Preparatory Colloquium Section I

Report of the Turkish National Group *

Prepared by:
Assistant Prof. Dr. Murat Önok[1]
Assistant Prof. Dr. Baris Erman[2]
Dr. Güçlü Akyürek[3]

(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 in Turkey[4]. 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[5].

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

[1] Koç University Law Faculty

[2] Yeditepe University Law Faculty, Department of Criminal Law and Criminal Procedure

[3] Galatasaray University Law Faculty, Department of Criminal Law and Criminal Procedure

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

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

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

accessed from Turkey[6]. 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 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

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

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[7]. If, for instance, a person would attack another

[7] ARTUK/GÖKCEN/YENİDÜNYA, p. 1051.

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 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) [8]. 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 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

[8] 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.

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[9]. However, in cases of cyber crimes, positive conflicts pose a more significant problem than negative ones.

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[10]. 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, 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.

[9] See: TEZCAN/ERDEM/ÖNOK, p. 161.

[10] TEZCAN/ERDEM/ÖNOK, p. 161-162.

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[11]. 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[12], or the criminal content being uploaded from Turkey[13].

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

[11] See: ÖZBEK, p. 193.

[12] DEMİRBAŞ, p. 141.

[13] ÖZBEK, Veli Özer / KANBUR, M. Nihat / BACAKSIZ, Pınar / DOĞAN, Koray / TEPE, İlker, Türk Ceza Hukuku Genel Hükümler, Ankara, 2010, p. 141.

if the perpetrator aimed for a result to appear specifically on Turkish territory[14].

Additionally, the principle of ubiquity is criticised for being out-dated[15]. However, there are also differing opinions that support a wide definition of territoriality, whilst agreeing that some jurisdictional problems might arise[16].

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 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

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

[14] ÖZBEK, p. 194.

[15] ÖZBEK, p. 191.

[16] ARTUK/GÖKCEN/YENİDÜNYA, p. 1051.

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).

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).

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[17]. However, there also exists another opinion defending the current Turkish provisions, and considers them as a conscious choice of the Turkish legislator[18].

Do you consider cyber crime offences a matter that a state can regulate on its own? If so,

[17] ARTUK/GÖKCEN/YENİDÜNYA, p. 1050.

[18] ÖZGENÇ, İzzet, Türk Ceza Hukuku, 5e, Ankara, 2010, p. 770.

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.

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[19].

(D) Cooperation in criminal matters

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

A. General Information

[19] 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.

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.

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"[20] not be applied in the territory of another state absent the consent of the local government[21].

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

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

[20] As opposed to the "jurisdiction to prescribe", which is limitless.

[21] 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..

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[22] 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[23] 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.
- 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.)

---

[22] 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]

[23] "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]

- 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[24] 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.

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

[24] '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).

(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[25] should be mentioned. The purpose of this Law is to establish effective 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

[25] Published in the Official Journal of 10/11/2008.

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[26] (18/4/1960; 18/4/1960)
- European Convention on Mutual Assistance in Criminal Matters[27] (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)
- 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[28] (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)

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

[27] Turkey also ratified the 1978 Additional Protocol, but not the 2001 Second Additional Protocol.

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

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
- 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[29], 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[30].

In the particular field of telecommunication, Turkey is a member of the International Telecommunication Union, and has ratified[31] the Final Acts of the Plenipotentiary Conference held in Antalya (2006) and embodying the "Instrument amending the Constitution of the International Telecommunication Union".

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

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

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

[31] Law no. 6011 of 23/07/2010.

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.[32]

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 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

[32] 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

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[33]. 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.

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

[33] 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.

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[34]:

- 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;

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

- 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.

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)[35].

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."'[36]

E) HUMAN RIGHTS CONCERNS

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. 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

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

[36] 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].

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.