Preparatory Colloquium
Verona (Italy), *28 – 30 November 2012*
Section I - Information Society and Penal Law

REPORT OF THE TURKISH NATIONAL GROUP*

Vesile Sonay DARAGENLI EVIK, Hasan SINAR, Baris ERMAN, Gülsah KURT[1]

(B) Criminalisation

(1) Which specific legal interests are deemed to be in need of protection by criminal law (e.g., integrity of data processing systems, privacy of stored data)?

There are several legal interests protected by various criminal offences, some of which have been criminalised under the Turkish Penal Code (TPC), whereas others can be found in specific laws. As a result, it is necessary to mention these legal interests according to different criminal offences.

The crime of "illegally entering an IT system or staying there" protects the security of IT systems, data security, and privacy. As for the crime of "prevention of the functioning, or destruction of an IT system, destruction or manipulation of data", it is the interest of the authorised person to be able to access the IT system or to data protected within.

The crime of "obtaining illegal benefits through IT systems" protects the material or moral rights that are subject to the illegal benefit obtained through the offence. The legal interest protected by the crime of "fraud in debit and credit cards" is personal property, trust of the general public towards valid and persuasive legal documents. As for the crimes of "storing personal data" and "giving or obtaining personal data", the protected legal interests are the privacy of persons, and data security. Following these criminal offences, the crime of "failure in destroying personal data" protects not only the privacy and data security, but also the trustworthiness and functioning of the state administration. The crime of "violation of the confidentiality of communication" protects the interest of persons regarding the confidentiality of the private communication, whereas the crime of "prevention of the communication" it is the freedom of communication without undue interruption that is being protected.

The crime of "theft through the abuse of IT systems" protects the private property, while the crime of "pornography / obscenity" protects the general morals and, in particular, the healthy sexual development of minors.

The crime of "illegally copying or using software", regulated under the Turkish Intellectual Property Law (IPL), protects the financial and personal rights of the author on the software.

Additionally, crimes regulated under the Electronic Signature Law (ESL), "illegally using e-signature data, illegally

---

* 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.

[1] Assoc. Prof. Dr. Vesile Sonay Daragenli Evik, Galatasaray University Law Faculty, Department of Criminal Law and Criminal Procedure Law.
Assistant Prof. Dr. Hasan Sinar, İstanbul Kemerburgaz University Law Faculty, Department of Criminal Law and Criminal Procedure Law.
Assistant Prof. Dr. Baris Erman, Yeditepe University Law Faculty, Department of Criminal Law and Criminal Procedure.
Dr. Gülsah Kurt, Galatasaray University Law Faculty, Department of Criminal Law and Criminal Procedure Law

obtaining, giving, copying data or tools, illegally creating an e-signature, falsification of electronic certificates", mainly protect data security and public trust of the general public towards valid and persuasive legal data.

As a last point the crime of "providing access to gambling and betting activities in abroad through internet or other means", as regulated under the Law on Gambling and Betting Games, has been introduced in order to protect the general morals, and the financial interests of state-regulated gambling organisations.

(2) Please give typical examples of criminal laws concerning;

(a) attacks against IT systems

Art. 243 TPC regulates a criminal offence of "illegally entering, or staying in an IT system", punishable with a prison sentence of up to one year or with a fine. It is a mitigating circumstance that the object of the offence is an IT system that may be used in exchange for a fee. If, however, as a result of the conduct, data included in the IT system in question has been erased or manipulated, the sentence shall be aggravated to that of prison from six months to two years.

Art. 244/1 TPC provides for a criminal offence of obstructing or disturbing the functioning of an IT system, and punishes such acts with a prison sentence of up to five years. Art. 244/2 TPC regulates the offence of "corrupting, destroying or manipulating data, rendering data inaccessible, inserting data into the IT system, or sending existing data elsewhere", punishable with a prison sentence from six months up to three years. An aggravating circumstance has been regulated under art. 244/3 TPC, according to which the sentence shall be aggravated by one half, if the object of the criminal conduct is an IT system belonging to a bank or credit institution, or to a public institution.

Art. 244/4 TPC provides for a criminal offence of "obtaining illegal benefits through IT systems", punishable with a prison sentence of two to six months, as long as such conduct does not constitute another criminal offence.

It is mentioned in the doctrine that the lack of a criminal offence regarding "obtaining data from an IT system" would cause a gap in criminalisation. However, this gap can be filled through art. 136 TPC (illegally obtaining personal data), and, regarding copyright infringements, through art. 71 IPL.

(b) Violation of IT privacy

Art. 132 TPC regulates the offence of "violation of confidentiality of communications". According to this regulation, it is an act punishable with a prison sentence from one to three years to violate the confidentiality of communications between persons. The sentence shall be doubled in cases where the conduct involves the recording of communications. Those who illegally disclose the content of the communication shall be punished with a prison sentence of two to five years. The same sentence shall be applicable if the disclosure has been realised via press or similar media.

Art. 134 TPC provides for a criminal offence generally protecting the private life of persons. According to the regulation, any act of violating the private life of a person is punishable with a prison sentence of one to three years. In cases where the violation occurs through recording images or sounds, the sentence shall be doubled. Illegal disclosure of such images and sounds is a separate offence punishable from two to five years under art. 134/2 TCP. As such, any conduct related to privacy that does not fall under other criminal offences shall be punishable under this regulation.

Art. 135 TPC provides for a prison sentence of six months to three years for those who illegally record personal data, followed by art. 136, which criminalises illegally giving, disseminating or obtaining personal data as an act punishable with a prison sentence from one to four years.

Art. 138 TPC criminalises the failure to destroy personal data within IT systems despite the fact that the legal period of time regarding their destruction has expired. Such conduct is subject to a prison sentence from six months to one year.

(c) forgery and manipulation of digitally stored data

According to art. 244/2 TPC it is a criminal offence to corrupt, destroy, manipulate data within an IT system, rendering such data inaccessible, inserting data into the system, or sending such data elsewhere. Such conduct is punishable with a prison sentence from six months to three years.

In addition, art. 245 TPC criminalises the debit and credit card fraud. This article includes three separate criminal offences, one of which regards the forgery, selling, giving, buying or receiving of false debit or credit cards connected with bank accounts belonging to other people. According to the article 245/2, such conduct is punishable with a prison sentence of three to seven years. Under the Law on Debit and Credit Cards (art. 3/e), a "credit card" has been defined in a way to encompass the "card number without the requirement of the material existence of the card". As such, the electronic forgery of the card number would suffice in order to fulfil the requirements of art. 245 TPC.

(d) distribution of computer viruses

As there is no separate offence under Turkish law regarding the distribution of computer viruses, such conduct shall be considered according to art. 244 TPC (obstructing or disrupting an IT system, destroying or manipulating data within an IT system), as explained above.

If, through the distribution of a computer virus, the hardware of an IT system has been harmed, the conduct could also be considered under the criminal offence of "intentionally damaging property" (art. 151 TPC).

(e) crimes related to virtual identities of users, e.g., forging, stealing or damaging virtual personalities

There are no specific criminal offences regarding the virtual identities of users. Such conduct may be considered under the general offence of "violation of the private life" (art. 134 TPC), libel and slender (art. 125 TPC), or illegally obtaining, giving or disseminating personal data (art. 136), as long as these articles are applicable. If the conduct does not fulfil the specific elements of these offences, it can be punishable under art. 244/4 TPC (obtaining illegal benefit through the abuse of IT systems).

(f) other innovative criminal prohibitions in the area of ICT and internet, e.g., criminalisation of the creation and possession of certain virtual images, violation of copyright in the virtual sphere.

In general, the violation of financial interests on copyrights has been regulated as a criminal offence under IPL art. 71. According to the article, the intentional dissemination and distribution of copyright protected data through any means, and the possession or storage of such data for purposes other than self-use is punishable with a prison sentence of one to five years and with a fine. As such, any Internet content that has the characteristics of a "copyright protected work" could be the object of this offence.

Additional art. 4 IPL specifically addresses "content providers" infringing copyrights under the same law, providing for a notify-and-remove 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 this case, 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.

Another innovative criminal prohibition in the area of ICT and the Internet is the criminal offence regarding e-signature fraud. Art. 16 ESL regulates acts of "illegally obtaining, giving, copying, reconstructing signature creating data or tools, or creating an unauthorized electronic signature through using tools obtained illegally" as a criminal offence punishable with a prison sentence of one to three years in addition to a fine. Art. 17 ESL deals with the crime of "fraud in electronic certificates", providing for a prison sentence of two to five years for those who, in full or in part, forge a false electronic certificate, or falsify valid electronic certificates, or those who knowingly use such certificates.

(3) How is criminal conduct (actus reus) typically defined in these crimes (by description of act, by consequence, other)? How is the object defined ("data", "writings", contents)?

In most cases, the criminal conduct has been typified as alternative acts. An exception is art. 243 TPC, where the act of "entering, and staying in an IT system" is a compound of two consecutive acts building the criminal conduct.

Again, in most IT-related crimes, the criminal conduct has been defined by description of the act. Consequences following the conduct have only been regulated under art. 243 TPC, where the destruction or manipulation of data "as a consequence" of illegally entering an IT system has been described as a consequence-based aggravating circumstance.

In some cases, crimes in the area of ICT have been defined as endangerment offences. The crime of entering, and staying in an IT system is punishable even if no harm has resulted from the act. Thus, it falls under the category of abstract endangerment offences. However, most crimes in this area require a clear harmful result as part of the legal definition.

As to the object of the crimes, the terms "IT systems" and "data stored within IT systems" has repeatedly been used under in defining the crimes of "entering, and staying in IT systems" (art. 243 TPC), "obstructing the functioning of an IT system" (art. 244/1 TPC), "corrupting, destroying, manipulating data within IT systems, or rendering such data inaccessible" (art. 244/2 TPC).

Articles 135, 136 and 138 TPC are related to "personal data", although the definition of this term is not included within the regulations of these articles. In fact, there is an on-going debate in Turkish legal doctrine as to the scope of the concept "personal data", as shall be explained below.

Another point to be mentioned under this title is the definition of the "through press or similar media" under art. 6 TPC. According to this article, any mention of the said term within the Code would encompass acts committed through electronic media, including the Internet. The term has been used in various places, sometimes as an element of crime, in other instances as an aggravating circumstance. The term has also been mentioned in art. 132 TPC regarding the disclosure of contents of a private communication, and in art. 134 TPC, regarding the illegal distribution of images or sounds concerning the private life of individuals. As a result, these crimes shall be deemed as "realised through press or similar media", if they are committed through the use of the Internet.

(4) Is criminal liability for certain cyber crime limited to particular groups of perpetrators and/or victims?

Under Turkish law generally there are no limitations for certain cyber crime related offences regarding particular groups of perpetrators and/or victims. However, it is an aggravating circumstance in the crimes of storing, giving, distributing or obtaining personal data (arts. 135, 136 TPC), if this crime has been committed by a public servant in abuse of his or her authority. In addition, the crime of "failure in destroying personal data" (art. 138 TPC) can only be committed by a person legally obligated to erase or destroy personal data at the expiration of legally set time periods.

Another instance, where a specific group of perpetrators has been defined as an aggravating circumstance can be found under the ESL. According to arts. 16 and 17, the sentence shall be doubled if the perpetrator is an "employee of the electronic certificate service provider".

(5) Does criminal liability in the area of ICT and internet extend to merely reckless or negligent conduct?

In general, criminal liability in the area of ICT and Internet only encompass conduct with intent. However, the consequence-oriented aggravating circumstance as defined under art. 243/2 TPC under the crime of "entering, and staying in an IT system", provides for an aggravation of the sentence, if "as a consequence of said conduct, data has been destroyed or manipulated". Such consequence-oriented aggravation can result in the criminal liability of the perpetrator, even if he or she did not intent the consequence, but solely the initial act, whereas the consequence may have been the result of negligence by the perpetrator, according to art. 23 TPC.

(6) Are there specific differences between the definition of cyber crimes and "traditional" crimes?

There are no specific differences between the definition of cyber crimes and traditional crimes. However, many of the crimes mentioned above, in particular, the crimes of entering an IT system (art. 243 TPC), violation of the confidentiality of communications (art. 132 TPC), disclosure of images or sounds related to the private life of individuals (art. 134/2 TPC), recording, giving, distributing or obtaining personal data (arts. 135, 136 TPC) include the requirement that such conduct to be committed "illegally". The predominating opinion of the legal doctrine holds that the specific mentioning of the "illegality" of the conduct means that the intent of the perpetrator should include the illegal nature of his or her conduct for these crimes.

(C) Legislative technique

(1) Are there specific problems with respect to the principle of legality (e.g., vagueness, open-ended reference of the crime definition to other regulations)?

Although certain concerns exist regarding the principle of legality, these problems are not related to IT-specific crimes defined under arts. 243-245 TPC, but rather to other crimes that can be committed through the use of IT systems, i.e. Violation of the private life of individuals (art. 134 TPC), crimes of illegally storing, giving or obtaining personal data (art. 135-136 TPC), and failure to destroy personal data (art. 138 TPC).

The object of the crime of violation of the private life has only been defined as "private life of individuals", without any restrictions regarding the criminal conduct. This concept has not been clearly constructed, is subject to discussions in

criminal law literature, and is a particularly vague concept in its scope[2], it is held that this crime could create problems regarding the principle of legality[3].

The criminal conduct of the crime provided under art. 135 TPC is defined as "illegally recording personal data". However, the term "personal data" has not been defined by law. A draft proposal for a Law on Personal Data has been prepared by the government, and the proposal has been sent to the Turkish Parliament in 2008. Although it is expected that this new law would define the concept of "personal data", it has still not entered into force. The motives of Art. 135 TPC state that "personal data" should be interpreted as "any information related to a real person". However, the "Regulation on the Processing and Protection of Confidentiality in Electronic Communications", in force since 24 July 2012, defines personal data as "any information related to real or legal persons, whose identity is determined or determinable". As such, there is a discrepancy between various possible definitions of the same term that constitutes the object of the crimes under arts. 135-136 and 138 TPC. The term can only be interpreted through the incorporation of other legal texts, and would still be vague. As a result, there exists a heavy criticism in the Turkish legal literature about the conformity of this crime with the principle of legality[4]. The legal opinion holds that a consequence of this problem is that the said articles are almost never applied in practice[5].

As an additional point regarding the principle of legality, the crime of "violation of the confidentiality of communications" has also been criticized for being extremely vague in its definition. According to this criticism, the terms "communications" and "confidentiality of communications" bear an extremely broad and vague sense, resulting in a breach of the principle[6].

In addition to crimes regulated under the TPC, another regulation causing problems regarding the principle of legality is the measure of "blocking access" under the Law on the Regulation of Internet Broadcasting and on Combatting Crimes Committed Through Internet Broadcasting (Internet Law). It should be mentioned that this problem does not arise from the definition of a criminal offence, but is rather the result of the application of a measure. As such, the principle in question is "nulla poena sine lege". 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[7]. 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 service provider of the content 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

---

[2] ZAFER, Hamide, Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması, Istanbul, 2010, s. 55, ŞEN, Ersan, "5237 sayılı Türk Ceza Kanunu'nda Özel Hayata Karşı Suçlar", İstanbul Barosu Dergisi, Vol: 79, Issue: 2005/3, p. 716.
[3] AKYÜREK, Güçlü, Özel Hayatın Gizliliğini İhlal Suçu, Seçkin, Ankara 2011, p. 189.
[4] ŞEN, p. 718; AKYÜREK, p. 202.
[5] AKYÜREK, p. 202.
[6] ŞEN, p. 712.
[7] 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.

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.

The problem regarding the principle of legality is that the measure ordered by an administrative authority involves an assessment on the level of suspicion regarding the commission of a criminal offence. In addition, such measures mostly involve people not related to Turkey, who, according to Turkish legal practice, would be the sole persons eligible to file a motion to annul the measure. Since these people rarely resort to such legal actions, and since users are not accepted as an eligible party to challenge the decision of the Presidency, the result is an indefinite ban, or blockage of access, to certain websites. The measure does not have any time limit, and is not necessarily followed by a criminal prosecution. This is particularly the case, if the identity of the suspect cannot be determined. Therefore, it can be argued that the measure of blocking access, when applied by the Presidency, no longer fulfils the characteristics of a criminal procedural measure, and lacks the element of provisionality[8]. It rather aims, like a security measure, at the prevention of a dangerous activity. However, security measures are also bound by the principle of legality, and can only be ordered by the court, upon a valid criminal sentence. Thus, the administrative measure provided by the Turkish Internet Law does cause problems regarding the principle of legality.

(2) How does legislation avoid undue chilling effects on legitimate use of ICT or of the Internet?

Until now, the Turkish legislator avoided criminalising dual-use software and other conduct that can follow legitimate as well as illegitimate purposes online. However, it would be necessary to mention the undue chilling effects created by the measures provided by the Turkish Internet Law, and particularly their application in practice.

In practice, courts and the Presidency ordering the blocking of an alleged illegal content under art. 8 of the Turkish Internet Law choose to block the access to the entire domain or server, instead of focusing on the specific file. "This (…) resulted not only in blocking the alleged illegal content, but also millions of web pages carrying perfectly legal content through those blocked domains"[9]. A prominent example of such practice has been the blocking of Youtube, as a consequence of content allegedly defaming Atatürk. The ban continued for two years, and prevented users from accessing the whole website[10]. As a result, legitimate use of these domains is being suppressed with insufficient access to legal remedies.

A memorandum[11] (dated 1 March 2010) published by the Board of IT Technologies and Communications, Presidency of Telecommunications mentions that websites with illegal content are being warned through notifications before ordering a blocking of the said site. According to this memorandum, this "warn and remove" system resulted in the removal of 3521 different contents. It should be mentioned that this system has neither been mentioned in the Internet Law, nor in the Regulation that has entered into force as its by-law[12].

---

[8] AKDENİZ, Yaman; Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship, p. 32, http://www.osce.org/fom/41091 (access date: 31.08.2012)

[9] AKDENİZ, Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship, p. 28, http://www.osce.org/fom/41091 (access date: 31.08.2012)

[10] http://haber.mynet.com/youtubea-erisim-engellendi-275750-guncel/ (access date: 18.08.2012)

[11] http://www.guvenliweb.org.tr/istatistikler/files/pdf/ihbar_istatistikleri_01.03.2010.pdf (access date: 20.08.2012)

[12] By-Law on the Regulation of Internet Broadcasting, 30.11.2007 tarihli ve 26716 sayılı Resmi Gazete.

It should also be mentioned that no statistical data regarding the total number of blocked websites is available since 2009. The memorandum mentioned above included the latest statistical data available. Since May 2009, the Presidency is refraining from sharing this information, even following legal claims under the Public Information Law. There is an ongoing administrative legal action about the matter[13].

(3) How does criminal legislation avoid becoming obsolete in light of rapid technological innovation? E.g.,

- how are changes in the use of internet and social networks taken into account?

- how is the law adapted to technological progress (e.g., by reference to administrative regulations)?

Criminal legislation regarding ICT entered the Turkish criminal legal system in 1991, through the addition of arts. 525a-525d to the (now abrogated) Criminal Code Nr. 765. The definition included some technology-specific wording, and vague terms regarding the object of the crimes. (such as "systems automatically processing data"), which were out-dated and soon caused gaps in criminalisation. With the entry into force of the 2005 Turkish Criminal Code Nr. 5237, these definitions have been changed significantly. However, it must be noted that the amount of criminalised activities is not very high, and still does not include all types of infractions that evolve through technological innovation.

The lack of specific criminal offenses not only results in gaps of criminalisation, but also in overlapping criminal offenses, or overcriminalisation. As an example, the lack of a "skimming" type of offense results in the sentencing of the perpetrator because of various independent offenses (theft, falsification, credit card fraud and, in some cases, obstruction of an IT system).

Crime definitions regarding IT criminality do not involve any references to administrative regulations. Although laws and by-laws related to ICT do give some authority to the Board and the Presidency, these powers are limited to surveillance, monitoring, regulation and administration of measures or fines related to these activities. However, it must be noted that such administrative measures include the blocking of websites, which results in a quasi-criminal mechanism, as mentioned above.

As a result, it can be said that the Turkish legislator does not take any particular precautions for crimes becoming obsolete through technical innovations.

(D) Extent of criminalisation

(1) To what extent do criminal laws cover mere preparatory acts that carry a risk of furthering abuse, e.g., acquisition or possession of software that can be used for "hacking", "phishing", computer fraud, or bypassing download protection? If so, has there been controversy about introducing such laws? Have legislatures made specific efforts to avoid over-criminalization?

Preparatory acts regarding IT criminality are rarely included in the crime definitions. However, there are two instances where acquisition of possession of material that can be used in crimes involving IT systems has been criminalised.

---

[13] AKDENİZ, Yaman, "TİB'e Erişim Engelleme İstatistiklerini Gizlemekten Dava", 13 Mayıs 2010, Bianet (http://bianet.org/bianet/ifade-ozgurlugu/121956-tibe-erisim-engelleme-istatistiklerini-gizlemekten-dava) (*access date: 26.08.2010)*

According to art. 72 IPL, it is a crime punishable by a prison sentence from six months to two years "to produce, offer, sell or ***possess for purposes other than self-use*** programs or technical hardware that have the aim of neutralizing additional programs built to prevent a computer program from being illegally copied".

Additionally, art. 245/2 TPC provides for a crime of "forgery, selling, giving, buying or receiving of false debit or credit cards connected with bank accounts belonging to other people", punishable with a prison sentence of three to seven years.

Although art. 243 TPC regarding "illegally entering, and staying in an IT system" constitutes a crime of abstract endangerment, it can't be said to criminalise mere preparatory acts, since entering illegally would constitute a part of the criminal conduct for the crime of "hacking", art. 244 TPC. Nevertheless, the crime defined under art. 243 TPC has been criticised in the legal doctrine for being too vague and for not including any criteria for a conduct to become harmful to the victim.

There is no widespread legal debate about the inclusion of preparatory acts in crime definitions. However, there are several "warning" accounts about the general trend to include an increasing number of preparatory acts in other legal systems, and it is deemed as an example of "risk criminal law"[14].

(2) To what extent has the mere possession of certain data been criminalised? In what areas, and on what grounds? How is "possession" of data defined? Does the definition include temporary possession or mere viewing?

The crime of "obscenity" or pornography defined under art. 226 TPC has been modelled after the German Criminal Code, and includes two types of conduct where the mere possession of pornographic (in the wording of the definition: "obscene") material is a punishable act. Such instances include the possession of pornographic material involving children (punishable with a prison sentence from two to five years) and "hard pornography" defined as pornography involving violence, animals, dead human bodies or "unnatural" sexual behaviour (punishable with a prison sentence of one to four years). Naturally, the term "unnatural sexual behaviour" is extremely vague, and can be interpreted as to include homosexuality, BDSM or fetishism. Such an interpretation would result in the punishing of otherwise legal activities, would violate the prohibition of discrimination, and ultimately, the human rights of the involved.

Another example for a crime of possession of data is provided by the IPL, art. 71. According to this crime definition, it is an act punishable with a prison sentence of one to five years to "possess for purposes other than self-use, or to store" copyright-protected material.

Additionally, the crimes of "illegally obtaining personal data" (art. 136 TPC) and "failing to destroy personal data" (art. 138 TPC) may be mentioned as examples indirectly criminalising the act of possessing certain types of data.

[14] See, i.e. ERMAN, Baris, "Ceza Hukukunun Dönüsümü", Prof. Dr. Duygun Yarsuvat'a Armagan, in print.

(3) To the extent that possession of or granting access to certain data have been defined as criminal, does criminal liability extend to service providers (e.g., hosting or access providers)? What are the requirements of their liability, especially concerning mens rea?

Are providers obliged to monitor and control what information they provide or offer access to? Are providers obliged to provide information on the identity of users? Are providers obliged to prevent access to certain information? If so, under what conditions, and at whose cost? Is there criminal liability for violating such obligations?

According to art. 4 of the Internet Law, the author, or content provider, is primarily responsible by his or her own content. However, links to other websites provided by the content provider may result in his or her criminal liability, under the condition that the presentation of the linked content makes it obvious that the content provider accepts the linked content as his or her own, and intents that users access the linked content.

According to art. 6 of the Internet Law, access providers are not obligated to check whether contents users access through their systems are illegal or not. However, they are obligated to comply with the restraining orders issued by the Presidency of Telecommunications, and have to block access to banned sites insomuch as their technical configuration allows this. Non-compliance with this obligation does not result in any form of criminal liability.

According to art. 8/b of the By-Law on the Regulation of Internet Broadcasting, the access provider is obligated to store traffic data related to its services for the duration of one year, and provide for their authenticity, integrity and confidentiality. In case of non-compliance with this obligation, the access provider is subject to an administrative fine.

An additional obligation of the access provider is to give the telephone numbers used to provide access to the Internet and data related to its users to the Presidency of Telecommunications. Again, this obligation is not bound with any sort of administrative or criminal liability.

The hosting provider is not obligated to check the content about its illegality, according to art. 5 of the Internet Law. It is, however, obligated to remove illegal if it has been notified about its existence. The notification occurs following the rules of arts. 8 and 9 of the Internet Law. The former concerns notifications of a court or the Presidency, while the latter is related to real or legal persons whose legal interests have been affected by the content in question. According to art. 9 of the Internet Law, any person claiming to be affected by an illegal content may notify the content provider or the hosting provider, requesting its removal and replacement with a reply sent by the notifying person. Failing to comply with this "right to reply and removal", however, does not result directly in the criminal liability of the hosting provider, except when it can be proven that the hosting provider has acted as an accomplice to the crime, and shared the criminal intent.

(4) What general, in particular constitutional limits to criminalising conduct have been discussed with respect to ICT and internet crime (e.g., freedom of speech, freedom of the press, freedom of association, privacy, "harm principle", requirement of an act, mens rea requirements)?

The main point of concern regarding Internet crimes in Turkey is the freedom of speech and Internet censorship. This concern is mainly related to the regulations and application of the measure on blocking websites. According to the OSCE report: "The use of the blocking orders to silence speech amounts to censorship and a violation of Article 10 of

ECHR"[15]. This practice results in a "prior restraint", which may result in censorship, particularly in cases regarding Internet press[16].

Internet censorship has again been a major point of discussion with the entry into force of the "Rules and Procedures on the Safe Use of the Internet", issued by the Presidency of Telecommunications, on 22 August 2011. These rules included an obligation for Internet access providers to introduce filtering options for families, children and schools. These filters have to comply with "black and white lists" created by the Presidency. Users who choose the "child protection" option would only be able to access sites on the white list, while the filter for "family protection" would automatically ban the sites on the "black list". For users not choosing any filtering option, any site not banned by the Presidency or by court order would be accessible, as before. Although these lists are optional, it is a cause concern about the freedom of expression that lists are prepared by a central governmental authority. In addition, schools are obligated to choose the "family protection" type of filtering, and are not free to choose between various type of protection.

Another point of concern is the "harm principle", according to which only conduct causing harm or immanent danger may be subject to criminal liability. As explained above, most of the crimes provided under the TPC require a specific harm or at least a concrete danger to occur as a result of the conduct. However, art. 243 TPC regarding "entering, and staying in an IT system does not follow this model, and criminalizes any action without any condition regarding the possibility of harm, or intent towards causing harm. As such, it is a crime of abstract endangerment, and is not subject to any constraint regarding the mens rea.

Other concerns regarding the principle of culpability especially arise because of the practical implementation of the regulations by courts. Due to technical difficulties in investigating IT related crimes, and due to the adaptation issues of the prosecutors and courts, sometimes the standards of strict culpability are not met. As a result, people can be sued or held responsible just for owning the telephone line linked to the IP number that has been used to Another point of concern is the "harm principle", according to which only conduct causing harm or immanent danger may be subject to criminal liability. As explained above, most of the crimes provided under the TPC require a specific harm or at least a concrete danger to occur as a result of the conduct. However, art. 243 TPC regarding "entering, and staying in an IT system does not follow this model, and criminalizes any action without any condition regarding the possibility of harm, or intent towards causing harm. As such, it is a crime of abstract endangerment, and is not subject to any constraint regarding the mens rea.

Other concerns regarding the principle of culpability especially arise because of the practical implementation of the regulations by courts. Due to technical difficulties in investigating IT related crimes, and due to the adaptation issues of the prosecutors and courts, sometimes the standards of strict culpability are not met. As a result, people can be sued or held responsible just for owning the telephone line linked to the IP number that has been used to

A similar problem arises regarding web 2.0 applications, where the traditional concepts of "content provider" and "hosting provider" are not easily distinguishable. There are no specific regulations concerning the actors of such

[15] AKDENİZ, Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship, p. 30, http://www.osce.org/fom/41091 (access date: 31.08.2012)
[16] Ibid, p. 31.

platforms and their duties to prevent criminal activity within their area of responsibility. This creates a "grey area", where the criminal liability of such actors is not easily determinable.

(5) Does the law provide for criminal sanctions specifically targeting cyber criminals, (e.g., a temporary ban from using the internet)?

There are no specific criminal measures or sanctions targeting cyber criminals. However, a general rule (art. 50/1/d TPC) allows the court to sentence criminals to alternatives for criminal punishment instead of a prison sentence of up to one year. These sanctions are not mentioned according to a *numerus clausus* principle. As a result, it is possible for a court to introduce a temporary ban for a particular offender from using the Internet, if it regards this sanction to be beneficial for special preventive purposes.

(E) Alternatives to Criminalisation

(1) What role does criminal law play in relation to other ways of combatting abuse of ICT and the Internet? What is the relationship of civil and administrative sanctions (payment of damages, closing of enterprise, etc.) to criminal sanctions in the area of ICT?

Criminal law always plays a leading role in the struggle against the abuse of ICT and the Internet. Turkish legislator always considers the criminal law measures as the best effective legal tools; thus there is a constant tendency on using the criminal law tools to solve the legal problems of ICT and the Internet. Therefore, civil and administrative measures have a secondary role in the field of ICT and the Internet.

In some cases, civil and administrative measures have regulated in a combined manner with criminal measures. For instance, although Law Nr. 5651 mainly regulates the liability of providers and procedures of fighting with Internet crimes; Article 9 of Law Nr. 5651 specifically deals with private matters and regulates 'content removal' and 'right to reply' as non-criminal measures.

According to Article 9, people who claim that their rights are infringed by content on a website may contact to the content provider –or the hosting provider if the content provider cannot be contacted – and request the removal of the infringing content.

The complainants have also a right to reply in Article 9(1) and may request the content or hosting provider to publish their reply on the same web page, the infringing content was published for 1 week.

If the content or hosting providers are failed to comply with a 'removal request' within 48 hours of receipt of request, the complainant can take his case to a local Criminal Court of Peace within 15 days and request the court to issue a removal order and enforce his right to reply as provided under Article 9(1).

(2) What non-criminal means of combatting offensive websites are used/propagated (e.g., closing down websites, blocking access to websites)?

Although criminal law measures are the most preferable tools to struggle with ICT problems, they are not eligible to use in all problems. Offensive websites and particularly illegal and harmful content carried out in those web sites is a major problem that requires the aid of non-criminal means. In Turkish law, the struggle against these sort of offensive websites is legislated in Law Nr. 5651- "The Law on the Regulation of the Broadcasting on the Internet and Fighting Against Crimes Committed Through Internet Broadcasting".

In Law Nr. 5651, "blocking Access to websites" is designed both as a criminal procedure measure and also as an administrative measure. However, in 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.

(3) To what extent are ICT users expected to protect themselves (e.g., by encryption of messages, using passwords, using protective software)? Are there sanctions for not protecting one's computer to a reasonable extent, e.g., by using anti-virus software or protecting access to private networks by password? Does the lack of reasonable self-protection provide a defence for defendants accused of illegally entering or abusing another person's network or abusing their data?

In Turkish legal system, governmental bodies (such as Telecommunications Communication Presidency-*afterwards Presidency*) play a proactive role for the protection of children, young people and families against the illegal and harmful content on the net. The main purpose of the Presidency is to centralize, from a single unit, the surveillance of communications and execution of interception of communications warrants subject to different laws in Turkish legal system. Under Law Nr. 5651, the Presidency was chosen as the organisation responsible for monitoring Internet content and executing blocking orders issued by judges, courts and public prosecutors.

Therefore, the burden of the protection of ICT users usually taken over by the Presidency and ICT users are not much expected to protect themselves by using encryption, passwords or any kind of protective software.

However, a self-protection choice is also provided to ICT users. In February 2011 Turkish government implemented an internet filtering system for citizens which supposed to be enforced in August 2011. Although the 'original' filtering system was compulsory with 4 different profiles when it was first announced; the government had to revise it after the increasing 'censorship' claims of ICT industry and different NGO'S. In November 2011 the new 'revised' internet filtering system which is a voluntary model with 2 different profiles implemented. In this model, ICT users have a right to choose one of the 'family' or 'child' profiles which are meant to protect minors from illegal and harmful content on the Net.

Article 7 of Law Nr. 5651 regulates the mass use providers, including internet cafes which needs to fulfil specific requirements in terms of the protection of their computers to a certain extent. Mass use providers are required under Article 7(2) of Law Nr. 5651, to deploy and use filtering tools approved by the Telecommunications Communication Presidency to block access to illegal Internet content. Mass use providers who operate without an official permission would face administrative fines between 3,000 TL and 15,000 TL.

The illegally entering or abusing another person's network or abusing their data is designed as an offence in Article 243 of Turkish Penal Code and the lack of reasonable self-protection does not provide any kind of defence for the perpetrators.

(F) Limiting anonymity

(1) Are there laws or regulations obliging internet service providers to store users' personal data, including history of internet use? Can providers be obliged to provide such data to law enforcement agencies?

Internet service *(hosting)* providers are regulated at Article 5 of Law Nr. 5651. This provision is introduced a notice-based liability system which is in line with Article 15 of the EU E-Commerce Directive. According to this provision,

there is no general obligation to monitor the information which the hosting companies store, nor do they have a general obligation to actively seek facts or circumstances indicating illegal activity.

However, through Article 5(2), the hosting companies are obliged to take down illegal or infringing content once served with a notice through the Presidency or subject to a court order according to the Article 8 of Law Nr. 5651.

Access providers are also regulated at Article 6 of Law Nr. 5651 and it introduces similar obligations and requirements for Access providers with hosting companies.

Apart from the regulation in Law Nr. 5651, the government published a specific regulation in October 2007 named as "*Regulations Governing the Access and Hosting Providers"* which includes the principals and procedures for granting activity certificates for such providers.

According to the Article 15 and 16, only the traffic data has to be stored by Access providers (for 1 year) and hosting providers (for 6 months). However, there is no regulation which obliges those providers to store users' personal data or to provide such data to law enforcement agencies.

(2) Are there laws or regulations obliging an internet service provider to register users prior to providing services?

As mentioned above, "*Regulations Governing the Access and Hosting Providers"* introduces an obligation on the service (both hosting and Access) providers to store "traffic data" for a certain period. Apart from this obligation, service providers are not obliged to register users prior to providing services.

(3) Are there laws or regulations limiting the encryption of files and messages on the internet? Can suspects be forced to disclose passwords they use?

There are no laws or regulations in Turkish legal system limiting the encryption of files or messages on the Internet.

(G) Internationalisation

(1) Does domestic law apply to data entered into the internet abroad? Is there a requirement of "double criminality" with respect to entering data from abroad?

There are no specific laws on the application of Turkish law to data entered in abroad. Therefore, general rules of Turkish criminal law have to be applied in such cases as well. A brief summary of the rules concerning the application of Turkish law on the offences committed in abroad is in below:

In principal, Turkish laws are applied for the offences that are committed in Turkey (Article 8 of Turkish Penal Code-TPC). In this context, it is necessary to mention that the Turkish penal code defines the concept of territoriality in an extremely broad sense. According to Article 8, any crime shall be considered as committed in Turkey if the conduct has been in part or in full perpetrated on Turkish territory or if the result has occurred in Turkey. Thus, any act of entering data into the Net in abroad shall be deemed to have been committed in Turkey.

However, there also are certain exceptions which Turkish laws can be applied for the offences committed in abroad.

The first exception is the commitment of an offence in abroad by a Turkish citizen, regulated in Article 11 of TPC. If a Turkish citizen, excluding the offences listed in Article 13, commits an offence in a foreign country which requires punishment with a minimum limit of less than one year imprisonment according to the Turkish laws, and if the offender is found in Turkey, then he is punished according to the Turkish laws provided that he is not convicted in the said foreign country for the same offense and there is possibility to proceed a trial in Turkey. Where the offence

requires a prison sentence with a minimum limit of less than one year, the trial is filed only upon rise of complaint by the injured party or the foreign country. In such case, the complaint has to be brought within six months as of the date of entry of the citizen into Turkey.

The second exception is the commitment of an offence in abroad by a foreigner, regulated in Article 12 of TPC:

(1) If a foreigner, excluding the offences listed in Article 13, commits an offence in a foreign country causing injury to Turkey, which requires a punishment with a minimum limit of less than one year imprisonment, and if the offender is found in Turkey, then he is punished according to the Turkish laws. However, the trial is filed upon request of the Ministry of Justice.(2) If the offence mentioned in the afore subsection is committed with the intension of causing injury to a Turkish citizen or a legal entity incorporated according to the Turkish laws and subject to special law, and if the offender is found in Turkey, then the perpetrator is punished according to the Turkish Laws upon complained of the injured party provided that that he is not convicted in the said foreign country for the same offense.(3) If the aggrieved party is a foreigner, he is tried upon request of the Ministry of Justice in case of existence of the following conditions; a) Where the offence requires punishment with a minimum limit of less than three years imprisonment according to the Turkish Laws; b) Where there is no extradition agreement or the demand of extradition is rejected by the nation where the crime is committed or the person accused of a crime holds citizenship.(4) A foreigner who is convicted of an offence in a foreign country within the scope of first subsection, or the action filed against him is extinguished or the punishment is abated, or the offence committed is not qualified for the prosecution, then a new trial can be filed in Turkey upon request of the Ministry of Justice.

Turkish laws can also be applied in case of commitment of certain "catalogue offences" designed in Article 13 of TPC by the citizens or foreigners in a foreign country. However, cyber crimes are not listed in these catalogue offences.

Lastly, Turkish Penal Code does not recognize the requirement of "double criminality" for offences committed in Turkey (under the principle of territoriality), offences that have been committed against the security of state or against Turkish citizens and legal entities.

(2) To what extent has your country's criminal law in the area of ICT and Internet been influenced by international legal instruments?

Since technology is always one step ahead of the law, the area of ICT and Internet constitute a hard task for national legislators. Therefore, international legal instruments (and legislations in comparative law) are the first sources that are taken into consideration while preparing laws or regulations on ICT and internet.

The first criminal law legislation in the area of ICT was "The Offences Committed Via Computers"-(Article 525a-d of former Turkish Penal Code) enacted in 1991. This former and current (Article 243-246 of Turkish Penal Code) "computer crimes" laws of turkey are highly influenced by the Directives of EU.

In the same context, "The Law on the Regulation of the Broadcasting on the Internet and Fighting Against Crimes Committed Through Internet Broadcasting" (Law Nr. 5651) is also influenced by international legal instruments. Some specific provisions (e.g. the liability of internet providers-Article 4-7) are taken from EU Electronic Commerce Directive and consistent with the EU legislation.

Nevertheless, it is important to stress that Turkey has not signed the European Convention on Cybercrime yet. Therefore there still are some gaps that need to be filled by the signing and ratification of the Convention. However,

some specific provisions of Convention, as in "content related offences-*Child Pornography*" has taken into account in the preparation process of the sexual offences in Turkish Penal Code 2005.

(3) Does your country participate in discussions about the harmonisation of cybercrime legislation (such as the U.N. intergovernmental expert group on cybercrime)?

Despite the fact that the Turkish government is always willing to participate in almost all international legislative activities including the discussions about the harmonisation of cybercrime legislation; the Government is not that willing to announce its work to public by delivering regular reports or by another means.

Therefore, we are not fully informed about the recent contribution of Turkish government on the discussions about the harmonisation of cybercrime legislation. However, several NGO's working in the field of ICT and the Internet are following the recent improvements on international and comparative cybercrime legislation.

(H) Future developments

Please indicate current trends of legislation and legal debate in your country concerning ICT and internet crime.

The current trend of ICT legislation in Turkey is essentially focused on the improvement of electronic commerce. Therefore there are several law drafts concerning the regulation of e-commerce activities in order to meet the requirements of contemporary era.

The first draft is "The Law on the Regulation of Electronic Commerce" which has been prepared to accomplish full harmonisation with the EU E-Commerce Directive. The Draft particularly concerns restrictions regarding spam mail and the protection of personal data in e-commerce activities. Such violations regarding these activities shall be subjected to criminal responsibility.

Another draft is "The Law on The Protection of Personal Data" which has been prepared to provide adequate standards for the protection of personal data for all users.