# SUÇ VE CEZA

CEZA HUKUKU DERGİSİ

OCAK
ŞUBAT
MART
2013

**SAYI**
**1**

TCHD
TÜRK
CEZA HUKUKU
DERNEĞİ
TARAFINDAN
ÜÇ AYDA BİR
YAYIMLANIR.

**SUÇ VE CEZA**
**CRIMEN E POENA**

**CEZA HUKUKU DERGİSİ**
ISSN: 1308-0474

**Sahibi**
**Türk Ceza Hukuku Derneği İktisadi İşletmesi adına**
Av. Fikret İlkiz

**Genel Yayın Yönetmeni**
Av. Fikret İlkiz

**Sorumlu Müdür**
Prof. Dr. Yener Ünver





**Abone Bilgisi**
Cemile Meral
0212/511 54 32 Dahili: 112
cemile.meral@damgada.com

**İletişim Adresi**
Türk Ceza Hukuku Derneği
Maçka Cad. No:11 Kazım Gerçel Apt. K. 2 D. 3
Maçka-İstanbul Tel: (0-212 343 80 80)

**Basım Yeri**
Net Kırtasiye Tan. ve Matbaa San. Tic. Ltd. Şti
Taksim Cad. Yoğurtçu Faik Sok. No:3 Taksim
Beyoğlu/İSTANBUL
(Sertifika No: 13723) Tel: (0-212 249 40 60)

**Basım Tarihi**
Aralık 2013

# İçindekiler

*Preparatory Colloquium Section III*

# SECTION 3: CONCEPT PAPER AND QUESTIONNAIRE

**Prof. Dr. Johannes F. Nijboer**

### (A) Scope of questionnaire (see Introduction and Annex)

The questions in this Section generally deal with "cyber crime." This term is understood to cover criminal conduct that affects interests associated with the use of information and communication technology (ICT), such as the proper functioning of computer systems and the internet, the privacy and integrity of data stored or transferred in or through ICT, or the virtual identity of internet users. The common denominator and characteristic feature of all cyber crime offences and cyber crime investigation can be found in their relation to computer systems, computer networks and computer data on the one hand and to cyber systems, cyber networks and cyber data on the other hand. Cyber crime covers offenses concerning traditional computers as well as cloud cyber space and cyber databases.

National rapporteurs can contact the general rapporteur in case of further inquiries or questions: Prof. Dr. J.F. Nijboer: J.F.Nijboer@law.leidenuniv.nl

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

**(C) Information and Intelligence: building information positions[1] for law enforcement**

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

(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?

(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?

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

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

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

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

**(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?

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

(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?

1 Building up information positions is part of the so-called intelligence-led-policing (ILP). ILP can be defined as s a conceptual framework of conducting policing as an information-organizing process that allows law enforcement agencies in their preventive and repressive tasks.

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

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

**(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?

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

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

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

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

**(F) ICT in the trial stage**

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

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

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

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

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

*Preparatory Colloquium Section III*

# ANNEX - INFORMATION SOCİETY INCLUDING INFORMATION TECHNOLOGY) AND CRIMINAL JUSTICE

**Prof. Dr. Johannes F. Nijboer**

*Evan Ratliff, an American journalist, tried to vanish in the digital world for a month. He travelled through the United States with a different identity. This experiment was linked to a contest and people 'online' tried to find him. After a month of travelling, trying to be invisible, it seemed impossible in our current information society. Being completely anonymous is not possible due to digital traces. These traces contain for example payments, travelling information and communications.*[1]

***Preamble***

This preparatory document contains a number of observations and reflections that are relevant for the development of a questionnaire for Section III – ***criminal procedure***. It has been prepared by Professor Johannes F. Nijboer of the University of Leiden (NL) with the assistance of Mrs. Sanne Kruithof MSc of the University of Leiden. The text was submitted to the AIDP for its preparatory meeting in Siracusa (December 3 and 4, 2010). It is revised for its use as a background document for the draft questionnaire as it stands after the meeting of the rapporteurs in Freiburg im Breisgau (November 20 + 21, 2011).

**(A) Some general considerations**

The (post)modern society of today is dramatically different from that of – let us say – 30 years ago. This is true for most countries and regions, even if they are still subject to relatively scarce resources or subject to foreign exploitation of the resources they have. Even in the middle of

1 < http://www.wired.com/vanish/2009/11/ff_vanish2/> <http://www.marketingfacts.nl/berichten/20100923_picnic10_evan_ratliff_wired_over_digitaal_verdwijnen/>

deserts, high seas, and rainforests mobile telephones and internet can be found. The fast developments in high-tech crime (cybercrime, computer crime)[2] are interrelated to the borderless opportunities of ***IT*** and ***ICT***.[3] But the same applies for the (professional) acts, tools, and instruments within the criminal justice system. Today it appears that even the question of ***"hacking"*** (which constitutes a crime in most jurisdictions) can be legitimate for police investigations as a means for collecting information. This information may include data that even can be used in evidence.[4] The last decades of the twentieth century and the beginning of the third millennium have witnessed many new findings and insights. Scientific and technical findings succeed each other with an accelerating speed. Almost all aspects of society are influenced by IT and ICT. It is often difficult to see where developments start, let alone where they stop or are interrupted. Private spheres and public spheres are both affected in a way that makes it steadily more and more difficult to distinguish these two, with for instance an enormous impact for the life of individuals – and the very concept of (social) life as well as the protection of real of privacy.[5] Ratliff (see quotation above) tried to expose this impact on private and public spheres – and the intertwining and mutually interference of these two - with his experiment to vanish for a month. One's very existence can be recorded, registered, and monitored in many ways – without escape. Besides the impact on private and public spheres, the same goes in an institutional sense for the impact on the ***"life"*** of organizations. This can vary from simple groups, communities and networks or firms to international networks of cooperation, multinational enterprises, non-governmental organizations (NGO's) et cetera. Part of the complexity of the developments is related to the ***convergence of technologies***, for instance in nanotechnology, biotechnology and information technology.[6] They create possibilities and

2 See R.C. van der Hulst & R.J.M. Neve, ***High-tech crime, soorten criminaliteit en hun daders***, Den Haag: WODC, 2008.

3 Especially within the context of the criminal process the combination of Information Technology and Information and Communication Technology makes it difficult to distinguish both.

4 See J.J. Oerlemans, Hacken als opsporingsbevoegdheid, ***Delikt en Delinkwent*** 2011, p. 888-908.

5 We will come back to this.

6 See C.J. de Poot, M.P.C. Scheepmaker, Voorwoord, in: ***Technology, cognitie en justitie***, Justitiële Verkenningen 2008/1; Boom Juridische Uitgevers, Den Haag, 2008.

opportunities: on the one side for criminal activities, on the other side for the reactions to this. New forms of criminality, that are related to new technologies can be investigated by applications of techniques that are familiar to the same forms of conduct – e.g. the investigation of internet crime by the use of the internet itself. But science and technique in a broad sense have also an enormous impact on the traditional justice systems. Technological developments and innovations have major consequences for the criminal process. These consequences can theoretical be divided into two groups: alterations and modifications of and additions to existing instruments, procedures et cetera versus (totally) new instruments, procedures et cetera. An example of the first category would be the replacement of paper court files by electronic ones, an example of the second is the Automatic Number Plate Recognition (ANPR) as it is used to trace, locate and follow cars and individuals.[7]

The types of technologies that draw special attention in the field of the criminal process are the ones that can be used for the detection of persons and acts, the ones that influence human behavior and the ones that help in reconstruction events. Again we give an example of each: refined chemical tests for the detection of biological traces (as part of crime scene investigation) for the first category, electronic surveillance for the second category and computer reconstruction of traffic accidents for the third category. The boundaries between different technologies in applied contexts are not always easy to discern: as said before, there is or can be a convergence. Even the boundary between "real" things and artificial ones is fluent. Is a DNA-fingerprint ***"real evidence"?*** Or can it better be described as an artifact? And what about statistical information produced by national offices, that most of their data and analyses present in a complex form, with – interlinked - click tabs for the numbers, the graphics, the maps.[8] Within the actual text we will now focus on a part of these numerous developments.

---

7 Cf. J.F. Nijboer, Signalement: Automatic Number Plate Recogniotion (ANPR), ***Expertise en Recht*** 2011/6 (in print).

8 See P. van den Hoven, ***The rubber bands are broken; opening the 'punctualized' European administration of justice***, .....

(Post)modern society often is characterized as an ***"information society",*** because of the widely spread availability and usage of Information and Communication Technology (ICT). The role of ICT is deeply related to scientific and technological developments in general, as generally described before. A few typical features of these developments are (a) the global impact of all kinds of applications, (b) the fast sequence of innovations, (c) the radical changes in the daily work of almost everyone, (d) the transcendent character of changes across natural borders, national borders and limits of time and space, (e) the availability of directly applicable mass data, (f) the loss of traditional monopolies in information, (g) the application of ICT related surveillance devices in different contexts.

**A short explanation:**

**Ad a**. Through the combination of integrated computer networks and wireless connections virtually al kind of natural and physical borders can be passed. The very notions of time and place become relative. Within the context of the criminal process one can think of the interrogation of persons (witnesses, suspects) via satellite connections and closed circuit television (CCTV). A DNA-database can be searched within a short period, even by persons in another country (as is the case in the countries that belong to the "Prüm area" within Europe[9]).[10]

**Ad b.** It is only twenty years ago that elaboration and storage of text by the use of "floppy disks" was an innovation. Today, we might smile when we realize ourselves the speed by which these disks were replaced by CD-ROMs, DVDs and USB-sticks. Sometimes it is argued that it will last for decades before information storages will reach a level of standardization that is equal to the physical "book".[11]

**Ad c.** Due to the endless variety of functions almost everyone has undergone a dramatic change in activities. We buy goods and services on internet (including the check-in for a flight). We inform our contacts from the train or car when we expect to arrive late. But also organizations,

9 Austria, the BENELUX countries, France, Germany, Spain

10 See G. Vermeulen, ***Free gathering and movement of evidence in criminal matters in the EU***, Antwerp: Maklu, 2011.

11 Umberto Eco, Jean-Claude Carrière & Jean-Philippe de Tonnac. ***N'espérez pas vous débarrasser des livres.*** Grasset & Fasquelle 2009.

including state agencies, have access to data related to virtually anyone. The latter makes our identities vulnerable for purposes of fraud, by the way. Especially the mass storage of information, that can be instantly checked (the running of a DNA-database) is something we will give special attention to in relation to the criminal process, for instance because of the fundamental change in nature or character of the criminal investigation. The already mentioned use of ***ANPR*** (combined by the collection of the registered passing of cars at the automatic 'checkpoints') is an example.[12] Turning our focus towards the criminal trial it should be noticed that digital case files – with multiple connection kits or apps – have made their entrance: presentations in a multi-modal way (including "***live***" presentations by audiovisual and digital/virtual reconstructions et cetera).

**Ad d.** This aspect was already touched upon before. The transnational mobility of persons, goods and services has a multiple impact on our daily life. It also has tremendous consequences in the area of the criminal justice system(s). But it is not only state borders that become less important - it also pertains to natural and physical borders.

**Ad e.** Like just said about DNA-databases, it can be said that in general enormous quantities of information are available for direct use. Think of internet searches with "machines" like Google. Above this kind of general public availability, many special databases and other "***things***" that contain information are there - most in the commercial sphere, but also in other spheres like (again) the criminal justice system.

**Ad f.** This is a more complex issue. Of course, it is the case that new markets sometimes spoil older market situations (e.g. the availability of the full content of a book on internet). Traditionally diverse aspects of the state function typically are part of state monopolies. This is the case for aspects of the criminal process too. Here several issues arise, varying from investigative journalism to the ***"free market"*** of forensic expertise. Especially in the field of patented technology and science we can observe

12 And what about the database of the (private) organization that runs the public transport chip-cards in The Netherlands? Or the databases of mobile telephone and internet traffic kept by providers of such services?

very complex interrelations between industry and state as well as private agencies (again converging technologies can serve as examples). With some exaggerations we might make a comparison between the "military-industrial complex" in the time of the Cold War and the "forensic-industrial complex" of today.

Ad g. Another feature of today's life is the application of surveillance devices. We find them in the physical world as camera surveillance at gas stations, shopping malls or streets, amusement centres, in busses, trams, metros, trains and ferries, and – last but not least in department stores and in the corridors of hotels (as IMF president Dominique Straus-Kahn found out in New York). But the use of mobile phones and internet can be under surveillance as well: today there is a discussion in The Netherlands about the legality of a high tech content inspection modus used by two phone companies (KPN and Telfort). The discussion concerns the question whether or not this would be only legal for the investigative and security authorities of the state; the companies involved contend that they only look at the nature of the use, not the content of the communications actions of their customers. Also interesting is the – already mentioned - storage of information by providers and on the chips in devices like public transport chip cards. Often it is very easy to obtain an overview of the journeys of the user during the last month or even longer back in time.

**(B) Criminal procedure**

One of the main areas of the criminal justice system is ***fact-finding and evidence*** in relation to crime and punishment. It should be noted that many classical crimes can also be committed with the involvement of modern techniques, but that there are also relatively new crimes that are inherently connected to those techniques. From a procedural point of view this is important, since it is the substantive criminal law that denominates the ***"investigandum"*** and ***"probandum"*** from the very beginning in the investigation. (As we will see later on the concept of investigation in the traditional sense has become problematic as well.) It goes without saying that new forms of criminality require their own forms of investigation tools and methods. This pertains in special for the

domain of ICT crimes (cybercrime[13]).

But there is more, especially in relation to specified databases for instance. The police, the prosecution service, the judiciary, the defense, they all operate in the middle of the information society, and they use the possibilities and opportunities at great length. Although in the context of the criminal process the center of our attention will be on the impact of the information society on the earlier stages of the process, it should be noted that also in the sphere of sentencing and the execution of (namely) prison sentences applied databases are used. In The Netherlands this is the case for the database(s) on imposed sanctions (***"sentencing"***) The availability of new techniques, especially in the ICT world sometimes in combination with other techniques (for example DNA-databases) has dramatically changed the primary processes within the criminal justice system. On one hand the criminal justice system use the new (ICT) technologies available in their daily processes. Take for example the role of paper court files in many countries with a traditional continental system: in high speed many information streams are canalized through electronic systems. Modern courtrooms often are equipped with ICT devices of a rich variety. The application of long distance live connections for a direct interrogation of witnesses or defendants via a satellite is not exceptional any more. On the other hand new techniques influence the investigation and the collection of evidence (in particular within the earlier stages of the process – or even in a broad sense the pre-procedural stage -). We will come back to this in the following paragraph.

**(C) Intelligence and evidence**

Since some decades it is not unusual to distinguish between strategic or tactical information that is available to the police and/or prosecution and information that can be used as evidence. The first kind of information is as "steering" information for the investigation. The mostly used label is ***"intelligence".*** Such information is never fully disclosed in concrete cases. For a long period the distinction between

13 See U. Sieber, Mastering complexity in the global cyberspace, in M. Delmas-Marty et al. (eds.), *Les chemins de l'harmonisation penale*, Paris 2008, p. 127-202.

intelligence and evidence was mainly applied in the Common Law countries. Today, the availability and application is widely spread through non-Common Law countries as well. (This gives – by the way - ground to raise the question whether or not the Common Law concept of ***"admissibility"*** of evidence within this context could be a fruitful one in non-Common Law jurisdictions.)

In combination with certain kinds of expertise even the existence of ***"forensic intelligence"*** is a matter of fact. With this context one can think of the combination of information from different databases (DNA-profiles, financial data from the banking branches or tax See U. Sieber, Mastering complexity in the global cyberspace, in M. Delmas-Marty et al. (eds.), ***Les chemins de l'harmonisation penale***, Paris 2008, p. 127-202. offices, travel data, license plate numbers, finger prints). In relation to the investigation of organized crime and terrorist cases the boundaries between classical police work and the work of secret services and other types of intelligence services has become fluent. The same applies for the sharing of information across national borders. An eye catching example of transnational information exchange on a daily basis is the connection between forensic DNA-databases within a growing number of EU-countries on the basis of the ***"Treaty of Prüm"*** (and the subsequent EU regulation that has extended its scope). The existence and the use of enormous amounts of operational information is sometimes referred to as the ***"information position"*** of investigative and prosecutorial authorities. From this perspective it is ***"saillant"*** that the presiding Procurator-General of The Netherlands in a television interview indicated that the "information position" of the Dutch prosecution service in relation to organized crime was very much ameliorated since about ten years, but that budget cuts cause a limitation to the extent to which indeed criminal investigations could be started (he spoke of about 25% of the known crimes).

Actually this means that there is a world of information or ***"intelligence"*** available apart from the explicit decisions to enter into a criminal process. There is no a priori reason to assume that in other areas the situation would be very different: the mere fact that many data are available changes the classical picture of investigation. An investigation

will often be started on the basis of already existing knowledge. The very decision to act in a concrete case therefore is more than traditionally a matter of choice, it appears. And the choices that are made can be perceived as conscious policies of the authorities. The use of technology and relatively new techniques by the police, but also by private parties such as private protection companies, influences the information position of the police and other investigative or intelligence services compared to earlier times. The possibility comes into existence that technology changes very much the ***'beginning'*** of the concrete criminal investigation. With the use of technology it is possible to monitor persons or groups and try to reveal criminal acts, even from before they actually happen. Earlier, at least in a more classical view, the criminal acts themselves were the starting point of an investigation. ***"Reactivity"*** makes steadily more room for ***"pro-activity".*** Besides the influence of technology on (classical) police work, the use of technology has also consequences for the public space. Amongst others Nunn[14] states that the police and other agencies, like private security firms, transforms in – so called- 'surveillance machines'. The use of all kinds of (surveillance) techniques instigates the debate on privacy, we will come back to this later on. Here the notions of the surveillance society and the surveillance state apply.

**(D) Sources of information (intelligence)**

It should not be overseen that in many cases information that is useful for criminal justice purposes is derived from open sources. Especially ICT plays a predominant role. Internet is a big (open) source of information, internet investigation has become an usual tool in many cases. Besides information that can be found on the internet another tool is information which is collected by civilians. A new tool in the Netherlands is a request from the police to civilians to upload their photos and videos from a event made by their mobile phones.

Apart from information from more open sources, it is often possible for the investigating authorities to use information from other more

14 Nunn (2001), 'Police technology in cities – changes and challenges', Technology in Society 23, 11-27.

closed government or non-government sources. An – earlier mentioned - example is again the information from public transport (chip)cards or telecommunication-data recorded in databases. Here, it should also be stressed that in most countries there is a vast amount of legislation that obliges providers of ICT services to keep data collected and to make them available to the criminal authorities. It is well known that anti-terror laws have substantially contributed to this state of affairs.[15] Because of the development of technology, there has been a development of investigative tools too. A few of them have been mentioned earlier. As stated before one of the features of the development of technologies is the loss of traditional monopolies in information. This loss of monopoly is bilateral, on one hand information can be retrieved from more 'open' sources, largely the internet, on the other hand investigative tools are not only available for the government (police), but also for private parties, mainly private security companies. These companies do not exist due to the developments in technology, they have their history back in time when guilds existed. With the grow of the welfare state, (over a long period in the XXth century), the monopoly of the state went bigger, including fields of security and investigation. Recently the welfare state, respectively the monopolies of the state, is/are decreasing. This development gives multiple opportunities for e.g. privately-held security companies. This kind of interrelations fit well into the idea that the state is being transformed into a network state, in which information technology (IT) and information and communication technology (ICT) form the essential organizational principle. This means no less than that the whole concept of the state is changing, including the criminal justice system.

### (E) The role of the media

Earlier we mentioned the fact that much information comes from open sources. The availability of such sources is connected to the activity of publishers, providers etc. From a wider perspective it seems to be

15 A. Oehmichen, *Terrorism and anti-terror legislation - the terrorised legislator? A comparison of counter-terrorism legislation and its implications on human rights in the legal systems of the United Kingdom, Spain, Germany, and France*, Antwerpen: Intersentia, 2009.

important not to overlook the role of the media. Investigative journalism has become a frequent phenomenon nowadays.

**(F) Human rights and fundamental freedoms**

It cannot be denied that the societal changes and the related changes in the operation of the criminal justice systems raise many new problems and questions in the area of human rights and fundamental freedoms. Think of the conditions under which biological samples are taken from suspected or other persons in order to produce DNA-profiles to be included in forensic DNA-databases. Or the application of devices for direct interception of private discussions.

Criminal procedure laws traditionally strike balances between human rights and (necessary) limitations to civil freedoms in the interest of public and state interests. Much of the case law of Human Rights Courts, such as the European Court of Human Rights (ECtHR) is related to such issues. In the elaboration of the subject "The Information Society and Criminal Procedure" this area must have major attention. During the last decades most countries have sharpened their legislation for reasons of security and the struggle against terrorism and organized crime in a way that fundamental rights like privacy and physical freedom are sometimes very much limited. There is growing attention in the literature in this field, both from the perspective of Human Rights and of Criminal Procedure. Within the field of human rights the national aspects of the criminal procedure are intertwined with international (global and regional) aspects. Therefore there is a good reason to look closely to the domain that in the work of the AIDP should be covered by the questionnaires and reports in the Sections III and IV.

**(G) Some closing remarks**

It goes without saying that there is much more to say about the impact of the ***"information society"*** on the criminal process – especially in relation to ICT and converging techniques. We just mention here the development in facial recognition on the bases of databases of photographs and the use of surveillance cameras. Another important aspect that should be given attention to is the occurrence of false

recognitions or identifications (false positives) in the area of surveillance and as a product of the combination of information from different sources. Further we can add the (only at first glance) more ***"simple"*** error rates in forensic science on the bases of random matches in a DNA database or the risks of change or contamination during the chain of custody of forensic samples (and the use of ***""track and trace"*** systems to limit that kind of risk). When ever such subjects are looked at, there is almost every time at least one or two connections to ICT as well.

From a more distant point of view, it is good to ask the question whether or not the information society in relation to the ***"surveillance state",*** the ***"intelligence state"*** and the ***"database state"*** affects the whole basis of the traditional criminal process from its beginning and at the same time in its focus, where the ***"investigandum"*** and ***"probandum***" appears to be more on deviant (and risky?) behavior than on criminal behavior in a stricter sense.

# TURKISH NATIONAL REPORT

**Prof. Dr. Serap Keskin Kiziroğlu***
**Ar. Gör. Fulya Eroğlu****
**Ar. Gör. 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.

* Istanbul Okan University Law Faculty, Department of Criminal Law and Criminal Procedure Law.

** Yeditepe University Law Faculty, Department of Criminal Law and Criminal Procedure Law.

*** Dokuz Eylül University Law Faculty, Department of Criminal Law and Criminal Procedure Law.

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.

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

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

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

2 Dr. İhsan 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.

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 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, photography, 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.

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.

**(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 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,

**(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

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

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).

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.

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

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.

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.

# BÖLÜM 3: KAVRAM AÇIKLAMASI VE SORULAR

**Prof. Dr. Johannes F. Nijboer**

**(A) Soruların kapsamı (bkz. Giriş ve Ek)**

Bu Bölümdeki sorular, genel olarak "siber-suç" ile ilgilidir. Bu terim; bilgisayar sistemlerinin ve internetin düzgün işleyişi, bilgi ve iletişim teknolojilerine (BİT) veya bunlar aracılığıyla transfer edilen veya saklanan verilerin bütünlüğü ve gizliliği, ya da internet kullanıcılarının sanal kimlikleri gibi BİT kullanımıyla bağlantılı menfaatleri etkileyen suç oluşturan fiilleri kapsayacak şekilde kullanılmaktadır. Siber-suçluluk alanına giren bütün suçların ve siber-suç soruşturmalarının ortak paydası ve karakteristik özelliği; bunların, bir taraftan bilgisayar sistemleri, bilgisayar ağları ve bilgisayar verileri ile ve diğer taraftan siber sistemler, siber ağlar ve siber verilerle olan ilişkilerinde bulunabilir. Siber suç alanı, geleneksel bilgisayarların yanında çevrim içi bilgi dağıtımı (cloud cyber space) ve siber veri tabanlarıyla ilgili suçları da içine alır.

Ulusal raportörler, daha fazla bilgi almak ya da soru sormak için genel raportör ile bağlantıya geçebilirler: Prof. Dr. J.F. Nijboer (J.F.Nijboer@law.leidenuniv.nl)

**(B) Genel Sorular**

(1) Ceza muhakemesi usulü bağlamında (adli tıbbı da içerecek şekilde) BI ve BIT uygulamaları için kullanılan güncel (hukuki veya sosyo-hukuki) tanımlar var mıdır? Cezai süreç bağlamında bu gibi kavramsal tanımlar literatüre, mevzuata, mahkeme kararlarına ve ilgili uygulamalara nasıl yansımaktadırlar?

(2) Ceza adaleti sistemi içinde bilgi BİT'in yürütülmesinden sorumlu belirli kurumlar ve/veya görevli birimler var mıdır?

(3) Ceza adaleti sistemine BİT ile ilişkili hizmetler sunan özel (ticari) kuruluşlar (şirketler) var mıdır? Eğer varsa, bunlara örnek verebilir misiniz? Ne gibi sınırlara uyulması gerekmektedir?

**(C) Bilgi ve İstihbarat: Kanun uygulayıcı makamlar için bilgi istihbaratı pozisyonları [1] oluşturma**

(1) BİT'le bağlantılı hangi teknikler kanun uygulayıcı makamlara yönelik bilgi istihbaratı pozisyonları oluşturmak için kullanılmaktadır?

(2) Kanun uygulayıcı makamların hangi tür kamusal (örn: DNA veritabanları) ya da özel (örn: Yolcu isim kaydı (PNR) verileri ya da SWIFT verileri gibi finansal veriler) veri tabanlarına erişimi mümkündür?

(3 Veri madenciliği ve veri eşleştirme olarak adlandırılan teknikler uygulanabilmekte midir? Eğer uygulanabilir ise, bu teknikler potansiyel faillerin veya risk gruplarının profillerini oluşturmada kullanılabilmekte mi? Eğer kullanılabilir ise, kanun uygulayıcı makamlar için özel araçlar geliştirilmiş midir?

(4) Zorlayıcı tedbirler (ör: haberleşmenin denetlenmesi) bilgi istihbaratı pozisyonu oluşturmak için kullanılabilmektedir midir?

(5) Hangi özel sektör aktörleri ( ör: internet sağlayıcıları ya da telekom şirketleri) kanun uygulayıcı makamlar için bilgi muhafaza etmektedirler ya da etmek mecburiyetindedirler?

(6) Hangi özel sektör aktörleri kanun uygulayıcı makamlara bilgi sağlayabilir veya bilgi sağlamak mecburiyetindedirler?

(7) Bilgi istihbaratı pozisyonları oluşturma konusunda yargısal denetim bulunmakta mıdır?

**(D) Ceza soruşturmasında BİT**

(1) Kanun uygulayıcı makamlar, gerçek zamanlı olarak a) e-trafik verilerine, b) içerik verilerine müdahale edebilir mi?

---

1 Bilgi istihbaratı pozisyonları oluşturma, istihbarat-odaklı-polis faaliyeti (ILP) olarak adlandırılan olgunun bir parçasıdır. ILP kanun uygulayıcı makamların önleyici ve bastırıcı görevlerini gerçekleştirmelerine imkan veren bir bilgi-düzenleme süreci olarak yürütülen polislik faaliyetlerinin kavramsal çerçevesi olarak ifade edilebilir.

(2) Kanun uygulayıcı makamlar; a) e-trafik verileri; b)içerik verileri bakımından, bilgi sistemlerine erişim/bunları durdurma/arama/bunlara el koyma imkânlarına sahip midir?

(3) Telekom şirketleri ya da servis sağlayıcılar, verilerini kanun uygulayıcı makamlar ile paylaşmaya zorlanabilirler mi? Buna uygun hareket etmemeleri halinde, zorlayıcı tedbirler ya da yaptırımlar uygulanmakta mıdır?

(4) Kanun uygulayıcı makamlar kamera ile izleme yapabilmekte midir? Bu makamlar gerçek ve tüzel kişileri işbirliğine zorlayabilirler mi?

(5) Kanun uygulayıcı makamlar, sorgulamaları (şüpheli, görgü tanığı) sesli ve görüntülü kayıt altına alabilmekte midir ya da almak zorunda mıdır?

**E) BİT ve deliller**

(Aşamalar zinciri: elektronik delillerin toplanması / depolanması / tespit edilmesi / üretilmesi / sunulması / değerlendirilmesi)

(1) BİT ile ilişkili bilgilere özgü herhangi bir delil kuralı var mıdır?

(2) BİT ile ilişkili delillerin bütünlüğü (örneğin delillerle oynama veya kurallara aykırı biçimde işleme) ve güvenliği (örn: hack'leme) ile ilgili herhangi bir kural var mıdır?

(3) BİT ile ilişkili bilgilere özgü olarak delillerin kabul edilebilirliğine (hukuka uygun elde edilmiş delil ilkesi dahil olmak üzere) ilişkin herhangi bir kural var mıdır?

(4) BİT ile ilişkili delillerin ortaya çıkarılması ve açıklanmasına ilişkin özel kurallar var mıdır?

(5) BİT ile ilişkili delillerin değerlendirilmesi (ispat değeri) için özel kurallar var mıdır?

**(F) Duruşma aşamasında BİT**

(1) Mahkemede ICT ile ilişkili deliller nasıl sunulabilir veya sunulmalıdır?

(2) Uzak mesafe sorgulamalarında uydu bağlantıları gibi uygulamalar kullanılabilir mi?

(3) Dijital ve sanal teknikler olayın (ölümler, trafik kazası) canlandırılmasında kullanılabilir mi?

(4) Ses ve görüntü teknikleri duruşmada delil sunmak için kullanılabilir mi? (en basit şekliyle: fotoğraflar ve sesler)

(5) "Yazılı kağıt" halindeki cezai dava dosyaları "elektronik" olanlarla değiştirilebilir mi? Yargılamanın dijitalleştirilmesi yönünde herhangi bir gelişme bulunmakta mıdır?

# EK – BİLGİ TOPLUMU ( BİLGİ TEKNOLOJİSİ DAHİL OLMAK ÜZERE) VE CEZA ADALETİ

**Prof. Dr. Johannes F. Nijboer**

Evan Ratliff, Amerikalı bir gazeteci, dijital dünyanın içinde bir ay boyunca kaybolmayı denedi. Farklı bir kimlikle Birleşik Devletleri gezdi. Bu deney bir yarışma ile bağlantılıydı ve "çevirim içi" olarak kişiler onu bulmaya çalıştı. Bir ay seyahatin sonunda, görünmez olmaya çalışmanın, şu anki toplumumuzda olanaksız olduğu ortaya çıktı. Tamamıyla anonim olmak, dijital izler nedeniyle mümkün değildir. Bu izler, örneğin ödemeleri, seyahat bilgilerini ve iletişimleri içermektedir[1].

**Giriş**

Hazırlık niteliğindeki bu doküman III. Kısım- ceza yargılaması- sorularının oluşmasında yardımcı bir takım gözlem ve düşünceleri içermektedir. Leiden Üniversitesi'nden (Hollanda) Profesör Johannes F. Nijboer tarafından Leiden Üniversitesi'nden Sanne Kruithof''un (MSc) yardımıyla hazırlanmıştır. Metin Uluslararası Ceza Hukuku Derneği'ne (AIDP) Siracusa'daki hazırlık toplantısı için sunulmuştur (3 ve 4 Aralık, 2010). Freibourg im Breisgau'daki raportörlerin toplantısından sonra (20+21 Kasım, 2011) taslak soruların şu anki halinin oluşumunda arka plan belgesi olarak kullanım için gözden geçirilmiştir.

**(A) Bazı genel değerlendirmeler**

Günümüz (post) modern toplumu –diyebiliriz ki- 30 yıl öncekinden önemli ölçüde farklıdır. Bu, göreceli olarak kıt kaynaklarla karşı karşıya olsalar ya da kendi kaynakları dışarıdan sömürüye maruzkalmış olsa bile, çoğu ülke ve bölge için geçerlidir. Çöllerin, açık suların ve yağmur ormanlarının ortasında olsa bile

1 <http://www.wired.com/vanish/2009/11/ff_vanish2/> <http://www.marketingfacts.nl/berichten/20100923_picnic10_evan_ratliff_wired_over_digitaal_verdwijnen/>

cep telefonları ve internete ulaşılabilmektedir. İleri teknoloji suçlarındaki (siber suç, bilgisayar suçu)[2] hızlı gelişmeler BT (IT) ve BİT'in[3] sınır tanımayan olanaklarıyla ilişkilidir. Fakat aynı şey ceza adaleti sistemi içerisindeki (profesyonel) hareketler, aletler ve araçlar için de geçerlidir. Bugün öyle görünüyor ki, (birçok yargı çevresinde suç niteliği taşıyan) "bilgisayar korsanlığı" (hacking) sorunu polis soruşturmalarında bir bilgi toplama yöntemi olarak meşru olabilmektedir. Hatta bu bilgi delil olarak kullanılabilecek veri bile içerebilmektedir.[4]

Yirminci yüzyılın son yirmi-otuz yılı ve üçüncü milenyumun başlangıcı birçok yeni bulgu ve kavrayışa şahit olmuştur. Bilimsel ve teknolojik bulgular artan bir hızla birbirini izlemiştir. Toplumun neredeyse her alanı BT ve BİT'ten etkilenmiştir. Gelişmelerin nerede durduğunu ya da kesintiye uğradığını anlamak bir yana, nerede başladığını kavramak dahi genellikle zordur. Hem özel alan hem de kamusal alan, bu ikisini birbirinden ayırmayı gittikçe daha da güçleştirecek şekilde, örneğin bireylerin yaşamı ve (sosyal) hayat kavramının kendisi, bunun yanı sıra özel hayatın gerçekliğinin korunması[5] üzerinde derin izler oluşacak biçimde - etkilenmiştir. Ratliff (bkz. yukarıdaki alıntı) özel ve kamusal alanlardaki bu etkiyi –ve bu ikisinin iç içe geçmişliğini ve bunlar arasındaki karşılıklı müdahaleyi ortaya koymaya çalıştı. Bir kişinin bizzat varoluşu, bundan kaçış olmaksızın, birçok şekilde kayıt altına alınabilir, tescillenebilir ve izlenebilir. Özel ve kamusal alanlar üzerindeki etkinin yanı sıra, aynı durum kurumsal anlamda kuruluşların "yaşam"ına etkisi açısından da geçerlidir. Bu, basit gruplardan, cemiyetlerden ve iletişim ağlarından ya da firmalardan; ortaklıkların, çok uluslu teşebbüslerin, sivil toplum kuruluşlarının (STK) vb. uluslararası iletişim ağlarına kadar değişkenlik gösterebilir. Bu gelişmelerin karmaşıklığının bir yanı da, örneğin nanoteknoloji,

2 Bkz. R.C. van der Hulst & R.J.M. Neve, *High-tech crime, soorten criminaliteit en hun daders*, Den Haag: WODC, 2008

3 Özellikle cezai süreç bağlamında, Bilgi Teknolojileri ve Bilgi İletişim Teknolojilerinin birleşimi, bunları birbirinden ayırt etmeyi güçleştirmektedir.

4 Bkz. J.J. Oerlemans, Hacken als opsporingsbevoegdheid, *Delikt en Delinkwent* 2011, p. 888-908.

5 Buna geri döneceğiz.

biyoteknoloji ve bilgi teknolojisinde olduğu gibi, *teknolojilerin yakınsaması* ile ilgilidir.[6] Bunlar olasılıklar ve fırsatlar yaratmaktadırlar: bir taraftan suç faaliyetleri için, diğer taraftan ise buna duyulacak tepkiler için. Suçluluğun, yeni teknolojilerle bağlantılı olan yeni şekilleri, aynı davranış biçimlerine benzer teknik uygulamalar ile soruşturulabilir- ör: internet suçunun internetin kendisi kullanılarak soruşturulması. Fakat geniş anlamda bilim ve tekniğin de geleneksel adalet sistemi üzerinde muazzam bir etkisi olmuştur. Ceza yargılaması için teknolojik gelişmelerin ve yeniliklerin çok esaslı sonuçları vardır. Bu sonuçlar teorik olarak iki gruba ayrılabilir: var olan araçların, usullerin vb. değiştirilmesi, uyarlanması ve bunlara eklemeler yapılması ve buna karşılık (tamamıyla) yeni araçların, usullerin vb. oluşması. İlk gruba örnek olarak kağıt üzerindeki dava dosyalarının elektronik olanlarla yer değiştirmesi ilk gruba bir örnek olarak verilebilecekken, arabaların ve kişilerin izlerini sürmek, yerlerini belirlemek ve bunları takip etmekte kullanılmasıyla, Otomatik Plaka Tanıma Sistemi (ANPR) ikinci gruba örnek olarak verilebilir.[7]

Ceza yargılaması alanında özellikle dikkat çeken teknoloji çeşitleri, kişileri ve hareketleri algılayıp ortaya çıkarabilenler, insan davranışlarını nüfuz altına alabilenler ve olayların canlandırılmasına yardımcı olanlardır. Tekrar her birine bir örnek verilirse: biyolojik izlerin ortaya çıkmasını sağlayan incelikli kimyasal testler (olay yeri incelemesinin bir parçası olarak) ilk gruba, elektronik gizli takip ikinci gruba ve trafik kazalarının bilgisayar canlandırmaları ise üçüncü gruba örnek olacaktır. Uygulama içerisinde, değişik teknolojiler arası sınırları ayırt etmek her zaman kolay olmamaktadır: daha önce de belirtildiği gibi, bir yakınsama söz konusu olacaktır ya da olabilir. "Gerçek" olaylarla yapay olanlar arasındaki sınır dahi belirgin değildir. Bir DNA-parmak izi "gerçek delil" midir? Yoksa insan ürünü olarak adlandırmak daha doğru bir niteleme mi olur? Peki ya çoğu veri ve analizin, sayılar, grafikler ve haritalar için-

6 Bkz. C.J. de Poot, M.P.C. Scheepmaker, Voorwoord, in: *Technology, cognitie en justitie*, Justitiële Verkenningen 2008/1; Boom Juridische Uitgevers, Den Haag, 2008.

7 Cf. J.F. Nijboer, Signalement: Automatic Number Plate Recogniotion (ANPR), *Expertise en Recht* 2011/6 (in print).

birbirine bağlanmış- sekmeler ile karmaşık bir şekilde sunulduğu, ulusal makamlarca yapılan istatiksel bilgiler...[8] Şimdi ise esas metin içerisinde bu sayısız gelişmelerden bir kısmı üzerinde duracağız.

(Post)modern toplum, Bilgi ve İletişim Teknolojilerinin (BİT) çok geniş bir alana yayılmış ulaşılabilirliği ve kullanımı nedeniyle genellikle bir "*bilgi toplumu*" olarak nitelendirilmektedir. Daha önce de belirtildiği gibi BİT'in rolü genel anlamda bilimsel ve teknolojik gelişmelerle yakından ilintilidir. Bu gelişmelerin birkaç tipik özelliği; (a) çok çeşitli uygulamaların global etkisi, (b) art arda hızla gelen yenilikler, (c) neredeyse herkesin günlük işlerindeki köklü değişiklikler, (d) doğal sınırlar, ulusal sınırlardaki değişimin ve zaman ve mekanın limitlerinin aşkın karakteri, (e) doğrudan uygulanabilir kütle verinin ulaşılabilirliği, (f) geleneksel bilgi tekellerinin kayboluşu, (g) farklı bağlamlarda BİT bağlantılı gizli takip cihazlarının kullanılması.

**Kısa bir açıklama:**

a. İç içe geçmiş bilgisayar ağlarının ve kablosuz bağlantıların birlikte kullanılmasıyla sanal olarak her çeşit doğal ya da fiziki sınırlar aşılabilir haldedir. Zaman ve mekan nosyonları göreceli hale gelmiştir. Cezai süreç bağlamında uydu bağlantıları ya da kapalı devre kamera sistemleri (CCTV) yoluyla kişilerin (tanıkların, şüphelilerin) sorguya çekilebileceğini düşünmek artık mümkündür. Bir DNA-veri tabanının kısa bir süre içinde, hatta başka bir ülkede yaşayan kişilerce bile (Avrupa'daki "Prüm Bölgesi" ne dahil ülkeler arasında olduğu gibi[9]) araştırılması mümkündür.[10]

b. Metin detaylandırmak ve depolamak için "disket"lerin kullanılışının bir yenilik olması üzerinden sadece 20 yıl geçmiş bulunuyor. Bugün, bu disketlerin yerini almış olan CD-ROM'ların, DVD'lerin ve USB'lerin hızını düşündüğümüzde ise

8 Bkz. P. van den Hoven, *The rubber bands are broken; opening the 'punctualized' European administration of justice*, .....

9 Avusturya, Benelüks, Fransa, Almanya, İspanya

10 Bkz. G. Vermeulen, *Free gathering and movement of evidence in criminal matters in the EU*, Antwerp: Maklu, 2011.

kendi kendimize gülebiliriz. Zaman zaman bilgi depolamanın fiziksel anlamda bir "kitabınkine" eş değer bir standardizasyon düzeyine ulaşmasının on yıllar süreceği öne sürülüyor[11].

c. İşlerin sonsuz çeşitliliği içinde neredeyse herkes faaliyetlerinde çok geniş kapsamlı değişiklikler yaşadı. İnternetten (bir uçuş için check-in yapmak dahil olmak üzere) ürün ve hizmet satın alıyoruz. Geç kalacağımızı düşündüğümüzde muhataplarımızı arabadan veya trenden bilgilendiriyoruz. Fakat bunun yanında kurumların, devlet daireleri dahil olmak üzere, neredeyse herkes hakkında verilere ulaşımı var. Bu ulaşım imkanı ise kimliklerimizi sahtekarlık girişimlerine karşı savunmasız bırakıyor. Özellikle bilginin hemen o anda taranabilecek şekilde (DNA-veri tabanının çalışma şekli) yığın halinde depolanması, cezai süreç ile ilişkisi açısından, ceza soruşturmasının mahiyeti ve karakterindeki temel değişiklik örneğinde olduğu gibi, özel olarak üzerine eğileceğimiz bir konu. Daha önce bahsedilmiş olan ANPR'nin kullanımı (otomatik "kontrol noktaları"nda araçların kayıtlı geçişi ile birlikte kullanıldığında) da bir örnek oluşturuyor[12]. Ceza duruşmaları bakımından ise- birçok uygulama ve kitlerle bağlantılı - dijital dava dosyalarının da uygulamaya geçmeye başladığına dikkat edilmelidir: çeşitli türlerde sunumlar. ("canlı" sunumlar da dahil görsel - işitsel ve dijital/sanal canlandırmalar vb. ile)

d. Bu noktaya daha önceden değinilmişti. İnsanların ürünlerin ve hizmetlerin ulus aşırı devinimi günlük hayatımızda birçok etkiyle sonuçlanmıştır. Bu devinimin ceza yargılaması sistem(leri) alanında da çok önemli sonuçları vardır. Ancak daha az önemli görünmeye başlayan sadece devlet sınırları değildir – bu konu aynı zamanda doğal ve fiziksel sınırları da ilgilendirmektedir.

---

11 Umberto Eco, Jean-Claude Carrière & Jean-Philippe de Tonnac. *N'espérez pas vous débarrasser des livres*. Grasset & Fasquelle 2009.

12 Peki ya Hollanda'da çipli toplu taşıma kartlarını yöneten (özel) kurumların veri tabanları? Ya da o hizmetlerin sağlayıcılarınca tutulan cep telefonu ve internet trafiğinin veri tabanları?

e. DNA-veri tabanları için az önce söylendiği gibi, muazzam miktarda bilginin de genel olarak doğrudan kullanıma açık olduğu söylenebilir. Google gibi "mekanizmalar"la internet aramalarını düşünün. Bu tip genel kamuya ulaşılabilirliğin dışında, birçok özel veri tabanları ve bilgi içeren diğer "şeyler" de – en çok ticari alanda olmakla beraber aynı zamanda (yine) ceza yargılaması sistemi gibi diğer alanlarda da – bulunmaktadır.

f. Bu daha karmaşık bir meseledir. Yeni pazarlar elbette var olan eski pazar dengelerini bozabilmektedir. (ör: bütün bir kitap içeriğinin internette ulaşılabilir olması). Geleneksel olarak devlet işleyişi dahilinde türlü konular genel olarak devlet tekellerinin parçasıdır. Cezai süreç safhaları da bunlardan bir tanesidir. Bu alanda araştırmacı gazetecilikten adli tıp uzmanlıklarının "serbest piyasa"sına kadar çeşitli meseleler ortaya çıkmaktadır. Özellikle bilim ve patentli teknolojiler alanında sanayi ve özel kuruluşların yanı sıra devlet arasında çok karmaşık karşılıklı iç ilişkiler gözlemleyebiliriz (yine yakınsayan teknolojiler burada örnek olabilir). Biraz mübalağa ile Soğuk Savaş zamanındaki "askeri-sanayi tesisleri" ile günün "adli-sanayi tesisleri" arasında bir karşılaştırma yapabiliriz.

g. Günümüz yaşantısının bir başka özelliği ise takip araçlarının kullanımıdır. Fiziksel dünyada; benzin istasyonlarında, alışveriş merkezlerinde ya da sokaklardaki, eğlence parklarında, otobüslerde, tramvaylarda, metrolarda, trenlerde, vapurlarda ve son fakat bir o kadar da önemli olarak marketlerde ve otel koridorlarında (IMF Başkanı Dominique Straus-Kahn'ın New York'ta deneyimlediği gibi) kamera takibi şeklinde görüyoruz. Ancak cep telefonları ve internet kullanımı da aynı şekilde takip altında olabiliyor: Bugün Hollanda'da iki telefon şirketi (KPN ve Telfort) tarafından kullanılan ileri teknoloji içeren denetim yöntemlerinin yasallığı üzerinde tartışılmakta. Tartışma konusu bu yöntemlerin sadece devletin soruşturma ve güvenlik otoriteleri tarafından kullanılması söz konusu olduğunda ancak yasal olup olmayacağı yönündeyken; söz

konusu şirketler, müşterilerinin haberleşme faaliyetlerinin içeriğine değil, sadece kullanım tiplerine baktıklarını iddia ediyorlar.

Daha önce bahsi geçen, sağlayıcılar tarafından ya da toplu taşımada kullanılan çipli kartlarda söz konusu olduğu gibi çiplerde bilgi depolanması da yine ilgi çekici bir husus. Bir kullanıcının son bir ayda hatta daha da geriye giderek, yaptığı yolculukların genel bir özetine erişmek genellikle oldukça kolay.

**(B) Ceza Muhakemesi**

Ceza adaleti sisteminin temel faaliyetlerinden biri, suç ve ceza ile bağlantısıyla, *maddi gerçeği araştırma ve delillerdir.* Birçok klasik suçun modern teknolojilerin yardımıyla da işlenebileceği göz önünde bulundurulmalıdır ancak göreceli olarak daha yeni, doğası gereği bu tekniklerle bağlantılı suç tipleri de bulunmaktadır. Usulî bakış açısından bu önemlidir çünkü soruşturmanın en başından itibaren "investigandum" ve "probandum"u (soruşturma ve ispat faaliyetlerini) belirleyen maddi ceza hukukudur (Daha sonra göreceğimiz üzere, kalsik anlamda soruşturma kavramı da tartışmalı bir hale gelmiştir.) Suçluluğun yeni çeşitlerinin yeni soruşturma araçları ve yöntemleri gerektirdiği açıktır. Bu durum özellikle BİT suçlarında (siber suçlar[13]) geçerlidir.

Fakat, özellikle belirli veri tabanları ile ilişkili olarak daha fazlası söz konusudur. Polis, savcılık, hakimler, savunma, bunların hepsi bilgi toplumu içinde faaliyet göstermekte, imkan ve fırsatlarını son haddine kadar kullanmaktadırlar. Cezai süreç bağlamında ilgimizin odağı, sürecin erken safhalarında bilgi toplumunun etkisi olacaksa da mahkumiyet ve (özellikle) hapis cezalarının infazı alanında da uygulamalı veri tabanlarının kullanıldığı akılda tutulmalıdır. Hollanda'da, hükmedilen yaptırımlar üzerine olan veri taban(lar)ı ile ilgili durum budur ("hüküm verme").

Özellikle BİT dünyasında bazen başka tekniklerle de birlikte (DNA-veri tabanları gibi) kullanılan yeni tekniklerin ulaşılabilirliği

13 Bkz. U. Sieber, Mastering complexity in the global cyberspace, in M. Delmas-Marty et al. (eds.), *Les chemins de l'harmonisation penale*, Paris 2008, p. 127-202.

ceza adaleti sisteminde en başta gelen süreci önemli ölçüde değiştirdi. Bir taraftan ceza yargılaması sistemi günlük süreçlerde yeni (BİT) ulaşılabilir teknolojileri kullanmaktadır. Geleneksel kıta sisteminden birçok ülkede kağıt dava dosyaların rolünü ele alırsak: birçok bilgi akışı yüksek hızda elektronik sistemlerle yönlendiriliyor. Modern duruşma salonları genellikle zengin çeşitlerle BİT aletleri ile donatılmış halde. Bir tanığın ya da sanığın vasıtasız olarak sorgulanması için uydu bağlantısı yoluyla canlı uzak mesafe görüşmelerinin yapılması artık sıra dışı bir durum olmaktan çıktı. Öte yandan yeni teknikler sorgulamayı ve delillerin toplanmasını (özellikle sürecin ilk aşamalarında ya da geniş anlamda, yargılama öncesi dönemde de) etkiliyor. Bu konuya bir sonraki paragrafta geri döneceğiz.

**(C) İstihbarat ve delil**

Son yirmi-otuz yıldır polisin ve/veya savcılığın kullanabildiği stratejik ya da taktiksel bilgi ve delil olarak kullanılabilecek bilginin ayrımını yapmak sıra dışı bir olay değil. İlk tipteki bilgi, soruşturma için "yönlendirici" bilgidir. Çoğunlukla kullanılan niteleme ise "istihbarat"tır. Bu tip bilgiler somut olaylarda hiçbir zaman tamamen açıklanmaz. Uzun bir süre boyunca istihbarat ve delil arasındaki ayırım Anglosakson hukuk sistemini esas alan devletlerde ağırlıklı olarak uygulanmaktaydı. Günümüzde, Anglosakson sistemi dışındaki hukuk sistemlerini benimsemiş ülkelerde de ulaşılabilirliği ve uygulaması oldukça genişlemiştir. (Yeri gelmişken bu durum, Anglosakson Hukukunda, bu bağlam içinde, delilin "kabul edilebilirliği" kavramının bu sistemi benimsememiş yargı alanlarında verimli olup olmayacağı sorusunun sorulmasına zemin hazırlar niteliktedir)

Belli başlı birtakım uzmanlık alanlarıyla birlikte kullanıldığında "adli istihbarat"ın varlığı bile üzerinde tartışma yaratan bir mesele olmaktadır. Bu bağlamda farklı veri tabanlarından elde edilmiş bilgilerin birlikte kullanılması düşünülebilir (DNA-profilleri, banka şubelerinden ya da vergi dairelerinden finansal veriler, seyahat verileri, plaka numaraları, parmak izleri). Organize suç ve terör dosyalarının soruşturulmasıyla bağlantılı olarak klasik polis faaliyetleri ile gizli istihbarat teşkilatları ve diğer istihbarat teşkilatlarının faaliyetleri

arasındaki sınırlar belirsizleşmeye başlamıştır. Aynı durum ulusal sınırlar ötesiyle bilgi paylaşımında da geçerlidir. AB dahilinde giderek artan sayıda ülkede, "Prüm Anlaşması" (Treaty of Prüm) (ve anlaşmanın kapsamını genişleten sonraki AB düzenlemeleri) esaslarına göre ülkelerin adli DNA-veri tabanları arasında kurulmuş bağlantı ulus aşırı günlük bilgi değişiminin dikkat çekici bir örneğidir.

Muazzam miktarda işletimsel bilginin bulunması ve kullanılması, kimi zaman soruşturma ve savcılık güçlerinin "bilgi istihbaratı pozisyonu" olarak anılır. Bu bakış açısıyla Hollanda Başsavcısının bir televizyon röportajında Hollanda savcılık teşkilatının "bilgi istihbaratı pozisyonunun" (aşağı yukarı son on yılda organize suçlar bakımından çok daha iyi bir duruma geldiğini; ancak bütçe kesintilerinin, ceza soruşturmasının başlatılmasını bile zorlaştıracak seviyeye ulaştığını belirtmesi çarpıcıdır (Bilinen suçların aşağı yukarı %25'inden bahsetmiştir).

Esasen bu, açıkça bir cezai sürece dahil edilenler dışında, bir bilgi veyahut bir "istihbarat" dünyasının mevcut olduğu anlamına geliyor. Durumun diğer alanlarda çok daha farklı olabileceğini düşündürecek a priori bir gerekçe yer almıyor: sadece birçok verinin ulaşılabilir olduğu gerçeği bile tek başına klasik soruşturma tablosunu değiştirmekte. Bir soruşturma genelde daha önce elde olan bir bilgi üzerinden yola çıkılarak başlayacaktır. Bu nedenle somut bir olayda harekete geçme kararının kendisi geleneksel olmanın ötesinde, öyle görünüyor ki bir tercih meselesidir. Yapılan bu tercihler de iktidarların bilinçli politikaları olarak algılanabilir. Teknolojinin ve görece yeni tekniklerin polis tarafından, fakat aynı zamanda özel güvenlik şirketleri gibi taraflarca da kullanılması, eskiye oranla, polis ve diğer soruşturma ve istihbarat teşkilatlarının "bilgi istihbaratı pozisyonu"nu etkilemektedir. Teknolojinin somut ceza soruşturmalarının "başlangıcını" oldukça etkilediği ihtimali gerçeğe dönüşmektedir. Teknolojinin kullanımıyla insanları ya da grupları izlemek ve suç teşkil eden fiilleri, hem de henüz fiiller gerçekleşmeden ortaya çıkarmak mümkün olmaktadır. Eskiden, en azından daha klasik bir bakış açısıyla, suç hareketlerinin- suç teşkil eden fiillerin kendisi soruşturmanın başlangıç noktasıydı. "Tepki" (reaktivite) git gide çekilip "önleme"ye-(pro-aktivite) yer açmaktadır.

Teknolojinin (klasik) polis faaliyeti üzerindeki etkisi dışında, teknolojinin kullanımının kamusal alanda da sonuçları olmaktadır. Diğerlerinin yanında Nunn[14], polis ve özel güvenlik firmaları gibi diğer teşkilatların – sözde – "izleme mekanizmaları"na dönüştüğünü ifade etmektedir. Envai çeşit (izleme) tekniğin(in) kullanımı özel hayat üzerine tartışmaları körüklemektedir. Bu noktaya daha sonra geri döneceğiz. Burada gözetim toplumu ve gözetim devleti nosyonları geçerlidir.

**(D) Bilgi kaynakları (istihbarat)**

Ceza adaleti amaçları için gerekli bilginin birçok davada açık kaynaklardan elde edildiği göz ardı edilmemelidir. Özellikle BİT hakim bir roldedir. İnternet büyük bir (açık) bilgi kaynağıdır, internet araştırması birçok dava için olağan bir araç haline gelmiştir. İnternette bulunabilecek bilginin yanı sıra, bir başka araç, sivil halk tarafından toplanmış bilgidir. Polisin halktan, bir olayın kendi cep telefonları ile çektikleri fotoğraf ve videolarını yüklemelerini talep etmesi Hollanda'da yeni bir araç olarak kullanılmaktadır.

Daha açık kaynaklardan edinilen bilginin yanı sıra, soruşturma güçleri tarafından daha kapalı devlet kaynaklarından ya da sivil kaynaklardan edinilmiş bilginin kullanılması da sık sık mümkün olmaktadır. yine daha önce bahsi geçmiş olan, ulaşım kartlarındaki çiplerden ya da veri tabanlarında kayıtlı telekomünikasyon verilerinden edinilmiş bilgiler bunlara örnektir. Burada altı çizilmesi gereken bir nokta şudur ki birçok ülkede verilerin toplanıp saklanmasını ve ceza makamlarına ulaşılabilir kılınmasını kural altına alan bir düzenleme yığını bulunmaktadır. Anti-terör yasalarının işlerin bu hale gelmesine çok büyük oranda katkıda bulunduğu pekala bilinmektedir.[15]

Teknolojinin gelişimi nedeniyle, soruşturma araçlarında da gelişimler olmuştur. Bir kısmına daha önce değinildi. Daha önce de belirtildiği gibi teknolojilerin gelişiminin özelliklerinden biri

14 Nunn (2001), 'Police technology in cities – changes and challenges', Technology in Society 23, 11-27.

15 A. Oehmichen, *Terrorism and anti-terror legislation - the terrorised legislator? A comparison of counter-terrorism legislation*

süregelmiş bilgi tekellerinin kaybolmasıdır. Bu tekel kayboluşu karşılıklıdır; bir taraftan bilgi daha "açık kaynaklardan", çoğunlukla internetten, elde edilebilmektedir; diğer taraftan ise soruşturma-araştırma araçları artık sadece devlet (polis) elinde değil, aynı zamanda, esas olarak özel güvenlik şirketleri olmak üzere, özel tarafların da ulaşımına açıktır. Bu şirketlerin varlığının sebebi teknolojik gelişmeler değildir. Bunların geçmişi loncaların varlığına kadar uzanır. Refah toplumunun yükselişi ile (20. yüzyılda uzun bir süreç içinde), devlet tekeli, soruşturma ve güvenlik alanlarını da kapsayacak şekilde genişledi. Son zamanlarda refah devleti, onu takiben devlet tekelleri azalmaktadır. Bu gelişme örneğin özel güvenlik şirketleri için birçok imkan sağladı. Bu tür iç ilişkiler, devletin, bilgi teknolojilerinin (BT) ve bilgi ve iletişim teknolojilerinin (BİT) başlıca örgütsel temeli oluşturduğu bir iletişim ağı devletine dönüştüğü fikriyle oldukça uyuşmaktadır.

**(E) Medyanın rolü**

Birçok bilginin açık kaynaklardan geldiği gerçeği üzerinde daha önce durduk. Bu tip kaynakların ulaşılabilirliği yayıncıların, sağlayıcıların vb. aktiviteleri ile ilişkilidir. Daha geniş bir perspektiften bakıldığında medyanın rolünü gözden kaçırmamanın da önemli olduğu anlaşılmaktadır. Günümüzde araştırmacı gazetecilik yaygın bir fenomen haline gelmiştir.

**(F) İnsan hakları ve temel özgürlükler**

Toplumsal değişimlerin ve ceza yargılama sistemi işleyişinde, buna bağlı olarak meydana gelen değişikliklerin insan hakları ve temel özgürlükler alanında birçok yeni sorun ve soruyu da beraberinde getirdiği inkar edilemez. Adli DNA-veri tabanlarına dahil edilmek üzere, DNA-profilleri oluşturmak için şüpheli veya diğer kişilerden biyolojik numunelerin alındığı koşulları düşünün, ya da özel görüşmelerin dinlenmesi amacıyla donanımlara başvurulduğunu.

Ceza muhakemesi kanunları geleneksel olarak, kamu ve devlet çıkarları doğrultusunda, sivil özgürlüklere getirilen (gerekli) kısıtlamalar ile insan hakları arasındaki dengeyi sağlamaktadır. İnsan

Hakları Mahkemelerinin pek çok içtihadı, örneğin Avrupa İnsan Hakları Mahkemesi (AİHM) gibi, bu tür sorunlarla ilgilidir. Konunun detaylandırılmasında "Bilgi Toplumu ve Ceza Muhakemesi" alanı özellikle dikkate alınmalıdır. Son yirmi-otuz yılda çoğu ülke güvenlik ve terör ve organize suçlara mücadele nedeniyle yürürlükteki yasaları özel hayat ve bedensel özgürlük gibi temel hakları zaman zaman son derece kısıtlayacak bir biçimde katılaştırmıştır. Bu alanda literatürde hem İnsan Hakları hem de Ceza Muhakemesi bakış açılarından artan bir ilgi söz konusudur. İnsan hakları alanında, ceza muhakemesinin ulusal yönleri ile uluslar arası (küresel ve bölgesel) yönleri iç içedir. Bundan dolayı, AIDP'nin çalışmalarında III. ve IV. Bölümlerindeki sorular ve raporlarla incelenmiş alana yakından bakmakta fayda vardır.

**(G) Birkaç kapanış uyarısı**

"Bilgi toplumunun" cezai sürece etkisi hakkında – özellikle BİT ve yakınsayan tekniklere ilişkin olarak- söylenecek çok daha fazla şey olduğunu belirtmeye gerek yoktur. Burada sadece fotoğraf veri tabanları üzerinden yüz tanımadaki gelişmelerden ve gözetleme kameralarının kullanımına değinilmiştir. Değişik kaynaklardan elde edilen bilgilerin birlikte kullanılması sebebiyle izleme alanında meydana gelen yanlış tanıma ya da teşhisler de dikkat çekilmesi gereken başka bir önemli noktadır. Buna, adli tıp alanında DNA veri tabanında tesadüfi eşleşmeler ya da adli tıp numunelerinin gözetim altında iken değişmesi ya da bozulması (ve bu tarz bir riski sınırlamak için kullanılan "takip ve izleme" sistemlerinin kullanılması) sebebiyle meydana gelen (sadece ilk bakışta) "basit" hata payları da eklenebilir. Bu olaylar incelendiğinde ise neredeyse her seferinde de BİT ile ilişkili en az bir ya da iki bağlantının varlığı görülmektedir.

Daha dışarıdan bir bakış açısıyla, "gözetim devleti", "istihbarat devleti" ve "veri tabanı devleti" ile bağlantılı olarak bilgi toplumunun, geleneksel cezai sürecin tüm temelini başından itibaren ve odak noktası da dahil olmak üzere; "investigandum" (soruşturma) ve "probandum"un (ispat faaliyetleri), dar anlamıyla suç oluşturan davranış üzerinden değil de, daha çok sapkın (ve riskli?) davranış üzerinden yürütüldüğü bir şekilde, değiştirip değiştirmediği sorusunun sorulması faydalı olacaktır.

*Hazırlık Kollokyumu Bölüm III*

# TÜRKİYE ULUSAL GRUP RAPORU

**Prof. Dr. Serap Keskin Kiziroğlu***
**Ar. Gör. Fulya Eroğlu****
**Ar. Gör. İlker Tepe*****

## (B) Genel Sorular

**(1) Ceza muhakemesi usulü bağlamında (adli tıbbı da içerecek şekilde) BT ve BIT uygulamaları için kullanılan güncel (hukuki veya sosyo-hukuki) tanımlar var mıdır? Cezai süreç bağlamında bu gibi kavramsal tanımlar literatüre, mevzuata, mahkeme kararlarına ve ilgili uygulamalara nasıl yansımaktadırlar?**

TCK m. 243'ün (Bilişim Sistemine Girme Suçu) metninde bir bilişim sistemi tanımı yapılmamış olsa bile madde gerekçesinde bilişim sistemi şöyle tanımlanmıştır: *"Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir."*

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun m. 2'de;

Bilgi: Verilerin anlam kazanmış biçimini,

Erişim: Bir internet ortamına bağlanarak kullanım olanağı kazanılmasını,

Erişim sağlayıcı: Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri,

İçerik sağlayıcı: İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri,

* İstanbul Okan Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı.

** Yeditepe Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı.

*** Dokuz Eylül Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı.

İnternet ortamı: Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortamı,

İnternet ortamında yapılan yayın: İnternet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği verileri,

İzleme: İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesini,

Kurum: Telekomünikasyon Kurumunu,

Toplu kullanım sağlayıcı: Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı,

Trafik bilgisi: İnternet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerleri,

Veri: Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri,

Yayın: İnternet ortamında yapılan yayını,

Yer sağlayıcı: Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri, ifade eder.

Ceza Muhakemesinde Ses ve Görüntü Bilişim sistemlerinin Kullanılması Hakkında Yönetmelik m. 3'de;

Bilişim sistemi: Bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistemi,

SEGBİS: UYAP Bilişim Sisteminde ses ve görüntünün aynı anda elektronik ortamda iletildiği, kaydedildiği ve saklandığı Ses ve Görüntü Bilişim Sistemini,

UYAP Bilişim Sistemi: Adalet hizmetlerinin elektronik ortamda yürütülmesi amacıyla oluşturulan bilişim sistemini, ifade eder.

Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik[1] m. 4'de (BİT anlamında):

1 Danıştay İdari Dava Daireleri Kurulu'nun kararıyla yürütmesi durdurulmuştur.(YD.İtiraz No:2012/578 Tarih.06.12.2012)

İletişimin dinlenmesi ve kayda alınması: Telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmaların dinlenmesi ve kayda alınması ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi ve kayda alınmasına yönelik işlemleri,

İletişimin tespiti: İletişimin içeriğine müdahale etmeden, iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemleri,

İşletmeci: Türk Telekomünikasyon Anonim Şirketi de dâhil olmak üzere, Telekomünikasyon Kurumu ile yapılan görev sözleşmesi, imtiyaz sözleşmesi, bu Kurumdan alınan telekomünikasyon ruhsatı veya genel izin uyarınca telekomünikasyon hizmetleri yürüten ve telekomünikasyon alt yapısı işleten şirketleri,

Sinyal bilgisi: Bir şebekede haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veriyi,

Sinyal bilgilerinin değerlendirilmesi: İletişimin içeriğine müdahale niteliğinde olmayıp yetkili makamdan alınan karar kapsamında sinyal bilgilerinin iletişim sistemleri üzerinde bıraktığı izlerin tespit edilerek, bunlardan anlamlandırılan sonuçlar çıkarmak üzere gerçekleştirilen değerlendirme işlemlerini,

Telekomünikasyon: İşaret, sembol, ses ve görüntü ile elektrik sinyallerine dönüştürülebilen her türlü verinin; kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektro kimyasal, elektro mekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınmasını,

Teknik araçlarla izleme: Ceza Muhakemesi Kanununun 140 ıncı maddesinin birinci fıkrasında sayılan suçlar dolayısıyla yapılan soruşturmalarda, suçun işlendiğine ilişkin kuvvetli şüphe sebeplerinin bulunması ve başka suretle delil elde edilememesi hâlinde şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyerinin teknik araçlarla izlenmesi, ses veya görüntü kaydının alınması işlemini,

Veri taşıyıcısı: İletişimin tespiti, dinlenmesi ve kayda alınması, gizli soruşturmacı ve teknik araçlarla izleme tedbirlerinin uygulan-

ması neticesinde elde edilecek ses ve görüntü bilgilerinin kaydedileceği araçları, ifade eder.

Yargıtay uygulamalarında TCK m. 243'ün gerekçesinde yer alan tanımın esas alındığı bilinmektedir:[2]

*"Bilişim sistemi; verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemler olup, ... (Yargıtay 11 CD, 23.03.2009, E: 2008/16004 - K. 2009/2891)"*

*"Bilişim sisteminden amaç, verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma olanağını veren manyetik sistemlerdir. Bilişim alanı ise, bilgileri depo ettikten sonra bunları otomatik olarak işleme tabi tutan sistemlerden oluşan alanlardır... ( Yargıtay CGK, 17.11.2009, E: 2009/11- 193 – K: 2009/268)"*

**(2) Ceza adaleti sistemi içinde bilgi BİT'in yürütülmesinden sorumlu belirli kurumlar ve/veya görevli birimler var mıdır?**

Bilgi Teknolojileri ve İletişim Kurumu: Telekomünikasyon sektörünü düzenleme ve denetleme fonksiyonunun bağımsız bir idari otorite tarafından yürütülmesi amacıyla 27.1.2000 tarihli ve 4502 sayılı Kanunla kurulan Telekomünikasyon Kurumu, 10.11.2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu ile yeni bir düzenlemeye tabi olmuş ve adı Bilgi Teknolojileri ve İletişim Kurumu olarak değiştirilmiştir. 2813 sayılı Telsiz Kanunu yeni bir düzenleme ile Kanunun adı Bilgi Teknolojileri ve İletişim Kurumunun Kuruluşuna İlişkin Kanunu olarak değiştirilmiştir.

Telekomünikasyon İletişim Başkanlığı: 23.07.2005 tarihli Resmi Gazetede yayımlanarak yürürlüğe giren 5397 sayılı Kanun ile kurulmuş olup, 23 Temmuz 2006 tarihinden itibaren ilgili mevzuatın ön-

2 TCHD üyelerimizden Yargıtay Cumhuriyet Savcısı Dr. İhsan Baştürk, konuya ilişkin göndermiş olduğu bir e-posta ile, bizim de katıldığımız şu tespitlerde bulunmuştur: Türk hukukunda, "internet", "internet ortamı", "web sayfası", "web sitesi", "yayın", "İnternet Servis Sağlayıcı (İSS)" ve "erişim sağlayıcı" sözcükleri sorunlara yol açabilecek şekilde, terminoloji birliği sağlanmadan kullanılmaktadır. Ayrıca "bilgisayar kütüklerinde aramayı" düzenleyen CMK 134. maddesinde yer verilmeyen, "diğer uzak bilgisayar kütükleri ve çıkarılabilir donanımlar" gibi kavramlara Adli ve Önleme Aramaları Yönetmeliğinde yer verilmiş olması, mahkemelerin konuya ilişkin farklı kararlar vermesine neden olmaktadır.

gördüğü iş ve işlemleri tek merkezden yürütmektedir.

23.05.2007 tarihli Resmi Gazetede yayımlanan 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile Telekomünikasyon İletişim Başkanlığı'nın Kanunda sayılan İnternete ilişkin görevleri de yapması düzenlenmiştir. Bu doğrultuda anılan görevleri yerine getirmek üzere İnternet Daire Başkanlığı kurulmuştur.

Başkanlık, Bilgi Teknolojileri ve İletişim Kurumu bünyesinde doğrudan Kurum Başkanına bağlı olarak faaliyet göstermekte olup, Telekomünikasyon İletişim Başkanı ile Hukuk, Teknik İşletme, Bilgi Sistemleri, İdari ve İnternet Daire Başkanlıklarından oluşmaktadır. Başkanlıkta, Millî İstihbarat Teşkilatı Müsteşarlığı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığının ilgili birimlerinden birer temsilci bulunmaktadır.

Adalet Bakanlığı Bilgi İşlem Dairesi: Bakanlık'ta ilk otomasyon çalışmalarına 1998 yılında başlanmıştır. Çalışmaların sistemli ve planlı bir şekilde yürütülmesi amacıyla 1999 yılında Bilgi İşlem Dairesi Başkanlığı kurulmuştur. 15/05/2001 tarih ve 4674 Sayılı Kanunun 7. maddesi ile eklenen 2992 Sayılı Kanunun 22/A maddesinde, Bilgi İşlem Dairesi Başkanlığının görevleri belirtilmiştir.

Bunların yanında Türkiye'de görev yapan diğer birimler şu şekilde sıralanabilir:

Emniyet Genel Müdürlüğü Bilişim Suçlarıyla Mücadele Daire Başkanlığı: Bilişim teknolojileri kullanılarak işlenen suçların soruşturulması ve dijital delillerin incelenmesi için destek veren görevli daire başkanlıklarının ve taşra teşkilatındaki birimlerin dağınık yapısının tek bir çatı altında toplanmasını, mükerrer yatırımların önüne geçilmesini, bilişim suçlarıyla mücadelenin etkin ve verimli olarak yürütülmesini sağlamak amacıyla 2011/2025 sayılı Bakanlar Kurulu Kararı ile Emniyet Genel Müdürlüğü bünyesinde Bilişim Suçlarıyla Mücadele Daire Başkanlığı kurulmuştur. Bilişim Suçlarıyla Mücadele Daire Başkanlığı merkez ve il birimlerinin kurulumunun tamamlanmasına yönelik çalışmalarına hızla devam edilmektedir.

Jandarma Kriminal Daire Başkanlığı Bilişim Teknolojileri İnceleme Labratuvar Amirliği: Görevi, idarî ve adlî soruşturmalar ile adlî kovuşturmalarda; uzmanlık alanına giren konularla ilgili elde edilen ve ilgili hakim veya mahkeme, gecikmesinde sakıncası bulunan hallerde Cumhuriyet savcısının kararı üzerine gönderilen bulguların bilimsel usullerle inceleme ve değerlendirmesini yaparak rapor tanzim etmektir.

Adli Tıp Kurumu Fizik İhtisas Dairesi: Mahkemeler ile hakimlikler ve savcılıklar tarafından gönderilen silah, mermi, yazı (grafolojik - daktiloskopik), fotoğraf, resim, imza, imza niteliğini taşıyan parmak izleri ile radyolojik, radyoizotop, klimatolojik, diğer fiziksel materyal ve olaylarla ilgili olarak incelemeler yaparak sonucunu bir raporla tespit eder.

Fizik ihtisas dairesi altında, dijital verilerin incelenmesi ile ilgilenen bir "Bilişim ve Teknoloji Suçları Şubesi" bulunmaktadır.

**(3) Ceza adaleti sistemine BİT ile ilişkili hizmetler sunan özel (ticari) kuruluşlar (şirketler) var mıdır? Eğer varsa, bunlara örnek verebilir misiniz? Ne gibi sınırlara uyulması gerekmektedir?**

Ceza adaleti sistemine BİT ile ilişkili hizmetler sunan özel (ticari) kuruluşlar (şirketler) bulunmamaktadır. Ancak CMK uyarınca gerçek ya da tüzel kişilerin uzman mütalaasına başvurmak mümkündür.

**(C) Bilgi ve İstihbarat: Kanun uygulayıcı makamlar için bilgi istihbaratı pozisyonları[3] oluşturma**

**(1) BİT'le bağlantılı hangi teknikler kanun uygulayıcı makamlara yönelik bilgi istihbaratı pozisyonları oluşturmak için kullanılmaktadır?**

Bilgi İstihbaratı Pozisyonları oluşturmak için iletişimin tespiti, dinlenmesi, kaydı ve sinyal bilgilerinin değerlendirilmesi, optik ve

3 Bilgi istihbaratı pozisyonları oluşturma, istihbarat-odaklı-polis faaliyeti (ILP) olarak adlandırılan olgunun bir parçasıdır. ILP kanun uygulayıcı makamların önleyici ve bastırıcı görevlerini gerçekleştirmelerine imkan veren bir bilgi-düzenleme süreci olarak yürütülen polislik faaliyetlerinin kavramsal çerçevesi olarak ifade edilebilir.

akustik teknik araçlarla izleme, bunların kaydedileceği veri taşıyıcıları, fizik kimliğin tespiti kapsamında parmak izi, avuç içi izi, fotoğraf gibi verilerin alınması ve ilgili veri tabanlarına depolanması söz konusu olmaktadır.

Bu bağlamda, PVSK Ek madde 7 ve Jandarma Teşkilat, Görev ve Yetkileri Kanunu Ek madde 5'te, kolluk görevlilerinin istihbarat faaliyetlerinde, casusluk suçları hariç olmak üzere TMK m. 10 kapsamına giren suçların önlenmesi amacıyla iletişimin denetlenmesi ve teknik araçla izleme tedbirlerine başvurabilecekleri düzenlenmektedir. Ayrıca Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nun (MİT Kanunu) 6. maddesinde de, Anayasa'da belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde, Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesine ilişkin olarak, telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabileceği belirtilmektedir.

Ayrıca kanun uygulayıcı makamlara yönelik bilgi istihbaratı pozisyonları oluşturmak için ise şu tekniklere başvurulduğu bilinmektedir: imaj alma, silinen dosyaları elde etme (geri kazanma), kelime listesi oluşturma, kelime araması yapma, şifre elde etme, registry (kütük kayıtları) inceleme, metadata (üst veri) inceleme.

**(2) Kanun uygulayıcı makamların hangi tür kamusal (örn: DNA veritabanları) ya da özel (örn: Yolcu isim kaydı (PNR) verileri ya da SWIFT verileri gibi finansal veriler) veri tabanlarına erişimi mümkündür?**

CMK'nın 332. maddesi cumhuriyet savcılarına, hakim veya mahkemelere her türlü bilgiyi her türlü kurumdan istemek yetkisini veren bir madde görünümündedir. Bu maddeye göre, suçların soruşturulması ve kovuşturulması sırasında cumhuriyet savcısı, hakim veya mahkeme tarafından yazılı olarak istenilen bilgilere on gün içinde cevap verilmesi zorunludur. Bu süre içinde cevap verilmesi imkansız ise, sebebinin ve en geç hangi tarihte cevap verilebileceğinin aynı sürede bildirilmesi gerekmektedir.

Türk Hukukunda kişisel verilerin korunmasına ilişkin bir kanun da henüz bulunmamaktadır. Bu konuda Kişisel Verilen Korunması Kanunu Tasarısı bulunmakla birlikte bu tasarı henüz kanunlaşmamıştır. Bu nedenle verilere ulaşılması konusu, TCK'da özel hayatın gizliliğini ve kişisel verileri koruyan bazı suç tipleri de göz önüne alındığında tartışma konusu olmuştur. Kamusal olarak ulaşılabilecek tartışmasız tek veri Adli Sicil Kanunu çerçevesinde tutulan adli sicillerdir.

Türkiye'de henüz bir DNA veri tabanı yoktur. Konuya ilişkin bir kanun tasarısı bulunmakla birlikte, bu tasarı henüz kanunlaşmamıştır.

Türkiye'de mevcut veri tabanları şu şekilde sıralanabilir: PVSK kapsamında parmak izleri ve fotoğrafların kayıt altına alındığı bir veri tabanı bulunmaktadır. Buraya PVSK m. 5/1 kapsamında sayılmış kişilerden alınan parmak izleri ve fotoğraflar, olay yerinden elde edilen ve kime ait olduğu henüz tespit edilmemiş olan parmak izleri, kimliği belirlenmek istenen ancak nüfusa kayıtlı olmadığı için kimliği tespit edilemeyen kişilerin parmak izleri ve fotoğrafları ile CGİK m. 21'e göre hükümlülerden alınan parmak izleri kaydedilir. Ayrıca PVSK 4/A maddesi uyarınca, kendisinden kimlik ibrazı istenmesine rağmen, nüfusa kayıtlı olmadığı için kimliği tespit edilemeyen kişilerin nüfusa kayıtları için gerekli işlemler yapıldıktan sonra, PVSK m. 5'e göre fotoğraf ve parmak izi tespit edilerek kayda alınır.

PVSK'nın 5. maddesine göre parmak izi ve fotoğraflar bu amaca özgü sisteme kaydedilerek saklanır; ancak hangi sebeple alındığı sisteme kaydedilmez. Bu sistemde yer alan bilgiler, kimlik tespiti, suçun önlenmesi veya yürütülmekte olan soruşturma ve kovuşturma kapsamında maddi gerçeğin ortaya çıkarılması amacıyla mahkeme, hakim cumhuriyet savcısı ve kolluk tarafından kullanılabilir. Kolluk birimleri kimlik tespiti yapmak ya da olay yerinden alınan parmak izlerini karşılaştırmak amacıyla doğrudan bu sistemle bağlantı kurabilir. Sistemde kayıtlı bilgilerin hangi kamu görevlisi tarafından ve ne amaçla kullanıldığının denetlenmesine imkan tanıyan bir güvenlik sistemi kurulur. Sistemde yer alan kayıtlar gizlidir; kişinin ölümünde itibaren on yıl her halde kayıttan itibaren seksen yıl geçtikten sonra silinir.

Ayrıca Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun'un 18/4. maddesine göre, koruma tedbiri olarak uygulanan ve güvenlik tedbiri olarak hükmedilen spor müsabakalarını seyirden yasaklama tedbirine ilişkin bilgiler Emniyet Genel Müdürlüğü bünyesinde tutulan bu amaca özgü elektronik bilgi bankasına derhal kaydedilir. Bu bilgi bankasına spor kulüplerinin ve federasyonların erişimi sağlanır. Yasaklanan kişilere ilişkin bilgiler, ilgili spor kulüplerine ve yurt dışında yapılacak müsabaka öncesinde müsabakanın yapılacağı ülkenin yetkili mercilerine bildirilir.

Bir diğer veri tabanı ise Türk Silahlı Kuvvetleri İç Hizmet Kanuna dayanarak oluşturulmaktadır. Bu kanunun 61. maddesinde erbaş ve erlerin kıta ve askeri kurumlara katılış ve ayrılışlarında yapılacak olan genel sağlık muayenelerine ilişkin sonuçların sağlık fişlerine kaydedileceği, komutan ve amirlerin de bu muayene sonuçlarına göre personelin sağlık durumunu takip ve kontrol edecekleri düzenlemesine yer verilmiştir.

**(3) Veri madenciliği ve veri eşleştirme olarak adlandırılan teknikler uygulanabilmekte midir? Eğer uygulanabilir ise, bu teknikler potansiyel faillerin veya risk gruplarının profillerini oluşturmada kullanılabilmekte mi? Eğer kullanılabilir ise, kanun uygulayıcı makamlar için özel araçlar geliştirilmiş midir?**

Türkiye'de risk grubu profili oluşturulması söz konusu olmamaktadır. Zira veri tabanlarındaki veriler kanunda belirlenen sürelerin geçmesi ile silinmektedir.

Genel olarak, veri madenciliği ise, verilerin farklı bir bakış açısından analiz edilmesi ve kullanışlı bilgi halinde özetlenme sürecidir. Teknik olarak veri madenciliği, büyük ve birbiriyle ilişkili veri tabanları içinde düzinelerce alan arasında korelasyonlar ve düzenler bulma sürecidir. Bu bağlamda veri madenciliği ve veri eşleştirme noktasında Kriminal Polis Laboratuarları Daire Başkanlığı uygulamaları ve Başkanlık bünyesinde kurulan amirliklerin görev tanımları değerlendirilebilir.

A.- Konuşmacı Kimliklendirme ve Tanıma Büro Amirliğinin Görevleri: Kim tarafından üretildiği belli olmayan bir konuşmanın,

kimliği belirli bir kişiye ait olup olmadığını ve kim tarafından üretildiği belli olmayan iki ayrı konuşmanın aynı kişi tarafından üretilip üretilmediğini belirlemek.

B.- Kayıt Güvenilirliği Büro Amirliğinin Görevleri: Herhangi bir ses kaydının ilk oluşturulduğundaki içeriğinde, başka seslerin ya da konuşmaların eklenmesi, silinmesi, yer değiştirilmesi ya da kayıt sinyaline ait herhangi bir bilginin değiştirilmesi gibi amaçlarla yapılmış fiziksel ya da elektronik bir müdahalenin bulunup bulunmadığını belirlemek.

C.- Kayıt İyileştirme Büro Amirliğinin Görevleri: Herhangi bir ses kaydında, işitilmek istenen konuşma, gürültü ya da konuşma dışı sesleri, diğerlerine göre daha belirgin hale getirmek.

D.- Sinyal Çözümlemesi Büro Amirliğinin Görevleri: Herhangi bir ses kaydı içeriğindeki seslerin ne sesi olabileceğine yönelik nitel ve seslerin düzeyi ile ilgili nicel analizler yapmak.

E.- Konuşmacı Özellikleri Belirleme Büro Amirliğinin Görevleri: Kayıt içerisindeki bir konuşmanın üreticisinin kişisel özelliklerini ortaya koymak,

F.- Ses ve Konuşma İncelemeleri Servisleri:

*Konuşmacı Kimliklendirme ve Tanıma:* Konuşmacı kimliklendirme ve tanıma incelemesi, bilinmeyen bir sesin, bir ya da daha fazla bilinen sesle tanımlanması ya da elenmesi amacıyla işitsel ve görsel olarak karşılaştırılması biçiminde tanımlanabilir. Bu çalışmanın temel olarak dayandığı varsayım; seslerin, kendi başına sahip olduğu karakteristikler ve özellikler yardımıyla çeşitli analiz teknikleri ve yöntemleri uygulanarak diğerlerinden ayırt edilmesidir.

Yıllardır yapılan çalışmalar şekil, parametre, işlemler ve sonuçları bakımından tartışmalara yol açmıştır. Düşük sayıdaki benzer çalışmalarda ortaya çıkan farklılıklar ve sonuçlardaki oranlar sadece ses tanıma ve tanımlama işleminde kullanılan yöntemin güvenilirliği ve kabul edilebilirliği konusunda soru işaretlerinin artmasına neden olmuştur.

*Kayıt Güvenilirliği:* Kayıt güvenilirliği kısaca, kaydın orijinalliğinin araştırılmasıdır. Kayıt güvenilirliği incelemelerinde genel olarak kayıt üzerinde ekleme, çıkarma ve diğer müdahalelerin bulunup bulunmadığına yanıt aranmaktadır.

*Data İncelemeleri:* Bilişim Teknolojileri alanında kullanılan, hard disk, CD, DVD, Blue Ray vb, Akıllı Telefon ve cep telefonları, SIM kart, smart kart, taşınabilir bellek, hafıza kartları, tablet ve dizüstü Bilgisayar, MP3/MP4 çalar, kamera, fotoğraf makinesi, içerisinde veri saklayabilen diğer elektronik cihazlar üzerinde bilimsel olarak kabul edilen metotları uygulayarak teknik inceleme yapar. Teknik inceleme, sayılan cihazların içerisinde gizli, silinmiş, şifreli ve korumalı olarak bulunan bilgilerin tekrar geri getirilmesi süreçlerini de kapsar.

**(4) Zorlayıcı tedbirler (ör: haberleşmenin denetlenmesi) bilgi istihbaratı pozisyonu oluşturmak için kullanılabilmekte midir?**

İletişimin denetlenmesi tedbiri ile teknik araçlarla izleme tedbirlerinin uygulamasının yürütülmekte olan soruşturma veya kovuşturma kapsamında uygulanabilir. Bu tedbirlerin sona ermesi halinde dinlemenin içeriğine ilişkin kayıtların en geç on gün içinde yok edilmesi yükümlülüğü vardır. CMK hükümleri çerçevesinde istihbarî amaçlı bilgi havuzu oluşturmak maksadıyla bu tarz tedbirlere başvurulamaz.

Ancak önleyici kolluk faaliyeti kapsamında PVSK Ek madde 7'de belirtilen koşul ve sınırlamalar çerçevesinde istihbarî amaçlı iletişimin denetlenmesi, teknik araçla izleme gibi tedbirlere başvurulabilmektedir. Bu hükme göre, casusluk suçları hariç olmak üzere TMK m. 10 kapsamına giren suçların önlenmesi amacıyla hakim kararı veya gecikmesinde sakınca bulunan hallerde Emniyet Genel Müdürü veya İstihbarat Dairesi Başkanının yazılı emriyle, telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir. Gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmidört saat içinde yetkili ve görevli hâkimin onayına sunulur. Hâkim, kararını en geç yirmidört

saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde tedbir derhal kaldırılır. Bu halde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir.

PVSK Ek madde 7'ye göre, istihbarat faaliyetlerinde, casusluk suçları hariç olmak üzere TMK m. 10 kapsamına giren suçların önlenmesi amacıyla ve hakim kararı alınmak koşuluyla teknik araçla izleme yapılabilmektedir.

PVSK'daki bu maddelere paralel düzenlemeler Jandarma Teşkilat, Görev ve Yetkileri Kanununda da bulunmaktadır.

Ayrıca Milli İstihbarat Kanunu'nun 6. maddesine göre de, kanunda belirtilen görevlerin yerine getirilmesi amacıyla, Anayasa'da belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde, Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesine ilişkin olarak, hâkim kararı veya gecikmesinde sakınca bulunan hallerde MİT Müsteşarı veya yardımcısının yazılı emriyle telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir. Gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmidört saat içinde yetkili ve görevli hâkimin onayına sunulur. Hâkim, kararını en geç yirmidört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde tedbir derhal kaldırılır. Bu halde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir.

PVSK ek 7. maddesinde ayrıca, bu maddenin uygulanmasına ilişkin esas ve usullerin bir yönetmelik ile düzenleme altına alınabileceği belirtilmiştir. Söz konusu yönetmelik, "Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi Ve Kayda Alınmasına Dair Usul Ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev Ve Yetkileri Hakkında Yönetmelik"tir (Resmi Gazete Tarihi : 10/11/2005, Resmi Gazete Sayısı : 25989).

"Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirinin Uygulanmasına İlişkin Yönetmelik" hakkında ise yürütmenin durdurulması kararı verilmiştir. 06.12.2012 tarihinde Danıştay İdari Dava Daireleri Kurulu tarafından verilen kararın gerekçesinde, ilgili kanunda yönetmelik ile düzenlenebilecek alanlar arasında bu konulara yer verilmemiş olduğu, kanun koyucunun bu alanı ayrıntılı bir şekilde kanunda düzenlemeyi tercih ettiği belirtilmiş ve Adalet Bakanlığı'nın konuya ilişkin düzenleme yetkisinin bulunmadığı ifade edilmiştir.

Değinmek gerekir ki, sayılan bu düzenlemelere dayanılarak elde edilen deliller, önleyici faaliyet kapsamında elde edilmiş olup, hiç bir şekilde yargılamada bir suçun ispatında kullanılmamalıdırlar. Yargılamada yalnızca, yargılama tedbirlerine ilişkin kanun maddelerine göre elde edilmiş delillere başvurulabilecektir. Ancak uygulamamızda, önleyici tedbirlere ilişkin hükümlere dayanılarak elde edilen verilerin, yargılama aşamasında delil olarak kabul edilmesi söz konusu olmaktadır. İstihbarî faaliyet kapsamında toplanan bu verilerin ceza yargılamalarında, mahkumiyet hükümlerine esas teşkil ettikleri davalara rastlanmaktadır.

**(5) Hangi özel sektör aktörleri (ör: internet sağlayıcıları ya da telekom şirketleri) kanun uygulayıcı makamlar için bilgi muhafaza etmektedirler ya da etmek mecburiyetindedirler?**

Türk Telekomünikasyon Anonim Şirketi de dâhil olmak üzere, Telekomünikasyon Kurumu ile yapılan görev sözleşmesi, imtiyaz sözleşmesi, bu Kurumdan alınan telekomünikasyon ruhsatı veya genel izin uyarınca telekomünikasyon hizmetleri yürüten ve telekomünikasyon alt yapısı işleten tüm şirketlerin mecburiyeti vardır:

2007 tarihli 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'a ve bu Kanun'a göre yürürlüğe konulan İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik hükümlerine göre İnternet toplu kullanım sağlayıcılarının İç IP Dağıtım Loglarını elektronik ortamda kendi sistemlerine kaydetmek yükümlülükleri vardır.

5651 sayılı Kanun'un 6/1-b maddesinde de, erişim sağlayıcıların sağladıkları hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlü oldukları belirtilmektedir. Aynı maddenin son fıkrasında ise, bu yükümlülüğü yerine getirmeyen erişim sağlayıcısına Başkanlık tarafından onbin Yeni Türk Lirasından ellibin Yeni Türk Lirasına kadar idarî para cezası verileceği hüküm altına alınmıştır.

Ayrıca, İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik, ticarî olmayan İnternet toplu kullanım sağlayıcılara bir yükümlülük yüklemektedir. Anılan Yönetmeliğe göre işyerlerinde, otellerde vb. tüm yerlerde iç IP dağıtım loglarını toplu kullanım sağlayıcılar elektronik ortamda kendi sistemlerine kaydetmekle yükümlü tutulmuştur.

İnternet toplu kullanım sağlayıcılar açısından kanunda yer almayan bilgi muhafaza yükümlülüğünün yönetmelikle getirilmiş olması ve bu kayıtların ne kadar süre saklanacağı, herhangi bir mercie tesliminin gerekip gerekmediği hukukun genel ilkelerine aykırı olduğu gibi iletişim özgürlüğü yönünden de güvenceden yoksun bir durum ortaya çıkarmaktadır.

**(6) Hangi özel sektör aktörleri kanun uygulayıcı makamlara bilgi sağlayabilir veya bilgi sağlamak mecburiyetindedirler?**

Maddi gerçeği ortaya çıkarmaya elverişli ve hukuka uygun elde edilen tüm bilgi, belge ve bulgular delil olarak kullanılabilir (CMK m. 217/2). Bu bağlamda kanun uygulayıcı makamlar da hukuka uygun yöntemler kullanmak suretiyle bir suç olgusuna ilişkin tüm verilere ulaşma imkânına sahiptir. Bu bağlamda talep edilmesi halinde bütün özel sektör aktörleri kanun uygulayıcı makamlara talep edilen bilgileri sağlamakla yükümlüdür.

Ayrıca Milli İstihbarat Kanunu m. 6 uyarınca, MİT, bakanlıklar ve diğer kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim alt

yapısından kendi görev sahasına giren konularda yararlanabilmek, bunlarla irtibat kurabilmek, bilgi ve belge almak için gerekçesini de göstermek suretiyle yazılı talepte bulunabilmektedir.

Teknik araçla izleme tedbirinin istihbarî amaçla uygulanması haline ilişkin hükümler de bulunmaktadır. PVSK Ek m.7'de de, kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşların ihtiyaç duyulan bilgi ve belgelerinden yararlanabilmek için gerekçesini de göstermek suretiyle yazılı talepte bulunulabileceği belirtilmektedir. Bu kurum ve kuruluşların kanuni sebeplerle veya ticari sır gerekçesiyle bu bilgi ve belgeleri vermemeleri halinde ancak hakim kararı ile bu bilgi ve belgelerden yararlanılabilir. PVSK'da yer alan bu hükme, Jandarma Kanunu Ek m. 5/5'te de yer verilmiş olup, söz konusu iki maddenin lafzı arasında herhangi bir fark bulunmamaktadır.

Elektronik Haberleşme Kanunu da 12/5. maddesinde, işletmecilerin, elektronik haberleşme sistemleri üzerinden milli güvenlikle ve kanunlarda getirilen düzenlemelerle ilgili taleplerin karşılanma-bilgBTdT1 sına yönelik teknik alt yapıyı, elektronik haberleşme sistemini hizmete sunmadan önce kurmakla yükümlü olduklarını hüküm altına almıştır.

**(7)**

**(D) Ceza soruşturmasında BİT**

**(1) Kanun uygulayıcı makamlar, gerçek zamanlı olarak a) e-trafik verilerine, b) içerik verilerine müdahale edebilir mi?**

5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"un 8. maddesindeki koşullar çerçevesinde, internet ortamında yapılan ve içeriği kanunda sayılan belli suçları (*intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma, sağlık için tehlikeli madde temini, müstehcenlik, fuhuş, kumar oynanması için yer ve imkan sağlama, 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar*) oluşturduğu konusunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilebilmektedir. Erişimin engellenmesi kararı, soruşturma evresinde hakim, kovuşturma evresinde ise mahkeme tarafından verilebilmektedir. Soruşturma aşamasında gecikmesinde sakınca bulunan bir hal söz konusu ise, cumhuriyet savcısı da karar verebilmektedir, ancak bu kararın 24 saat içinde hakim tarafından onaylanması gerekmektedir. Aksi halde cumhuriyet savcısı tarafından derhal kaldırılır.

İçerik veya yer sağlayıcının yurt dışında bulunması halinde, veya bunlar yurt içinde olsalar bile çocukların cinsel istismarı veya müstehcenlik suçlarını oluşturan yayınlar söz konusu ise, erişimin engellenmesi kararı re'sen Başkanlık tarafından verilir.

Erişimin engellenmesi kararının derhal ve en geç kararın bildirilmesi anından itibaren 24 saat içinde uygulanması gerekir. Koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen yer veya erişim sağlayıcılarının sorumluları, fiil daha ağır cezayı gerektiren bir başka suçu oluşturmadığı takdirde, altı aydan iki yıla kadar hapis cezası ile cezalandırılır. İdari tedbir olarak verilen erişimin engellenmesi kararının yerine getirilmemesi halinde ise, erişim sağlayıcısına, on bin TL'den yüz bin TL'ye kadar idari para cezası verilir.

Ayrıca Elektronik Haberleşme Kanunu'nun 12/1-g maddesinde, işletmecilere getirilebilecek yükümlülükler arasında, "kanunlarla yetkili kılınan ulusal kurumlarca yasal dinleme ve müdahalenin yapılmasına teknik olanak sağlanması" sayılmıştır.

**(2) Kanun uygulayıcı makamlar; a)e-trafik verileri; b)içerik verileri bakımından, bilgi sistemlerine erişim/bunları durdurma/arama/bunlara el koyma imkânlarına sahip midir?**

CMK'da bilgi sistemlerini durdurmayı ya da bunlara elkoymayı öngören bir düzenlemeye yer verilmemektedir. CMK'da yalnızca "postada elkoyma" tedbiri düzenlenmiş olup, bu düzenlemenin kıyasen uygulanması da mümkün değildir. Zira özgürlük sınırlayıcı nitelikteki konularda kıyas yapılması mümkün olamaz.

Bununla birlikte CMK'nın 134. maddesinde, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoymaya ilişkin bir düzenleme bulunmaktadır. Bu düzenleme kapsamında bilgi sistemlerine erişim mümkün olmakla birlikte, bu tedbir kapsamında yalnızca erişim bilgisine sahip içerik kopyası çıkarılabilmektedir. Ayrıca CMK'nın 135. maddesi kapsamında da telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi söz konusu olabilmektedir.

Konu ile ilgili özel bir düzenleme 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"da yer almaktadır. Bu kanunun 8. maddesindeki koşullar çerçevesinde, internet ortamında yapılan ve içeriği kanunda sayılan belli suçları (*intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma, sağlık için tehlikeli madde temini, müstehcenlik, fuhuş, kumar oynanması için yer ve imkan sağlama, 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar*) oluşturduğu konusunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilebilmektedir. (Ayrıntısı için bkz. D/(1) kapsamında verilen cevap)

**(3) Telekom şirketleri ya da servis sağlayıcılar, verilerini kanun uygulayıcı makamlar ile paylaşmaya zorlanabilirler mi? Buna uygun hareket etmemeleri halinde, zorlayıcı tedbirler ya da yaptırımlar uygulanmakta mıdır?**

CMK'nın 332. maddesinde konuya ilişkin genel bir hüküm yer almaktadır. Buna göre, suçların soruşturması sırasında cumhuriyet savcısı tarafından yazılı olarak istenilen bilgilere on gün içinde cevap verilmesi zorunludur. Buna aykırı hareket edilmesi halinde TCK'nın 257. maddesinde yer alan "görevi kötüye kullanma" suçunun uygulama alanı bulacağı kanunda açıkça belirtilmiştir.

CMK'nın 332. maddesinde bilgi istenilen kurumun niteliği belirtilmemekte, genel bir ifadeye yer verilmektedir. Genel hüküm niteliğindeki 332. maddenin yanı sıra CMK'nın 137. maddesinde de usulüne uygun şekilde verilmiş olan telekomünikasyon yoluyla iletişimin denetlenmesi kararlarının yerine getirilmesine ilişkin bir düzenleme yer almaktadır.

CMK'nın 137. maddesine göre, cumhuriyet savcısı veya görevlendirdiği adli kolluk görevlisi, kanuna uygun şekilde verilmiş karar gereğince, iletişimin tespiti, dinlenmesi ve kayda alınması işlemlerinin yapılmasını ve bu amaçla cihazların yerleştirilmesini, telekomünikasyon hizmeti veren kurum ve kuruluşların yetkililerinden yazılı olarak isteyebilir. Bu isteğin ilgililer tarafından derhal yerine getirilmesi gerekmektedir, aksi halde zor kullanılabilir.

Ayrıca Milli İstihbarat Teşkilatı Kanunu'nun 6. maddesinde, Milli İstihbarat Teşkilatının, Bakanlıklar ve diğer kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim alt yapısından kendi görev sahasına giren konularda yararlanabilmek, bunlarla irtibat kurabilmek, bilgi ve belge almak için gerekçesini de göstermek suretiyle yazılı talepte bulunabileceği de belirtilmektedir.

Elektronik Haberleşme Kanunu m. 12'de de "işletmecilerin hak ve yükümlülüklerine" ilişkin özel bir düzenleme yer almaktadır. Söz konusu maddenin ikinci fıkrasının (g) bendinde, işletmecilere getirilebilecek olan yükümlülükler arasında, "kanunlarla yetkili kılınan ulusal kurumlarca yasal dinleme ve müdahalenin yapılmasına teknik

olanak sağlanması" sayılmıştır. Ayrıca yine aynı maddenin beşinci fıkrasında, işletmecilerin, elektronik haberleşme sistemleri üzerinden, kanunlarda getirilen düzenlemelerle ilgili taleplerin karşılanmasına yönelik teknik alt yapıyı, elektronik haberleşme sistemini hizmete sunmadan önce kurmakla yükümlü oldukları belirtilmektedir.

**(4) Kanun uygulayıcı makamlar kamera ile izleme yapabilmekte midir? Bu makamlar gerçek ve tüzel kişileri işbirliğine zorlayabilirler mi?**

CMK'nın 140. maddesinde "teknik araçlarla izleme" tedbiri öngörülmüştür. Kanunda sınırlı sayıda sayılan bazı suçların işlendiği konusunda kuvvetli şüphe sebeplerinin bulunması ve başka suretle delil elde edilememesi halinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ile işyerinin teknik araçlarla izlenmesi, ses ve görüntü kaydı alınması mümkündür.

PVSK Ek m.7'de de, istihbarat faaliyetlerinde, TMK m.10 kapsamına giren suçların önlenmesi amacıyla ve hakim kararı alınmak koşuluyla, teknik araçlarla izleme yapılabileceği belirtilmektedir. Ayrıca kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşların ihtiyaç duyulan bilgi ve belgelerinden yararlanabilmek için gerekçesini de göstermek suretiyle yazılı talepte bulunabilir. Bu kurum ve kuruluşların kanuni sebeplerle veya ticari sır gerekçesiyle bu bilgi ve belgeleri vermemeleri halinde ancak hakim kararı ile bu bilgi ve belgelerden yararlanılabilir.

PVSK'da yer alan bu hükme, Jandarma Kanunu Ek m. 5/5'te de yer verilmiş olup, söz konusu iki maddenin lafzı arasında herhangi bir fark bulunmamaktadır.

Ayrıca, 2911 sayılı Toplantı ve Gösteri Yürüyüşleri Kanunu'nun 13/2. maddesine göre, toplantı ve gösteri yürüyüşleri sırasında hazır bulunan hükümet komiseri, toplantıyı teknik ses alma cihazları, fotoğraf ve film makineleri gibi araçlarla tespit ettirebilmektedir.

İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik'in 9. maddesinde de, işyerlerinin uyması gereken kurallar arasında, işyerlerine giren ve çıkanların tespiti amacıyla gerekli kamera kayıt sisteminin kurulacağı da yer almaktadır. Yönetmelik'te, bu sistem

aracılığıyla elde edilen kayıtların yedi gün süreyle saklanacağı ve yetkili makamlar haricindeki kişi ve kuruluşlara verilemeyeceği hüküm altına alınmıştır.

Türkiye'de "MOBESE" sisteminin bulunup bulunmadığı konusuna da değinmek gerekir. Türk hukukunda, bilinen anlamda "MOBESE" kameralarının kullanımına ilişkin kanuni bir dayanak bulunmamaktadır. Bu tür bir sistem yalnızca 2918 sayılı Karayolları Trafik Kanunu'nda öngörülmektedir. Söz konusu kanunun Ek 16. maddesi uyarınca, belediyeler tarafından kendi bütçe kaynakları kullanılarak, karayollarında can ve mal güvenliğini sağlamak, düzenli ve güvenli trafik akışını temin etmek amaçlarına hizmet etmek üzere kurulmuş veya kurulacak elektronik sistemlerin Emniyet Genel Müdürlüğünce trafik ihlallerinin tespiti amacıyla kullanılması mümkündür. Ancak kurulan bu sistem aracılığıyla ulaşılan görüntüler yalnızca Ek 16. maddede belirtilen amaçlar doğrultusunda kullanılabilecektir. Belirtilen amaçlar arasında bir suça ilişkin delil elde etmek, suçun önlenmesini sağlamak ya da suç tespiti gibi bir amaca yer verilmemiştir. Bu durumda hukukumuzda yalnızca Karayolları Trafik Kanunu kapsamında genel bir elektronik izleme sistemi kurmak mümkündür ve bu sistem aracılığıyla elde edilen görüntülerin de yalnızca ilgili maddede belirtilen amaçlar doğrultusunda kullanılabilme olanağı mevcuttur. Bu amaçlar dışındaki bir kullanım kanuna aykırı olacaktır. Ancak uygulamacılar tarafından, MOBESE kameraları aracılığıyla elde edilen görüntüler, ilgili kolluk görevlileri tarafından gerekli görülmesi halinde, ileriki bir soruşturmada kullanılmak üzere saklandığı ifade edilmektedir. Belirtmek gerekir ki, söz konusu görüntü kayıtlarının bu şekilde saklanması mevcut kanuni düzenlemelere aykırılık teşkil etmekle birlikte, TCK'nın 138. maddesinde düzenlenen "verileri yok etmeme" suçunu da oluşturmaktadır.

Ayrıca uygulamada, herhangi bir kanuni dayanağı bulunmamasına rağmen, CMK kapsamında gerçekleştirilen bir arama işlemi sırasında kolluk görevlilerinin söz konusu işlem sırasında kamera kaydı aldığı olaylara sıklıkla rastlanmaktadır.

**(5) Kanun uygulayıcı makamlar, sorgulamaları (şüpheli, görgü tanığı) sesli ve görüntülü kayıt altına alabilmekte midir ya da almak zorunda mıdır?**

Tanık dinlenmesi sırasında ses ve görüntü kaydı alınması kural olarak ihtiyaridir. Ancak bazı tanıkların dinlenmesinde ses ve görüntü kaydı alınmasının mecburi olduğu kanunda belirtilmiştir. Bu kapsamda, mağdur çocukların, duruşmaya getirilmesi mümkün olmayan ve tanıklığı maddi gerçeğin ortaya çıkarılması bakımından zorunlu olan kişilerin tanıklığında ses ve görüntü kaydı yapılması zorunludur (CMK 52/3).

Bu bağlamda, 2012/20 sayılı ve Çocuk İzlem Merkezi (ÇİM) konulu genelge uyarınca (4 Ekim 2012 tarih ve 28431 sayılı Resmi Gazete), çocuk istismarının önlenmesi ve istismara uğrayan çocuklara etkin bir şekilde müdahale edilmesi amacıyla, pilot şehirlerde Çocuk İzlem Merkezleri kurulmuştur. Çocuk İzlem Merkezleri Yönetim ve Koordinasyon Kurulu'nun 22.10.2012 tarihli ve 2012/1 sayılı kararlarında şu hususlar belirtilmiştir:

1. Cumhuriyet savcısının emir ve talimatları doğrultusunda, mağdur çocuğun beyanının alınmasını müteakip, ilgili mevzuatında öngörüldüğü şekilde ÇİM'de mağdurun veya velisinin rızası alınarak vücudu üzerinde dış veya iç beden muayenesi yapılacak, vücudundan örnek alınması, psikiyatrik muayenesinin gerçekleştirilmesi ve gerektiğinde fizikî bulguların görüntülerinin kaydedilmesi sağlanacaktır.
2. Mağdur çocuğun beyanı ilgili mevzuatına uygun olarak; Cumhuriyet Savcısı ya da zorunlu hallerde Cumhuriyet Savcısının emir ve talimatı doğrultusunda kolluk görevlisi tarafından, vekili huzurunda, ÇİM'de görevli ve bu konuda eğitim almış uzman bir kişi vasıtasıyla, aynalı bir odada, ses ve görüntü kaydı yapılmak suretiyle alınacaktır.
3. Bütün bu süreçte mağdurun mahremiyetine azami dikkat gösterilecektir.
4. ÇİM'de yapılan işlemler hastane otomasyon sistemine kayıt edilmeyecektir.

5. Görüşme ve muayeneler tamamlandıktan sonra elde edilen tüm bilgi ve belgeler bir rapor haline getirilerek, ses ve görüntü kayıtları ile birlikte ilgili Cumhuriyet Başsavcılığına gönderilecektir.

Ayrıca tanık için tehlike arz eden hallerde veya maddi gerçeğin ortaya çıkarılması bakımından tehlike doğuran hallerde hakimin hazır bulunma hakkı olan kişileri duruşması salonundan çıkarması mümkün olmaktadır. Bu gibi durumlarda da tanığın ses ve görüntü kaydının alınması zorunlu olup, kişilerin cevap hakkı saklı tutulmuştur (CMK 58/3).

CMK m. 147/1-h bendinde ise, şüpheli veya sanığın ifadesinin alınması veya sorgusunda, bu işlemlerin kaydında teknik imkanlardan yararlanılacağı belirtilmektedir. Kanunda yer alan düzenleme "yararlanılır" demek suretiyle bu konuyu takdire bırakmamış, söz konusu yöntemlerin kullanılmasını zorunlu tutmuştur. 14.12.2011 tarih ve 150 No'lu SEGBİS genelgesinde de CMK 147/1-h bendi gereği ses ve görüntü kaydı almanın zorunlu olduğu hususunun gözden kaçırılmaması gerektiği belirtilmektedir.

CMK m. 180'e göre de, naip veya istinabe yoluyla dinlenen tanık ya da bilirkişinin aynı anda görüntülü ve sesli iletişim tekniğinin kullanılması suretiyle dinlenmesi olanağı bulunmaktadır. Ayrıca sanığın duruşmadan bağışık tutulduğu hallerde de görüntülü ve sesli iletişim tekniğinin kullanılması suretiyle sorgusu yapılacaktır.

Bunların dışında ise kural olarak ceza muhakemesinde ses ve görüntü alıcı aletlerin kullanılması yasağı vardır. Kural olarak, adliye binası içerisinde ve duruşma başladıktan sonra duruşma salonunda her türlü sesli veya görüntülü kayıt veya nakil olanağı sağlayan aletler kullanılamaz. Bu hüküm, adliye binası içerisinde ve dışındaki diğer adlî işlemlerin icrasında da uygulanır.

### E) BİT ve deliller

**(Aşamalar zinciri: elektronik delillerin toplanması / depolanması / tespit edilmesi / üretilmesi / sunulması / değerlendirilmesi)**

#### (1) BİT ile ilişkili bilgilere özgü herhangi bir delil kuralı var mıdır?

Türk hukukunda BİT ile ilişkili bilgilere özgü herhangi bir delil kuralı mevcut değildir. Bunlar da genel kurala tabidirler. Yargılamada delil hiyerarşisi de öngörülmemektedir. Hukuka uygun olmak koşuluyla, maddi olayı ispata yarayan her şey delil olarak kabul edilir ve aralarında bir derecelendirme kural olarak söz konusu değildir.

Ancak mevzuatın teknolojinin oldukça gerisinde kalmış olması ve uygulamada karşılaşılan sorunlar göz önünde bulundurularak, bu delillerin güvenilirlikleri tartışma konusu olmuştur. Uygulamada, özellikle elde edilme aşamasında manipülasyona oldukça müsait yapıda olduklarından bu delillerin güvenilir deliller olarak kabul edilmemesi gerektiği doktrinde ifade edilmektedir. Nitekim söz konusu delillere müdahale olanağı, diğer delillere nazaran çok daha geniştir. Ayrıca Türk uygulamasında yer alan pek çok davada, BİT ile ilişkili bilgilere özgü delillerin, olay sonrasında şüpheli dışındaki kişilerce - şüpheli aleyhine delil olarak kullanılması amacıyla - üretilmiş olabileceğine ilişkin son derece ciddi şüpheler bulunmaktadır. Bu sebeplerle de söz konusu delillerin hiç bir şekilde yargılamada delil olarak kullanılmaması gerektiğine ilişkin görüşler ileri sürülmektedir.

Türk Ceza muhakemesi uygulamamızda gelinen aşamada, dijital deliller bir nevi, engizisyon yargılamasındaki "ikrar delili" niteliğine büründürülmüş durumdadır. Oysa, bu deliller, ancak hukuka uygun süreçle olaya ilişkin maddi delillere ulaşmada bir araç olarak kullanılmalı ve yalnızca onları destekleyici bir niteliği haiz olmalıdır. Günümüz Türk ceza muhakemesi hukukunda, sahte dijital delillerin oldukça rahat şekilde üretildikleri, bunların dosyalarda yer aldıkları ve hatta başka delile ihtiyaç duyulmaksızın yalnızca bunlara dayanılarak mahkumiyet hükümleri verildiği görülmektedir. Mevcut bu durum Türk uygulaması açısından ancak, sanığın suçluluğunu ispat için uygulanan bir "dijital işkence" olarak nitelendirilebilir.

**(2) BİT ile ilişkili delillerin bütünlüğü (örneğin delillerle oynama veya kurallara aykırı biçimde işleme) ve güvenliği (örn: hack'leme) ile ilgili herhangi bir kural var mıdır?**

BİT ile ilişkili delillerin bütünlüğü ve güvenliğine ilişkin herhangi bir özel hüküm bulunmamaktadır. Bu tür deliller bakımından genel kurallar geçerlidir. Ancak bu durum gelişen teknoloji karşısında uygulama bakımından önemli sorunlara neden olmaktadır. Özellikle bu delillerin güvenilirliği sağlanamamaktadır.

BİT ile ilişkili delillerin bütünlüğü ve güvenliğinin ihlali halinde TCK'daki bazı suç tiplerinin oluştuğu söylenebilmektedir. Bu bakımdan somut olaya göre, TCK'da yer alan haberleşmenin gizliliğini ihlal (TCK m. 132), özel hayatın gizliliğini ihlal (TCK m. 134), bilişim sistemine girme (TCK m. 243), bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme (TCK m. 244) suçları gündeme gelebileceği gibi, TCK'nın 281. maddesinde yer alan "suç delillerini yok etme, gizleme veya değiştirme" suçu da oluşabilecektir. Ancak uygulamada delil güvenliğinin denetlenmesi sağlıklı şekilde yapılamadığından, söz konusu suçları oluşturacak bir ihlalin varlığı tespit dahi edilememektedir.

Özellikle bilgisayar kütüklerinde arama işlemlerinin yapılması sırasında, bilgisayardan kopya çıkarılması sırasında bilgisayara yeni bir verinin yüklenip yüklenmediği kuşkusu doğabilmektedir. Bilgisayar verilerinin kopyalanması konusunda hash değerleri alınsa da, uygulamada kopyalama işleminin başında bilgisayara yeni veri yüklenmiş olabileceği şüpheleri doğmaktadır. Aynı şekilde CD ya da cep telefonu gibi eşyalara elkonulması durumunda da benzer kuşkular gündeme gelmektedir. Nitekim çoğu zaman CD, harici bellek ya da bilgisayarların kopya çıkarma işlemi, uzun vakit alacağı gerekçe gösterilerek, kolluk merkezinde yapılmaktadır. Bu durumda kopya çıkarma işlemi günlerce sürebilmekte ve ilginin katılımı sağlanamamaktadır. Bu durumda hash değeri alınmış olsa bile işlem sırasında yeni bir verinin eklenmesinden sonra kopyanın çıkarılmış olabileceği şüpheleri doğmaktadır.

Benzer sorunlar cep telefonları (özellikle akıllı telefonlar) aracılığı ile ulaşılan verilerin ispat değeri bakımından da söz konusudur. Teknolojik gelişmeler göz önünde bulundurularak, cep telefonları-

nın aranması ve bunlara el konulmasına ilişkin özel düzenlemelere sistemimizde yer verilmemiştir. Bunlara da her eşya gibi klasik el koyma işlemi uygulanmaktadır. Ancak el koyma işleminin ardından bunlara herhangi bir verinin eklenip eklenmediği sorusuna net cevap verilememektedir. Nitekim uygulamamızda karşılaşılan önemli bir davada cep telefonuna el konulduğu zaman itibariyle telefon rehberinde yer almayan bazı isimlerin, yargılama sürecinde telefon rehberinde bulunduğu görülmüştür. Yapılan itirazlar ve incelemeler sonrasında, yetkililer tarafından, telefona elkonulduktan sonra, kolluk merkezinde, söz konusu verilerin "sehven" yüklenmiş olduğu açıklaması yapılmıştır.

**(3) BİT ile ilişkili bilgilere özgü olarak delillerin kabul edilebilirliğine (hukuka uygun elde edilmiş delil ilkesi dahil olmak üzere) ilişkin herhangi bir kural var mıdır?**

Türk ceza muhakemesinde vicdani kanaat sistemi geçerlidir. Bu bağlamda hukuka uygun şekilde elde edilmiş olmak koşuluyla her şey delil olarak kabul edilebilir. BİT ile ilişkili delillerin kabul edilebilirliğine ilişkin özel ayrık bir düzenleme bulunmamaktadır. Söz konusu delillerin güvenilirliği doktrinde oldukça yoğun şekilde tartışılıyor olmakla birlikte bunlar da genel kurallara tabidir.

Türk hukukunda hukuka aykırı deliller ise hiçbir şekilde kabul edilmemektedir. Hukuka aykırı deliller konusunda, Türk mevzuatında son derece katı bir sistem benimsenmiştir. Gerek TC Anayasası'nda gerekse ceza muhakemesi kanununda bu kural açık bir şekilde ortaya konulmuştur. Anayasada hukuka aykırı şekilde elde edilmiş olan "bulgulardan" söz edilmekte ve bunların "delil" niteliğini taşımadığı ortaya konulmaktadır. Anayasanın 38. maddesinde hiç bir istisnaya yer verilmeden, hukuka aykırı şekilde elde edilen bulguların delil olamayacağı belirtilmektedir. Ceza Muhakemesi Kanunu'nda da ispatın ancak hukuka uygun şekilde elde edilmiş delillerle mümkün olduğu (CMK 217/2) ve hükmün hukuka aykırı delile dayanması durumunun, hükmün bozulması sonucunu doğuracağı (CMK 289/i) düzenlenmiştir.

Ayrıca Türk ceza hukuku sisteminde "zehirli ağacın meyvesi de zehirlidir" kuralı da geçerli olup, hukuka aykırı şekilde elde edilmiş bir delil aracılığıyla ulaşılan bütün diğer deliller de hukuka aykırı kabul edilmekte ve hükme esas alınmamaktadır.

Hukuka aykırılık konusunda herhangi bir istisna tanınmamaktadır. Bu bağlamda, nisbi hukuka aykırılık – mutlak hukuka aykırılık, şekli hukuka aykırılık - maddi hukuka aykırılık ya da hukuka önemli aykırılık – önemsiz aykırılık gibi ayrımlara gidilmemektedir. Bu tür bir ayrıma Türk hukukunda da yer verilmesi gerektiğini düşünen bazı yazarlar olsa da, bu düşünce Türk hukukunda yer bulmamıştır. Yargıtay'ın ise, hukuka aykırılığın "nisbi- mutlak" ya da "önemli-önemsiz" gibi çeşitli ayrımlara tabi tutulmasının mümkün olmadığı açıkça vurguladığı kararları bulunmakla birlikte, aksi yönde vermiş olduğu bazı kararları da mevcuttur. Ceza muhakemesinin amacı hukuka uygun yollarla ve insan haklarına saygılı biçimde, maddi gerçeğe ulaşmaktır. Bu da kanunlar ile belirlenen delil elde etme kurallarına, bunlara ilişkin usullere her koşulda uyulması gerektiği anlamına gelir. Hukuka aykırılığa göz yumarak hukukun tesisi mümkün değildir.[4]

**(4) BİT ile ilişkili delillerin ortaya çıkarılması ve açıklanmasına ilişkin özel kurallar var mıdır?**

CMK'nın "bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" başlıklı 134. maddesi konuya ilişkin bir düzenleme içermektedir. Bu maddeye göre, bir suç dolayısıyla yapılan soruşturmada, başka türlü delil elde etme imkanının bulunmaması halinde şüphelinin kullandığı bilgisayar ve bilgisayar ile bilgisayar kütüklerinde arama yapılması, bilgisayar kayıtlarından kopya çıkarılması, bu kayıtların çözülerek metin haline getirilmesi mümkündür. Bu tedbire başvurulması için cumhuriyet savcısının istemi üzerine sulh ceza hakiminin karar vermesi gerekmektedir.

Tedbirin "şüphelinin kullandığı" bilgisayar hakkında uygulanması gerektiği hükümde belirtilmiş olmakla birlikte, özellikle işyerlerin-

4 KESKİN, Serap, Ceza Muhakemesi Hukukunda Temyiz Nedeni Olarak Hukuka Aykırılık, Alfa, İstanbul, 2007, s. 182 – 183.

de bu tedbir uygulandığı zaman, söz konusu koşula gereğince dikkat edilmemektedir. Özellikle işyerleri gibi farklı kişilerin kullanımındaki bilgisayarların mevcut olduğu yerlerde bu tedbir uygulanırken, bilgisayarı şüphelinin kullanıp kullanmadığına dikkat edilmemekte ve tedbirin uygulandığı mekandaki bütün bilgisayarlarda arama yapılmaktadır. Bu sebeple de söz konusu tedbirin uygulanmasına ilişkin özel bir kural olmasına rağmen uygulamada buna her zaman riayet edilmediği görülebilmektedir.

Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde ise, çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için bu araç ve gereçlere el koymak mümkündür. Şifrenin çözülerek gerekli kopyaların alınması halinde ise el konulan cihazlar gecikmeksizin iade edilmelidir.

Bu hükmün uygulaması da elde edilen delillerin güvenilirliğini zedeler şekilde gerçekleştirilmektedir. Maddede yazılı gerekçelerle el konulan bilgisayarlarda kopyalama işlemi kimi zaman günler alabilmektedir. Bu durumda da kopyalama sırasında herhangi bir işlem tanığının hazır bulunması sağlanamamaktadır. Dolayısıyla da kopya çıkarılmadan önce bilgisayara herhangi bir verinin yerleştirilip yerleştirilmediği tam olarak bilinememektedir. Başlı başına buna ilişkin kuşku bulunması dahi bu yolla elde edilen delilin güvenilirliğini zedelemektedir. Güvenilirliği bu şekilde zedelenmiş bir delilin ise yargılamada kullanılması mümkün olmamalıdır. Ancak uygulamada bütün şüphelere rağmen, hatta bazı davalarda bu tür şüphelerin doğruluğunu gösterir uzman raporlarının sunulmuş olmasına karşın bu deliller yargılamada kullanılmakta ve bunlara dayanılarak mahkumiyet hükümleri tesis edilmektedir.

CMK 134. maddeye göre, bilgisayar veya bilgisayar kütüklerinde elkoyma işlemi sırasında bütün verilerin yedeklemesi yapılır. Belirtmek gerekir ki, Adli ve Önleme Aramaları Yönetmeliği'nin 17. maddesinde, bu işlemin bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanacağı hükmü yer almaktadır. Yönetmeliğin, bir hakka ilişkin olarak, kanun hükmünde öngörülenden daha geniş bir sınırlandırma getirmesi mümkün ola-

mayacağından, bu yönetmelik maddesinin uygulanmasında kanunda öngörülen sınırların ötesine geçilmemesi gerektiğine dikkat edilmelidir.

Ayrıca, istemesi halinde, elde edilen yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilir. Ancak dikkat etmek gerekir ki, şüpheli veya müdafiine elde edilen yedeğin bir kopyasının verilmesi için, kendisinin buna ilişkin bir istekte bulunması gerekmektedir. Bu tür bir istek bulunmadığı takdirde cumhuriyet savcılığının ya da kolluğun şüpheli veya müdafiine bir yedek çıkarmak yükümlülüğü bulunmamaktadır. Uygulamada şüpheli veya müdafii elde edilen kopyanın bir örneğini istediklerinde, kolluk görevlileri, yanlarında kopya çıkaracakları bir materyalin (CD, harici disk vb.) bulunmadığını söylemektedirler. İstekte bulunan şüpheli veya müdafiin kendi imkanlarıyla ve derhal bu tür materyal getirebilmeleri halinde onlara bir kopyanın verilmesinin mümkün olduğunu belirtmektedirler. Bu durumda da istekte bulunan kişi, derhal CD ya da harici hard disk vb. alıp bunu kolluğa teslim etmek zorunda kalmaktadır. Bunun için de tedbire başvurulan yer ve saat ne olursa olsun kişiler söz konusu materyalleri temin edebilecekleri imkanlar aramak zorunda kalmaktadır.

Bazı davalarda ise şüpheli müdafiilerine, kanun hükmü gereği istekleri üzerine verilmiş olan kopyalar, "içlerinde suç unsuru taşıyan veriler barındırdıkları" gerekçesiyle kolluk tarafından geri istenmiştir. Nitekim, soruşturma sırasında yapılan inceleme sonucunda bilgisayar içerisinde suç teşkil eden bazı bilgiler bulunduğu ve çıkarılan kopyada da bilgisayardaki bütün bilgilerin kopyası mevcut olduğundan, söz konusu kopyanın da suç teşkil eden bilgiler içermekte olduğu belirtilmiştir. Ayrıca şüpheli müdafilerine, "ellerindeki kopyaları teslim etmemeleri halinde haklarında soruşturma başlatılacağı" da söylenmiş ve müdafiiler, talepleri üzerine kolluk tarafından kendileri için çıkartılmış olan kopyaları iade etmeye zorlanmışlardır. Bu uygulamanın herhangi bir kanuni dayanağı bulunmamakla birlikte söz konusu uygulama sebebiyle kolluk güçleri herhangi bir yaptırıma da maruz kalmamışlardır.

**(5) BİT ile ilişkili delillerin değerlendirilmesi (ispat değeri) için özel kurallar var mıdır?**

Söz konusu delillerin ispat değerine ilişkin özel bir düzenleme bulunmamaktadır. Bu deliller de vicdani kanaat sistemi içerisinde genel kurala tabidir. Ancak bunların elde edilme safhalarında uygulamadan kaynaklanan bazı sorunlar nedeniyle delillerin güvenilirliği açısından haklı kuşkular doğabilmektedir. Özellikle bilgisayar kütüklerinde arama işlemlerinin yapılması sırasında, bilgisayardan kopya çıkarılması sırasında bilgisayara yeni bir verinin yüklenip yüklenmediği kuşkusu doğabilmektedir. Aynı şekilde CD ya da cep telefonu gibi eşyalara elkonulması durumunda da benzer kuşkular gündeme gelmektedir.

Söz konusu deliller, ispat değeri bakımından genel kurallara tabi olsalar da, mevzuatın teknolojinin çok gerisinde kalmış olması ve dolayısıyla uygulamada yaşanan sorunlar nedeniyle, bu delillerin güvenilirliği ciddi tartışmalara neden olmuştur.

**(F) Duruşma aşamasında BİT**

**(1)**

uygun olarak verilebilir. Talep veya itiraz halinde ise ses ve görüntü kayıtları, soruşturma ve kovuşturma makamı gözetiminde ilgilisine izletilebilmektedir (Yön. 8).

Uygulamada ses ve görüntülerin kayda geçirilmesi çok uzun süreler alabilmekte, bazen kayıt yapıldıktan aylar sonra bu kayıtlar tutanağa geçirilerek ilgililere teslim edilmektedir. Bu uygulama sebebiyle savunma hazırlama konusunda güçlükler yaşanmaktadır. Bazı davalarda bu kayıtlar tutanağa dönüştürülmeden savunma yapılmak zorunda kalınmakta ve bu kayıtlar ancak karardan sonra tutanak haline getirilerek dosyaya konulmaktadır. Ayrıca bu gecikme sebebiyle, öngörülen itiraz kanun yolu da etkin şekilde işletilememektedir.

Ayrıca CMK'nın 137/2. maddesinde, telekomünikasyon yoluyla iletişimin denetlenmesi tedbiri çerçevesinde elde edilen kayıtların, cumhuriyet savcılığınca görevlendirilen kişiler tarafından çözülerek metin haline getirileceği hüküm altına alınmaktadır.

Konuyla ilişkili olabilecek bir başka madde ise, CMK'nın 209/2 maddesidir. Bu hükme göre sanığa veya tanığa ait kişisel verilerin yer aldığı belgelerin, açıkça istemeleri halinde kapalı oturumda okunmasına mahkemece karar verilebilir. Bu bağlamda BİT'e ilişkin ve delil niteliği taşıyan bilgilerin kişisel veri niteliği taşıması halinde bu delillerin ( yani verilerin) kapalı oturumda ortaya konulması sağlanarak bir güvence oluşturulabilir. Ancak belirtmek gerekir ki, henüz Kişisel Verilen Korunması Hakkında Kanun tasarı halinde bulunduğundan, kişisel verilerin korunmasının tam olarak sağlanabildiğini söylemek de mümkün değildir. Zira uygulamada bazı davalarda, kişilerin mahrem alanlarına ilişkin bazı telefon görüşme kayıtlarının, somut olay ile bir bağlantıları bulunmamasına rağmen, yargılamada okundukları görülmüştür.

Görüldüğü üzere mevzuatta, BIT ile ilişkili delillerin metin haline getirilerek, birer "belge delili" niteliğine büründürülmesi ve bu şekilde yargılamada sunulabilmesine ilişkin bazı hükümler yer almaktadır. Bununla birlikte söz konusu delillerin nitelikleri göz önüne alındığında keşfe de konu olmalarının mümkün olduğu görülmektedir. Türk ceza muhakemesi hukukunda bu deliller bakımından genel

hükümlere başvurularak, bunların keşfe konu edilmelerine engel bir hüküm bulunmamaktadır. Uygulamada özellikle bilirkişi ve uzmanlar tarafından, bu delillerin mahkemelerde keşfe konu edildikleri örnekler karşımıza çıkmaktadır.

Bu delillerin, keşif aracılığıyla muhakemede sunulmaları, "delillerin doğrudan doğruyalığı ilkesi" de dikkate alındığında daha yerinde bir yöntemdir. Nitekim örneğin, bir ses kaydı söz konusu olduğunda yalnızca bu kayıtta sarf edilen cümleler değil, aynı zamanda kişinin ses tonu veya kullandığı ses tonlaması dahi yargılamada vicdani kanaatin oluşması bakımından önem arz edebilmektedir. Bu bakımdan söz konusu delillerin metin haline getirilerek mahkemede "belge delili" olarak sunulmaları "delillerin doğrudan doğruyalığı ilkesi" ile çelişen ve yerinde olmayan bir yöntemdir.

**(2) Uzak mesafe sorgulamalarında uydu bağlantıları gibi uygulamalar kullanılabilir mi?**

Bu tür bir yöntem "Ses ve Görüntü Bilişim Sistemi" (SEGBIS) ile Türk ceza yargısında uygulama alanı bulmaktadır. Bu sistem, ifade alma ve sorgu işlemleri ile duruşmaların video kaydına alınması, yargı çevresi dışında bulunan ve hazır bulunamayan kişilerin video konferans yoluyla dinlenmesi ve ifadelerinin kayda alınması amaçlarıyla getirilmiştir. Bu yöntemle gerçekleştirilen sorgu işlemleri, istinabe suretiyle gerçekleştirilmiş sayılmadığından, CMK'da istinabe yasağı getirilen hallerde de bu yöntem kullanılarak sorgunun yapılması mümkündür.

Ceza Muhakemesi Kanunu belli durumlarda ses ve görüntü kaydını zorunlu tutmaktadır. Bu bağlamda, kural olarak tanık dinlenmesi sırasında ses ve görüntü kaydı alınması ihtiyari olmakla birlikte, bazı tanıkların dinlenmesinde ses ve görüntü kaydı alınması mecburidir. Bu kapsamda, mağdur çocukların, duruşmaya getirilmesi mümkün olmayan ve tanıklığı maddi gerçeğin ortaya çıkarılması bakımından zorunlu olan kişilerin tanıklığında ses ve görüntü kaydı yapılması zorunludur (CMK 52/3).

Ayrıca hakimin, kanuna uygun şekilde, hazır bulunma hakkı olan kişileri duruşması salonundan çıkardığı durumlarda tanığın ses ve

görüntü kaydının alınması zorunlu olup, cevap hakkı saklı tutulmuştur (CMK 58/3). CMK m. 147/1-h bendi uyarınca da, şüpheli veya sanığın ifadesinin alınması veya sorgusu sırasında ses ve görüntü kaydı alınmalıdır.

CMK m. 180'e göre de, naip veya istinabe yoluyla dinlenen tanık ya da bilirkişinin aynı anda görüntülü ve sesli iletişim tekniğinin kullanılması suretiyle dinlenmesi olanağının bulunması halinde bu yöntem kullanılarak ifadelerinin alınacağı belirtilmektedir. Değinmek gerekir ki, SEGBİS, tarih itibariyle CMK'daki düzenlemelerden daha sonra oluşturulmuş olup, maddede geçen "olanağın bulunması" koşulunun artık bu sistemle her koşulda gerçekleşmiş olduğunu kabul etmek gerekir. Nitekim, 14.12.2011 tarih ve 150 No'lu SEGBİS genelgesinde de CMK m. 180'deki durumlar, ses ve görüntü sisteminin kullanılmasının zorunlu olduğunun belirtildiği alanlardan birisidir.

Ayrıca sanığın duruşmadan bağışık tutulduğu hallerde de görüntülü ve sesli iletişim tekniğinin kullanılması suretiyle sorgusu yapılacaktır. 14.12.2011 tarih ve 150 No'lu SEGBİS genelgesinde bu durum da, söz konusu tekniğin kullanılmasının zorunlu olduğu durumlar arasında sayılmaktadır.

Mazeretleri nedeniyle hazır bulunamayan kişiler ise SEGBİS ile dinlenebileceği gibi SEGBİS üzerinden duruşmalara da katılabilirler. Bu durumda kolluk görevlileri ilgili kişiyi dinlemenin yapılacağı yerde hazır etmekle görevlidir. Bunun için, talep eden makam, dinleme yapacağı kişinin kimlik bilgilerini, dinleme zamanını ve dinleme için yapılması gereken hazırlıkları ilgili kolluk birimine bildirir. İlgili kolluk birimi, yeterli sayıda kolluk görevlisinin dinleme işlemi sırasında hazır bulunmasını sağlar (Yön. m. 13)

Ayrıca teknik yapının hazır olması halinde ceza infaz kurumundaki kişiler de SEGBİS aracılığı ile dinlenebilirler ve duruşmalara katılabilirler. Bu durumda da, Talep eden makam, dinleme yapacağı kişinin kimlik bilgilerini, dinleme zamanını ve dinleme için yapılması gereken hazırlıkları ilgili ceza infaz kurumu yönetimine bildirir ve ilgili ceza infaz kurumu görevlisi kişiyi dinlemenin yapılacağı yerde hazır etmekle görevlidir (Yön. m. 14) Bunun yanı sıra, bir tedavi kurumunda bulunanlar veya yargı çevresi dışında bulunan kişiler de bu yöntemle dinlenebilir ve duruşmaya katılabilir (Yön. 15,16).

Söz konusu Yönetmeliğe göre, dinleme sırasında dinlenecek kişinin bulunduğu yerde Cumhuriyet savcısı veya hâkimin hazır bulunması, talep eden makamın isteğine bağlıdır (Yön. m. 18). İlgililere görüntü ve ses kaydının yapılacağı konusunda bilgi verilir (Yön. m. 19). Kimlik tespitine ilişkin tutanak zorunluluk nedeniyle haricen tutulmuş ise taranıp, aslı ile aynı olduğuna dair ibare eklenerek, yine elektronik imza ile imzalanmak suretiyle dinleme talep eden makama, UYAP Bilişim Sistemi üzerinden gönderilir. Belge asılları ise mahallinde saklanır (Yön. m. 20).

Belirtmek gerekir ki, CMK'da ses ve görüntü alınmasını öngören bir hüküm olmamasına rağmen, 14.12.2011 tarih ve 150 No'lu SEGBİS genelgesinde, "sevk tutuklamaları" sırasında da bu yöntemlerden faydalanmak gerektiğine değinilmiştir. "Sevk tutuklamaları" sırasında bu yöntemlerin kullanılmasının *uygulamadan kaynaklanan mağduriyetleri gidereceği* belirtilmiştir. Ayrıca Ceza Muhakemesinde Ses Ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmeliğinin 17. maddesinde de söz konusu yöntemin kullanılacağı alanlar arasında, yakalama halinde ve yakalanan kişinin yetkili hakim/mahkeme karşısına çıkarılmasına kadar geçen sürede tutuklanmasına karar verildiği hallerde de yetkili Cumhuriyet savcısı, hâkim veya mahkemece uygun görülmesi halinde SEGBİS'in kullanılması suretiyle de dinlenebileceği hüküm altına alınmıştır (Yön. m. 17).

Bunların yanı sıra, Tanık Koruma Kanunu çerçevesinde de söz konusu uygulamanın yapılması mümkündür. Tanık Koruma Kanunu'nun 5/1-b maddesi gereğince, duruşmada hazır bulunma hakkına sahip bulunanlar olmadan dinlenmesi ya da ses veya görüntüsünün değiştirilerek özel ortamda dinlenmesi mümkündür. Tanık Koruma Kanunu'nun 9/2. maddesinde ise, Ceza Muhakemesi Kanununun 58 inci maddesinin üçüncü fıkrasının uygulanmasına mahkemece karar verilmesi hâlinde, dinleme sırasında tanığın görüntü veya sesi değiştirilerek tanınması engellenebileceği hüküm altına alınmıştır.

**(3) Dijital ve sanal teknikler olayın (ölümler, trafik kazası) canlandırılmasında kullanılabilir mi?**

Ceza yargılamasında dijital ve sanal teknikler ile olayın canlandırılmasını sağlamak bakımından özel düzenlemelere yer verilmemiştir. Kanun koyucu bu tür bir delil sunma yöntemini öngörmemiştir. Bununla birlikte bu gibi yöntemlerin kullanılması bakımından bir engel de bulunmamaktadır.

Söz konusu yöntemlerin kullanılması, genellikle uzman ve bilirkişi faaliyetini gerektiren konularda gündeme gelebilmektedir. Ancak Türk uygulamasında bilirkişiler çoğunlukla yazılı şekilde görüş bildirmekle yetinmektedir. Bilirkişi ya da uzman sıfatıyla davaya katıldıkları durumlarda kendilerine doğrudan soru yöneltme imkanı bulunmaktadır. Ancak mevzuatta engelleyici bir düzenleme bulunmamasına rağmen bilirkişi ve uzmanların dijital ve sanal teknikleri kullanma yoluna gittikleri dava sayısı son derece azdır.

**(4) Ses ve görüntü teknikleri duruşmada delil sunmak için kullanılabilir mi? (en basit şekliyle:fotoğraflar ve sesler)**

Ses ve görüntü teknikleri duruşmada delil sunmak için kullanılabilmektedir. Bu konuda telekomünikasyon yoluyla iletişimin denetlenmesi tedbiri kapsamında elde edilen delillere ilişkin bir düzenleme CMK'da yer almaktadır. Buna göre, CMK kapsamında alınmış karara dayanılarak gerçekleştirilen telekomünikasyon yoluyla iletişimin denetlenmesi tedbiri gereğince tutulan kayıtlar, cumhuriyet savcılığınca görevlendirilen kişiler tarafından çözülerek metin haline getirilmektedir. Yabancı dildeki kayıtlar ise, tercüman aracılığıyla Türkçe'ye çevrilecektir (CMK m. 137/2).

Ancak bu hüküm yalnızca telekomünikasyon yoluyla iletişimin denetlenmesi tedbiri kapsamında elde edilen delillere ilişkin özel bir düzenlemedir. Bu hüküm, tarafın getirdiği, ses ve görüntü içeren delillerin mahkemede izlenmesi ve/veya dinlenmesine vb. engel değildir. Vicdani kanaat sisteminin benimsendiği Türkiye'de, ceza yargılamasında, hukuka uygun olarak elde edilmiş her şey delil olarak sunulabilmektedir. Bu bakımdan maddi olayı ispata ilişkin ses ve görüntü kayıtları duruşmada delil sunmak için kullanılabilmekte, bu tür deliller keşfe konu olabilmektedir.

Türk ceza yargı sisteminde söz konusu teknikleri kullanmak mümkün olmakla birlikte, uygulamada yazılı savunma alışkanlığı yerleşmiş olduğundan bu tür yöntemlere başvurulan davaların sayısının oldukça az olduğunu belirtmek gerekir.

Bunun yanı sıra Türk ceza muhakemesi hukukunda, tanıkların ses ve görüntü teknikleri aracılığıyla dinlenmesine ilişkin özel hükümler de bulunmaktadır. (Bkz. (F) grubu sorular, soru (2) kapsamında verilen cevap)

**(5) "Yazılı kağıt" halindeki cezai dava dosyaları "elektronik" olanlarla değiştirilebilir mi? Yargılamanın dijitalleştirilmesi yönünde herhangi bir gelişme bulunmakta mıdır?**

Türkiye'de başlatılan Ulusal Yargı Ağı Bilişim Sistemi kapsamında (UYAP), yargıda bilişim teknolojileri uygulama alanı bulmuştur. Bu çerçevede UYAP ile entegrasyon sağlanan Adli Sicil Bilgi Sistemi'nden sabıka kayıtları, MERNİS'ten nüfus kayıtları ve Adres Kayıt Sistemi'nden adres kayıtları, POLNET'ten ehliyet kayıtları, Merkez Bankasından döviz kurları, TAKBİS'ten tapu ve kadastro kayıtları yargı birimlerince otomatik olarak anında alınabilmektedir. Ayrıca yapılan tebligatların da UYAP üzerinden takibi mümkün kılınmıştır.

UYAP Bilişim Sistemi 2000 yılında iki aşamalı olarak başlatılmış bir proje olup, 2001 yılında Adalet Bakanlığı Merkez Birimlerinin otomasyonunu sağlayan UYAP I projesi tamamlanmış, 2005 yılında adli ve idari yargı birimleri, adli tıplar, ceza tevkif evlerinin otomasyonunu kapsayan UYAP II tamamlanarak faaliyete geçirilmiştir. Yargıtay'da UYAP yazılımlarını kendisine uyarlayarak UYAP Bilişim Sistemi içerisinde yer almıştır.

Ceza Muhakemesi alanında bilişim teknolojilerini etkin kılmak amacıyla ise, 02.07.2012 tarihinde yapılan bir kanun değişikliği ile Ceza Muhakemesi Kanunu'na 38/A hükmü eklenmiştir. Bu hüküm uyarınca ceza muhakemesi işlemleri bakımından da "Ulusal Yargı Ağı Bilişim Sistemleri" kullanılacaktır. Buna göre, ceza muhakemesi işlemlerine ilişkin her türlü bilgi, belge ve karar UYAP vasıtasıyla iş-

lenecektir. Ayrıca ceza muhakemesi hukukunda da elektronik imza kullanımı, yine yapılan bu kanun değişikliği ile Türk yargı sistemine getirilmiştir.

Ancak belirtmek gerekir ki, kurulan UYAP sisteminin uygulaması henüz sorunsuz şekilde gerçekleştirilememektedir. Hala sisteme geçirilemeyen pek çok dosya bulunmaktadır. Yerel Mahkemelerdeki teknik eksikler ve iş gücü gibi gerekçelerle bütün dosyaların sisteme geçirilmesi işlemleri tamamlanamamıştır. Ayrıca bazı zamanlarda, çeşitli teknik yetersizlikler sebebiyle sisteme etkin ve hızlı bir şekilde ulaşım da sağlanmayabilmektedir. Ceza muhakemesi bakımından söz konusu sisteme geçilmesine ilişkin yasal düzenleme de temmuz 2012 tarihi itibariyle gerçekleştirilmiş olduğundan, günümüze kadar geçen sürede tüm belgelerin sisteme geçirilmesi mümkün olmamıştır.

*Preparatory Colloquium Section IV*

# SECTION 4: CONCEPT PAPER AND QUESTIONNAIRE

**Prof. Dr. André Klip**

**(A) Scope of questionnaire (see Introduction and Annex)**

The questions in this Section generally deal with "cyber crime." This term is understood to cover criminal conduct that affects interests associated with the use of information and communication technology (ICT), such as the proper functioning of computer systems and the internet, the privacy and integrity of data stored or transferred in or through ICT, or the virtual identity of internet users. The common denominator and characteristic feature of all cyber crime offences and cyber crime investigation can be found in their relation to computer systems, computer networks and computer data on the one hand and to cyber systems, cyber networks and cyber data on the other hand. Cyber crime covers offenses concerning traditional computers as well as cloud cyber space and cyber databases.

National rapporteurs can contact the general rapporteur in case of further inquiries or questions: Prof. Dr. André Klip: andre.klip@maastrichtuniversity.nl

**(B) Jurisdictional issues**

(1) (a) How does your country locate the place of the commission of a crime in cyberspace? (b) Does your national law consider it necessary and possible to locate the place where information and evidence is held? Where is the information that one can find on the web? Is it where the computer of the user is physically present? Is it there where the provider of the network has its (legal or factual) seat? Which provider? Or is it the place where the individual who made the data available? If these questions are not considered to be legally relevant, please state why.

(2) Can cyber crime do without a determination of the locus delicti in your criminal justice system? Why (not)?

(3) Which jurisdictional rules apply to cyber crime like hate speech via internet, hacking, attacks on computer systems etc? If your state does not have jurisdiction over such offences, is that considered to be problematic?

(4) Does your national law provide rules on the prevention or settlement of conflicts of jurisdiction? Is there any practice on it?

(5) Can cyber crime do without jurisdictional principles in your criminal justice system, which would in essence mean that national criminal law is applicable universally? Should this be limited to certain crimes, or be conditional on the basis of a treaty?

**(C) Substantive criminal law and sanctions**

(1) Which cyber crime offences under your national criminal justice system do you consider to have a transnational dimension?

(2) To what extent do definitions of cyber crime offences contain jurisdictional elements?

(3) To what extent do general part rules on commission, conspiracy or any other form of participation contain jurisdictional elements?

(4) Do you consider cyber crime offences a matter that a state can regulate on its own? If so, please state how a state may do that. If not, please state why it cannot do that.

(5) Does your national criminal provide for criminal responsibility for (international) corporations/ providers? Does the attribution of responsibility have any jurisdictional implications?

**(D) Cooperation in criminal matters**

(1) To what extent do specificities of information technology change the nature of mutual assistance?

(2) (a) Does your country provide for the interception of (wireless) telecommunication? Under which conditions?

(b) To what extent is it relevant that a provider or a satellite may be located outside the borders of the country?

(c) Does your national law provide for mutual legal assistance concerning interception of telecommunication? Did your country conclude international conventions on it?

(3) To what extent do general grounds for refusal apply concerning internet searches and other means to look into computers and networks located elsewhere?

(4) Is in your national law the double criminality requirement for cooperation justified in situations in which the perpetrator caused effects from a state in which the conduct was allowed into a state where the conduct is criminalised?

(5) Does your national law allow for extraterritorial investigations? Under which conditions? Please answer both for the situation that your national law enforcement authorities need information as when foreign authorities need information available in your state.

(6) Is *self service* (obtaining evidence in another state without asking permission) permitted? What conditions should be fulfilled in order to allow self service? Please differentiate for public and protected information. What is the (both active and passive) practice in your country?

(7) If so, does this legislation also apply to searches to be performed on the publicly accessible web, or in computers located outside the country?

(8) Is your country a party to Passenger Name Record (PNR) (financial transactions, DNA-exchange, visa matters or similar) agreements? Please specify and state how the exchange of data is implemented into national law. Does your country have an on call unit that is staffed on a 24/7 basis to exchange data? Limit yourself to the issues relevant for the use of information for criminal investigation.

(9) To what extent will data referred to in your answer to the previous question be exchanged for criminal investigation and on which legal basis? To what extent does the person involved have the possibility to prevent/ correct/ delete information? To what extent can this information be used as evidence? Does the law of your country allow for a Notice and

Take-Down of a website containing illegal information? Is there a practice? Does the seat of the provider, owner of the site or any other foreign element play a role?

(10) Do you think an international enforcement system to implement decisions (e.g. internet banning orders or disqualifications) in the area of cyber crime is possible? Why (not)?

(11) Does your country allow for direct consultation of national or international databases containing information relevant for criminal investigations (without a request)?

(12) Does your state participate in Interpol/ Europol/ Eurojust or any other supranational office dealing with the exchange of information? Under which conditions?

**(E) Human rights concerns**

Which human rights or constitutional norms are applicable in the context of criminal investigations using information technology? Is it for the determination of the applicable human rights rules relevant where the investigations are considered to have been conducted? How is the responsibility or accountability of your state involved in international cooperation regulated? Is your state for instance accountable for the use of information collected by another state in violation of international human rights standards?

**(F) Future developments**

(1) Modern telecommunication creates the possibility of contacting accused, victims and witnesses directly over the border. Should this be allowed, and if so, under which conditions? If not, should the classical rules on mutual assistance be applied (request and answer) and why?

(2) Is there any legal impediment under the law of your country to court hearings via the screen (skype or other means) in transnational cases? If so which? If not, is there any practice?

(3) Is there any other issue related to Information society and international criminal law which currently plays a role in your country and has not been brought up in all the questions before?

*Preparatory Colloquium Section IV*

# ANNEX - CONCEPT PAPER

**Prof. Dr. André Klip**

## (1) Introduction

The fact that modern society has changed into an information society may have dramatic consequences for various aspects of international criminal law. This justifies renewed attention within our association. It is not the first time that the AIDP looked into the topic, albeit quite some years ago, and things have changed.[1] Among other things, the globalisation of our society means that human behaviour may have its effect at many more locations than the place where the initiator of the conduct acted. Google earth, Street View, and Facebook and Hyves make clear to us that for many there is little that others may not be able to see. Big Brother is watching us, what are the implications for international criminal law? Cloud computing raises the question of where data are stored and which legislation applies to it.[2]

In the context of criminal law these extraterritorial effects of conduct may result from the use of certain technologies, such as telecommunication, computers and the web. Hackers may enter a network or an individual computer located in one state from a computer located at the other side of the world. Hate speech may be uttered through twitter, email messages or you tube tapes and have a global expansion. With regard to the material conduct various issues concerning jurisdiction over the conduct and its locus arise.

With regard to the investigations into crimes committed in modern times, the information society leads to new situations and raises new questions. The investigation into an international network for the production of child pornography and the dissemination of its products may require to visit websites, to enter their protected areas, to look into mail boxes, discussion and news groups and to identify the individual IP-addresses of computers.

---

1 See the general report by Cole Durham, The Emerging Structures of Criminal Information Law: Tracing the Contours of a New Paradigm, 64 RIDP 1993, p. 79-117.

2 See Laviero Buono, the Global Challenge of Cloud Computing and EU Law, Eucrim 2010, p. 117-124.

Also wireless means of communication poses new problems to the law enforcement agencies, because the transmission of data may involve various states or international organisations. The person using a cell phone in one state may converse with a person in another state. However, the satellite (s) transmitting the conversation may be located in other states or in space. What does this mean for the possibilities of intercepting the conversation?

In times in which there are various situations in which it is important to have a certain position of information that will enable the state to prevent or respond to terrorist attacks, states have concluded so called Passenger Name Record agreements. In addition, states have developed (common) databases that may be consulted directly without intervention of the state that supplied the information. For instance, within some states of the European Union, the DNA-database provides for direct consultation whether a new sample matches DNA-profiles already present in the national database and that of the "cooperating" state.

Thus far, despite its presence for quite some decades already, the emergence of cyber crime did not lead to much legislative activity on the international level. The main documents are the Convention on Cybercrime,[3] and its Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.[4] The drafters of the Convention on Cybercrime did relate the necessity of the convention to developments in the society as a whole.[5] What other instruments exist on an inter-

3 Budapest, 23 november 2001, ETS 185, as of 8 November 2010 30 ratifications.

4 Strasbourg, 28 January 2003, ETS 189, as of 8 November 2010 18 ratifications.

5 In the preamble to the Convention on Cybercrime the necessity of international legislation in a global information society has been descr bed with the following arguments: "Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation; Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks; Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks; Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies; Believing that an effect ve fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters."

national, regional or national level? Despite the fact that states may legislate, technological steps may make the role of private parties increasingly important.

**(2) Focus on international aspects**

As a thumb rule, relevant for the National Rapporteurs of section 4, it is important that the focus will always be on the international aspects of each segment of their national law. For instance, when rules applicable to the collection and value of evidence are identified, for section 4 it is more important to know how it is determined which state can apply its legislation on it, than to characterise the nature of this evidence in the evidentiary context of the national criminal justice system. The focus of the National Report will always be on the description of the national legal situation in an international context.

**(3) Questions related to jurisdiction over crimes and the locus of the crimes**

With the growing importance of the technical developments old legal concepts may have difficulties to keep pace. Whereas in the past it was relatively easy to locate conduct to a specific location (locus delicti), it increasingly becomes difficult to locate conduct in cyberspace. States generally have a tendency to prevent negative conflicts of jurisdiction and have increasingly extended the scope of application of their criminal law. They intended to solve the problem by widening jurisdictional principles. Additionally, the cross-border nature of the offence as such has increased multiple jurisdiction.

As a consequence of the practice of widening the extraterritorial application of criminal law, positive conflicts exist by definition. Numerous questions can be raised as a result of it. Should this be prevented? Is this problematic? Does this lead to real problems in practice, or is it in essence an academic problem?[6]

6 In a recent comparative study commissioned by the Netherlands' Ministry of Justice, Klip and Massa conclude that there are hardly any prosecutions for crimes with a locus delicti outside a state's territory. See André Klip and Anne-Sophie Massa, Communicerende grondslagen voor extraterritoriale rechtsmacht, Maastricht University 2010 http://www.wodc.nl/onderzoeksdatabase/vestiging-rechtsmacht.aspx?cp=44&cs=6802

The fact that if all states extend their jurisdiction, automatically concurrent jurisdiction comes into being, raises the question whether certain crimes, for which it may be difficult to find the locus delicti, could do without a locus. A key question is thus whether modern crimes can do without jurisdictional principles, which would in essence mean that national criminal law is applicable universally. Is this a road to follow? Should this be limited to certain crimes, for instance crimes, for which there is a conventional basis to criminalise and vest extraterritorial jurisdiction over it,[7] or should this be allowed for all crimes? In the latter situation, national criminal is applicable all over the world, which does seem to be an attractive situation. Could that be solved by allowing for prosecution in cases of a relevant nexus only? To what extent does the concurrent jurisdiction in practice lead to inertion? Does it lead to a *bystander effect*, in which states do not investigate or prosecute crimes committed outside the country, because there are many other states that may have jurisdiction over the offence?

Another way to approach things could be that for certain crimes, for which the locus delicti is difficult to find or does imply concurrent jurisdiction, supranational adjudication should be provided. The advantage would be of course that a supranational tribunal would have the power to solve the jurisdictional conflict in a manner binding to the states involved. Additionally, a more specialised tribunal and prosecution could deal with specific forms of transnational crime, which go far beyond the possibilities of national law enforcement authorities. How would an international responsibility for corporations actually work? However, it also means that1(n)115t86 dwln968 225.1934 more spemight934 6(nab40(hed, ine

information society of today and for the coming decades? Could we do without it? Which issues are at stake if the rule would be abolished? Could the interests protected by the double criminality rule be safeguarded in other manners?

**(4) Questions related to investigations**

Thus far, the rules on the collection of evidence outside the territory have been very straightforward and clear. If law enforcement agencies need information and evidence from elsewhere, they must request foreign authorities to produce it. Police officers of one state may not go without permission to the territory of another state to get what they need. The circumstances currently are somewhat different than in the past, because telecommunication networks may enable law enforcement agencies to obtain information and evidence without leaving their own country. A preliminary question is whether it is necessary and possible to locate the place where information and evidence is held? Where is the information that one can find on the web? Is it where the computer of the user is physically present? Is it there where the provider of the network has its (legal or factual) seat? Which provider? Or is it the place where the individual who made the data available?

In the context of the information society and obtaining information and evidence for purposes of criminal investigation various situations deserve attention, presumed it is still possible to locate information and evidence: 1. Open information and evidence. This is information which is publicly accessible simply by surfing through the net. 2. Protected information. Information which cannot be publicly accessed, but which may be accessed by hacking. 3. Information and evidence that require to take over a computer or network located in another country.

States continue to have rather strict rules prohibiting the physical presence of foreign law enforcement agents on their territory.[8] Do these rules still apply in the context of modern crimes? Do these rules also

8 Police officers may only enter another country and perform their duties if this finds a basis in a codified international agreement or on the basis of ad hoc permission. The use of coercive measures is generally ruled out. With minor exceptions, such as the apprehension of a fugitive in the case of a cross border hot pursuit. See, e.g. Article 41 of the Convention Implementing the Schengen Agreement.

apply when law enforcement agents do not physically enter the territory of another state, but do search in networks or computers located in another state. Do the same rules apply and if so, how do they apply? If the rules prohibiting physical presence do not apply, why is that so?

The consequences of not applying the regular rules on mutual assistance in criminal matters are more than symbolic. It would lead to a situation in which assistance from another country is no longer requested and given, but simply obtained through *self service*. This would result in a situation in which traditional grounds for refusal (double criminality, nature of the crime, double jeopardy etc) could no longer be applied. Would it be possible or necessary to reduce the application of grounds for refusal in this area? What are the (theoretical/ practical) consequences of accepting self service as one of the modalities for international assistance in criminal matters?

Once again, it seems that technical possibilities may determine the legal developments and possibilities. This phenomenon may lead to highly interesting theoretical questions about where the primacy for the development of the law should be. However, there are also questions of a more practical legal nature. An example of that relates to the interception of wireless telecommunication. If two persons converse by making use of cell phones, it may involve six states.[9] Should all these states have a say in whether conversations may be intercepted? Or should this be limited to the state that wishes to intercept and why (not)?

Some states and international organisations possess satellites or other devices that enable them to have a clear and detailed picture of every place in the world. Should the law regulate the use for purposes of criminal investigation and prosecution? If so, on which level should this be regulated, national or international and what are the issues at stake?[10]

9 Gert Vermeulen, Wederzijdse rechtshulp in strafzaken in de Europese Unie, dissertation Gent 1999, p. 224-293.

10 It reminds us of the "telescreens" predicted by George Orwell in his famous novel 1984.

**(5) Questions related to classical mutual assistance in criminal matters**

To what extent does the information society change the nature of classical mutual assistance?[11] Although some forms of self service may come up and may even be legally accepted, it is unlikely that international mutual legal assistance in criminal matters will completely disappear with the further development of the information society.

The very fact that it has become increasingly simple to speak with persons abroad through audio-visual techniques (Skype, videoconference) raises the question whether this should not lead to a higher threshold for extradition for the purposes of prosecution. If the accused is not present in the state that prosecutes him extradition is likely to take place. In light of the serious infringement on the liberty of the accused, the question may be raised whether it should be preferred to conduct the trial via a video-link. Also the presumption of innocence would oppose burdensome extradition. Should we reserve extradition for convicted persons? Do we envisage a virtual court room, in which hearings may take place, whilst nobody is present in the real court room?

Similarly, modern telecommunication creates the possibility of contacting accused, victims and witnesses directly. Should this be allowed, and if so, under which conditions? If not, should the classical rules on mutual assistance be applied (request and answer) and why? The very fact that a lot of information is freely accessible anyway and that in many cases persons involved have submitted the information voluntarily, raises the question why states should still have the power to control whether assistance will be given or not. On the other hand, the view on whether a certain act is within the realm of freedom of speech or a serious crime of breaking confidentiality may differ. Imagine, the US wants certain information in order to investigate the fact that numerous secret and restricted documents concerning the Iraq war have been made available through wikileaks.

What about obligations to retain data on information transmission? Do providers have the obligation to organise their network in such a manner

11 It is interesting to see that the Convention on Cybercrime completely follows the classical principles of international cooperation in criminal matters: a request send by one state to another to render assistance.

that they may comply with all different and complicated request for assistance from law enforcement agencies of other states? How could this be done with providers not having a seat in the relevant state? Also of a more general nature is, apart from the relevant legislation, the question whether states do have the know-how to deal with crimes committed in the information society. Do law enforcement agencies have the expertise to effectively investigate and enforce the offences in cyberspace?

### (6) Questions related to obtaining an information position[12]

Especially as part of a package of measures related to combating terrorism states are eager to obtain a good information position in order to prevent terrorist attacks or other crimes from taking place. Given the use of air traffic in the past, as a means of terrorist attacks, states have given priority to have more knowledge on passengers and on freight. Regarding passengers, so called Passenger Name Records agreements have been concluded.[13] Also in other areas, such as financial transactions and visa matters, data are exchanged.

We must be aware of the fact that we are entering here the sphere of privacy law. Whereas on the hand, it should be prevented that the focus of our discussions should be on the elements of the protection of privacy, it is, on the other hand, inevitable that some elements of privacy law will be discussed. National Rapporteurs are requested to focus on the use made for criminal investigations of data submitted or exchanged under PNR (financial transactions or any other) agreements for criminal investigation, not for other purposes such as immigration policy or data retention rules in general. To what extent will the data be exchanged for criminal investigation and on which legal basis? To what extent does

12 It is referred to the definition given by Hans Nijboer, General Rapporteur to Section III: "The existence and the use of enormous amounts of operational information is sometimes referred to as the ***information position*** of investigative and prosecutorial authorities.

13 The EU concluded agreements with the United States and with Australia on this matter. See http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/431&format=HTML&aged=0&language=EN&guiLanguage=en Council Decision 2010/16/CFSP/JHA of 30 November 2009 on the signing, on behalf of the European Union, of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, OJ 2010, L 8/11.

the person involved have the possibility to prevent/ correct/ delete information? To what extent can exchanged information be used as evidence?[14]

A further recent development is the establishment of supranational databases and the online consulting of each other's databases. An example of that relates to the EU, in which some Member States have established a mechanism to retrieve data on DNA, licence numbers of vehicles and finger prints directly from another Member State.[15] One of the consequences is, that the state whose data is used, no longer is requested to give information and does not take a decision in individual cases to do so. It also means that grounds for refusal are no longer considered and applied in the initial stage of information exchange.[16] Is this a good development? Within the EU further plans have been developed to create direct access to the criminal records of all Member States.[17] Is that a good thing? Can similar developments be identified in other regions of the world?

**(7) Questions related to direct enforcement**

The almost unlimited possibilities of information technology do raise questions with regard to whether states may directly enforce judgments, notifications, provisional measures etc by making use of information technology, without asking permission of whatever other state.

---

14 In the EU context, a special legal instrument has been adopted regulating the data protection rules in international cooperation in criminal matters. See Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ 2008, L 350/60.

15 Council Decision 2009/1023 of 21 September 2009 on the signing, on behalf of the European Union, and on the provisional application of certain provisions of the Agreement between the European Union and Iceland and Norway on the application of certain provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, and the Annex thereto, OJ 2009, L 353/1; Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross- border cooperation, particularly in combating terrorism and cross-border crime, OJ 2008, L 210/1.

16 However, the relevant legal instruments stipulate that if the information is to be used as evidence, a regular request for international assistance must follow.

17 Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ 2009, L 93/23.

In a situation in which there is a legal decision that a certain website must close down, because it contains child pornography, hate speech or other illegal material, should it be allowed for law enforcement agencies to hack that site in order to prevent it from further committing crimes?

The notification of judgements, decisions, summons and other legal documents may have legal consequences. Should the law attach these consequences also to notifications send by information technology?[18] Similarly, should states have the competence to impose upon banks and other financial institutions to confiscate certain financial means in order to keep this for purposes of confiscation of proceeds from crime?

**(8) Concluding remarks**

In sum, at first sight, it seems that the impact of the information society to international criminal law is threefold. The first is that the information society creates a transnational threat for certain legal goods, whilst other may remain unaffected by it. The second is that the information society creates, on the other hand, a tool for criminal justice. The third major impact relates to sovereignty. What does sovereignty mean in our age? Traditionally, the concept of sovereignty gives states a monopoly on the application of criminal law and criminal procedure, based on the territoriality principle. The information society has seriously decreased (or maybe even taken away) the value and importance of territoriality. What does this mean for sovereignty? In sum, the focus of this section is on the extraterritoriality of the conduct, the extraterritoriality of the investigation and the extraterritoriality of the enforcement.

18 In 2010, e.g., the German postal services introduced the electronic Zustellung, equal to a formal notification by an usher.

*Preparatory Colloquium Section IV*

# REPORT OF THE TURKISH NATIONAL GROUP

**Assistant Prof. Dr. Murat Önok***
**Assistant Prof. Dr. Barış Erman****
**Dr. Güçlü Akyürek*****

## (B) Jurisdictional issues

### (1) (a) How does your country locate the place of the commission of a crime in cyberspace?

The Turkish law regulates the place of the commission of a crime under art. 8/1 of the Turkish Criminal Code (TCC), together with the principle of territoriality. The provision is as follows: "Turkish law shall be applied to crimes committed in Turkey. The crime shall be deemed to have been committed in Turkey if the conduct has been committed in whole or in part in Turkey, or if the result has occurred in Turkey". Following paragraphs of the same article concern instances where the principle of territoriality is expanded (in cases like the flagship principle).

Although art. 8/1 only mentions the "applicability of Turkish law", it is generally understood that the article actually concerns the jurisdiction of Turkish criminal courts, and defines the place of the commission of the crime.

In establishing the *locus delicti,* art. 8/1 TCC combines initiatory and terminatory theories of territoriality and adopts the principle of ubiquity like the German criminal law, according to which, both the place of the commission of the conduct, as well as the place where the result occurs, are considered as places of the commission of the crime. Thus, any content that can be accessed from any person in Turkey can possibly be described as a crime committed

* Koç University Law Faculty
** Yeditepe University Law Faculty, Department of Criminal Law and Criminal Procedure
*** Galatasaray University Law Faculty, Department of Criminal Law and Criminal Procedure

in Turkey[1]. Unlike art. 9 of the German Criminal Code, the Turkish article 8 does not provide any further specification the term "result", and refrains from narrowing it down to a "typical", "direct" or "effective" result. As a consequence, any result attributable to the criminal conduct may trigger the territorial jurisdiction of Turkish courts[2].

Since crimes committed in cyberspace may, in many cases involve more than one jurisdiction, the acceptance of the principle of ubiquity can cause several problems regarding conflicts of jurisdiction (particularly positive conflicts), and the exercise of jurisdictional authorities in cases of criminal procedure and sentencing.

Nonetheless, in Turkish criminal law literature, it is widely accepted that crimes committed in cyberspace should be accepted as committed in Turkey if the criminal content has been uploaded by a content provider in Turkey, stored in servers existing in Turkey, or has been accessed from Turkey[3]. Furthermore, in case of accessing a specific content from Turkey, it is widely deemed irrelevant whether a "pull-technology" (i.e. any method of access depending on the will of the end-user) or a "push-technology" (i.e. any method depending on the will of a person exercising control over the content, such as the content provider or the host) has been used.

The role of access providers on the *locus delicti* is rather obscure. Although, as a rule, access providers are not responsible for failing to exercise control over contents provided by third parties (as provided by art. 6 of the Law 5651 on the Regulation of Publications on the Internet and on Combating Crimes Committed Through such Publications – Internet Law), this doesn't necessarily mean that their actions or contributions cannot be taken into

1 DEMİRBAŞ, Timur; Ceza Hukuku Genel Hükümler, 8ᵉ, Ankara, 2012, p. 140-141; ÖZBEK, Veli Özer, Müstehcenlik, Ankara, 2009, p. 190-191.

2 TEZCAN, Durmuş / ERDEM, Mustafa Ruhan / ÖNOK, Murat, Uluslararası Ceza Hukuku, Ankara, 2009, p. 89.

3 ARTUK, Mehmet Emin / GÖKCEN, Ahmet / YENİDÜNYA, Caner; Ceza Hukuku Genel Hükümler, 4ᵉ, Ankara, 2009, p. 1051.

account when determining the place where a crime has been committed. As mentioned above, art. 8 clearly defines the term "a crime committed in Turkey" as to include "any conduct committed in whole or in part in Turkey". The term "conduct" is to be understood as any action or omission pertaining to the material element of a criminal offense as defined by the Turkish criminal law, that has a casual effect on the realization of the result (or the violation of the legal interest) of that offense. As such, since access providers are not considered as "perpetrators" for crimes committed by other actors, the mere fact that an access provider is situated in Turkey should not mean that the principle of territoriality could be applied on a specific crime.

Art. 4/2 of the Turkish Internet Law provides that content providers shall be responsible for extraneous content they provides links for, if, taking into account the form of presentation, it is obvious that he or she adopts the content, and intents that the end user accesses that content. It should be emphasized that, in criminal law, the mere action of providing a link would, as a rule, only result in a responsibility for being an accessory to the crime. According to Turkish criminal law, this would not be sufficient to deem that the crime was committed in Turkey, if the person providing the link would be situated in Turkey, whereas the actual content would be present in another country. However, as a result of the wide interpretation of the principle of ubiquity, the crime would have to be deemed to have been committed in Turkey at the latest when the original content is accessed from an end user situated in Turkish territory.

It should be noted that the principle of ubiquity as adopted by art. 8 TCC is strongly criticised by the Turkish criminal law literature, particularly for crimes committed on the cyberspace. This issue is further addressed under B/5.

**(b) Does your national law consider it necessary and possible to locate the place where information and evidence is held? Where is the information that one can find on the web? Is it where the computer of the user is physically**

**present? Is it there where the provider of the network has its (legal or factual) seat? Which provider? Or is it the place where the individual who made the data available? If these questions are not considered to be legally relevant, please state why.**

Since the place of the information is not relevant for the determination of the jurisdiction, it is not considered as a problem of primary concern for the power to adjudicate in criminal matters. However, the exercise of jurisdictional powers may sometimes depend on the information to be stored in servers located in Turkey. This is particularly the case when the cooperation of a server located abroad is needed in order to investigate or prosecute a criminal conduct committed in Turkey (in the sense of art. 8 TCC). In such cases, the rules on judicial assistance and cooperation in criminal matters shall be applicable, even though Turkey accepts its power to adjudicate due to the principle of territoriality.

However, the most important point of relevance regarding the location of the information does not arise directly from the criminal justice system, but rather from the Turkish Law of Internet. According to art. 8 of the Law, a precautionary measure may be applied to websites with criminal content, banning access to such content. This precautionary measure is, as a rule, to be ordered by a judge during a criminal investigation, or by a court during trial (after the indictment). In urgent cases, an order by a prosecutor may initiate the measure; however, this order is subject to judicial review within 24 hours). However, in cases where the content provider or the host of the content is situated abroad, or where the offense concerns sexual abuse of children or pornography, the measure may be taken by an administrative authority (the Presidency of Telecommunications). According to the legal practice of Turkey, only the respondent of an administrative or legal measure may bring a motion to dismiss the measure. Since, however, the respondents of this administrative measure are mostly situated abroad, the orders of the Presidency of Telecommunications can rarely be challenged before Turkish courts, and, as a result, have permanent effects. It is therefore important for the Turkish legal practice to determine the location of a particular piece of information or evidence.

In the Turkish legal practice, there is a general consensus on the fact that a piece of information is located at any place where it is stored. This may mean the place where the servers of the host and/or the content provider are situated, or where the computer of a user is located (if that user downloaded the information to his or her own computer).

This question may bear particular importance if the data was is not stored by the person exercising control over the said data, as may be the case if a particular piece of information is stored abroad through the use of cloud computing technology. Although, in such cases, the user may be considered as "owning" or "possessing" a particular piece of information, the place where that information is located would be different from the location of the user.

Access providers, as discussed under (1/a), cannot be held responsible for the actions or omissions of content providers or hosts, but they may be considered as "possessing" a piece of information (such as data legally retained by access providers) as long as they have control over it. Such information can be said to be "located" where the access provider is situated.

The legal seat of a host is also relevant for purposes of the Law of Internet. The authority of the Presidency of Telecommunications to issue banning orders depends on the host "being situated abroad". This would mean that its legal seat is to be taken into account. In addition, for purposes of the applicability of judicial assistance and cooperation in criminal matters, the legal seat of a host is important in determining the respondent state.

**(2) Can cyber crime do without a determination of the locus delicti in your criminal justice system? Why (not)?**

The determination of the *locus delicti* is necessary in order to determine whether or not the double criminality rule is to be applied to a certain crime. The Turkish Criminal Code requires the double criminality rule in cases where the power to adjudicate bases on active personal jurisdiction. Although, in most cases, cyber crimes shall be deemed to have been committed in Turkey

due to the ubiquity principle, the *locus delicti* could be relevant when, even after the implementation of the ubiquity principle, the crime can still be considered as committed abroad. This may happen when the cybercrime in question does not arise from the "content" of a website, but rather from an attack using the Internet or other international networks, or a physical attack against computer systems[4]. If, for instance, a person would attack another person's computer in order to obtain that person's personal data, the principle of territoriality would not be applicable if both parties are abroad. In such cases, the principle of personality would have to be applied.

Another issue regarding the determination of the *locus delicti* is the acceptability of extradition requests from Turkey. According to art. 18 TCC, only perpetrators that committed a crime outside of the Turkish territory may be subject to extradition. In other words, if it is established that a cyber crime has been committed in Turkey due to the ubiquity principle, the perpetrator cannot be extradited by Turkey, but must be prosecuted by Turkish authorities.

The *locus delicti* is also important for the applicability of the principle of *ne bis in idem*. In general, the Turkish criminal law applies *ne bis in idem* internationally, which means that any judgment passed by a court on the same material event prevents Turkish courts from trying a case. However, crimes deemed to have been committed in Turkey are exempt from this rule (art. 9 TCC). As a result, a person that commits a crime in Turkey and is then convicted or acquitted abroad, may again be subject to trial for the same conduct by Turkish courts. There exist two further exceptions: In case of crimes against the Turkish state committed abroad, the principle of *ne bis in idem* may be disregarded upon the request of the Minister of Justice (art. 12/4, only applicable for crimes for which the lower limit of punishment is set as a minimum of 1 year of imprisonment). Additionally, some crimes falling under universal jurisdiction of Turkish courts (genocide, crimes against humanity, migrant smuggling, human trafficking) or under the

4 ARTUK/GÖKCEN/YENİDÜNYA, p. 1051.

principle of protection (crimes against the state), may be tried again before Turkish courts in spite of an existing conviction or acquittal by a foreign court (art. 13/3 TCC)[5]. For cyber crimes, this would mean that any conduct deemed to have been committed in Turkey would be eligible for a trial before Turkish courts, even if there is an existing sentence by other courts. In addition, cyber crimes against the Turkish state, such as the unlawful dissemination of Turkish state secrets, could be tried before Turkish courts without taking into account previous sentences of foreign courts, even if the conduct and the result of the offense occurred exclusively outside Turkey.

Lastly, the *locus delicti* has an effect on sentencing. Crimes committed outside the Turkish territory shall not be punished with a higher sentence than the upper limit of punishment for an equivalent offense provided by the *lex loci* (art. 19 TCC). This rule is not to be applied in cases of the offense being committed against a Turkish real or legal person, or against the security of Turkish Republic. This provision is not only the basis for the *double criminality rule* in cases of active personal jurisdiction, but also limits the legal limits of sentencing applicable to courts.

**(3) Which jurisdictional rules apply to cyber crime like hate speech via internet, hacking, attacks on computer systems etc? If your state does not have jurisdiction over such offences, is that considered to be problematic?**

There are no specific jurisdictional rules regarding cyber crimes under Turkish law. As a result, objective or subjective territorial jurisdiction shall be applicable in most cases due to the ubiquity principle as explained above. It should be noted that most, if not all cases of public defamation of persons (art. 125 TCC), denigration of the Turkish nation (art. 301 TCC), incitement of a group of

5 Turkey reserved its right not to recognise the effects of ne bis in idem principle in cases when the crime has occurred on its territory, in accordance with art. 35 of the 1972 European Convention on the Transfer of Proceedings in Criminal Matters, and art. 53 of the 1970 European Convention on the International Validity of Criminal Judgments. For detailed information, see: TEZCAN/ERDEM/ÖNOK, p. 121.

people to animosity against another (art. 216 TCC) and other crimes committed through forms of expression, would fall under the jurisdiction of Turkish courts due to the principle of territoriality. However, other grounds for establishing jurisdiction may come into consideration for crimes committed on the cyber space, such as attacks against other computer systems or networks, illegally obtaining personal data of others, or hacking.

Turkish criminal courts may also have jurisdiction on the following grounds: active personal jurisdiction (art. 10, 11 TCC) or passive personal jurisdiction (art. 12/2 TCC), the protective principle for crimes against the state (arts. 12/1, 13/1/b TCC), and universal jurisdiction (arts. 13/1/a, 13/1/c-i TCC). It should be noted that the list of crimes for which universal jurisdiction is applicable under Turkish law is very extensive, and encompasses not only core crimes against the international community (genocide and crimes against humanity), but also many transnational crimes (such as migrant smuggling, human trafficking, torture, polluting the environment, drug trafficking, forgery of money, solicitation for prostitution, etc. However, crimes under universal jurisdiction can only be subject to a criminal investigation or prosecution upon a request by the Minister of Justice (art. 13/2 TCC). In addition, crimes may be prosecuted by Turkish courts due to the complementary principle, according to which, a crime committed outside the Turkish territory by a non-Turkish citizen against another non-Turkish citizen may, be prosecuted by Turkish courts if the perpetrator is caught in Turkey and his or her extradition is not possible (art. 12/3).

According to arts. 11, 12 TCC, in cases of active and passive personal jurisdiction, the lower limit provided by Turkish law for the punishment of the crime cannot be lower than 1 year of imprisonment (in case of active personal jurisdiction, crimes with a punishment of lower than 1 year of imprisonment may still be prosecuted by Turkish courts upon the impeachment of the victim or the government of the *locus delicti* state). The limit is 3 years of imprisonment for cases falling under the principle of complementarity (art. 13/3 TCC), and the request of the Minister of Justice is required.

As such, if a crime cannot be considered as having been committed in Turkey, other principles may apply in order to establish the jurisdiction of Turkish courts. This may be the case where the entire conduct and the result of a crime as provided by law happened outside the territory of Turkey, but either the perpetrator or the victim was of Turkish nationality, or the crime was committed against the interests of the Turkish Republic. For example, the dissemination of (Turkish) state secrets online would fall under the protective principle (art. 13/1/b TCC) and would establish jurisdiction for Turkish criminal courts.

The lack of jurisdiction is rarely considered as a problem, because Turkish courts tend to have excessive jurisdiction for many cyber crimes. The only problem may be that some conduct that is generally considered as criminal by other legal systems may have not been defined as criminal offenses under Turkish law. This is the case for "hate speech". Although a comparable criminal offense (incitement of a group of people towards animosity against another – art. 216 TCC) exists under the Turkish Criminal Code, it does not include many of the types of behaviour generally defined as "hate speech" by other legal systems. In many such cases, the Turkish criminal offense on "defamation of persons" (art. 125) would be applicable. However, this offense not only requires a specific person or a group of people determined specifically to be addressed by the perpetrator, the punishment provided for its basic form is lower than 1 year of imprisonment, which would mean that any grounds other than territoriality would not be applicable for such crimes.

**(4) Does your national law provide rules on the prevention or settlement of conflicts of jurisdiction? Is there any practice on it?**

The principle of complementarity (explained under B/3) was accepted to avoid negative conflicts of jurisdiction, in accordance with art. 2 of the European Convention on the International Validity of Criminal Judgments[6]. However, in cases of cyber crimes, positive conflicts pose a more significant problem than negative ones.

6 See: TEZCAN/ERDEM/ÖNOK, p. 161.

One method of avoiding positive jurisdictional conflicts under Turkish law is the provision of the art. 19 TCC that allows taking into consideration the upper limit of punishment applicable to the same conduct according to the law of the *locus delicti*. However, as explained above (under B/2), this provision cannot be implemented when the territorial principle is applicable.

The Turkish criminal system has also tried to mitigate the vast excessiveness of the jurisdiction through introducing a checks-and-balances system that requires the request of the Minister of Justice as a precondition of exercising jurisdiction for certain extraterritorial crimes: crimes under the principles of universality (art. 13/2 TCC), crimes committed against the state (except crimes against state security) (art. 12/1 TCC) and when the complementary principle is to be applied (art. 12/3 TCC). In addition, some extraterritorial crimes can only be prosecuted upon a complaint by the victim or the government of the *locus delicti* state: crimes falling under active personal jurisdiction, for which the lower limit of punishment is lower than 1 year in prison according to Turkish law (art. 11/2 TCC), and crimes falling under passive personal jurisdiction (art. 12/2 TCC).

As a last possibility in a regional international level, Turkey has the possibility to transfer criminal proceedings according to the European Convention on the Transfer of Criminal Proceedings. If Turkey agrees with another State Party to the Convention to transfer a proceeding in order to overcome a positive conflict of jurisdiction, it can do so under this or a similar treaty[7]. However, there are no notable examples for this in practice.

**(5) Can cyber crime do without jurisdictional principles in your criminal justice system, which would in essence mean that national criminal law is applicable universally? Should this be limited to certain crimes, or be conditional on the basis of a treaty?**

The adoption of the ubiquity principle in determining the territorial jurisdiction of Turkish courts leads to several problems,

7 TEZCAN/ERDEM/ÖNOK, p. 161-162.

which is also a point of criticism among the majority of the Turkish legal doctrine. Consequences of the excessive applicability of territorial jurisdiction arise in criminal procedure as well as substantive criminal law.

In Turkish law, if the jurisdiction is established based on territoriality, the principles of double criminality and *ne bis in idem* are not applicable. This means that any person committing a conduct from abroad may be prosecuted by Turkish courts, if the result of that conduct occurred in Turkey, and if the person is caught by Turkish authorities, without taking into account whether or not the same conduct is defined as a criminal offense in the country of origin, and whether the subject was tried and convicted or acquitted by a court of another country. Apart from the general point of concern regarding the "non-interference in internal affairs" principle, some practical drawbacks of this result can be listed as follows:

a) In case of a simultaneous application of the same principles by various states a person may be under a disproportionate threat of punishment for a certain criminal act.

b) A person not aware of the applicability of the Turkish law on his or her conduct may have acted in full disregard of the fact that he or she might be criminally liable according to the law of a state foreign to that person.

c) If the principle of territoriality is also to be applied in cases of a "pull-technology", the fact that the result has occurred in Turkey may even be outside the ability of the perpetrator to control the outcomes of his or her actions. As such, the territorial jurisdiction may be based on random events rather than actions controlled by free will.

d) Turkey would be under the threat of becoming a "haven" for the prosecution of cyber crimes, for which the victims, in their view, do not find sufficient protection from their national legal systems.

There are also some points of concern arising from the criminal procedure system. These can be listed as follows:

a) The vast number of cases falling under the territorial jurisdiction of Turkey would make it a burden for the court system to deal with. Turkey would be forced to use a selective approach to such cases, which would not only be unlawful according to the Turkish criminal procedure system, but also unconstitutional due to the violation of the principle of equality.

b) Turkey would be forced to resort to international criminal assistance and cooperation in order to gather evidence for a crime committed on its territory. This would mean that the principle of double criminality would have to be respected.

c) In most cases, Turkey would be able to investigate and prosecute due to the territorial principle, but would not be able to conclude the trial phase. This would be the case if the accused or the defendant is outside of Turkey (trials and sentencing *in absentia* are as a rule not permitted in the Turkish criminal justice system – trials may only proceed for "fugitive" defendants, while sentencing *in absentia* is only possible if the defendant has previously appeared and interrogated before the court).

d) The same is true for the lack of evidence. According to Turkish law, prosecutors are subject to a very strict principle of legality in pursuing evidence and in filing indictments. In other words, as a rule, prosecutors do not have discretionary powers, neither on whether or not to investigate, nor on whether or not to file an indictment in the face of sufficient evidence. It is also widely accepted that Turkish courts retain the power to make further investigations during the trial phase (following the inquisitorial system). As a result, the mere fact that a particular piece of evidence is situated abroad shall not hinder a Turkish prosecutor from investigating of from filing an indictment in a criminal proceeding, however important that piece of evidence may be for the case. If, however, that piece of evidence cannot be obtained until the end of the trial phase, it is probable

that such cases would not result in a conviction, although they would cost substantial amounts of time and money for the state[8]. Therefore, the rules concerning the power to adjudicate and to exercise jurisdiction should be in harmony to prevent unnecessary or unfruitful criminal investigations.

There exist several views in the Turkish doctrine that support the need to restrict the existing principles, particularly for cyber crimes. Such recommendations typically involve the adoption of stronger nexus between the conduct and Turkey, requiring either the presence of the server where the data is stored[9], or the criminal content being uploaded from Turkey[10].

Another suggestion is to make the applicability of the territorial principle dependable from the will of the perpetrator: the crime should only be considered as having been committed in Turkey if the perpetrator aimed for a result to appear specifically on Turkish territory[11].

Additionally, the principle of ubiquity is criticised for being outdated[12]. However, there are also differing opinions that support a wide definition of territoriality, whilst agreeing that some jurisdictional problems might arise[13].

It is indeed necessary to adopt a jurisdictional principle that would affect the restriction of the territorial principle for cyber crimes. However, the fact that cyber crimes are a major cause for problems arising from a positive conflict of jurisdictions only indicates that the real problem is caused by an excessive definition of territorial jurisdiction. As such, any solution based on restricting the jurisdiction solely for cyber crimes would be palliative in nature. A thorough international system to avoid or overcome conflicts of jurisdiction would be more favourable. This could be in

8 See: ÖZBEK, p. 193.
9 DEMİRBAŞ, p. 141.
10 ÖZBEK, Veli Özer / KANBUR, M. Nihat / BACAKSIZ, Pınar / DOĞAN, Koray / TEPE, İlker, Türk Ceza Hukuku Genel Hükümler, Ankara, 2010, p. 141.
11 ÖZBEK, p. 194.
12 ÖZBEK, p. 191.
13 ARTUK/GÖKCEN/YENİDÜNYA, p. 1051.

the form of an international convention, setting standards for territoriality stricter than existing international instruments. This system could also include a simple conflict-solving mechanism, such as a permanent body with the sole purpose of arbitrating conflicts of jurisdiction. The authority of this body may also be limited to some types of criminal conduct, such as cyber crimes, but it would be more advisable not to.

In contrast, the formation of a supranational body to rule over cyber crimes is neither advisable, nor, in our opinion, possible. This would mean that an elaborate international tribunal would be founded, which would require infinite funding because of the immense quantity of cyber crimes occurring in global scale. In addition, an international regulation of the cyber space could lead to an excessive restriction of civil liberties, and could prove a futile effort: international legal instruments would be overly inefficient and would easily become obsolete in the light of the rapid development in the field of information technology.

**(C) Substantive criminal law and sanctions**

**(1) Which cyber crime offences under your national criminal justice system do you consider to have a transnational dimension?**

It should be noted that in most cases, the "transnational" dimension of cyber crimes does not arise from the nature of the offenses, but rather from the typical methods of their perpetration. In that sense, they differ from truly transnational crimes, such as migrant smuggling, exportation or importation of drugs, or bribery of international public officials.

The first group of criminal offenses that are frequently committed on international networks are crimes against computer systems, such as hacking or cracking. Although a transnational element is not necessary for such conduct, it is a fact that most of these crimes are committed either using anonymising systems or proxies situated abroad in order to prevent backtracking. As such,

internationalised criminal investigations may be called for. This is particularly the case for acts of cyber-terrorism.

Another group of cyber crimes that can be deemed as "transnational" may be child pornography. Although the crime itself can hardly be considered as "transnational", and can be committed on a truly national level, the modus operandi of international criminal networks and organisations specialised in this area mostly involves the use of the Internet.

As a similar group, crimes against intellectual property could be mentioned. Again, the Internet is frequently used as a modus operandi for a crime that is not necessarily committed transnationally.

A true transnational cyber crime under Turkish legal system is the providing of access to gambling and wagering games abroad (see the answer below).

**(2) To what extent do definitions of cyber crime offences contain jurisdictional elements?**

The only example of a jurisdictional element in the definition of a cyber crime is the offense of "providing access from Turkey to gambling and wagering games abroad through the Internet or through other means", as provided by the Law on the Regulation of Wagering and Games of Chance in Football Matches and Other Sports Competitions, art. 5. This crime expressly requires for the gambling or wagering to happen outside of Turkey, while the action of "providing access" to such games would have to be perpetrated from the Turkish territory.

Another specific rule regarding jurisdictional elements with relation to cyber crimes can be found under the Turkish Law of Internet, according to which the procedural measure of banning access to criminal content on the Internet may be exercised by the administrative authority of Presidency of Telecommunications, if either the host or the content are situated abroad (see B/1/b).

**(3) To what extent do general part rules on commission, conspiracy or any other form of participation contain jurisdictional elements?**

There exist no specific rules on any part of participation containing jurisdictional elements. Due to the principle of accessoriness (art. 40 TCC), all actions or omissions of people participating in the crime of another are bound to the conduct of the actual perpetrator. This means that only the perpetrator committing the crime shall be taken into account when determining the *locus delicti*. In case of more than one person co-perpetrating the crime, the fact that one of them has committed the crime in whole or in part on Turkish territory would be sufficient to establish territorial jurisdiction.

In case of other forms of participation (accessorship, aiding and abetting, instigation), the crime is considered as committed in Turkey only if the actual perpetrator committed the crime in Turkey. In other words, if the actual perpetrator committed the crime abroad, territorial jurisdiction shall not be established, even if the participators realised their contributions or instigated the crime from Turkey.

Conspiracy as a form of participation does not exist under Turkish law. There is only the crime of membership in a criminal organisation, where special rules concerning aiding and abetting apply (art. 220 TCC). As such, any person becoming a member to a criminal organisation that is active in Turkey would have committed that crime in Turkey.

The majority opinion in the Turkish legal literature criticises this lack of jurisdictional elements to the rules on participation for causing gaps in criminal liability[14]. However, there also exists another opinion defending the current Turkish provisions, and considers them as a conscious choice of the Turkish legislator[15].

14 ARTUK/GÖKCEN/YENİDÜNYA, p. 1050.

15 ÖZGENÇ, İzzet, Türk Ceza Hukuku, 5e, Ankara, 2010, p. 770.

**(4) Do you consider cyber crime offences a matter that a state can regulate on its own? If so, please state how a state may do that. If not, please state why it cannot do that.**

In order to ensure effective international judicial assistance and cooperation in criminal matters, to create the possibility to extradite cyber criminals, a harmonisation process for cyber crimes is advisable. However, an overcriminalisation or overregulation restricting human rights and civil liberties that are the essence of the activity in international digital networks should be avoided. Particularly, users should not be forced to use identity-revealing software or methods in order to prevent crime, as this would cause the suppression of legal opposition in repressive regimes. Additionally, the privacy of users should not be compromised. As an additional drawback of overcriminalisation it should be considered that any international instrument excluding some states would lead to the creation of safe havens, particularly in the field of cyber crimes. It is also not advisable to adopt international principles or provisions that would undermine procedural or constitutional guarantees, or that would cause criminal liability for the possession of data or software that can be used for legitimate purposes, or for mere preparatory acts.

As mentioned above, the process of harmonisation should not lead to the creation of a supranational body with the authority to rule over cyber crimes or applying precautionary measures such as blocking or restricting access to content found online.

**(5) Does your national criminal provide for criminal responsibility for (international) corporations/ providers? Does the attribution of responsibility have any jurisdictional implications?**

According to Turkish law, legal persons cannot be "perpetrators" of crimes, but can be subject to confiscation of goods and benefits, if certain crimes have been committed intentionally by a real person to the benefit of that legal person (art. 20, 60 TCC). There are no specific rules of jurisdiction for the application of this

measure. As a result, goods and benefits of legal persons situated abroad may be subject to confiscation by Turkish courts, provided that the crime has been committed in Turkey, or the jurisdiction of Turkish courts can be established on other grounds. However, Turkey can only exercise this jurisdiction for goods and benefits that are present on Turkish territory, such as accounts in banks operating under Turkish law, since it would not have the authority to enforce a confiscation order in another country.

Additionally, international hosting companies can be subject to banning orders for the content they host, under the Turkish Law of Internet. However, these orders are not considered as criminal sanctions, but rather procedural and/or administrative measures, to be ordered in cases where a sufficient level of suspicion exists pointing to the commission of crimes listed under the same article[16].

**(D) Cooperation in criminal matters**

**(1) To what extent do specificities of information technology change the nature of mutual assistance?**

**A. General Information**

Classical methods of legal cooperation fall short of the needs in fighting cyber crimes for the following reasons:

a) Cyber criminality is a new phenomenon, the modus operandi of cyber criminals is very diverse, and new modalities of commission of cyber crimes appear every day. As a result, law enforcement officials involved in the fight against cybercrime need to possess very deep technical knowledge. Hence, they need to be trained, and their knowledge needs to be updated constantly. As a result, units involved in legal cooperation also need to have the requisite technical and technological knowledge in order to be able to appropriately deal with assistance requests.

16 This list includes the following crimes: Incitement to suicide, sexual harassment of children, facilitating the abuse of narcotic drugs, providing material dangerous to public health, obscenity / pornography, providing place or means for gambling, and crimes against the memory of Atatürk.

b) The definition of both the concept of "cyber crime", and the different types of cyber crimes in not uniform in comparative law. This is a problem since inconsistencies between the substantive criminal law of different states pose an obstacle to legal cooperation. Furthermore, the "double criminality" requirement embodied in international cooperation (and extradition) treaties is also a challenge. Hence, it is important to harmonize, as far as possible, both substantive and procedural rules concerning cybercrime.

c) In addition, the fight against cybercrime, to make any sense, needs to be a global one, otherwise cybercriminals will easily find save havens from where to operate. Having 99 % of the international community cooperating is not sufficient since the lack of effort by the remaining 1 % may suffice to destroy the combined efforts of the rest.

d) In order to determine the applicable rules, it is important to assess the *locus commissi delicti*. In cyber crimes, this is one of the more contentious issues.

e) The spatial distance between the perpetrator and the victim is an element that might be found in other types of crimes as well, however, when it comes to cyber crime, this is the characteristic feature. The borderless nature of cyber crimes results in many states being involved. This leads to the well-known tension between the needs of criminal prosecution which demand the collection of all relevant evidence, wherever they may be found, and the classic requirement of international law based on the principle of sovereign equality of states, which demands that the "jurisdiction to enforce"[17] not be applied in the territory of another state absent the consent of the local government[18].

As a result, international legal cooperation is more important than ever in cyber crimes.

17 As opposed to the "jurisdiction to prescribe", which is limitless.

18 James Crawford. Brownlie's Principles of Public International Law (8th ed., Oxford: Oxford University Press, 2012), s.479; Malcolm N. Shaw. International Law (6th ed., New York: Cambridge University Press, 2008) s.645-6; Martin Dixon. Textbook on International Law (6th ed., Oxford: Oxford University Press, 2007), s.113..

f) Classical methods of cooperation demand the requesting and requested party to undergo lengthy administrative proceedings, and involve considerable paperwork. This takes time. Unfortunately, digital data may be irrecoverably lost within a very short period of time. Hence, international cooperation needs to work very fast.

**B. Specific Problems**

In practice, an often-encountered situation is where the host is outside national territory, and the content provider and/or victim is within national territory. In this case, the crime is deemed to have been committed in Turkey (TPC Art. 8). However, international legal cooperation has to be requested for the gathering of evidence abroad in respect of a crime committed in Turkey. In particular, in crimes committed through the use of social webs or web 2.0 applications of firms such as Google, Yahoo or Facebook, even if they have a representative or an office in Turkey, IP information has to be obtained from abroad. In this case, the fact that service providers located abroad are not obliged to comply with requests emanating from Turkish administrative and judicial authorities decreases the effectiveness of the national investigation considering that legal cooperation is subject to certain conditions (eg., double criminality) and that it takes some time. Even so, such conditions are necessary, since in their absence it would be possible to circumvent the guarantees afforded by national law.

Another major stumbling block before requests made by Turkey is the issue of protection of personal data. Many states were unwilling to cooperate with Turkey because of the lack of a legislative framework on the protection of personal data. Through a referendum held on 12/09/2010, a new paragraph has been added to Art. 20 of the Turkish Constitution entitled 'secrecy of private life':

Everyone has the right to request the protection of his/her personal data. This right includes being informed of, having access to and requesting the correction and deletion of his/her personal

data and to be informed whether these are used in consistency with envisaged objectives. Personal data can be processed only in cases envisaged by law or by the person's own consent. The principles and procedures regarding the protection of personal data are laid down in law.

Hence, a law enacted by the Parliament is required to give 'flesh and bone' to this abstract constitutional guarantee. The 2012 Progress Report on Turkey by the EU[19] has also highlighted the problem (p. 74):

With regard to respect for private and family life and, in particular, the right to *protection of personal data,* Turkey needs to align its legislation with the data protection *acquis* and set up a fully independent data protection supervisory authority. Turkey also needs to ratify both the CoE Convention for the protection of individuals with regard to automatic processing of personal data (CETS No 108) and the additional protocol to it on supervisory authorities and trans-border data flow (CETS No 181). The absence of data protection legislation hampers operational cooperation between police and judicial authorities and on counter-terrorism.

Articles 135 et seq. of the TPC penalize the unlawful use (obtaining, recording, diffusion, non-deletion) of personal data. However, there is no law explaining the conditions under which such acts are lawful. A memo prepared by the Ministry of Justice and found on the website of the Parliament[20] identifies, *inter alia*, the following problems caused by the lack of a law on the protection of personal data:

- It is not possible to enter into an operation cooperation agreement with Europol.

19 SWD(2012) 336 final, available at http://ec.europa.eu/enlargement/pdf/key_documents/2012/package/tr_rapport_2012_en.pdf [last visited 03/01/2013]

20 "Kişisel Verilerin Korunması Kanunu Tasarısı Hakkında Bilgi Notu" http://www.tbmm.gov.tr/arastirma_komisyonlari/bilisim_internet/docs/sunumlar/Adalet%20Bakanl%C4%B1%C4%9F%C4%B1%20Kanunlar%20Genel%20M%C3%BCd%C3%BCrl%C3%BC%C4%9F%C3%BC29-05-2012.pdf [last visited 02/01/2013]

- Existing cooperation and exchange of information and documents cannot be realized via electronic transmission lines, causing delays and failures.
- Turkey cannot benefit from the Schengen Information System and the Sirene Office (a system which allows the sharing of important data on issues such as car theft, passports, European Arrest Warrant, wanted people, unwanted foreigners, etc.)
- Security cooperation agreements cannot be made with certain states (France and Belgium)
- The Ministry of Foreign Affairs encounters difficulties and hesitations in the sharing of information with foreign States on issues such as military service, identity, nationality. Such data cannot be obtained from foreign States.
- Operational cooperation is not possible with EUROJUST with regard to transnational organized crimes.
- In the field of the judiciary, difficulties are encountered in extradition and the sharing of information and documents.
- All in all, the memo states that Turkey is qualified as an "unreliable State" with regard to data protection.

Turkey has been working on a specific law dealing with the issue since 1989, and various drafts have been prepared. A new Commission has been established in 2004, and the Draft prepared by the Ministry of Justice has been sent to the Office of the Prime Minister on 28/07/2006. This Office has submitted the Draft to the Parliament on 22/04/2008. The Draft could not be adopted by the Parliament before the general elections and became null and void by virtue of Art. 77 of the Internal Regulation of the Parliament. The Ministry of Justice informed on 15/09/2011 the Office of the Prime Minister in writing that it would be appropriate to renew the Draft. Hence, the Draft is now before the Office of the Prime Minister. It is reported in the media that it should be submitted to the Parliament very soon.

On the other hand, it is important to note the unanimous finding of violation of Art. 10 (freedom of expression) of the European Convention on Human Rights by the European Court of Human Rights in *Ahmet Yildirim v Turkey* (18/12/2012). The case concerned a court decision to block access to Google Sites, which hosted an Internet site whose owner was facing criminal proceedings for insulting the memory of Atatürk. As a result of the decision, access to all other sites hosted by the service was blocked. The press release by the Registry of the Court summarizes the judgment as follows:

The Court observed that the blocking of access to the applicant's website had resulted from an order by the Denizli Criminal Court in the context of criminal proceedings against the owner of another site who was accused of insulting the memory of Atatürk. The court had initially ordered the blocking of that site alone. However, the administrative authority responsible for implementing the order (the TİB) had sought an order from the court for the blocking of all access to Google Sites, which hosted not only the offending site but also the applicant's site. The court had granted the request, finding that the only way of blocking the site in question was to bar access to Google Sites as a whole.

Although neither Google Sites nor Mr Yıldırım's own site were concerned by the abovementioned proceedings, the TİB made it technically impossible to access any of those sites, in order to implement the measure ordered by the Denizli Criminal Court.

The Court accepted that this was not a blanket ban but rather a restriction on Internet access. However, the limited effect of the restriction did not lessen its significance, particularly as the Internet had now become one of the principal means of exercising the right to freedom of expression and information. The measure in question therefore amounted to interference by the public authorities with the applicant's right to freedom of expression. Such interference would breach Article 10 unless it was prescribed by law, pursued one or more legitimate aims and was necessary in a democratic society to achieve such aims.

A rule was "foreseeable" in its application if it was formulated with sufficient precision toenable individuals – if need be, with appropriate advice – to regulate their conduct.

By virtue of Law no. 5651, a court could order the blocking of access to content published on the Internet if there were sufficient reasons to suspect that the content gave rise to a criminal offence. However, neither Google Sites nor Mr Yıldırım's site were the subject of court proceedings in this case. Although the decision of 24 June 2009 had found Google Sites to be responsible for the site it hosted, no provision was made in Law no. 5651 for the wholesale blocking of access as had been ordered by the court.

Nor did the law authorise the blocking of an entire Internet domain such as Google Sites.

Moreover, there was no evidence that Google Sites had been informed that it was hosting content held to be illegal, or that it had refused to comply with an interim measure concerning a site that was the subject of pending criminal proceedings. The Court observed that the law had conferred extensive powers on an administrative body, the TİB, in the implementation of a blocking order originally issued in relation to a specified site. The facts of the case showed that the TİB had had little trouble requesting the extension of the initially limited scope of the blocking order.

The Court reiterated that a restriction on access to a source of information was only compatible with the Convention if a strict legal framework was in place regulating the scope of a ban and affording the guarantee of judicial review to prevent possible abuses.

However, when the Denizli Criminal Court had decided to block all access to Google Sites, it had simply referred to an opinion from the TİB without ascertaining whether a less far-reaching measure could have been taken to block access specifically to the site in question. The Court further observed that there was no indication that the Criminal Court had made any attempt to weigh up the various interests at stake, in particular by assessing whether it had been necessary to block all access to Google Sites. In the Court's

view, this shortcoming was a consequence of the domestic law, which did not lay down any obligation for the courts to examine whether the wholesale blocking of Google Sites was justified. The courts should have had regard to the fact that such a measure would render large amounts of information inaccessible, thus directly affecting the rights of Internet users and having a significant collateral effect.

The interference resulting from the application of section 8 of Law no. 5651 had thus failed to meet the foreseeability requirement under the Convention and had not afforded the applicant the degree of protection to which he was entitled by the rule of law in a democratic society. The Court also pointed out that Article 10 § 1 of the Convention stated that the right to freedom of expression applied "regardless of frontiers".

The effects of the measure in question had therefore been arbitrary and the judicial review of the blocking of access had been insufficient to prevent abuses. There had therefore been a violation of Article 10 of the Convention.

**(2) (a) Does your country provide for the interception of (wireless) telecommunication? Under which conditions?**

The issue is regulated by Articles 135 et seq. of the Criminal Procedure Code (CPC). Detection (location), monitoring (listening) and recording of communications is subjected to very strict rules. The provisions in question cover any form of communication, thus also comprising electronic means of communication. However, the wording of the relevant provisions and the regulation which specifies the details of the implementation of these measures[21] seem to take as reference audio communication (namely, telephones) alone. There is no specific provision in the Regulation concerning electronic communication, and the various provisions refer to the 'listening' of communications.

21 Regulation on Procedures and Rules on the Detection, Listening, Evaluation of Signal Information and Recording of Telecommunication, and the Establishment, Duties and Powers of the Telecommunications Directorate' (published in the Official Journal no. 25989 of 10/11/2005).

Under Art. 135 (1) CPC:

- There must be strong grounds of suspicion.
- There must be no other means of collecting evidence.
- A warrant issued by the judge or, where a delay is detrimental, the decision of the public prosecutor is necessary. In the latter case, the public prosecutor shall immediately submit his decision to the judge for approval and the judge shall decide on this matter within twenty four hours, at the latest. Upon expiry of this period or if the judge denies approval, such measure shall be lifted by the public prosecutor immediately.

Further conditions:

- The suspect's communication with persons who are entitled to refrain from acting as a witness shall not be recorded. If such a situation is understood after the recording, the recorded material shall be destroyed immediately (Art. 135 (2) CPC).
- The maximum duration of the measure is three months, however this period can be extended one more time. For crimes committed within the activities of a criminal organization, the judge may decide to extend the duration as many times as necessary, each time for no longer than one month. Hence, in this latter case, there is, in fact, no statutory limitation concerning the maximum duration of the measure (Art. 135 (3) CPC).
- This measure may only be applied with regard to certain crimes (Art. 135 (6) CPC):

1. Migrant smuggling and trafficking in human beings (Articles 79 and 80 of the Turkish Penal Code – hereinafter 'TPC'),
2. Intentional killing (Arts. 81-3 TPC),
3. Torture (Arts. 94-5 TPC),
4. Rape (Art. 102 TPC),

5. Sexual abuse of children (Art. 193 TPC),
6. Manufacturing and trafficking of drugs and stimulants (Art. 188 TPC),
7. Counterfeiting of money (Art. 197 TPC),
8. Founding an organization with the aim of committing criminal offences (Art. 220 TPC, with the exception of paragraphs 2, 7 and 8),
9. Prostitution (Art. 227 (3) TPC),
10. Corruption in tenders (Art. 235 TPC),
11. Bribery (Art. 252 TPC),
12. Laundering of assets deriving from crime (Art.282 TPC),
13. Armed criminal organization (Art. 314 TPC) or supplying such organizations with weapon (Art. 315 TPC),
14. Crimes against state secrets and espionage (Arts. 328-31, 333-7 TPC),
15. Gun smuggling, as defined in the Law on Fireguns and Knifes and other Tools (Art. 12 of this Act),
16. the crime of embezzlement defined in Arts. 22 (3) and (4) of the Banks Law,
17. the crimes defined in the Law on Combatting Smuggling which require imprisonment,
18. the crimes defined in Arts. 68 and 74 of the Law on Protection of Cultural and Natural Assets.

As can be seen, the crimes in the field of informatics embodied in the TPC (Arts. 243-5) are not covered by the catalogue. In addition, many classic crimes that can be committed through the use of information systems are also not covered.

In addition, Law no. 5809 on Electronic Communication[22] should be mentioned. The purpose of this Law is to establish effective

22 Published in the Official Journal of 10/11/2008.

competition in the sector of electronic communication through regulation and control, to protect the rights of the consumers, to extend services nationwide, to use resources effectively and productively, to promote technological developments and new investments in the field of communication network and service, and to lay down the procedures and principles concerning these issues (Art. 1). As such, this is not a law concerning criminal matters. There are no provisions on procedural criminal law, including international co-operation, although the law does include certain substantive criminal law provisions (Art. 63) punishing acts such as unlawfully providing service, or establishing or running facilities, in the field of electronic communication service. The Law also provides for the establishment of a special unit, the Institution on Information Technologies and Communication, entrusted with various duties in the field of electronic communication (Art. 6).

**(b) To what extent is it relevant that a provider or a satellite may be located outside the borders of the country?**

As far as the application of the rules on interception of telecommunications is concerned, it makes no difference. With regard to telephone tapping, what matters is for the suspect/defendant whose communications will be intercepted to be found in Turkish territory.

However, Turkish law does not provide for a rule allowing searches through remote access to the platform where the data is stored.

With regard to interception of the transfer of data, this is only possible through access providers located in Turkey. However, in practice, there is no infrastructure to support the monitoring and recording via access providers of electronic communication on the Internet. In practice, only IP addresses are retrieved. As for e-mail address information, firms such as Yahoo and Gmail are contacted in order to convince them to hand over the requested data, as a result of which computers can be seized in order to analysed the data they contain.

**(c) Does your national law provide for mutual legal assistance concerning interception of telecommunication? Did your country conclude international conventions on it?**

The Turkish legislator has not opted for enacting a general law regulating different aspects of legal co-operation. Similarly, there is no specific rule on legal assistance concerning the particular issue of interception of telecommunications. Therefore, there is no generally applicable framework, and the specific rules regarding different types of co-operation are to be found in either multilateral or bilateral treaties to which Turkey is a party. When there is legal cooperation in criminal matters, the national law of the requested State shall apply. Hence, if the interception of telecommunications is possible under Turkish law, this measure might be applied within the framework of the general rules on legal cooperation. In that sense, the fact that Turkey is not a party to international conventions on the matter is not necessarily an impediment. However, see the answers below with regard to the inadequacy of Turkish law and practice as regards the interception of electronic communications.

In practice, international legal cooperation in criminal matters is a matter entrusted with the Law no. 2992 (dated 1984) to the Directorate-General of International Law and Foreign Affairs, a governmental department within the Ministry of Justice. The Directorate receives requests for legal cooperation and directs them to the relevant authority. This task is fulfilled in accordance with the bilateral and multilateral international treaties to which Turkey is a party. In the absence of an applicable treaty provision, the Directorate acts according to international customary rules and the principle of reciprocity. In practice, requests are usually executed in the framework of the 1959 European Convention on Mutual Assistance in Criminal Matters.

Under Turkish law, when it comes to international legal co-operation, international treaties have even more importance when compared to many other states. This is because of Art. 90/*in fine* of our Constitution which reads: (as amended on 22 May 2004) '*International agreements duly put into effect bear the force of*

*law. No appeal to the Constitutional Court shall be made with regard to these agreements, on the grounds that they are unconstitutional. In the case of a conflict between international agreements in the area of fundamental rights and freedoms duly put into effect and the domestic laws due to differences in provisions on the same matter, the provisions of international agreements shall prevail*'.

Hence, once an international treaty has been ratified by Turkey, it directly becomes part of its national law. Furthermore, international agreements in the area of fundamental rights and freedoms shall prevail over national laws (however, they still rank below the Constitution). So, in case of conflict between a law enacted by the Parliament, and a treaty rule, the national courts must apply the rule embodied in the int'l. treaty. If treaties regulating international co-operation in criminal matters are to be accepted to belong to the corpus of human rights law, they would be superior in rank to our national statutes in the hierarchy of norms. This particular issue has only been discussed in a single textbook, where it is argued, drawing from German academic writings, that treaties regarding international legal co-operation do not belong to the category of human rights treaties. If this view is to be adopted, according to the largely prevailing understanding in Turkish academic writings and practice on the status (and rank) of international treaties not in the field of fundamental rights and freedoms, they rank equal with national law. Therefore, bilateral and multilateral treaties in matters of legal co-operation would not automatically supersede or prevail over national statutes. In case of conflict, national authorities would have to determine the applicable rule by relying on the general principles governing the relationship between rules of the same rank. Thus, a subsequent rule will supersede the previous one (*lex posteriori derogat priori*), and a special law will prevail over a general one (*lex specialis derogat generali*).

Turkey is a party to a variety of international treaties regarding co-operation in criminal matters. There are also several treaties that have been signed, but not yet ratified by Turkey. The distinction is

vital because signature does not suffice to be bound by the terms of the treaty. Under the Turkish constitutional system, in principle, ratification (antlaşmanın onaylanması) is the act that makes the treaty legally binding. So, ratification is the process whereby a state finally confirms its intention to be bound by a treaty that it has previously signed.

Having said that, international treaties signed or ratified by Turkey in the area of legal co-operation in criminal matters are the following (the first date indicates the date of entry into force at the int'l. level of the treaty, the second date indicates the date of ratification by Turkey. Only treaties that have entered into force (at the int'l. level) have been included).

- European Convention on Extradition[23] (18/4/1960; 18/4/1960)
- European Convention on Mutual Assistance in Criminal Matters[24] (12/6/1962; 22/9/1969)
- European Convention on the Transfer of Proceedings in Criminal Matters (30/3/1978, 28/1/1979)
- European Convention on the International Validity of Criminal Judgments (26/7/1974, 28/1/1979)
- European Convention on the Supervision of Conditionally Sentenced or Conditionally Released Offenders (22/8/1975, signed but not ratified)
- European Convention on the Punishment of Road Traffic Offences (18/7/1972, signed but not ratified)
- European Convention on the Suppression of Terrorism (4/8/1978; 20/8/1981)
- Additional Protocol to the European Convention on Information on Foreign Law (31/8/1979, 2/3/2005)

23 Turkey is also party to the Second Additional Protocol. However, the 1975 Additional Protocol has not yet been signed (or ratified/acceded) by Turkey.

24 Turkey also ratified the 1978 Additional Protocol, but not the 2001 Second Additional Protocol.

- Second Additional Protocol to the European Convention on Extradition (5/6/1983, 8/10/1992)
- Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (12/4/1982, 27/6/1990)
- European Convention on the Control of the Acquisition and Possession of Firearms by Individuals (signed but not ratified)
- Convention on the Transfer of Sentenced Persons[25] (1/7/1985, 1/1/1988)
- European Convention on the Compensation of Victims of Violent Crimes (signed but not ratified)
- Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1/9/1993, 1/2/2005)
- Criminal Law Convention on Corruption (1/7/2002, 1/7/2004)
- Council of Europe Convention on the Prevention of Terrorism (1/6/2007, 23/3/2012 ( (entry into force for Turkey 1.7.2012))
- Council of Europe Convention on Action against Trafficking in Human Beings (1/2/2008, signed on 19/03/2009 but not yet ratified)
- Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (1/5/2008, signed on 28/03/2007 but not yet ratified)

In addition, there are also various other conventions ratified by Turkey which include provisions regarding international legal co-operation. Some examples:

- UN Single Convention on Narcotic Drugs, 1961
- UN Convention for the Suppression of Unlawful Seizure of Aircraft, 16 December 1970

25 However, the 1997 Additional Protocol has not yet been signed (or ratified/acceded) by Turkey.

- UN Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, 23 September 1971 (and the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation)
- UN Convention on psychotropic substances, 1971
- UN Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, 1973
- UN International Convention against the Taking of Hostages, 17 December 1979
- UN Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, 1984
- United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988
- OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, 1997
- CoE Convention on the Protection of the Environment through Criminal Law, 1998
- CoE, Criminal Law Convention on Corruption[26], 1999
- UN International Convention for the Suppression of the Financing of Terrorism, 1999
- CoE Convention on Cybercrime, 2001

Finally, Turkey has concluded various bilateral extradition treaties, as well as treaties regarding general legal co-operation[27].

In the particular field of telecommunication, Turkey is a member of the International Telecommunication Union, and has ratified[28] the Final Acts of the Plenipotentiary Conference held in Antalya (2006) and embodying the "Instrument amending the Constitution of the International Telecommunication Union".

26 However, the 2003 Additional Protocol has not yet been signed (or ratified/acceded) by Turkey.

27 For a list, see http://www.uhdigm.adalet.gov.tr/sozlesmeler/ikitaraflisoz/ikili.html

28 Law no. 6011 of 23/07/2010.

The applicable legal framework concerning a request for legal co-operation will have to be assessed in light of these sources. In addition, the circulars issued by the Directorate-General on issues of international legal cooperation direct the practice (for example, the Circulars no. 66/1 and 69/1 of 1 March 2008).

Needless to say, Turkey may request or be requested co-operation from a state with which it does not share any multilateral or bilateral treaty. Such requests may be fulfilled based on reciprocity, but there will be no legal obligation to do so.

**(3) To what extent do general grounds for refusal apply concerning internet searches and other means to look into computers and networks located elsewhere?**

Under Turkish law there is no such measure. Hence, we cannot request it through international legal cooperation nor can we apply it when requested from us.

**(4) Is in your national law the double criminality requirement for cooperation justified in situations in which the perpetrator caused effects from a state in which the conduct was allowed into a state where the conduct is criminalised?**

According to Art. 5 of the 1959 European Convention on Mutual Assistance in Criminal Matters, any Contracting Party may reserve the right to make the execution of letters rogatory for search or seizure of property dependent on the condition that the offence motivating the letters rogatory is punishable under both the law of the requesting Party and the law of the requested Party. Under this provision, the execution of cooperation requests concerning seizure or detention of the suspect is dependent on the condition that the conduct for which cooperation is requested constitutes a crime under Turkish law. On the other hand, requests for cooperation which do not concern seizure or detention, and which fall outside Art. 5, are rejected on the basis of the "ordre public" provision in Art. 2 even where they concern acts which constitute crimes under Turkish national law.

In practice, cases where the result of the criminal act emerges in Turkey are problematic. In this case, by virtue of Art. 8 TPC, the crime is deemed to have been committed in Turkey. Since the principle of territoriality applies with regard to jurisdiction, the double criminality requirement has no scope of application. However, when it comes to retrieving the data abroad, international legal cooperation will be necessary, and this subject to the double criminality rule. This is a problem with regard to crimes such as insult, defamation, calumny, insult to the memory of Atatürk, insulting the Turkish nation committed through service providers found in states that have a more tolerant legislation or judicial practice than Turkey as regards freedom of expression. Although no double criminality requirement exists with regard to assumption of jurisdiction, the fact that legal cooperation requests directed to states such as the USA are doomed to be turned down, many crimes that cannot be punished in practice emerge.

**(5) Does your national law allow for extraterritorial investigations? Under which conditions? Please answer both for the situation that your national law enforcement authorities need information as when foreign authorities need information available in your state.**

With regard to national law enforcement authorities needing information: The Ministry of Justice participates on a regular basis to the meetings of the European Judicial Network, and cooperates in the sharing of information with the contact points of other states and in the execution of requests. Although Turkey is not a member to EUROJUST, the Ministry of Justice occasionally participates with observer status to its operational meetings.

The Ministry of Justice requests cooperation from the central authorities of foreign states through the Directorate-General of International Law and Foreign Affairs. The Directorate-General of the Turkish National Police requests information via Interpol. In the field of cybercrimes, the Department of Fight against Cybercrimes (operating within the Ministry of Justice), requests urgent traffic data information and measures concerning the

protection of data through 7/24 contact points in other states. Finally, requests are made to the relevant departments of hosting firms such as MSN, Google, YouTube, etc. concerning the protection of data in urgent cases.

With regard to foreign authorities needing information: The above-information also applies, *mutatis mutandis*, here.

**(6) Is *self service* (obtaining evidence in another state without asking permission) permitted? What conditions should be fulfilled in order to allow self service? Please differentiate for public and protected information. What is the (both active and passive) practice in your country?**

This issue is not regulated under Turkish national law. However, investigative authorities (the police and the Offices of the Public Prosecutor) access publicly accessible information and use it as evidence in the investigation. Since Turkey is not yet a party to the Convention on Cybercrime, our national authorities are unable to rely on Art. 32 of the Convention concerning remote access. Under customary international law, whereas a state may have a general power under international law to prescribe jurisdiction, the enforcement of that jurisdiction can generally take place only within its own territory. Turkey complies with the established international law understanding that the jurisdiction to enforce may not be exercised, without permission, on foreign territory. See, however, the answer to question 7.

**What is the (both active and passive) practice in your country?**

There is no applicable legislative framework to the issue. In practice, it is reported that bilateral negotiations are conducted with the representative of firms such as Youtube, Google, etc. in order to 'convince' them, for the sake of securing the continuation of their operations in Turkey, to voluntarily hand over the requested data.

In addition, the Directorate-General of the National Police has a protocol with Microsoft, according to which personal data is directly obtained without resorting to international legal cooperation.

Since there is no legislative framework in place, establishing, *inter alia*, the conditions for obtaining, storing and deleting private data, and no judicial and/or administrative review mechanisms to oversee compliance with such guarantees, this *de facto* way of operating is unlawful. As for publicly available information, this can be obtained directly by investigative authorities, there is no factual or legal problem in this aspect.

**What conditions should be fulfilled in order to allow self service? Please differentiate for public and protected information?**

When it comes to obtaining information and evidence for purposes of criminal investigation, a distinction can be made between three alternatives:

1. Open information and evidence, namely, information that is publicly accessible simply by surfing through the net. In this case, as provided for in the Convention on Cybercrime (Art. 32 (a)), a state should be able, without the authorisation of another state, to access publicly available (open source) stored computer data, regardless of where the data is located geographically.
2. Protected information, namely, information which cannot be publicly accessed, but which may be accessed by hacking. In this case, the authorization/consent of the relevant state should be required. Of course, the problem here is the determination of which the 'relevant' state might be. This is an issue discussed in the previous sections.
3. Information and evidence that require to take over a computer or network located in another country. In this case, states should not depart from the classical international law understanding that enforcement jurisdiction may not be exercised in the territory of another State without the consent of that State. In this option, States should resort to international cooperation.

**(7) If so, does this legislation also apply to searches to be performed on the publicly accessible web, or in computers located outside the country?**

There is no specific legislation concerning the issue. With regard to publicly accessible data, by virtue of Article 161 CPC, concerning the duties and powers of the prosecutor, the public prosecutor may directly gather, where technically possible, the relevant data, or he/she may request service providers located in Turkey to hand over the requested information. In case the relevant data has to be obtained from abroad, the general procedure concerning international legal assistance will apply.

**(8) Is your country a party to Passenger Name Record (PNR) (financial transactions, DNA-exchange, visa matters or similar) agreements? Please specify and state how the exchange of data is implemented into national law. Does your country have an on call unit that is staffed on a 24/7 basis to exchange data? Limit yourself to the issues relevant for the use of information for criminal investigation.**

Turkey is not a party to any international treaty concerning PNR. There is also no central national institution charged with gathering the relevant data or central system where such data is to be stored. Individual firms may store the relevant data, subject to applicable conditions established by civil aviation rules. In practice, each company operating in the field of civil aviation utilizes one of the available international systems.

Turkey has signed (over 30 years ago) but not ratified the 1981 European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. As explained above, the national law concerning data protection is yet to be adopted. However, within the Directorate-General of the Turkish National Police, 7/24 "tracking centres" (takip merkezleri) are being instituted.

**(9) To what extent will data referred to in your answer to the previous question be exchanged for criminal investigation and on which legal basis? To what extent does the person involved have the possibility to prevent/ correct/ delete information? To what extent can this information be used as evidence? Does the law of your country allow for a Notice and Take-Down of a website containing illegal information? Is there a practice? Does the seat of the provider, owner of the site or any other foreign element play a role?**

With regard to PNR, each airlines company stores its own data. If Turkey is requested assistance on this issue, public prosecutors will obtain the relevant information through the use of their investigative powers under Arts. 161-2 CPC.

**To what extent will data referred to in your answer to the previous question be exchanged for criminal investigation and on which legal basis?**

By virtue of Article 161 CPC, concerning the duties and powers of the prosecutor, the public prosecutor may request the relevant information to be handed over to the investigative authorities.

Data held by Turkish authorities is transmitted to the judicial and investigative authorities of other states in the framework of judicial and police cooperation. Requests for legal cooperation are executed, where necessary, by demanding based on applicable treaties or reciprocity, written guarantee that the transmitted data will only be used as evidence in the framework of the case being currently investigated.

**To what extent does the person involved have the possibility to prevent/ correct/ delete information?**

The individual has no control over such data. As explained above, the law concerning data protection is not yet into force.

**To what extent can this information be used as evidence?**

As long as the relevant data has been obtained in a lawful manner (for example, through an order of the prosecutor relying on his

powers under Art. 161) CPC, this information is admissible as evidence before courts of law. On the other hand, Turkey has a very strict exclusionary rule. By virtue of Art. 38 (6) of the Constitution, which states that '*Findings obtained through illegal methods shall not be regarded as evidence.*' illegally obtained evidence has to be excluded, regardless of its reliability and/or probative value.[29]

This rule applies to evidence obtained by investigative authorities as well as private individuals. In fact, it applies to all procedures, not only to the criminal sphere. We have no balancing tests (as opposed to states such as Germany) that may limit the application of the exclusionary rule. 'Good faith on the part of the violating officer', 'the silver platter doctrine', 'the independent source doctrine', 'the inevitable discovery doctrine', 'the attenuation exception regarding causality', drawing distinctions between testimonial and real/physical evidence, and similar limitation theories do not apply.

The "fruits of the poisonous tree" doctrine has full scope of application, evidence obtained as an indirect result of unlawfulness shall also be suppressed (though the Court of Cassation has, occasionally, held otherwise, see for example YCGK, 29.11.2005, 2005/7-144, 2005/150).

**Does the law of your country allow for a Notice and Take-Down of a website containing illegal information? Is there a practice? Does the seat of the provider, owner of the site or any other foreign element play a role?**

Hosting providers are not under a legal obligation to check the content about its illegality, according to art. 5 of the Internet Law. They are, however, obligated to remove any illegal content if they

29 Also see CPC Art. 206 (2): The request of presentation of evidence shall be denied if the evidence is unlawfully obtained.
CPC Art. 217 (2): The charged crime may be proven by using all kinds of legally obtained evidence.
CPC Art. 230 (1) (b): Evidence obtained by illegal methods that are included in the file shall be indicated clearly and separately in the reason for the judgment on the conviction of the accused.
CPC Art. 289 (1) (i): In cases where the judgment is based on evidence obtained by illegal methods, the judgment shall be reversed by the Court of Cassation, even if the defence has made no request on this ground

have been notified about its existence. The notification occurs following the rules of arts. 8 and 9 of the Internet Law. The former concerns notifications of a court or the Presidency, while the latter is related to real or legal persons whose legal interests have been affected by the content in question. According to art. 9 of the Internet Law, any person claiming to be affected by an illegal content may notify the content provider or the hosting provider, requesting its removal and replacement with a reply sent by the notifying person. Failing to comply with this "right to reply and removal", however, does not result directly in the criminal liability of the hosting provider, except when it can be proven that the hosting provider has acted as an accomplice to the crime, and shared the criminal intent.

However, if the illegal content concerns one of the crimes listed under art. 8 of the Turkish Internet Law, access to the content may be blocked by courts pending trial, or, in some cases, by the administrative authority of the Presidency of Telecommunications.

The measure of "blocking access to Internet content" has been regulated as a criminal procedural measure under art. 8 of Internet Law, to be ordered in cases where a sufficient level of suspicion exists pointing to the commission of crimes listed under the same article[30]. This measure is to be ordered by the judge (or, in urgent cases, by the prosecutor) during criminal investigation, and by the court during the trial. As such, the decision to block access shows the typical characteristics of a criminal procedural measure.

However, the Internet Law also authorizes the Presidency for Telecommunications to order the measure, if the content provider or the hosting provider resides in abroad, or, if the crime in question is the sexual harassment of minors, or pornography. In these cases, the Presidency can order the measure ex officio, notifying the prosecutor only about the identity of alleged perpetrators, if their identity can be determined. Failing to obey the decision of the Presidency can result in a fine, or even the annulment of the permit to act as an access provider.

30 This list includes the following crimes: Incitement to suicide, sexual harassment of children, facilitating the abuse of narcotic drugs, providing material dangerous to public health, obscenity / pornography, providing place or means for gambling, and crimes against the memory of Atatürk.

As can be seen, Turkish Internet law designates "blocking Access to websites" both as a criminal procedure measure and also as an administrative measure. Particularly, the excessive use of the latter measure brought the "internet censorship" into the agenda and created a real threat for media freedom and freedom of expression. Thus, there is an on-going campaign carried out by the representatives of ICT industry for the abolition or redesign of those measures.

An additional procedure using the "notice-and-take-down" system has been introduced regarding copyright infringements by the Turkish Intellectual Property Law, art. 71. Additional article 4 of the Law specifically addresses "content providers" infringing copyrights under the same law, providing for a notice-and-take-down system. According to this article, content providers violating copyrights shall only be criminally responsible if they have been duly notified by the copyright holders, and still persisted in the violation. In case of persistence by the content provider, the copyright holder shall inform the prosecutor, upon which the prosecutor may order the discontinuance of the service provided to the content provider. This order can only be lifted if the content provider removes the content infringing the copyright.

**(10) Do you think an international enforcement system to implement decisions (e.g. internet banning orders or disqualifications) in the area of cyber crime is possible? Why (not)?**

The establishment of such a system would not be welcome. It is important to provide individuals with appropriate guarantees and to protect freedom of expression. The fact that there is no such international system is a factor preventing overcriminalization. The existence of such system would only result in excessive control of the Internet environment. It would lead to the risk of states with an insufficient record and legislation on the protection of human rights and freedom of expression to implement their own legislation extraterritorially by taking advantage of different methods.

In addition, the establishment of such a system is also not technically feasible. Even if a handful of states were to opt to stay out of such system, cybercriminals would pursue their illegal activities from those territories. Hence, in practice, an international enforcement system would not provide significant added value to the contribution already obtained through international cooperation.

However, as a final note, the judge we have contacted within the Ministry of Justice's Department for Mutual Assistance in Criminal Matters believes that in case of specified crimes such as child pornography, a treaty adopted within the UN may establish such a system.

**(11) Does your country allow for direct consultation of national or international databases containing information relevant for criminal investigations (without a request)?**

National databases may be accessed directly by the prosecutor based on his general duties and powers concerning criminal investigations (Arts. 161-2 CPC). In Turkey there is a network called UYAP (which is the abbreviation for National Judicial Network Project). Public prosecutors may access the following records through this system: criminal records, registers of persons, investigation and prosecution files connected with the investigation being currently conducted, car and land registers, consular records concerning nationals living abroad.

As for records held by other states, Turkey cannot consult databases because there is no legal regulation on the issue in our national law, and Turkey is not a party to the Convention on Cybercrime, so that it cannot rely on Art. 32 of the Convention regarding remote access. Hence, with regard to international databases, investigative authorities would have to proceed within the framework of international legal cooperation.

**(12) Does your state participate in Interpol/ Europol/ Eurojust or any other supranational office dealing with the exchange of information? Under which conditions?**

Turkey participates to both Interpol and Europol.

Turkey has been a member state in Interpol since 1930. The INTERPOL National Central Bureau (NCB) for Turkey is part of the Central Directorate (there are also Local Directorates) of the Directorate General of the Turkish National Police (Emniyet Genel Müdürlüğü). All Turkish investigations with an international connection are conducted by INTERPOL Ankara, in coordination with the Turkish Ministry of Justice and partner law enforcement agencies in Turkey. Created in 1930, INTERPOL Ankara is one of the first and oldest INTERPOL NCBs. INTERPOL Ankara comprises a satellite unit within the Istanbul City Police Department, Turkey's largest police department. Its core missions comprise[31]:

- Cooperation with the international police community in investigating criminal activities and organizations;
- Taking necessary measures to prevent international crime;
- Monitoring and arresting international criminals and organizing their extradition, in liaison with partner NCBs;
- Submitting applications to the INTERPOL General Secretariat for the publication of all categories of notices;
- Sharing of INTERPOL criminal information and intelligence with Turkish authorities;
- Organizing training activities on international police cooperation matters to increase awareness within Turkish law enforcement agencies;
- Inform Turkish authorities about emerging international crime trends and techniques and methods adopted to prevent them.

31 http://www.interpol.int/Member-countries/Europe/Turkey [last visited 01/01/2013]

Since Europol is the law enforcement agency of the European Union, Turkey is not a member. However, there is a strategic agreement between Europol and Turkey (Agreement on Cooperation between the European Police Office and the Republic of Turkey, see, in particular, Articles 5-6 concerning requests for cooperation)[32].

Since Eurojust is an institution of the European Union, Turkey only occasionally sends representatives with observer status.

In general, it is stated that 'Turkey has a positive approach to judicial co-operation, more precisely; incoming requests are carried out in a flexible and a cooperative manner. Turkey carries out requests of mutual assistance in criminal matters basically within the framework of "European Convention on Mutual Assistance in Criminal Matters."'[33]

**(E) Human rights concern**

**(1) Which human rights or constitutional norms are applicable in the context of criminal investigations using information technology?**

In the context of criminal investigations using information technology, there are a lot of human rights and constitutional norms in Turkish law. First, Article 20 of the actual Constitution whose title is "Privacy" protects the right to privacy and family life. Its 2nd paragraph forbids any search of person or his belongings unless there is a judge decision or, in cases where delay is prejudicial, a written order an agency authorized by law which is lifted if it is not approved by the judge within 48 hours. Its 3rd paragraph added in 2010 allows treatment of personal data in cases described by law or where there is a personal consent. It recognizes also rights to access to these data, to demand correction or deletion and to check out whether they are properly used or not.

32 https://www.europol.europa.eu/sites/default/files/flags/turkey_.pdf [last visited 01/01/2013].

33 CyberCrime@IPA project, Turkey Country profile (Version 25 January 2011), (http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/cyber_cp_Turkey_2011_January.pdf), p. 37 [last visited 01.01.2013].

Nevertheless as the Law on Protection of Personal Data still is a draft before the Turkish Parliament, neither the personal data concept nor their legal treatment methods are described by law in general terms. Even if there are some particular legal provisions, for instance in the Criminal Procedure Code, we have not had any framework regulation on this issue yet.

Secondly, Articles 21 and 22 protect respectively inviolability of the domicile and freedom of communication along the same line with Article 20. They recognize the right at first and allow then any intervention (search, seizure or wiretapping) on condition that there is a judge decision or, in cases where delay is prejudicial, a written order an agency authorized by law which is lifted if it is not approved by the judge within 48 hours.

Thirdly, pursuant to the 6th paragraph of Article 38, any illegally obtained finding shall not be considered as evidence. This rule forbids use of evidence obtained through violation of legal provisions or legal principles. It binds both criminal investigation authorities and courts and there is no exception. Nevertheless "illegally obtained finding" concept is interpreted by courts, especially by the Court of Cassation whose case law can vary in time.

On the other side, Turkey has to respect the human rights norms stipulated by the European Convention on Human Rights as a contracting state. Thus, Article 6 related to the fair trial and Article 8 related to the private life are especially applicable to criminal investigations using information technology in the light of case law of the European Court on Human Rights. Moreover, pursuant to Article 90 of the Constitution, an international treaty ratified by Turkey bears the force of law and when there is a conflict between such a treaty concerning fundamental rights and a national law, the provisions of the former prevail.

**(2) Is it for the determination of the applicable human rights rules relevant where the investigations are considered to have been conducted?**

All of Turkish law enforcement authorities and courts must respect and apply above mentioned rules and norms. Thus, it is

clear that they are applicable to investigations conducted in Turkey and those conducted by foreign law enforcement authorities in the context of mutual assistance (e.g. rogatory). Consequently, if there is a violation of these rules, the Turkish authority (police, prosecutor or court) must not to consider this finding as evidence (Art. 38 par. 6 of the Constitution).

**(3) How is the responsibility or accountability of your state involved in international cooperation regulated?**

As there is not any special regulation on the responsibility or accountability of state involved in international cooperation regulated, general rules are applicable both on national and international levels. If such cooperation constitutes a violation according to the Turkish Law, victims may claim compensation from the Turkish State in the context of administrative law and even civil law. Then, if it constitutes an offence, the perpetrator-public officer is judged by courts (e.g. violation to privacy, Art. 134 of Turkish Penal Code; illegal recording of personal data, Art. 135 or misuse of public duty, Art. 257 etc.).

Moreover, it is possible that the international responsibility of Turkey comes into question through an application to the European Court on Human Rights (Art. 6 or 8 or 10).

**(4) Is your state for instance accountable for the use of information collected by another state in violation of international human rights standards?**

As above explained, Turkey is accountable both on national and international levels for the use of information collected by another state in violation of international human rights standards.

**(F) Future developments**

**Modern telecommunication creates the possibility of contacting accused, victims and witnesses directly over the border. Should this be allowed, and if so, under which conditions? If not, should the classical rules on mutual assistance be applied (request and answer) and why? Is there any legal**

**impediment under the law of your country to court hearings via the screen (Skype or other means) in transnational cases? If so which? If not, is there any practice?**

In Turkey, it is legally possible to contact witnesses and experts directly over the border through a videoconference link. Article 180 paragraph 5 of the Criminal Procedure Code states that witnesses and experts are simultaneously heard through a voice and image transmitting system, if available. This is also applicable to the hearing of victim and claimant (Art. 236 par. 1). On the other side, the Code does not allow any judgment in the absence of accused apart from legal special exceptions (Art. 193 par. 1). Nevertheless, interrogation of accused by the simultaneous videoconference possibility is one of these exceptions (Art. 196 par. 4). Especially some accused in need of a treatment in hospital have been so heard. The Ministry of Justice has issued on September 20th 2011 a Regulation on Use of Voice and Image Information System within the Criminal Procedure, which contains a detailed and technical explanation of this issue. Article 11 of the Regulation states that in the context of international mutual assistance, the concerned parties, in other words, Turkey and the other state, determine conditions of use of such system. However, its applicability requires a hard and expensive infrastructure and it is very problematic with regard to security of witnesses and authenticity of their depositions, courts traditionally prefer rogatory methods, even if they take much more time. We think that there should be a more secure and therefore more detailed regulation in this field, since the actual one does not serve this purpose.

Finally, as an exceptional case, pursuant to Article 5 of the Witness Protection Law, courts may hear an anonymous witness through a videoconference link, which changes his or her voices and images. This is a non-compulsory measure among others, but courts always apply it in such cases.

# BÖLÜM 4: KAVRAM AÇIKLAMASI VE SORULAR

**Prof. Dr. André Klip**

**(A) Soruların kapsamı (bkz. Giriş ve Ek)**

Bu Bölümdeki sorular genel olarak "siber suç" ile ilgilidir. Bu kavram, bilgisayar sistemlerinin veya İnternet'in düzgün işleyişi, bilişim ve iletişim teknolojisi vasıtası ile depolanan veya iletilen verilere ilişkin mahremiyet ve bu verilerin bütünlüğü, İnternet kullanıcılarının sanal kimlikleri gibi, bilişim ve iletişim teknolojisinin (BİT) kullanımı ile bağlantılı hukuksal değerleri etkileyen ve suç oluşturan fiilleri kapsayacak şekilde anlaşılmaktadır. Bütün siber suçların ve siber suç soruşturmasının ortak paydası ve karakteristik özelliği, bunların bir yandan bilgisayar sistemleri, bilgisayar ağları ve bilgisayar verileri ile, diğer yandan ise siber sistemler, siber ağlar ve siber veriler ile bağlantılı olmalarıdır.

Ulusal raportörler, başka soru veya açıklamalar için genel raportör Prof. Dr. André Klip ile bağlantıya geçebilirler: andre.klip@maastrichtuniversity.nl

**(B) Yargı yetkisine ilişkin sorunlar**

(1) (a) Ülkeniz, siber uzayda işlenen bir suçun işlendiği yeri nasıl belirlemektedir?

(b) Ulusal hukukunuz, bilginin ve delillerin bulunduğu yeri belirlemeyi zorunlu ve olanaklı görmekte midir? Ağda bulunabilecek olan bilginin yeri neresidir? Kullanıcının bilgisayarının bulunduğu yer midir? Ağ servis sağlayıcısının (hukuki veya fiili) yerleşim yeri midir? Hangi servis sağlayıcı dikkate alınmaktadır? Veya, veriyi ulaşılabilir kılan bireyin bulunduğu yer midir? Bu sorular hukuken geçersiz ise, lütfen bunun nedenini açıklayınız.

(2) Ceza adaleti sisteminizde siber suç, *locus delicti*'nin (suçun işlendiği yerin) saptanmasına muhtaç mıdır, değil midir? Neden (neden değil)?

(3) İnternet üzerinden nefret söylemi, hacking (bilgisayar sistemlerine izinsiz erişim), bilgisayar sistemlerine gerçekleştirilen saldırılar gibi siber suçlara yargı yetkisine ilişkin hangi kurallar uygulanabilir? Devletinizin bu gibi suçlara ilişkin yargı yetkisi bulunmamakta ise, bu durum bir sorun olarak kabul edilmekte midir?

(4) Ulusal hukukunuz, yargı yetkisi çatışmalarının önlenmesi veya bu konudaki anlaşmazlıkların giderilmesi bakımından kurallar öngörmekte midir? Bunlara ilişkin herhangi bir uygulama var mıdır?

(5) Ceza adaleti sisteminizde siber suçlar, yargı yetkisine ilişkin ilkeler olmadan da var olabilir mi? Esasında bu durum, ulusal ceza hukukunun evrensel olarak uygulanması anlamına gelecektir. Bu durum bazı suçlarla sınırlandırılmalı mıdır, ya da bir sözleşme temelinde koşula bağlanmalı mıdır?

**(C) Maddi ceza hukuku ve yaptırımlar**

(1) Ulusal ceza adaleti sisteminizde hangi siber suç tiplerinin sınır aşan boyutları olduğu kabul edilmektedir?

(2) Siber suç tiplerinin tanımlarında yargı yetkisine ilişkin unsurlar ne ölçüde yer almaktadır?

(3) Faillik, suç anlaşması veya diğer iştirak türlerine ilişkin genel kısımda yer alan kurallarda yargı yetkisine ilişkin unsurlar ne ölçüde yer almaktadır?

(4) Siber suç tiplerinin bir devlet tarafından kendi başına düzenlenebilecek bir sorun olduğunu düşünüyor musunuz? Eğer öyle ise, bir devletin bunu ne şekilde yapabileceğini belirtiniz. Eğer değil ise, neden yapamayacağını açıklayınız.

(5) Ulusal ceza adaleti sisteminiz, (uluslararası) tüzel kişilerin / servis sağlayıcıların ceza sorumluluğunu kabul etmekte midir? Sorumluluğun yüklenmesinin yargı yetkisine ilişkin sonuçları var mıdır?

**(D) Ceza hukukunda adli işbirliği**

(1) Bilişim teknolojisinin özellikleri karşılıklı yardımlaşmanın niteliğini ne ölçüde değiştirmektedir?

(2) (a) Ülkeniz, (kablosuz) telekomünikasyonun denetlenmesine ilişkin düzenlemeler öngörmekte midir? Hangi koşullarda?

(b) Bir servis sağlayıcının veya uydunun ülke sınırları dışında bulunması, ne ölçüde etkilidir?

(c) Ulusal hukukunuz, telekomünikasyonun denetlenmesi bakımından karşılıklı adli yardımlaşmaya ilişkin düzenlemeler öngörmekte midir? Ülkeniz bu alanda uluslararası sözleşmelere taraf olmuş mudur?

(3) İnternet üzerinden uygulanan arama tedbiri ve başka yerde bulunan bilgisayarların ve ağların içeriğinin denetlenmesine ilişkin başka yöntemler söz konusu olduğunda, bu yöndeki taleplerin reddine yönelik genel kurallar ne ölçüde uygulanabilmektedir?

(4) Failin davranışının, fiilin suç olarak düzenlenmemiş olduğu bir devlette gerçekleşip, fiilin suç olarak düzenlenmiş olduğu bir devlette etki doğurması halinde, ulusal hukukunuz adli yardımlaşma talebinin meşruiyeti bakımından çifte cezalandırma koşulunu aramakta mıdır?

(5) Ulusal hukukunuz ülke dışında ceza soruşturmalarına izin vermekte midir? Hangi koşullarda? Lütfen, gerek ulusal kolluk ve soruşturma makamlarının bilgiye ihtiyaç duyduğu haller, gerekse yabancı makamların devletinizde bulunan bilgiye ihtiyaç duyduğu haller bakımından ayrı ayrı yanıtlayınız.

(6) *Self service* (başka bir devlette bulunan delilin önceden izin almadan elde edilmesi) durumuna izin verilmekte midir? Self service durumuna izin verilebilmesi için hangi koşulların bulunması gerekir?

(7) Eğer yukarıdaki soruya verdiğiniz yanıt olumlu ise, söz konusu mevzuat, kamusal olarak erişilebilen ağlarda, ya da ülkenizin dışında yer alan bilgisayarlarda gerçekleştirilen arama tedbirlerine de uygulanabilir mi?

(8) Ülkeniz Yolcu İsim Kaydı (YİK) *(Passenger Name Record – PNR)* anlaşmalarına (mali işlemler, DNA alışverişi, vize sorunları v.b.) taraf mıdır? Lütfen, veri alışverişinin ulusal hukukta ne şekilde

uygulandığına ilişkin ayrıntılı bilgi veriniz. Ülkenizin veri alışverişi için 7/24 temelinde donanımlı personel bulunduran bir çağrı birimi mevcut mudur? Yanıtınızı, ceza soruşturmalarında kullanılan bilgilere ilişkin sorunlarla bağlantılı olarak sınırlandırınız.

(9) Yukarıdaki soruya verdiğiniz yanıtta sözü edilen veriler ceza soruşturması alanında ne ölçüde ve hangi hukuki temele dayanarak alışverişe tabi tutulabilir? İlgili kişi, bilgileri engelleme / düzeltme / silme imkanına ne ölçüde sahiptir? Bu bilgiler ne ölçüde delil olarak kullanılabilir? Ülkenizin hukuku, hukuka aykırı bilgiler içeren bir İnternet sitesinde uyar/kaldır sistemine izin vermekte midir? Servis sağlayıcının ya da site sahibinin bulunduğu yer veya diğer herhangi bir yabancı unsur burada rol oynamakta mıdır?

(10) Siber suç alanında (örn. İnternet yasaklama emirleri veya erişim koşullarının kaybına yönelik) kararların uygulanması bakımından uluslararası bir takip sisteminin oluşturulması mümkün müdür? Neden (neden değildir)?

(11) Ülkeniz, ceza soruşturmaları ile ilgili bilgileri içeren ulusal veya uluslararası veri tabanlarına doğrudan (talepte bulunmaksızın) başvuruya izin vermekte midir?

(12) Devletiniz Interpol/Europol/Eurojust veya bilgi alışverişi ile ilgili diğer herhangi bir ulusalüstü büroya katılmakta mıdır? Hangi koşullarla?

**(E) İnsan hakları sorunları**

Bilişim teknolojilerinin kullanıldığı ceza soruşturmaları bağlamında hangi insan hakları veya Anayasal normlar uygulanabilir niteliktedir? Soruşturmaların nerede yürütülmüş olduğunun kabulü, uygulanabilen insan hakları bakımından önem taşımakta mıdır? Uluslararası işbirliğine katılmış olduğunda devletinizin sorumluluğu ne şekilde düzenlenmiştir? Örneğin devletiniz, başka bir devlet tarafından uluslararası insan hakları standartlarına aykırı olarak toplanmış olan bilgilerden dolayı sorumlu tutulabilir mi?

**(F) Gelecekteki gelişmeler**

(1) Modern telekomünikasyon, sanıklar, mağdurlar ve tanıklar ile sınır ötesinden doğrudan bağlantı kurma imkânı tanımaktadır. Bu duruma izin verilmeli midir, ve eğer verilmeli ise, hangi koşullar altında? Eğer verilmemeli ise, karşılıklı adli yardımlaşmaya ilişkin klasik kurallar (talep ve cevap) uygulanmalı mıdır, neden?

(2) Ülkenizin hukukunda, sınıraşan davalarda mahkeme önünde ifadelerin görüntüleme yöntemi ile (Skype veya başka yöntemler kullanılarak) alınmasına karşı hukuki bir engel bulunmakta mıdır? Eğer öyleyse, bu engel nedir? Eğer değil ise, bunun herhangi bir uygulaması var mıdır?

(3) Bilişim toplumu ve uluslararası ceza hukuku ile ilgili olup ülkenizde günümüzde bir rol oynayan ve yukarıdaki sorularda değinilmemiş bulunan başka bir sorun var mıdır?

# EK- KAVRAM RAPORU

**Prof. Dr. André Klip**

## (1) Giriş

Modern toplumun bilgi toplumuna dönüşmesi gerçeği uluslararası ceza hukukunun farklı yönleri üzerinde çarpıcı sonuçlar doğurabilir. Bu durum, kurumumuzdaki yenilenen ilgiyi haklı çıkarmaktadır. Epeyce bir süre geçmiş olmasına rağmen, bu AIDP'nin konuyu ilk incelemesi değildir ve durumlar değişmiştir.[1] Başka hususların yansıra, toplumumuzun küreselleşmesi; insan davranışlarının, hareketi ilk başlatanın bulunduğu yer dışında birçok yerde de etkisi olabileceği anlamına gelmektedir. Google Earth, Street View, Facebook ve Hyves bize göstermiştir ki çoğu kişi için başkalarının göremeyebileceği çok az şey kalmıştır. Büyük Birader bizi gözetliyor, uluslararası hukuk için sonuçları ne oluyor? Bulut bilişim, verilerin nerede saklanacağı ve buna hangi mevzuatın uygulanacağı sorusunu ortaya çıkarmaktadır.[2]

Ceza hukuku bağlamında hareketin bu "sınırları aşan etkileri" telekomünikasyon, bilgisayar ve web gibi belirli teknolojilerin kullanılmasından kaynaklanabilir. Bilgisayar korsanları (hacker'lar) bir devletin sınırları içinde bulunan bir iletişim ağına veya kişisel bir bilgisayara dünyanın diğer bir ucunda bulunan başka bir bilgisayardan erişebilir. Nefret söylemleri Twitter, elektronik postalar ya da Youtube kayıtları aracılığıyla dile getirilebilir ve dünya çapında yayılabilir. Maddi unsurla bağlantılı olarak yargı yetkisi ve suçun işlendiği yer ile ilgili çeşitli sorunlar ortaya çıkabilmektedir.

Modern zamanlarda işlenen suçların soruşturmaları yönünden, bilgi toplumu yeni durumlar ve yeni sorular doğurmaktadır. Çocuk

1 Cole Durham tarafından hazırlanan genel rapora bakınız, The Emerging Structures of Criminal Information Law: Tracing the Contours of a New Paradigm, 64 RIDP 1993, p. 79-117.

2 Bkz. Laviero Buono, the Global Challenge of Cloud Computing and EU Law, Eucrim 2010, p. 117-124

pornografisi üretimi ve ürünlerinin dağıtımı sebebiyle uluslararası bir iletişim ağında yapılacak soruşturmalar internet sitelerinin ziyaret edilmesini, korunan alanlara girmeyi, mail kutularına, tartışma ve haber gruplarını incelemeyi ve bilgisayarların münferit IP adreslerini saptamayı gerektirebilir.

Ayrıca iletişimde kullanılan kablosuz yöntemler de, verilerin aktarımı birden çok devleti veya uluslararası kurumu ilgilendirebileceğinden, emniyet teşkilatı için yeni problemler yaratmaktadır. Bir ülkede bulunan bir kimse diğer bir ülkede bulunan biri ile cep telefonu kullanarak konuşabilir. Ancak, bu görüşmeyi ileten uydu(lar) başka ülkelerde veya uzayda yer alabilir. Bu durum görüşmeyi denetleme imkânları açısından ne ifade etmektedir?

Devletlerin terörist saldırılara karşılık verebilmesini veya bu saldırıları önlemesini sağlayacak belirli bir bilgi toplama pozisyonuna sahip olmanın önemli olduğu çeşitli durumların söz konusu olduğu zamanlarda, devletler Yolcu İsim Kaydı anlaşmalarını imzalamışlardır. Buna ek olarak, devletler bilgiyi sağlayan devletin müdahalesine gerek olmaksızın, doğrudan başvurulabilen (ortak) veri tabanları geliştirmişlerdir. Mesela Avrupa Birliğindeki bazı devletler arasında, DNA-veri tabanı, yeni bir örneğin daha önceden var olan bir DNA-profiliyle eşleşip eşleşmediği hususunda, ulusal veri tabanı yanında "işbirlikçi" devletin veri tabanına da ulaşma imkânı vermektedir.

Siber suçun ortaya çıkışı, uzunca bir süredir var olmasına karşın, bu zamana kadar uluslararası düzeyde fazla bir yasama faaliyetine neden olmamıştır. Bu konuyla ilgili temel dokümanlar, Siber Suç Sözleşmesi[3] ve bilgisayar sistemleri aracılığıyla işlenen ırkçı nitelikteki ve yabancı düşmanlığı niteliğindeki davranışların suç sayılmasına ilişkin Ek Protokolüdür[4]. Siber Suç Sözleşmesini kaleme alanlar, sözleşmenin gerekliliğini toplumun genelinde meydana gelen tüm gelişmelere bağlamışlardır[5]. Bunlardan başka uluslararası, bölgesel

3 Budapeşte,23 Kasım 2001,ETS 185, 8 Kasım 2010 itibariyle 30 onay.

4 Strasburg, 28 Ocak 2003,ETS 189, 8 Kasım 2010 itibariyle 18 onay

5 Siber Suç Sözleşmesi'nin girişinde global bilgi toplumunda uluslar arası yasal düzenlemelere duyulan ihtiyaç aşağıdaki tezlerle ifade edilmiştir. 'Öncelikli bir konu olarak, siber suçlara karşı toplumun korunmasını amaçlayan ortak bir ceza hukuku politikasının, diğer önlem-

ve ulusal düzeyde başka hangi belgeler bulunmaktadır? Devletler yasama yapabiliyorlarsa da, teknolojik ilerlemeler özel kurumların rolünü de giderek daha önemli hale getirebilmektedir.

**(2) Uluslararası yanlarına odaklanma**

Temel kural olarak, 4. bölümdeki ulusal raportörleri ilgilendiren, ulusal hukuk kurallarının her bölümünün uluslararası yönlerine odaklanılacağı önemlidir. Örneğin delillerin toplanması ve değeri belirlenmiş olduğunda, 4. bölüm için hangi devletin mevzuatının bunlara uygulanabileceğinin nasıl belirleneceğinin bilinmesi, bu delilin ulusal ceza yargılaması sisteminde delil mahiyetinin nitelendirilmesinden daha önemlidir. Ulusal raporun odağı her zaman, ulusal hukuk durumunun, uluslararası bağlam içinde izahı olacaktır.

**(3) Suçlar üzerinde yargılama yetkisine ve suçların işlendiği yere ilişkin sorular**

Eski hukuki kavramlar teknik gelişmelerin artan önemine ayak uydurmada zorluk çekebilir. Geçmişte hareketin yerini tespit edebilmek nispeten daha kolayken; siber alanda bu tespiti yapmak gitgide daha zor hale gelmektedir. Devletler genelde olumsuz yetki uyuşmazlığından kaçınma eğiliminde olup, kendi ceza hukuklarının uygulama alanlarını gittikçe genişletmişlerdir. Devletler bu problemi yargılama yetkisi kurallarının genişletilmesiyle çözmek niyetindedirler. Ayrıca bu gibi suçların sınır ötesi niteliği birden fazla yargılama yetkisinin bulunduğu durumları da çoğaltmıştır.

Ceza hukukunun sınır ötesi uygulamalarının genişletilmesi faaliyetlerinin sonucunda işin doğası gereği pozitif uyuşmazlıklar or-

---

ler dışında, uygun yasal düzenlemelerin uygulamaya konması ve uluslararası dayanışmanın teşvik edilmesi yollarıyla, izlenmesi gerektiğine kanaat getirilmiş; Bilgisayar ağlarının küreselleşmeye devam etmesi ve yakınlaşması ile dijitalleşmenin sebep olduğu büyük değişikliklerin bilincine varılmıştır. Bilgisayar ağları ve elektronik bilgilerin suç işlemek için kullanılması ve böyle bir suçla ilgili delillerin bu ağlar vasıtasıyla aktarılması ve saklanması riskinden dolayı kaygı duyulmuştur. Siber suçlarla mücadelede özel sanayi ve devletler arasındaki işbirliğine duyulan ihtiyaç ve bilgi teknolojilerinin gelişmesi ve kullanılmasındaki hukuki menfaatin korunma ihtiyacı kabul edilmiştir. Cezai konularda siber suçlarla etkili mücadelede yüksek, hızlı, iyi işleyen uluslararası dayanışmanın gerekliliğine inanılmıştır.'

taya çıkmaktadır. Bunun sonucunda pek çok soru ortaya atılabilir. Bu faaliyetler önlenmeli midir? Bu sorunsal bir durum mudur? Bu, uygulamada ciddi sorunlara neden olur mu yoksa sadece akademik bir sorunun temeline mi ilişkindir[6]?

Bütün devletlerin yargılama yetkisini genişletmesi, yarışan yargı yetkilerinin kendiliğinden ortaya çıkması sonucunu doğurur. Bu durum da suçun işlendiği yerin (locus delicit) bulunmasının zor olabileceği, bazı fiillerin suç mahalli olmadan da işlenip işlenemeyeceği sorusunu doğurur. Bu nedenle temel bir mesele, yargılama yetkisine ilişkin ilkeler olmadan, modern suçların oluşup oluşamayacağıdır ki bu da özünde ulusal ceza hukukunun evrensel olarak uygulanabilir olduğu anlamına gelecektir. Bu izlenebilir bir yol mudur? Bu husus belirli suçlarla, örneğin sözleşmesel esaslarla suç sayılan ve sınır ötesi yargılama yetkisi verilen suçlarla[7], sınırlandırılmalı mıdır, yoksa tüm suçlar için buna izin verilmeli midir? İkinci durumda, cazip bir çözüm gibi görünen, ulusal ceza hukukunun dünyanın her yerinde uygulanabilmesi söz konusudur. Bu durum sadece aralarında belirli bir bağ bulunan davaların kovuşturulmasına izin verilerek çözülebilir mi? Fiiliyatta yarışan yargı yetkisi ne derecede hareketsizliğe yol açar? Bu durum bazı devletlerin, ülke sınırları dışında işlenen suçlar hakkında suçu yargılama yetkisine sahip başka birçok devletin de olması sebebiyle, soruşturma veya kovuşturma yapmadığı, bir "müdahale etmeme etkisi"ne götürür mü?

Suçun işlendiği yeri belirlemenin zor olduğu veya suçun işlendiği yer nedeniyle yarışan yargı yetkisinin söz konusu olduğu bazı suçlarda uluslarüstü bir yargı yolu öngörmek de konuya başka bir yaklaşım yöntemi olabilir. Elbette bunun avantajı uluslarüstü mahkemenin katılan devletleri de bağlayacak şekilde hukuki uyuşmazlığı çözme gücüne sahip olması olacaktır. Ayrıca daha iyi uzmanlaşmış bir mahkeme ve kovuşturma, ulusal kanun uygulayıcı makamların

6 Yakın geçmişte Hollanda Adalet Bakanlığını tarafından gerçekleştirilmiş karşılaştırmalı bir çalışmada, Klip ve Massa Devletler' in ülke toprakları dışındaki suç mahallerinde (locus delicti) işlenen suçlar için neredeyse hiç kovuşturma yapılmadığı sonucuna varmışlardır. Bkz. André Klip ve Anne-Sophie Massa, Communicerende grondslagen voor extraterritoriale rechtsmacht, Maastricht University 2010 http://www.wodc.nl/onderzoeksdatabase/vestiging-rechtsmacht.aspx?cp=44&cs=6802

7 Örneğin, Siber Suç Sözleşmesi.

imkânlarının çok daha ötesine geçen, belirli tür sınır aşan suçların üstesinden de gelebilir. Kurumlar için bir uluslararası sorumluluk fiiliyatta nasıl işleyebilir? Ancak bu durum aynı zamanda, hukukun uygulanmasında daha fazla ayrışmaya götürecek, bir başka uluslararası mahkeme daha kurulabileceği anlamına da gelir.

Suçun işlediği yerin tespitinin zorluğuna eklenen bir unsur da, çifte cezalandırma gerekleridir. Evrensellik ilkesi dışındaki çoğu yargılama ilkesi, fiilin, işlendiği yerin hukukuna göre de suç teşkil etmesini gerektirmektedir. Bilgi toplumundaki gelişmeler dikkate alındığında, bu şartın hala amaca hizmet edip etmediği sorulabilir. Günümüz bilgi toplumu bağlamında ve gelecek on yıllarda, aranan çifte cezalandırma şartlarını sürdürmenin gerekçesi nedir? Bu olmadan da yapamaz mıyız? Kural kaldırılacak olsa, hangi meseleler tehlike altında olacaktır? Çifte cezalandırma kuralıyla korunan menfaatler, başka şekillerde güvence altına alınamaz mı?

**(4) Soruşturmalara ilişkin sorular**

Bu zamana kadar, ülke sınırları dışındaki delillerin toplanmasıyla ilgili kurallar, açık ve anlaşılırdı. Eğer kanun uygulayıcı makamlar başka bir yerdeki delile ve bilgiye ihtiyaç duyuyorlarsa, yabancı yetkililerden bunu talep etmek zorundadırlar. Bir ülkenin emniyet görevlisi ihtiyaç duyduğunu almak için başka bir devletin toprağına izinsiz olarak giremez. Mevcut durumdaki koşullar geçmişe göre oldukça farklıdır; çünkü telekomünikasyon ağları, kanun uygulayıcı makamların kendi ülkelerini terk etmeden bilgi ve delil elde etmelerine olanak sağlamaktadır. Sorulacak ilk soru bilginin ve delilin bulunduğu yeri belirlemenin gerekli ve mümkün olup olmadığı sorusudur. Birinin internet ağı üzerinde bulabileceği bir bilgi aslında neredediir? Bilgisayar kullanıcısının fiziksel olarak bulunduğu yerde midir? Ağ sağlayıcısının (hukuki ya da fiili olarak) bulunduğu yerde midir? Bu hangi ağ sağlayıcısıdır? Ya da veriyi erişilebilir kılan kişinin bulunduğu yer midir?

(Bilgi ve delillerin yerini tespit etmenin hala mümkün olduğu kabul edildiğinde) Bilgi toplumu ve cezai soruşturma amaçları için bilgi ve delil toplama kapsamında; birçok durum dikkate değerdir:

1. Aleni bilgi ve delil. Bu, internette gezinerek kolayca erişilebilecek halka açık bilgidir. 2. Korunan bilgi. Kamuya açık olmayan fakat hack'leme sonucunda elde edilebilecek bilgidir. 3. Başka bir ülkedeki bir bilgisayarın ya da bilgisayar ağının ele geçirilmesini gerektiren bilgi ve deliller.

Devletler, yabancı kanun uygulayıcı makamlarının temsilcilerinin kendi topraklarında fiziksel olarak bulunmasını yasaklayan katı kurallara sahip olmaya devam etmektedir[8]. Modern suçlar kapsamında bu kurallar yine de uygulanacak mıdır? Bu kurallar, kanun uygulayıcı makamların temsilcilerinin ülke topraklarına fiziken girmedikleri; fakat başka ülkede bulunan bir bilgisayarda veya bilgisayar ağında araştırma yaptıkları zaman da uygulanacak mıdır? Aynı kurallar uygulanacak mıdır ve eğer öyleyse bu kurallar nasıl uygulanacaklar? Fiziksel varlığı yasaklayan kurallar uygulanmayacaksa eğer, bunun sebebi nedir?

Cezai konularda yardımlaşma ile ilgili alışılmış kuralların uygulanmamasının sonucu sembolik olmaktan ötedir. Bu durum başka bir ülkeden bundan sonra yardım istenmemesine ve başka bir ülkeye yardım verilmemesine; ülkenin bilgiyi yalnızca kendi imkânlarıyla elde etmesine (self-servis) sebep olacaktır. Bu, reddin klasik gerekçelerinin (çifte cezalandırma, suçun doğası, çifte yargılama vb.) artık uygulanamayacak olması durumuyla sonuçlanabilecektir. Bu alanda ret sebeplerinin uygulamasını azaltmak mümkün veya gerekli olacak mıdır? Self-servisi cezai konularda uluslararası yardım yöntemlerinden biri olarak kabul etmenin (teorik/pratik) sonuçları nelerdir?

Bir kere daha, teknik imkânların hukuki ilerlemeleri ve imkânları belirleyebileceği anlaşılmaktadır. Bu olgu, hukukun ilerlemesi için önceliğin nerede olması gerektiği hakkında oldukça ilginç teorik sorulara götürmektedir. Bununla birlikte, daha ziyade pratik hukukun doğasıyla ilgili sorular da vardır. Bunun bir örneği kablosuz telekomünikasyona müdahale ile ilgilidir. Eğer iki kişi cep telefonu

8 Polis memurları, yalnızca kanunlaştırılmış bir uluslararası anlaşmaya veya somut olayda özel olarak verilen bir izne dayanarak başka bir ülkeye girebilir ve görevlerini yerine getirebilir. Zorlayıcı tedbirlerin kullanılması genel olarak kabul edilmemiştir. Sınır ötesi sıcak takip durumunda bir kaçağın yakalanması gibi küçük istisnalar ile birlikte bkz. Schengen Anlaşması Uygulama Sözleşmesi Md. 41

kullanarak konuşuyorlarsa; bu, altı devleti ilgilendiren bir konu olabilmektedir[9]. Bütün bu devletler, konuşmalara müdahale yapılıp yapılamayacağı konusuna dair söz hakkına sahip midir? Ya da bu, müdahale etmek isteyen devletle mi sınırlı olmalıdır? Öyleyse veya öyle değilse, neden?

Bazı devletler ve uluslararası örgütler, dünyadaki her yerin açık ve detaylı bir görüntüsüne sahip olmayı sağlayan uydulara ya da başka cihazlara sahiplerdir. Hukuk, bunun ceza soruşturması ve yargılaması amaçları için kullanılmasını düzenleyebilir mi? Eğer düzenleyebilirse, hangi seviyede düzenlenmelidir -ulusal mı uluslararası mı- ve bu durumda söz konusu olan sorunlar nelerdir[10]?

### (5) Cezai konularda klasik karşılıklı yardımlaşmaya ilişkin sorular

Bilgi toplumu, yardımlaşmanın doğasını ne ölçüde değiştirmiştir[11]? Her ne kadar kendi kullanacağın bilgiyi kendi başına elde etmenin bazı türleri gündeme gelmiş ve hukuken kabul edilmiş olsa da, bilgi toplumundaki ileri gelişmelerle, cezai konularda karşılıklı uluslararası adli yardımlaşmanın tamamen yok olması olası değildir.

Yurtdışında yaşayan insanlarla işitsel-görsel teknikler (Skype, video konferans) vasıtasıyla konuşmanın gittikçe daha kolay hale gelmediği gerçeği, suçluların kovuşturma amaçlı iadesinde daha yüksek bir eşiğe varmanın gerekip gerekmediği sorusunu doğurmaktadır. Sanığın yargılandığı ülkede bulunmaması halinde, iadenin gerçekleşmesi muhtemeldir. Sanığın özgürlüğüne ilişkin ciddi ihlaller göz önüne alındığında, duruşmanın video bağlantısı aracılığıyla yürütülmesinin tercih edilip edilmeyeceği sorusu gündeme gelebilir. Aynı zamanda masumiyet karinesi de suçluların iadesi kurumunun külfeti ile çatışacaktır. Suçluların iadesini, hakkında mahkumiyet kararı ve-

9 Gert Vermeulen, Wederzijdse rechtshulp in strafzaken in de Europese Unie, dissertation Gent 1999, p. 224-293.

10 George Orwell'ın ünlü romanı 1984 'te öngörülen televizyon ekranlarını hatırlatmaktadır.

11 Siber Suç Sözleşmesi'nin, cezai konularda uluslararası yardımlaşmayla ilgili klasik ilkeleri – yardım sağlanması için bir devlet tarafından diğerine gönderilen talep – tamamen benimsendiğini görmek ilginçtir.

rilmiş kişiler hakkında mı uygulamalıyız? Gerçek mahkeme salonunda kimse bulunmadığında, duruşmaların görülebileceği sanal bir mahkeme salonu mu tasarlamaktayız?

Benzer şekilde, modern telekomünikasyon; sanıklar, mağdurlar ve tanıklarla doğrudan iletişim kurulması ihtimalini yaratmaktadır. Buna izin verilmeli midir ve eğer izin verilirse hangi şartlar altında izin verilmelidir? Eğer verilmezse, yardımlaşmaya ilişkin klasik kurallar(talep ve cevap) uygulanmalı mıdır ve neden uygulanmalıdır? Birçok bilgiye her halükarda serbestçe erişilebiliyor olması ve birçok davada müdahil olan insanların bilgiyi iradi bir şekilde bildiriyor olmaları gerçeği, devletlerin neden hala, yardımın verilip verilmeyeceği konusunda kontrol yetkisine sahip olduğu sorusunu doğurmaktadır. Öte yandan, bir hareketin ifade özgürlüğünün veya ciddi bir suç olan gizliliğin ihlalinin alanına girip girmeyeceği düşüncesi farklılık gösterebilir. ABD'nin, Irak savaşıyla ilgili birçok gizli ve erişimi kısıtlanmış belgenin Wikileaks aracılığıyla erişilebilir kılındığı gerçeğini araştırmak için bazı bilgileri talep ettiğini farz ediniz.

Bilgi aktarımına dair verilerin korunmasına ilişkin yükümlülükler nelerdir? Ağ sağlayıcılarının, başka devletlerin kanun uygulayıcı makamları tarafından yapılan değişik ve karmaşık yardım talebine uyacak şekilde ağlarını düzenleme zorunluluğu var mıdır? İlgili devlette herhangi bir yeri olmayan ağ sağlayıcıları ile bu nasıl yapabilir? Ayrıca daha genel bir esas da, ilgili mevzuatın dışında, bilgi toplumunda işlenen suçlarla nasıl üstesinden gelineceğini devletlerin gerekli teknik bilgiye (know-how) sahip olup olmadığı sorunudur.

### (6) Bilgi pozisyonuna ulaşma ile ilgili sorular[12]

Özellikle, terör ile mücadele tedbirleri kapsamının bir parçası olarak, ülkeler, terör saldırıların ve diğer suçların meydana gelmesini engellemek için iyi bir bilgi pozisyonuna ulaşmak isterler. Geçmişte hava trafiğinin terör saldırılarında araç olarak kullanımı göz önünde bulundurulduğunda, devletler yolcular ve uçakların yükleri

12 Hans Nijboer tarafından verilen tanıma atıfta bulunulmuştur, 3.Bölümün Genel Raportörü: 'Muazzam miktarda işletimsel bilginin varlığı ve kullanılması bazen savcılık ve soruşturma makamlarının bilgi mertebesi olarak adlandırılmıştır.

hakkında daha fazla bilgi sahibi olmaya öncelik vermeye başladılar. Yolculara ilişkin olarak, Yolcu İsmi Kayıtları (PNR) anlaşmaları adıyla anılan anlaşmalar sonuçlandırıldı.[13] Finansal işlemler ve vize işlemleri gibi başka alanlarda da veri alışverişi yapıldı.

Burada özel hayatın gizliliğine ilişkin düzenlemelerin sınırları içine giriyor olduğumuz gerçeğinin farkında olmalıyız. Bu yüzden bir yandan tartışmalarımızın odak noktasının özel hayatın gizliliğin korunmasının unsurları üzerinde olması engellenmeliyse de, diğer bir taraftan, özel hayatın gizliliği hakkının bazı esaslarının incelenmesi kaçınılmaz olacaktır. Ulusal Raportörlerin, ceza soruşturmaları için yapılan PNR sözleşmesine göre, göç politikası veya genel olarak veri elde etme gibi diğer amaçlarla değil, ceza soruşturmalarında gönderilen veya değiş-tokuş edilen verilerin (finansal ya da herhangi diğer işlemler) kullanımına odaklanmaları istenmektedir. Veriler cezai soruşturmalarda hangi sınırlarda ve hangi yasal dayanaklarla karşılıklı değişilecektir? Söz konusu kişi ne ölçüde bilgi engelleme/ düzeltme/silme imkânına sahiptir? Değiş-tokuş edilen veriler ne ölçüde kanıt olarak kullanılabilir?[14]

Yakın zamanda olan bir başka gelişme ise uluslarüstü veri tabanlarının kurulması ve birbirlerinin veri tabanlarına çevrimiçi danışılabilmesidir. Buna bir örnek Avrupa Birliği'nde, bazı üye devletler arasında kurulmuş, doğrudan sisteme dâhil diğer bir üye devletin DNA, araç plakaları kodları ve parmak izleri verilerine ulaşabilmelerini sağlayan mekanizmadır[15]. Bunun sonuçlarından biri, artık verisi kul-

13 Avrupa Birliği bu konuyla ilgili olarak Amerika Birleşik Devletleri ve Avustralya ile anlaşmalar imzalamıştır. Bkz. http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/431&format=HTML&aged=0&language=EN&guiLanguage=en
Avrupa Birliği ve Amerika Birleşik Devletleri arasında, Terörist Finansmanı Takip Programı için, Avrupa Birliğinden Amerika Bileşik Devletlerine yapılan Finansal Mesajlaşma Verisi iletimi ve işlenmesi üzerine Anlaşma'nın, Avrupa Birliği adına imzalanması hakkında 30 Kasım 2009 tarih ve2010/16/CFSP/JHA sayılı Konsey Kararı, OJ 2010, L 8/11

14 AB bağlamında, cezai konularda uluslararası işbirliğinde veri koruma kurallarını düzenleyen özel bir hukuki doküman kabul edilmiştir. Bkz. Cezai konularda emniyet teşkilatları arası ve hukuki işbirliği çerçevesinde işlenmiş kişisel verilerin korunması hakkında 27 Kasım 2008 tarih ve 2008/977/JHA sayılı Konsey Çerçeve Kararı, OJ 2008, L 350/60.

15 Özellikle sınır ötesi suçlarla ve terörle mücadelede sınır ötesi işbirliğinin arttırılmasına ilişkin 2008/615/JHA sayılı Konsey Kararının ve Özellikle sınır ötesi suçlarla ve terörle mücadelede sınır ötesi işbirliğinin arttırılmasına ilişkin 2008/615/JHA sayılı Konsey Kararının uygulamasına ilişkin 2008/616/JHA sayılı Konsey Kararının ve Ekinin uygulanması

lanılan ülkeden, eskiden olduğu gibi veriyi almak için resmi talepte bulunulmaması ve devletlerin her seferinde gönderip göndermeme konusunda artık karar vermemesidir. Bu aynı zamanda ilk bilgi alışverişi aşamasında ret dayanaklarının artık dikkate alınmayacağı ve uygulanmayacağı anlamına da gelmektedir.[16]Bu olumlu bir gelişme midir? Avrupa Birliğinde tüm üye devletlerin adli sicil kayıtlarına da doğrudan erişim sağlayabilmek için daha ileri projeler de geliştirilmiş bulunmaktadır.[17] Bu olumlu bir şey midir? Dünyanın başka bölgelerinde de buna benzer gelişmeler tespit edilebilir midir?

### (7) Doğrudan infaza ilişkin sorular

Bilgi teknolojilerinin neredeyse sınırsız miktardaki ihtimali; devletlerin diğer devletlerden izin almaksızın, doğrudan; hükümleri, tebligatları ve geçici önlemleri vs. doğrudan uygulayıp uygulayamayacakları sorularını doğurmaktadır.

Nefret söylemi, çocuk pornosu veya diğer yasa dışı materyalleri içermesi sebebiyle, belli bir İnternet sitesinin kapatılması için yasal bir kararın söz konusu olduğu durumlarda; bu sitenin daha fazla suç işlenmemesi amacıyla, kanun uygulayıcı makamlar tarafından hack'lenmesine izin verilmeli midir?

Hükümlerin, kararların, mahkeme celplerinin ve diğer hukuki belgelerin tebliğinin bazı yasal sonuçları olabilmektedir. Yasa, bilgi teknolojileri aracılığıyla yapılan tebliğlere de bu yasal sonuçları bağlamalı mıdır?[18] Benzer şekilde, devletlerin, suçtan ötürü elde edilen gelire el koyma amacını gerçekleştirmek için, bazı finansal araçları ele geçirmek amacıyla, bankalar ve finansal kurumlar üzerinde dayatabileceği bir yetkisi var mıdır?

---

hakkında, AB, Norveç ve İzlanda arasındaki Anlaşmanın, AB adına imzalanması ve belirli hükümlerinin geçici olarak uygulanmasına ilişkin 21 Eylül 2009 tarih ve 2009/1023 sayılı Konsey Kararı, OJ 2009, L 353/121; Özellikle sınır ötesi suçlarla ve terörle mücadelede sınır ötesi işbirliğinin arttırılmasına ilişkin 23 Haziran 2008 tarih ve 2008/615/JHA sayılı Konsey Kararı, OJ 2008, L 350/60.

16 Bununla birlikte, ilgili yasal dokümanlar, eğer bilgi delil olarak kullanılacaksa, uluslar arası yardım(laşma) için uygun bir talebin yapılması gereğinden bahseder.

17 Üye devletlerarasında, adli sicil kayıtlarından elde edilen bilgilerin alışverişinin içeriğine ve organizasyonuna ilişkin 26 Şubat 2009 tarih ve 2009/315/JHA sayılı Konsey Çerçeve Kararı, OJ 2009, L 93/23.

18 Örneğin 2001 yılında Alman posta servisleri, mübaşir tarafından yapılan resmi tebligata eş değerde olacak şekilde elektronik teslimi (Zustellung) uygulamaya koymuşlardır.

### (8) Son Sözler

Özetle, ilk bakışta, bilgi toplumunun, uluslararası ceza hukukuna etkisinin üç bölümden oluştuğu görülmektedir. Birincisi, bilgi toplumu, bazı hukuki değerler için ulus aşırı bir tehdit yaratırken, diğerleri bundan etkilenmemiştir. İkincisi, bilgi toplumu, diğer taraftan, ceza adaleti için bir araç oluşturmaktadır. Üçüncü büyük etki ise egemenlikle ilgilidir. Bizim çağımızda egemenlik ne anlama gelmektedir? Geleneksel olarak, egemenlik kavramı ülkelere, ülkesellik ilkesine dayalı olarak ceza hukuku ve ceza muhakemesi hukukunun uygulaması konusunda bir tekel hakkı tanımaktadır. Bilgi toplumu, ülkesellik ilkesinin önemini ve değerini ciddi oranda azaltmıştır (ya da belki ortadan kaldırmıştır). Bu egemenlik için ne anlama gelmektedir? Özet olarak, bu bölüm; hareketin, soruşturmanın ve infazın sınırötesi karakterine odaklanmıştır.