Turkey)
Section III: Information Society and Penal Law

TURKISH NATIONAL REPORT*

Serap Keskin KIZIROĞLU* / Fulya EROĞLU / İlker TEPE*****

(B). 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 the criminal process?

There are no specific definitions for applications of IT and ICT within the Turkish Criminal Code (TCC) or the Criminal Procedure Code (CPC). However, the motives of art. 243 CPC regulating the crime of "illegally accessing an information system" defines the term "information system" as follows:

"Information system means any magnetic system that collects and arranges data and then puts them through automatic processing."

Art. 2 of the Law on Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting provides the following definitions:

Information: any meaningful form of data

Access: Obtaining the possibility of using an Internet medium through a connection.

Access provider: Any real or legal person who provides to access to the Internet for its users.

Content provider: Any real or a legal person, who produces, changes or provides any kind of information or data, which are provided to users over the Internet

Internet medium: The medium that is established on the Internet, and that is publicly accessible except communication and personal or corporate computer systems.

Internet broadcasting: Online data accessible by an indefinite number of persons.

Tracking: Monitoring information and data without affecting data on the Internet.

Institution: Telecommunication Institution

Public use provider: Any person, who provides facility to use the Internet for people in a specific place and in a specific time

Traffic data: The values about every kind of access to the Internet, such as parties, time, duration, the kind of the utilized service, the amount of the data which is transferred and access points.

Data: Any kind of values that can be processed by a computer

Broadcasting: Broadcasting on the Internet

Hosting provider: a real or a legal person who provides or operates a system containing services and content.

Art. 3 of the Regulation on the Utilization of Audio-visual Information Technology Systems in Criminal Procedure further provides the following definitions:

Information System: Any system consisting of a computer, peripherals, information infrastructure and programs, and that designated to process, to store and to transfer data.

SEGBIS: The Audio-Visual Information System that electronically transfers, records and stores sounds and images simultaneously.

---

* 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.

* Prof. Dr. Serap Keskin Kiziroğlu. Istanbul Okan University Law Faculty, Department of Criminal Law and Criminal Procedure Law.
** Ar. Gör. Fulya Eroğlu. Yeditepe University Law Faculty, Department of Criminal Law and Criminal Procedure Law.
*** Ar. Gör. İlker Tepe. Dokuz Eylül University Law Faculty, Department of Criminal Law and Criminal Procedure Law.

UYAP IT-System: The information system that is formed with purpose of enforcing justice services electronically.

The Regulation on the Application of the Measures Regarding the Interception of Communications, Undercover Agents and Technical Surveillance[1] provides the following definitions involving ICT (art. 4):

Wiretapping / Interception of communication: The proceedings for tapping conversations on telecommunications and tapping all sorts of communication by applicable tools.

Detection of communication: The proceedings for gathering information about calling, location and identification from the communication between communication tools, without interfering with the content of communication.

Operator: Companies operating telecommunication services and telecommunication substructure following a task-order contract, a franchise agreement, a telecommunication licence issued by this Institution or a general permit,

Signalling Information: Any kind of data that are processed for the purpose of communication transmission within a network or in order to invoice.

Evaluating signalling information: Any act of evaluation employed for determining the traces on communication systems, which are made by signalling information, and obtaining meaningful results from these traces, without interfering with the content of communication and based on a warrant by the competent authority.

Telecommunication: Transferring, sending and receiving signs, symbols, sounds, images and any kind of data that can be transformed to electrical signals; through cables, wireless, optical, electrical, magnetic, electromagnetic, electrochemical, electromechanical and other transferring systems.

Technical surveillance: Technical surveillance, audio or video recording of the suspect's or the defendant's actions in public places or in his/her working place; within the scope of an investigation regarding a crime listed under Criminal Procedure Code (CPC) art. 140/1, in cases of a high degree of suspicion and in the absence of possibility to obtain evidence by other means.

Data carrier: Instruments that are employed to record sounds and images, which are obtained through "interception of communication", "undercover investigation" and "technical surveillance" measures.

The Turkish Court of Cassation is known to adopt the definition as found under the motives of the law[2]:

"*Information system means, magnetic systems that collect and locate data and then provide the possibility to process them automatically*, *... (Turkish Court of Cassation, 11th Criminal Chamber, 23.03.2009, E: 2008/16004 - K. 2009/2891)"*

"*Information system means, magnetic systems that collect and locate data and then provide the possibility to process them automatically. Cyberspace means a space consisting of systems that store and later automatically process information (…)" (Turkish Court of Cassation, General Assembly of Criminal Chambers, 17.11.2009, E: 2009/11- 193 – K: 2009/268)*

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

Information and Communications Technologies Authority (ICTA): The Telecommunications Institution, which had been established by the Law 4502, dated 27.01.2000, has been renamed as the ICTA after the entry into force of the Electronic Communications Law (Law 5809, dated 10.11.2008), and has been designed to regulate and supervise the telecommunications sector as an independent administrative authority. With the new regulation, the Wireless Law (Law 2813) has been renamed "Law on the Establishment of the Information and Communications Technologies Authority".

Telecommunications Communication Presidency (TCP): This presidency has been established through Law 5397, dated 23.07.2005, and is operating under the relevant legislation as a central authority.

The presidency has been designed by the Law on the Regulation of Internet Publishing and on Combatting Crimes committed Through Such Publications (Law 5651) to function in the area of Internet publishing, and has powers to execute orders on banning websites issued by legal authorities, or, in some cases, to issue such orders *ex officio*. The Internet Bureau has been established to deal with such tasks.

The TCP operates under the direct authority of the President of the ICTA, and consists of Bureaus of Law, Technical Operations, Information Systems, Administration and the Internet Bureau. Each of the National Intelligence Organisation, the Turkish National Police Organisation, and the General Command of Gendarmerie send one representative to the TCP.

The Information Technologies Department of the Ministry of Justice: The Ministry has begun the automatizing process in

[1] A stay of execution order has been issued regarding this Regulation by the General Assembly of Administrative Chambers of the High Administrative Court (YD Appeal Nr. 2012/578, dated 06.12.2012

[2] Dr. Ihsan Baştürk, public prosecutor at the Turkish Court of Cassation, and member of the Turkish Association of Penal Law, has made the following statement, which we support: Under Turkish law, terms such as "Internet", "Internet medium", "web page", "website", "publication", "Internet Service Provider", and "access provider" are being used without any coherence, which causes problems. Additionally, the fact that some terms that are not included in legislation can be found in by-laws. An example for this is the term "other distant computer logs and removable hardware", which cannot be found under art. 134 CPC on the seizure of computer logs, but is regulated under the "Regulation on Judicial and Preventive Searches". As a result, different courts apply the same provisions differently.

1998. In 1999, the Information Technologies Department has been established in order to regulate and systemize the process. Art. 22/A of the Law 2992 as amended by the art. 7 of the Law 4674 dated 15.05.2001 determines the area of practice of the Information Technologies Department.

Other institutions under the Turkish system include:

Department of Combatting Cybercrime at the Turkish National Police Organisation: The Department has been established through the Decree nr. 2011/2025 of the Council of Ministers, in order to investigate crimes committed using IT, and to examine digital evidence. The department is centralized in order to overcome issues of coordination and to avoid repeated investments. Provincial agencies of the Department are in the process of being established quickly.

The IT Investigations Laboratory of the Gendarmerie Criminal Department: Creates expertise reports and affidavits for administrative and legal investigations and prosecutions regarding the scientific evaluation of evidence provided by the judge, court, or, in cases of emergency, by the prosecutor.

The Physical Expertise Department of the Institution of Forensic Medicine: The department deals with the scientific evaluation of physical material provided by courts, judges and prosecutors, such as weapons, ballistics, graphology, dactyloscopy, fotography, pictures, fingerprints used as autographs, radiology, radioisotopes, climatology, and, in addition, digital evidence, and creates expertise reports and affidavits.

The physical expertise department has a "Branch of Information and Technology Crimes", dealing with digital evidence.

(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?

There aren't any organisations that offer ICT related services to the criminal justice system in Turkey. However, it is possible to resort to the expertise of real persons or legal entities under the CPC.

(C) Information and Intelligence: building information positions for law enforcement

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

There are measures of interception of communication, technical surveillance, seizure of data carriers, obtaining data such as fingerprints, palm prints, photographs within the scope of physical identification. Data, obtained by these measures are stored in related databases.

Within this context, additional art. 7 of the Law on Duties and Powers of Police (LDPP) and additional art. 5 of the Law on the Organisation, Duties and Powers of the Gendarmerie (LODPG) regulate that law enforcement agencies may use measures of "interception of communications" and "technical surveillance", while performing intelligence services, in order to prevent the offences which are listed under art. 10 of the Law on Combatting Terrorism (LCT), except for espionage crimes. Art. 6 of the Law on State Intelligence Services and the National Intelligence Organisation regulates that measures of "interception of communications" and "technical surveillance" may be used in order to maintain State security, to uncover espionage activities, to spot activities regarding the revealing of state secrets and to prevent terrorist activities, in the case of serious danger against the essential features of the Turkish Republic as declared under Turkish Constitution or against the rule of law.

Also these techniques are used for building information positions in Turkey: taking image, reclamation of the files, which are deleted, composing word lists, examining registry, examining metadata.

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

According to art. 332 CPC, public prosecutors, judges and courts can request every kind of information from any institution. During investigation and prosecution of a crime, when a public prosecutor, judge or court sends a written request about any information, it has to be responded within ten days. If it is impossible to respond within this time, the reason of the delay and the latest date for the retrieval of the information must be notified within the same time (ten days).

According to Turkish Criminal Law, there is no specific law in force concerning the protection of personal data. There is a draft law called "Law on the Protection of Personal Data". Therefore the issue of accessing this kind of data has become a matter of discussion, especially in terms of the offences under Turkish Criminal Code (TCC) regarding the protection of privacy and personal data. The only kind of data accessible by public without any doubt, are criminal records that are public according to Criminal Records Code.

There are no DNA databases in Turkey. There is a draft law about DNA databases, but it is not legislated yet.

The databases in Turkey can be listed as below:

LDPP regulates a database for recording fingerprints and photographs. Fingerprints and photographs that are taken from persons are mentioned by LDPP art. 5/1; fingerprints that are taken from crime scene and belong to an unidentified person; fingerprints and photographs of persons who could not be identified because there was no birth record about him/her; fingerprints that are taken from convicts according to the Law on the Execution of Sentences and Measures (LESM), art. 21 are recorded to that database. Furthermore, according to art. 4/A LDPP, fingerprints and photos of persons who have been

asked for their proof of identification, but cannot be identified, because they are not registered, are to be taken and recorded following the procedure set forth under art. 5 LDPP.

According to LDDP art. 5, fingerprints and photographs are recorded and stored in the designated database without specifying the reason. Information in that database can only be used by courts, judges, public prosecutors and law enforcement agencies, with the purposes of identification, preventing crime or discovering the truth in an investigation or a prosecution. Law enforcement agencies can directly access this database with the purpose of identification or matching fingerprints that are taken from crime scene. A security system is established in order to record access information about which law enforcement agency used the information in the system and for what purpose. The records in the system are confidential; they are deleted ten years after the death of the person, and in any case they are deleted after eighty years from recording.

According to the Law on the Prevention of Violence and Disorder in Sports, art.18/4, Information about the measure of "banning from attending sports events" is immediately recorded in the designated database, which has been created within the Turkish National Police. Related sport clubs and federations can access that database. The information about the person who has been banned from watching sports events, are forwarded to the related sports clubs and, in cases of an event that will take place outside of Turkey, to the competent authorities of the foreign country, in which the event will be carried out, before the event.

Another database is created based on the Law on the Internal Services of the Turkish Armed Forces. Art. 61 of that law regulates that the results of the general health controls, which are carried out within the military services of privates and petty officers when participating and leaving their troops. The article also regulates that captains and commandants could check out the health conditions of the soldiers according to those records.

(**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**?

It is not possible to create profiles of potential perpetrators or risk groups in Turkey, because data in the databases are deleted within the limits of time provided by law.

In general, data mining is analysing data with another point of view and summarising them as useful information. Technically, data mining is finding patterns and correlations between large databases, which are related each other. Within this context, we can mention the duties of Criminal Police Laboratories Department and its subdivisions, which include data mining and matching.

A.- Speaker Identification and Recognition Department: This department analyses voice records produced by unidentified persons, matches them with identified voice records, and, if possible, identifies the owner. It also determines whether two separate records produced by unidentified persons have been created by the same person or not.

B.- Record Reliability Department: This department states whether a voice recording has been falsified by any physical or electronically intervention with an intention such as to add other voices or speeches, to delete, to change or to change any information about the recording signal.

C.- Audio Enhancement Department: This department clarifies any speech, noise or voices by reducing other speeches, which are expected to be perceived in a voice record.

D.- Signal Analysing Department: This department makes qualitative and quantitative analyses of the voices in a record, determining probable sources for the noise.

E.- Department of Determination of Speaker Characteristics: This department determines personal characteristics of the producer of a speech in a record.

F.- Voice and Speech Analysing Services:

Speaker Identification and Recognition: Speaker identification and recognition can be described as comparing an unknown voice with one or several known voices through a matching process by using audio-visual techniques. It aims to differentiate voices through their own characteristics and particularities through the use of different analysing techniques and methods.

Although this method is being used for many years, the parameters, procedures and results are controversial. Different results obtained from similar procedures and the produced matching proportions have raised questions about the reliability and acceptability of the method used.

Record Reliability: Record reliability means examining the originality of a record. In general, it is examined whether there was an addition, a removal or any other intervention on the record, or not.

Data Examinations: Data examinations are technical examinations that are applied by using established methods, on hard drives, CDs, DVDs, Blue Ray, Smart Phones, cell phones, SIM cards, Smart Cards, USB drivers, memory sticks, tablets, lap-tops, MP3/MP4 players, cameras, photograph machines and any other data carrier. These technical examinations contain recovering the information, which is hided, deleted, encoded or protected in the equipment mentioned above.

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

Interception of telecommunications and technical surveillance are coercive measures that can be utilized within an on-going criminal investigation or prosecution. Records obtained through these measures are to be destroyed within ten days after the completion of the procedure, if the criminal process has been terminated. According to the Turkish Criminal Procedure Code, art. 135, records resulting from these coercive measures cannot be used for building up information positions.

However, additional art. 7 LDPP allows law enforcement agencies to resort to interception of telecommunications and technical surveillance for intelligence reasons. According to this provision, telecommunications may be intercepted, tapped, recorded, and signalling information may be evaluated upon a judge's warrant, or, in cases of emergency, upon a written order by the General Director of Police or the Police Intelligence Department, in order to prevent crimes under art. 10 LCT, excluding espionage. In cases of emergency, the written order is to be forwarded to a judge's approval within 24 hours, who, in another 24 hours, is to decide about the order. The order is annulled immediately, if the time runs out, or if the judge does not approve the order. In this case, records of the measures are destroyed within 10 days. This procedure is taken into official records, which is subject to inspection.

Additional art. 7 LDPP provides that technical surveillance may be ordered accordingly.

Parallel provisions exist under the Law on the Organisation, Duties and Powers of the Gendarmerie (LODPG).

Additionally, Art. 6 of the Law on State Intelligence Services and the National Intelligence Organisation regulates that measures of "interception of communications" and "technical surveillance" may be used in order to maintain State security, to uncover espionage activities, to spot activities regarding the revealing of state secrets and to prevent terrorist activities, in the case of serious danger against the essential features of the Turkish Republic as declared under Turkish Constitution or against the rule of law. These are ordered upon a judge's warrant, and, in cases of emergency, a written order by the Secretary or Deputy Secretary of the National Intelligence Agency (MIT). A similar procedure for the judge's approval of the written order is provided in these cases.

Additional art. 7 LDPP also builds the basis for a Regulation on the application of the said article. This by-law came into force as the "Regulation on the Procedure and Principles of the Interception, Tapping, Evaluation of the Signalling Information, and Recording of Communications Through Telecommunication and on the Establishment, Powers and Authorities of the Telecommunications Communication Presidency" (Published in the Official Gazette dated 10.11.2005, Nr. 25989)[3].

It should be noted that any evidence obtained through the application of these provisions are among preventive measures, and cannot be used to prove any offence in a criminal trial. According to law, criminal prosecutions can only be based on evidence obtained through the application of procedural measures. However, in practice, courts do allow data obtained through preventive measures as evidence in criminal trial. There are cases where such data build a basis for conviction in criminal prosecutions.

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

All companies operating under a task-order contract, a franchise agreement, a telecommunication licence or general permit by the Telecommunications Institutions, including the government-operated Turkish Telecommunications Inc., are under a legal obligation to retain information for law enforcement agencies:

Art. 6/1-b of the Internet Law provides that access providers must retain traffic information on their services for a time of no less than 6 months and no more than 2 years, as specified by the Regulation, and to provide for their correctness, integrity, and confidentiality. The last paragraph of the same article puts those access providers who fail to comply with these conditions under an administrative fine of 10.000 – 50.000 Turkish Lira (equivalent of 5.000-25.000 USD). The time period for the data retention has been specified by the Regulation as 1 year. (art. 15/1-b of the Internet Regulation).

According to the Law on the Regulation of Internet Publishing and on Combatting Crimes committed Through Such Publications (Law 5651) [the Internet Law], and on the Regulation on the Internet Public Use Providers, such providers must record their internal IP logs electronically.

An additional obligation of the non-commercial public use providers has been regulated under the Regulation on the Internet Public Use Providers. According to this, such providers must record all Internet IP distribution logs at their working places, hotels, and other places, electronically. This data retention obligation that is not based on a legal framework and does not provide for any specification about the duration of the retention, whether such data is to be given to any authority, etc. For

[3] The "Regulation on the Application of the Measures of Interceptions of Telecommunications, Employing Undercover Investigators and Technical Surveillance as Provided under the Criminal Procedure Code" has been suspended by a stay of execution order of the High Administrative Court. The motives of the decision by the General Assembly of Administrative Chambers dated 06.12.2012 include the fact that the Criminal Procedure Code did not provide for a legal basis for this regulation, and that the legislator chose to regulate this area in great detail within the law instead. According to the High Administrative Court, this excludes the powers of the Ministry of Justice to pass a regulation on these measures.

this reason, it fails to comply with the general legal standards, and lacks the necessary guarantees regarding the freedom of communication.

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

Any information, document or discovery that is suitable to uncover the truth and that has been obtained legally can be used as evidence (art. 217/2 CPC). All law enforcing agencies can access all kinds of data regarding a criminal offence through using legal means. All private actors are obligated to oblige with requests of law enforcing agencies made accordingly.

Additionally, according to art. 6 of the Law on the National Intelligence Agency, the Agency (MIT) may make requests to ministries and other public agencies and archives of institutions providing public service, to electronic IT centres and the communications substructure companies in order to obtain information and documents, by providing legal grounds for such request.

There are also provisions on the application of technical surveillance for information building purposes. Additional art. 7 LDPP provides that the police may ask for relevant information and documents from public agencies and public service institutions by providing legal grounds for the request. In case such agencies and institutions refrain from complying on grounds such as protection of state secrets, a judge's warrant is needed to obtain the information or document. An identical provision is found under additional art. 5/5 LODPG, giving the same power to the Gendarmerie.

Art. 12/5 of the Electronic Communications Law provides that operators must establish on electronic communication systems the technical infrastructure necessary to be able comply with requests of law enforcing agencies in accordance with legal provisions relating to national security, before beginning to provide any service on electronic communication.

(7) Is there judicial control on building information positions?

As a rule, any preventive measure on interception of telecommunications and technical surveillance is only applicable following a warrant of a judge. However, in cases of emergency, a legally empowered administrative body (such as the head of the Intelligence Department of the Police, the Gendarmerie, or the Secretary of the National Intelligence Agency) are entitled to give a written order to initiate such measures. In these cases it is necessary to obtain an approval from a judge within a legal time limit of 24 hours. Otherwise, the measure is to be terminated immediately.

If these measures are applied illegally, criminal offences such as "violation of the confidentiality of communications" (art. 132 TCC), "violation of the privacy" (art. 134 TCC), "illegal entry into IT systems" (art. 243 TCC), "illegally obstructing, hacking, erasing or manipulating data in an IT system" (art. 244 TCC), "destroying, hiding or changing evidence of a crime" (art. 281 TCC), "violation of secrecy" (art. 285 TCC) may come into consideration.

(D) ICT in the criminal investigation

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

In Turkish law, here are no specific regulations on the real time interception of e-traffic data and content data. The coercive measure of "interception of telecommunications" under art. 135 CPC was not codified with ICT in mind. As a result, the text of the law includes the term "listening" as a real time interception method, which apparently relates to communication over the telephone.

However, content on the Internet may be barred from access following a decision of a judge or an order of the administrative authority. Under art. 8 of the Internet Law, Internet content may be barred from being accessed for specific crimes (incitement to suicide, sexual abuse of children, facilitating the use of narcotics, supplying material that causes health hazard, pornography, prostitution, providing space and means for gambling, offences under the Law on Crimes Against Atatürk), if probable cause exists. The warrant is issued by a judge during the investigation phase, and by the court during the prosecution. If, during the investigation, there is a case of emergency, the public prosecutor may issue a written order, which is subject to the approval of a judge within 24 hours. If the approval does not follow, the order is annulled immediately.

The warrant may also be issued directly by the TCP, if either the content provider or the hosting provider reside outside of Turkey, or, even when they reside within Turkey, the contents are related to the offences of sexual abuse of children or pornography.

The warrant to bar access must be executed within 24 hours of its issuing. Hosting or access providers that fail to comply with the warrant that was issued as a criminal procedure measure, are subject to a penalty of imprisonment from 6 months to 2 years, unless their omission constitutes another crime of heavier penalty. If the warrant was an administrative measure, in case of failure to comply with the barring order, the access provider shall be subject to an administrative fine of 10.000 – 100.000 Turkish Lira (an equivalent of 5.000-50.000 USD).

Additionally, art. 12/2-g of the Electronic Communications Law provides that operators might be put under a legal obligation to "provide technical means to legally authorised national institutions to lawfully intercept and listen to telecommunications".

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

There are no specific provisions on accessing, freezing or seizing information systems under CPC. CPC only includes specifications on "seizure of at the post", which cannot be extended to IT systems analogically. This follows from the general rule prohibiting analogy in matters that involve limitations of freedoms.

A specific provision on the search, copying and seizure of computers, computer programs and logs exists under art. 134 CPC. This provision allows law enforcement agencies to access and copy data carriers, but only through creating a disk image of the drive including access data (hash values). In other words, it is not legally permitted to access any IT system online and extract e-traffic or content data from it.

In addition to this, it should be repeated that art. 8 of the Internet Law allows for a barring order for online content involving some criminal offences (please see our answer to Question D/1).

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?

A general provision on the subject can be found under art. 332 CPC. According to this, any information requested by the public prosecutor in relation to a criminal investigation must be complied within 10 days. Failure to compliance is subject to a penalty under art. 257 TCC (criminal misconduct).

The said provision does not specify the type of entity that is under the legal obligation to share information with the prosecutor's office, and uses a general statement. In addition to art. 332 CPC, there is a specific provision on the execution of warrants regarding the interception of telecommunications under art. 137 CPC.

According to this article, the prosecutor or the judicial police officer appointed by him may request from representatives of agencies and institutions providing telecommunications services to execute of measures of interception, and to insert technical equipment for this purpose with a written order. This order is immediately to be complied with, under threat of forcible execution.

Additionally, according to art. 6 of the Law on the National Intelligence Agency, the Agency (MIT) may make requests to ministries and other public agencies and archives of institutions providing public service, to electronic IT centres and the communications substructure companies in order to obtain information and documents, by providing legal grounds for such request.

Another relevant provision on the "rights and obligations of operators" can be found under art. 12/2-g of the Electronic Communications Law. According to the said provision, the operators may be put under a legal obligation to "provide technical means to legally authorised national institutions to lawfully intercept and listen to telecommunications". Under par. 5 of the same article, operators must establish on electronic communication systems the technical infrastructure necessary to be able comply with requests of law enforcing agencies in accordance with legal provisions relating to national security, before beginning to provide any service on electronic communication.

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

Art. 140 CPC regulates the coercive measure of "technical surveillance". This allows law enforcement agencies to put the suspect's public activities and working place under technical surveillance, including audio-visual surveillance, if a high degree of suspicion exists for a crime listed under the same article, and, additionally, if no other means to obtain evidence exist.

Additional art. 7 LDPP and additional art. 5 of the Law on the Organisation, Duties and Powers of the Gendarmerie (LODPG) regulate that law enforcement agencies may use measures of "interception of communications" and "technical surveillance", while performing intelligence services, in order to prevent the offences which are listed under art. 10 of the Law on Combatting Terrorism (LCT), except for espionage crimes. The same articles provide that the police (or, in its case, the Gendarmerie) may ask for relevant information and documents from public agencies and public service institutions by providing legal grounds for the request. In case such agencies and institutions refrain from complying on grounds such as protection of state secrets, a judge's warrant is needed to obtain the information or document.

Additionally, art. 13/2 of the Law on Gatherings and Demonstrations (Law 2911) provides that the government commissar representing the government at demonstrations may order the recording of the demonstration with technical audio-visual equipment, including voice recorders or cameras.

Art. 9 of the Regulation on Internet Public Use Providers, such providers are under a legal obligation to establish closed-circuit cameras in order to record everybody entering or exiting their premises. These records are to be kept for seven days, and cannot be disclosed to anybody except for authorised public agencies.

Another issue regarding video surveillance is the legal grounds for CCTV cameras under Turkish law. Although the employment of such cameras for evidence gathering purposes is widespread in practice, there is no legal framework allowing this use. The legal basis for the "MOBESE" (Mobile Electronic System Integration) system is found under additional art. 16 of the Motorways Traffic Law (Law 2918). According to this provision, electronic systems may be established by the Turkish National Police in order to spot traffic violations for the purposes of ensuring the safety of people or property, provide for a

safe and orderly flow of traffic. However, video recordings obtained through this system can only be used for purposes specified under additional art. 16. These purposes do not include evidence gathering or crime prevention. As such, the only legal way to use MOBESE-footage is for general traffic purposes as stated under additional art. 16 of the Motorway Traffic Law. However, it is stated that in practice video recordings of MOBESE-cameras are kept by law enforcement officers, if they are deemed necessary for a possible criminal investigation in the future. It should be noted that such use is not only illegal within the existing legal framework, but also constitutes the crime of "illegally omitting to erase personal data" under art. 138 TCC.

In practice, it is also common procedure that law enforcement officers record the proceedings during a search-and-seizure within a criminal investigation, although there is no legal basis for this.

As mentioned above (see our answer to Question D/3), any natural or legal person is under a legal obligation to comply with a written request by a prosecutor demanding that a certain piece of information or document be handed over to law enforcement agencies (art. 332 CPC). Accordingly, surveillance footage legally obtained by private parties may be requested. Upon a failure to comply, such footage may be subject to a search-and-seizure measure.

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

Normally it is possible, but not mandatory, to record the interrogation of witnesses audio-visually. However, there are specific kinds of witnesses, for whom the recording is mandatory. According to this, an audio-visual recording must be made during the interrogation of victimised children, and of those who cannot be brought before the court during trial and whose testimony is indispensable for the uncovering of the truth (art. 52/3 CPC).

Within this context, Child Observation Centres have been established in some cities as a pilot study, in order to protect sexually abused children effectively, and to prevent children abuse, following the legal framework of the Decree Nr. 2012/20 on Child Observation Centres (published in the Official Gazette dated 4 October 2012, nr. 28431). The following issues have been specified with the decision nr. 2012/1 of 22.10.2012 of the Central Coordination Board of Child Observation Centres:

1. In accordance with the orders and directions of the public prosecutor, and following the statement of the victimised child, the victim shall be subject to external or internal bodily examination upon the victim's or his or her parents' consent, taking of body samples, psychological evaluation, and, if necessary, visual recording of physical evidence, following due procedure, at Child Observation Centres.
2. The statement of the victimised child shall be taken in a mirrored room, under audio-visual recording, by the public prosecutor, or, in cases of necessity, by a police officer following the prosecutor's orders, through a trained expert employed at the Child Observation Centre, and in the presence of the victim's attorney.
3. Utmost respect is to be shown to the privacy of the victim during the entire process.
4. Procedures within the Child Observation Centres shall not be recorded to the hospital automation system.
5. All information and documents obtained following the interviews and medical examinations shall be taken under record in form of a report, and shall be sent to the public prosecutor's office upon completion, including audio-visual recordings.

In addition to this, an audio-visual recording of the protected witness must be made. According to art. 58/3 CPC, the presiding judge may remove people, including the defendant, from the courtroom during the trial, if their presence poses danger to the witness. In these cases, a video recording of the testimony is to be taken, and those who have been removed retain their right to ask questions to the witness.

Art. 180 CPC provides the possibility to employ audio-visual recording technology during the interrogation of witnesses or experts that cannot be present before the interrogating authority, or at the trial.

Concerning the suspect or the defendant, it is specified under art. 147/1-h CPC, that during their interrogation during the investigation or the trial, technical means shall be employed to record the proceedings. The text does not leave room for discretion, and imposes a mandatory recording through the use of the term "shall be employed". The Decree Nr. 150 on the Audio-Visual IT System (SEGBIS) dated 14.12.2011 also states that such recordings are mandatory. Audio-visual recordings are also to be made when the suspect or the defendant is excused from being present at the trial.

Except for the instances stated above, it is generally prohibited to employ any means of audio-visual recording at criminal proceedings. As a rule, no such equipment may be used within the court building or at the courtroom during the trial. The same rule applies to other judicial proceedings within or without the court building.

(E) ICT and evidence (The chain of stages: collecting / storing / retaining / producing / presenting / evaluating electronic evidence)

(1) Are there any rules on evidence that are specific for ICT-related information?

There are no rules on evidence that are specific for ICT-related information in Turkish law. These are subject to general rules. No hierarchy of evidence exists in criminal procedure, either. Any information relevant to the case can be accepted as evidence, as long as it is collected legally, and there are no legal rules on the evidentiary value of specific types of evidence.

However, the credibility of ICT-related evidence is the point of an on-going debate in Turkish criminal procedure doctrine. It is a common concern that electronic evidence is open to external manipulation, particularly during the collecting stage. Therefore, many scholars express the opinion that ICT-related information should not be accepted as solid or credible evidence in criminal procedure.

Additionally, many specific cases in Turkish practice have presented serious doubts on the possibility that some pieces of electronic evidence have been produced purposefully after the supposed date of offence by people other than the suspect. For these reasons, a number of university professors on computer engineering have published a common declaration against the excessive and insecure use of electronic evidence in criminal trials, especially in case of corrupted data.[4] There are also views on a complete inadmissibility of electronic evidence in criminal procedure.

In practice, electronic evidence has gained the status of obtaining a confession in catholic inquisition. However, these pieces of evidence should only be used as a tool to obtain material evidence related to the case in a legal way, and should only have evidentiary value as to support such evidence. In the present-day Turkish criminal procedure practice, false electronic information is easily produced, collected as evidence, presented before the court and, in some cases, even accepted as a convicting proof in the absence of corroborating evidence. This situation can only be described as a "digital torture" in order to prove the defendant's guilt.

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

There are no specific rules on integrity and security of ICT-related evidence. General rules apply. However, this situation is leading to serious problems with regard to the technological progress. The security of electronic evidence is a problematic issue in practice.

It should be noted that some criminal offences would apply to actions breaking the integrity and security of electronic evidence. Offences in question could include the violation of communicational secrecy (art. 132 TCC), the violation of privacy (art. 134 TCC), illegal access to an IT-system (art. 243 TCC), hindrance or obstruction of the system, deletion or alteration of data (art. 244 TCC), aspersion (art. 266 TCC) or obscuring, hiding or altering criminal evidence (art. 281 TCC). However, due to lack of an effective controlling mechanism related to the integrity and security of evidence, it is nearly impossible to spot a violation of these provisions.

Doubts related to the manipulation of electronic data particularly arise during the taking of a disk image within the scope of search-and-seizure warrants on data carriers. Even if a secure hash value is generated during the copying, there are doubts that new data may have been added to the data carrier at the beginning of the copying process through the use of malware. Similarly, the seizure of CDs and mobile phones involves such doubts. Legally, the disk image must be taken on spot, without actually seizing the hardware, and a copy of the image must be handed over to the affected person, upon request. However, in practice, disk images of data carriers such as CDs, external hard drives or computer disks are being taken at police centres, on the grounds that the process shall take a long time otherwise. In these cases, the copying takes several days in the absence of the affected person. Thus, even if a secure hash value has been generated, it cannot be guaranteed that the disk image is taken without any alterations to the original.

Similar problems exist regarding the evidentiary value of data obtained through mobile phones (particularly smartphones). There are no specific provisions regarding the seizure of mobile phones and the data stored within. These devices are subject to a normal search-and-seizure procedure. This also brings about problems regarding the authenticity of electronic data obtained from mobile phones, particularly in the case of smartphones. In a particular case in Turkish practice, data belonging to some people have been found as recorded in an address book of a mobile phone, although these records have been proven not to exist at the beginning of the procedure. Following objections and examinations, it has been declared that the data had been "inadvertently" loaded to the mobile phone at the police station, by law enforcement officers, after the phone had been seized.

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

In the Turkish criminal procedure system, any judgment must be based on the intimate conviction of the court. Accordingly, anything can be accepted as evidence, as long as it has been collected legally. There are no exceptional provisions in the case of ICT related evidence. General rules apply to ICT-related information, notwithstanding the debate on their credibility.

In Turkish law, illegal evidence is completely inadmissible. The Turkish law adopts a very strict regime on unlawful evidence. The rule of total exclusion for unlawful evidence has been provided both under the Turkish Constitution and the Turkish CPC. A relevant provision can be found under art. 38 of the Constitution. According to this, findings obtained through illegal means cannot be accepted as evidence (art. 38 TC). This provision doesn't include any restrictions or exceptions. Additionally, the Turkish Criminal Procedure Code provides that proof can only be accomplished through lawfully obtained evidence (art. 217/2 CPC), and that any ruling based on illegal evidence shall be subject to reversal (art. 289/1 CPC).

[4] http://www.cmpe.boun.edu.tr/~say/dijitaldelil.htm

Additionally, the Turkish law adopts the principle of "the fruit of the poisonous tree", and thus excludes any evidence obtained indirectly through the use of unlawful evidence. As a result, evidence collected through illegal means can never be pulled into consideration at the judgment. There is no distinction between evidence collected by the state or by private persons in this regard.

The exclusionary rule doesn't have any exceptions. As a result, no distinction can be made between "absolute" and "relative" unlawfulness, or between "substantive" and "formal" unlawfulness of the evidence. The minority opinion in Turkish law that would allow such distinctions has not been widely accepted. In practice, contradictory examples of case law supporting both views exist. The aim of the criminal procedure is to obtain the truth through any legal means that respect the human rights. It is not possible to uphold the law through acquiescing unlawfulness.[5]

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

The Turkish Criminal Procedure Code provides a specific rule on the collection of ICT-related evidence. According to art. 134 CPC on "search and seizure on computers, computer programs and logs", data carriers used by the suspect may be subject to search-and-seizure, computer records may be copied, and these records may be transcribed, if no other evidence gathering methods are successful. This measure can only be ordered by the judge upon a request by the prosecutor.

Despite the fact that the provision expressly applies to the computer "used by the suspect", this condition is not duly respected in practice, particularly when the search is made in offices. In such cases, the search is mostly applied to all computers present, without determining which computer is used by the subject. As a result, it can be said that the existing rule concerning the application of the said measure is not upheld in practice.

If, due to the impossibility to crack a certain encryption, computer programs or logs cannot be copied during the procedure, or an encrypted piece of information cannot be accessed, the hardware can be temporarily seized in order to complete the process. After the completion, any piece of hardware must be returned to its owner.

In practice, this provision is applied as to damage the credibility of evidence. In some cases, the copying process on computers seized may take days. In such cases, it is not possible to ensure the presence of a procedural witness during the process. As a result, it is not possible to control the chain of evidence and to ensure that no external data have been introduced into the computer before taking a copy from it. This possibility alone is to damage the credibility of the evidence obtained through the said process. Such evidence should not be admissible in trial. However, in practice, there have been cases where such evidence has been admitted as basis for a conviction, even in the face of expert reports confirming suspicions that the evidence has been tempered with illegally.

Art. 134 CPC provides that all data must be backed-up during the seizure of computers and computer logs. The Regulation on Judicial and Preventive Searches provides under its art. 17, that this measure is also applicable to computer networks and other distant computer logs and their removable hardware. It should be noted that any provision limiting human rights and personal freedoms cannot be based on anything but organic laws. Thus, art. 17 of the Regulation cannot be implemented as to expand the limits of the legal framework of the CPC.

After taking the disk image of the data carrier, a copy of the back up is to be presented to the suspect or the defendant, upon their request. It should be stressed that a request of the suspect or the defendant is necessary for this. Without such request, the prosecutor or the police are not under a legal obligation to produce copies of the disk image. In practice, the suspect or the defendant that make a request for a copy, are confronted with the objection that the law enforcement officers do not have the equipment to burn the copy on (such as a CD-ROM, an external hard drive, etc.). In these cases, the suspect or the defendant is asked to provide a hard drive of the same specifications as the original data carrier. Thus, the subjects are requested to look for means to provide very specific technical equipment without any respect for the place or the time of the measure.

In other cases, it has been observed that the copy that had originally been handed over to the suspect and the defendant, has been recalled by the law enforcement agencies on the grounds that these copies "contain data that constitute a criminal offence". It has been stated that, during the investigation, some data within the computer had been found to constitute a crime, and the same data exists within the copy of the disk image. Defendants have been forced to hand over these copies, and told that they had to comply, unless they would face a criminal investigation. Although there is no legal basis for this practice, the police officers in question have not been subject to a criminal investigation or disciplinary action.

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

There are no specific rules on the probative value of ICT-related evidence under Turkish law. This kind of evidence is subject to the general rule of "conscientious conviction". However, there exist some well-founded doubts about the credibility of such evidence, due to problems arising from practice. Particularly, doubts arise about the possibility to introduce external data to a computer during the image-taking process as part of the search-and-seizure. Similar doubts arise about the seizure of CD-ROMs or smart phones.

[5] **KESKIN, Serap,** Ceza Muhakemesi Hukukunda Temyiz Nedeni Olarak Hukuka Aykırılık, Alfa, İstanbul, 2007, s. 182 – 183.

Although general rules do apply to the probative value of ICT-related evidence, this issue is highly controversial due to the fact that the legislation has been left behind the technological development, and to practical problems mentioned above.

(F) ICT in the trial stage

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

The Turkish legislation on criminal procedure contains provisions stipulating that ICT related evidence could be introduced in the trial as converted into written form. In addition, such evidence can be introduced as evidence by inspection, if applicable.

One such provision exists under the 2011 Regulation on the Utilisation of the Audio-Visual Information System (SEGBIS) in Criminal Procedure. According to this provision, records obtained through the SEGBIS are transcribed into digital minutes under the UYAP IT-System and are autographed electronically. For the transcribing procedure, appropriate software and/or hardware may be used (Art. 7 of the Regulation). Audio-visual recordings are not handed over to the parties, but copies of the transcriptions may be given. In case of demand or objection, audio-visual recordings may be opened for examination of the relevant person(s) in accompany of the prosecuting authority (Art. 8 of the Regulation).

In practice, transcribing the audio-visual data can take a long time. In some cases it may take months before the transcriptions are handed over to the parties. For this reason, difficulties occur during the preparation of the defence. In some cases, the defence may be called before the transcriptions have been submitted, and these records are only included in the case file after the ruling. Due to this delay, the legal recourse (objection) as provided by law cannot be taken effectively.

Additionally, recordings obtained through wiretaps are to be transcribed by persons assigned by the prosecutor, according to art. 137 CPC.

Another relevant provision (Art. 209/2 CPC) regulates that documents involving personal data related to the defendant or the witness may be read out at an *in camera* meeting, if the affected person expressly wishes so. Consequently, ICT related evidence involving personal data might be subject to the same process, thus ensuring the protection of privacy. However, since the Draft Law on the Protection of Personal Data has not yet been put into vigour, it should be stressed that matters regarding respect to personal data still have not been resolved fully in practice. Particularly, wiretap recordings involving the intimate sphere of persons are being introduced as evidence in spite of a complete irrelevance with the respective case.

As explained above, the Turkish legislation allows that ICT related evidence be transcribed into written form and subsequently introduced as document evidence in the trial. However, there are no rules preventing such evidence from being introduced as evidence by inspection or expertise. In the Turkish practice there are many examples where experts appointed by court or by parties have been assigned to inspect ICT related evidence.

Considering the directness of the evidence, the inspection of ICT related evidence in trial is a preferable method in respect to being transcribed into written form. This is especially the case for audio-visual recordings, where not only contents of the recordings, but also the tone or the intonation of the speaker may be important for the forming of a conscientious opinion. As such, the practice of transcribing said evidence and accepting their introduction as document evidence in the trial contradicts with the principle of the directness of the evidence, and, therefore should be avoided.

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

This method can be applied using the Audio-Visual Information System (SEGBIS). This system has been introduced for the audio-visual recording of testimonies, interrogations and trials, as well as the distant interrogation or hearing of persons outside the precinct of the court, who cannot be present during the process, by means of videoconference. This method is not regarded as a form of rogatory deposition, and thus may be applied even in cases where a deposition by proxy is forbidden by law.

In some cases, an audio-visual recording is mandatory under CPC. As a rule, the hearing of witnesses is optional. However, in cases where the witness is a child victim, or a person who cannot be brought before court (due to an illness, etc.) but who must be heard for revealing the truth, a recording is mandatory (Art. 52/3 CPC).

In addition, an audio-visual recording of the witness testimony must be made in cases where the judge removes from the courtroom a person who has the right to be present during trial (i.e. the defendant, or a mandatory attorney). In such cases, the right to respond has been secured by law (Art. 58/3 CPC).

Also, art. 147/1-h CPC provides that an audio-visual recording shall be made during the interrogation of the suspect or of the defendant (before the police, the prosecutor, the judge and/or during trial).

Art. 180 CPC regulates that witnesses or experts heard though proxy (either by rogatory appointment of another court, or by a proxy appointment of a member judge of the same court) should be heard through audio-visual distant interrogation method instead, if available. Since the SEGBIS has become effective after the entry into force of CPC, the said method should always be presumed available. Accordingly, the SEGBIS circular order No. 150 dated 14 December 2011 issued by the Ministry of Justice indicates that in cases provided under art. 180 CPC, the utilisation of the SEGBIS is obligatory.

Additionally, a defendant who has been excused from the trial according to art. 196 CPC shall be interrogated through the SEGBIS, as provided by the same circular order.

People that cannot be present during the trial due to any valid excuse can also join the proceedings or heard through the SEGBIS. In such cases, law enforcement officers are required to ensure the presence of the relevant person at the location where the distant interrogation shall take place. To this end, the requesting authority shall declare the identity of the person, the time and place of the hearing, and any preparations to be made beforehand to the relevant law enforcement agency. An appropriate number of law enforcement officers shall be present during the process (Art. 13, Regulation on the Utilisation of the Audio-Visual Information System in Criminal Procedure)

In addition, people held under detention may be interrogated distantly and may participate in the trial through the SEGBIS, if the technical requirements can be met. In this case, the requiring authority gives the necessary information to the penitentiary authority of the Institution where the person is detained (Art. 14, Regulation). People who are in a therapeutic institution or outside the precinct of the court may also be heard or may participate in the trial accordingly (Arts. 15, 16, Regulation).

According to the said Regulation, a prosecutor or judge may be present at the location of the person to be interrogated upon the express request of the requesting authority (Art. 18, Regulation). The affected person(s) are to be lectured about the process of audio-visual recording (Art. 19, Regulation). If, due to technical requirements, the identity check of the subject has been made externally in written form, the minutes of the identification process shall be scanned, verified as a copy of the original, autographed electronically, and sent to the requesting authority through the UYAP IT-System. Original documents are kept at the distant location (Art. 20, Regulation).

Another field of application for the SEGBIS is designated by the SEGBIS circular order No. 150 as so-called "dispatch detentions". A "dispatch detention" is a temporary pre-trial detention of a wanted person for whom an arrest warrant has been issued by a judge. If the person is arrested outside the precinct of the judge issuing the arrest warrant, and cannot be brought before the issuing judge within the same day, he or she is brought before a judge of the precinct where the arrest has been made. Upon ensuring that the person arrested is the same person for whom the warrant had been issued, this judge is entitled to put the person in a temporary detention until he or she is dispatched to the precinct of the issuing judge. The CPC doesn't include a provision on the utilisation of the SEGBIS during the detention hearing in case of dispatch detentions. However, the Regulation on the Utilisation of the Audio-Visual Information System and the SEGBIS circular order No. 150 expressly refer to dispatch detention hearings, allowing the use of the SEGBIS in such cases upon the approval of the prosecutor, the judge or the court in question (Art. 17, Regulation). The circular order recommends this method *"in order to overcome grievances resulting from the practice".* The grievances in question came into being from the protraction of the "temporary" detention due to technical difficulties in the transfer of suspects and defendants. As a result, many people put under dispatch detention were held for a prolonged time without having access to their files, and, in some cases, without having been told the exact charges for which they were being held.

Additionally, the Law on Witness Protection provides for a similar application for protected and/or secret witnesses. According to art. 5/1-b of the Law, secret witnesses may be heard during the trial in the absence of those who have the right to be present in the courtroom at the trial. In addition, their voice or appearance may be modified so as to prevent their identity from being determined. Art. 9/2 of the Law also provides that the image or voice of the witness may be modified if a protection order has been issued by the court in accordance with art. 58/3 CPC.

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

There are no specific regulations on the utilisation of digital and virtual techniques for the reconstruction of events during trial. The legislator did not provide a distinct method of introducing such evidence. However, there are no restrictions for the use of these methods as such.

The utilisation of the said methods can be possible particularly within the scope of expertise. However, in the Turkish criminal procedure practice, courts are usually contented with a mere submission of expert's reports. Legally, parties may direct questions at experts, both appointed by the court or by the parties, if these experts participate at the trial. However, courts mostly deny parties' requests on the participation of experts. As a result, the use of digital or virtual techniques during trials is extremely rare in practice, although there are no legal restrictions.

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

It is possible to present evidence at trial using audio-visual techniques.

As mentioned above, the law provides for the possibility to present the mere transcriptions of audio recordings obtained through wiretaps. According to this, persons assigned by the prosecutor shall transcribe such recordings. Recordings containing speech in foreign languages shall be translated by appointed translators (Art. 137/2 CPC). However, this provision does not prevent the presentation of the recordings in audio form.

Additionally, the said provision only refers to evidence obtained through the use of wiretap techniques by the investigating authority, and does not apply directly to the presentation of audio-visual evidence obtained through other means (such as by private recordings of the parties). The Turkish criminal procedure law adopts the system of conscientious conviction, and thus accepts all kinds of evidence, provided that they are not obtained illegally. As a result, audio-visual recordings related to the case at hand can be presented as direct inspection evidence during trial.

However, it should be noted that such techniques are rarely used in practice. It is a widespread habit to carry out the proceedings, including defence, in written form.

Additionally, there exist specific legal provisions on the use of audio-visual techniques during distant interrogation of suspects, defendants and witnesses (see: question F/2).

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

IT technology has been introduced into the Turkish criminal justice system through the introduction of the National Judiciary Informatics System (UYAP). Other state operated IT network systems have also been integrated into the UYAP, including the Judiciary Records Information System providing criminal records, the Central Civil Registration System (MERNIS) providing ID-records, the Address Registration System (AKS) providing address information, the Police IntraNet providing driver's licence and passport information, the Land Registry and Cadastre Information System (TAKBIS) providing land ownership information directly and in real-time. Additionally, legal notifications can be tracked over the UYAP.

The UYAP IT-System is a project that had been launched in two stages in 2000. The UYAP-I Project has been completed 2001 and achieved the automation of central services of the Ministry of Justice. The UYAP-II Project has been completed 2005, and achieved the automation of civil, criminal and administrative legal authorities, the Institution of Forensic Medicine, and penitentiary institutions. The Turkish Court of Cassation also participated in the UYAP IT-System by adapting the UYAP Software to its proceedings.

In order to integrate the utilisation of IT systems in criminal procedure, art. 38/A has been added to the Criminal Procedure Code through an amendment dated 2 July 2012. According to this provision, the UYAP IT system is to be used in criminal procedure. All kinds of information, all documents and decisions shall be processed through the UYAP System. Additionally, the use of electronic signature entered the Turkish criminal judiciary system with the same amendment.

It should be noted, however, that the application of the UYAP system is not yet problem free. There are still a large number of case files that could not have been transferred to the UYAP System, due to technical problems and/or lack of necessary manpower. Additionally, access to the system can be problematic from time to time. The short time span since the relevant legislation has been passed (July 2012) is another reason for the small number of documents transferred into the UYAP system.