Tools and Experience of Turkey in Coping IT Crimes

Mehmet Ali Gürol[†]

ABSTRACT

By no means rapid advances in technology affects the working and improvement of all systems built to increase the quality/standards of human living. Information technologies as the main driving force of technological progress today happen to be a sine qua non for all organizations hoping to keep pace with or surpass rivals. However, despite their vital advantages it is true that these create undesirable side effects that harm social systems and the rights of persons. Similar to all others in the world Turkey is trying to cope with the problem through creating an appropriate legal and administrative substructure trusted to discontinue or at least minimize such criminal acts.

Key words : IT Crime, Legislation, Crime Administration, Cyber Security

1. INTRODUCTION

In an age of transition from an industrial society to an information other, two basic targets of advanced industrial nations and newly industrialising nations hasting to evolve towards an information society are firstly to sustain their capabilities in information technology and secondly to built/create their national high speed information networks and telematic service systems[2]. This is quite understandable for today the implementation and betterment of such efforts is fully important for [the sustain ability of] businesses all over the world. One significant reason in such effort is the progress in IT leading the way to e-commerce where companies strive for higher shares from the growing "electronic market" in a highly competitive international media, also happening to be a perfect tool to introduce one's goods and services to the whole world through the Web[9].

In public management the approach to IT is not different than that of the private businesses. As mentioned in one recent OECD Report "The conventional wisdom is that government, by virtue of the fact that it is an information-intensive enterprise, is significantly impacted by computer and communications technology, referred to more generically…as information technology or IT." This is followed that governments of many OECD countries are the "early users" of IT "employing it for a range of applications including compiling statistics and supporting large transaction processing functions" (OECD, 1998). In regard to such technologies and their application said nations should be at a much further stage by now for

[†] Professor, Karamanoglu Mehmetbey University
Received : 2009-01-24, Accepted : 2009-03-10

the report is issued ten years before present time. Concerning with the present grade of Turkey in the global arena in readiness to information society According to the Global Technology Report 2007-2008 she ranks in 55 among 127 countries[12].

In common IT crimes are committed through PCs, in Internet space, credit cards, electronic devices and cellular phones. Whatever the method employed basic differences between types of such crimes depends on the purpose in committing the crime. As an example there are various ways in entering a PC system e.g. with the use of a virus or Trojan or forcing of open gates. The crucial point here is the act to enter the system. Methods used could only be the aggravating factors of the crime[1]. "Interpol has actively been involved for a number of years in combating Information Technology Crime... [by] harness[ing] the expertise of its members in the field of Information Technology Crime (ITC) through the vehicle of a 'working party' or a group of experts."[4]

Turkish legal system commonly used to have the necessary legal arrangements so the tools to prevent effects of IT crimes. However, pace in technology so such crimes necessitated the need for a particular law arranging such crimes. Accordingly, a recent law to "regulate Internet content and listing crimes to be committed on the Web" is passed by the Turkish Parliament last year (2007). Yet the adoption of the law is still not a full panacea by all means in coping with such crimes. The problem here is originating from the setbacks in application stemming from inefficiencies in the administrative mechanism to be discussed in following paragraphs.

2. LEGISLATION IN PREVENTING AND COPING WITH INFORMATION TECHNOLOGY CRIMES IN TURKEY

Fast progress and evolution [throughout the world] is highly connected with the increases in IT crimes. The expeditious evolution of these types of crimes and the heavy working of the legal system is contrary with one another where the latter is too slow to catch the former[6]. In global basis, two different methods are employed in regard to legal arrangements in IT crimes. In one, examples being USA, England, Ireland and Portugal, while there are concerning articles in current laws, in separate, there is a specific other created merely for such purpose. In contrary, within the other leaded by the German legislative system, IT acts of criminal nature are arranged through existing laws where no unique sections and laws exist for this purpose. This system tries to cope with such crimes by altering crime definitions in a way to cover [showing up] IT crimes rather than adding such acts [of a criminal nature] to existing laws.

Most common IT crimes Turkey faces today are the

· deterioration of (especially) commercial and private relations through sending e-mail in name of others,

· preparing Web pages in the name of others and sending e-mail and messages to other persons targeting the presentation of the Webpage while giving the phone number of the legally injured person in these messages,

· Theft through unauthorized access to personal or institutional computers and provision of concrete benefits by threatening with these stolen material,

· Provision of company Webpage domain names without permission and demanding large sums of money against those,

· Copying and selling of (especially) CDs with pornographic content,

Printing false documents[10].

Here it should be added that the act of "unauthorized access and listening in computer systems and services" also constitutes a constitutional crime for being contrary to the "privacy of personal life" article of the Turkish constitution.

Both in Turkish abrogated and present penal codes (Acts No. 765 and No.5237 respectively) legal regulations relating to IT are reserved under a separate section in penal code resembling to that of the France. The first arrangement relating to IT crimes in Turkish legal system is created in 1991 with an alteration in [abrogated] penal code no. 765 through the addition of a new chapter with heading "Crimes in IT Field." This is followed with changes in Ideas and Arts Act with the addition of the article "computer programmes expressed in any form other than their preliminary designs that could possibly take a programme form at a further stage" consequently accepting these as a "product" considering any illegal act against such products also a crime similar to others expressed in verbal or written form.

In current Turkish penal code (Act No. 5237) similarly there is a separate chapter on IT crimes arranging matters relating to "information system entrance (Article 243)", "hindrance, disruption, elimination or alteration of data (Article 244)", "abuse of bank or credit cards (Article 245)" and "application of security measures with legal persons (Article 246)." Apart from these articles than there are the Articles 142 and 158 relating to "qualified theft" and "qualified fraud" respectively, indicating "theft by use of IT systems" and "fraud by use of IT systems, banks or credit institutions" as aggravating reasons for such criminal acts.

Likewise, in Consumer Protection Act No. 4077 (date of issue February, 1995) with the alteration in 2003, the term "product" is defined in a way to include "intangible products prepared to be used in electronic media such as software, sound, vision, and alike." Said act also permits the implementation of distance agreements with the use of telephone, visual and alike devices in electronic media. It similarly allows the accomplishment of confirmation procedures of "electronic media agreements" within the new electronic media. Besides "use of signature formation data without consent", and "fraud in electronic certificates" also counted to be a crimal act as a requirement of the Consumer Protection Act.

The cooperation between content and communication providers supplying service in the Internet media has an significant role in fighting against IT crimes and increasing the quality of IT services. Targeting to close the gaps in IT field and establishing responsibility principles in parallel with the comparative law beyond balancing given targets through the distinction of the functions of IT service suppliers (similar to those legal arrangements in Germany (Tele-Services Act) and France (Digital Economy Security Act)) the act "Regulation of Internet Publications and Combating Crimes Committed through such Publication" (Act No. 5651) is adopted by the Turkish Parliament on May 2007. (YASAD, n.a.)

While the first half of the law covers criminal law matters, its second half regulates civil law aspects[7]. The law consists of seven sections where the first is on "purpose, contents and definitions" and the second relates to "responsibilities, obligations and control." For their keystone quality articles in the latter (section two) are given below in separate with some detail:

a. Freedom in reaching data and expression (Article No. 3): Principally persons have the right to reach data and to express [their ideas]. Such freedom can only be limited under conditions articulated in existing laws.

b. Lack of constraint principle (Article No. 4): There are no restrictions in activities relating to information network services. Starting, carrying out and ending of these activities are not subject to any permission or condition. However, [concerning] provisions in other laws are binding.

c. Obligation in information in general (Article No. 5): Location and access providers need to present the information relating to their name and surname, electronic communication address, controlling authority in case subject to any permission or control over their information network in their own contents.

d. Obligation in information in private (Article No. 6): Content provider, in case such content is related with the purchase of a good or service, is obliged to make available certain information relating to their name and surname, electronic communication and regular address, identity, and other contacting details of the representative in case the provider is settled in another country, price of the goods and services, whether tax and all other expenses are included in the price, validity period of the offer and price, etc.

e. Responsibilities of content providers (Article No. 7): The content provider is responsible from any content put to information network for use, while not being liable for content of the other that it [merely] supplies the connection.

Obligations of location providers (Article No. 8): Location provider has no obligation in controlling the content the location is provided, and inspecting any illegal activity.

The section also includes articles on "obligations of access and media providers" (Articles Nos. 9 & 10), "protection of data" (Article No. 11), "rules relating to shared users" (Article No. 12), "correction of content and hindrance of access" (Article No. 13) and "control" (Article No. 14). Third section titled "crimes regarding to secrecy, integration and provision of data" is followed by other sections as "crimes connected with the information system" (Section 4), "crimes connecting to content and administrative sanctions" (Section 5), "investigation and prosecution procedures" (Section 6), and "various and final articles" (Section 7).

However recent, and structured and equipped to meet any requirements in IT the law is critisized for various reasons. Primarily the critics are based on the fact that a constitutional freedom such as the "communication freedom" is now in the guidance of an administrative unit. This evokes the idea that the law is against the constitution[5]. It similarly calls for the discussion that whether access to pages open to world could be subject to limited access leading to censorship in Internet court order on the limitation of YouTube being a remarkable example in this case. It is said that the law has shortfalls for being prepared within a narrow span of time that makes it not satisfactory for all parties. Critics mention that there are articles in the law open to interpretation where these need to be rearranged through the contribution of specialists on information law, information media, civil society organizations (CSOs), and Internet users as a whole. Such debate today also calls in questions/matters like the freedom of people in the Internet, people's ideas on interactive communication and technology, parallelity of this law with others, whether it is possible to control future media with an out-of-date logic. (Sansüre Sansür. org, 2007)

3. ADMINISTRATIVE FACTORS THAT IMPEDE THE FUNCTIONING OF IT SYSTEM

While IT crimes growing in number as a result of the extensive use of computers is a problem itself, ways of investigation and methods in obtaining evidence practised by investigation authoritites additionally constitutes an important issue to be dealed with. Such hinderances originate from hefty difficulties in investing crimes beyond problems in suppliance of evidence deriving from the quality of information devices and the structure of information networks. A vast number of electronic recordings held in these devices do not merely keep evidence crucial in IT crime investigations, but also for crimes not related to IT[13].

Despite the well set so the sufficiency of the legal substructure/ content in fighting against IT crimes, deficiency and shortages in administrative system leading to poor appliance and functionability happens to be a major hampering factor restraining necessary action to be taken. This seems to be resulting from the lack of resources required to be allocated for such purpose rather than the poorness in organization and the competence and devotion of people doing the work where the insufficiencies in the former case seriously affect the effectiveness of the latter. Poor functioning of the administrative system originates from inefficiencies indicated below:

- Insuffiency in number of security forces: Number of police force to do the legal investigation following the [IT] crime is never enough. The problem basicly originates from wrongly use of human resources. Yet fortunately for the last few years members of police force educated in computer engineering/IT are set to right posts meaning that a police officer competent in IT crimes is now situating in IT crime units not another such as traffic or homicide[6].
- Judges and prosecutors: While it is true that laws cannot keep pace with IT crimes, any judge or prosecutor good in perceiving the case can be hasty in adapting any case to existing laws to foster the position of law before IT crimes. However in Turkey

such group are having difficulties in dealing with IT crime cases for their high age averages (especially in big cities) beyond their heavy work necessitating to deal with various types of cases leaving no free time to focus on recent technologies. Training programs can be arranged for such purpose where at present there are efforts to achieve that[6].

· Short of legal experts: Such shortage is both in qualitative and quantitative means. In Turkish legal practice the legal expert system has a vast application where in common referral to opinions of these group of people is the key to the solution. While the way followed in an ultimately technical field such as IT crimes is similar judges are having trouble in determining "what needs to be claimed from whom" in any case. While such gap is tried to be filled with academicians from technical universities and law faculties. However, an academician teaching computer engineering might not be good in reaching evidence for his/her lack of experience and knowledge in that reason being this kind of work evidently attaching to a distinct field of concern. The solution is the raising and employment of "judicial information experts" where the parliament needs to pass a law in judicial information for such purpose[6].

· Lack of necessary means and equipment: This results from the shortage of funds, omittance or poor support of R&D, and slow working of bureaucracy. Funding not available in right time consequently weakens fight against crime for advancing technology effecting results within that time lost [in the benefite of the criminal][6].

· Inadequate investment in knowledge and communication technologies: Turkey hoping and hasting to be a member of EU has to increase her investments in communication and knowledge technologies to get close to standards of Europe.

· Disparity in IT market size estimations: Estimations in regard to IT market sizes and their change in time are conducted by various organizations results in values that differ from one other for differences in the definitions of market in each[11].

Insufficiency of the IT substructure: Measures need to be taken for an efficient IT substructure permitting a qualified clustering and networking between organizations.

4. CONCLUSION AND COMMENTS

IT is a quantum leap parting present era from earlier promising ideal alterations effecting processes in production consequently the course of social life through reshaping working and living conditions (Gürol, 2007). Despite being the main source of all improvements in human living abuse/misuse of IT leads to crimes hasted to be prevented by government organizations concerning with the matter. Fighting IT crimes necessitates a well designed and well organized substructure that needs to be a balanced combination of legal and administrative arrangements. Combat against such crimes also requires international unity and mutual action to be effective for the problem is of global character rather than national. However as indicated by experience as the cooperation and coordination between the legal content and administrative bodies/application is not possible at all times/cases, identically same seems to be true for an effective worldly network/organizing/organization to do that.

While for the present Turkey managed to create the legal substructure/content in combating against IT crimes, to be effective she still needs a rather long way to go in face of the deficiencies in application originating from the inefficient functioning of the administrative body. In another words balancing of the legal content in IT crimes and functioning of the administrative system is not perfectly (at least satisfactorily) set yet. Consequently what is on paper do not always come to life and become effective because of the inadequacies in enforcement for reasons given above.

It is clear that Turkey both needs to actualize a reform in her administrative body and to evoke higher conscience in public opinion through education/training programs beyond the conveyance of vast information on the matter in order to be more effective and efficient in eliminating or at least minimizing such group of crimes. While in case of funds, material and other kind of tangible (solid) requirements this might not be an hefty problem, concerning with those of intangible others relating to human side of the matter there are serious setbacks. Convincing, reorganizing and directing of concerned key personnel in the administarive body and the general public on the issue is never easy for the resistance against change in human nature.

Yet, for the matter is ultimately young and not all clear at the moment in Turkey's present conditions, urgency in decisions and applications intending to reach a better functioning administrative system to cope with such crimes could lead to inefficiencies. While hardly possible in a rather short span of time (a year or less), such rehabilition effort could fruit in middle terms with sufficient backing and determination by the government authorities making two related parts (legal and administrative systems) to work together in a more cooperative and coordinative way for better results.

REFERENCES

[1] Cyber Security (n.a.) *Bilişim Suçlarının Kapsamı. (Content of IT Crimes).* http://www.cyber-security.org/datadetayall.asp?Data_id=356 Retrieved from the Internet on Sept 4, 2008. (In Turkish)

[2] Göker, A. (2000). *Enformasyon toplumu - bilgi toplumu (Information society - knowledge society).* http://www.inovasyon.org/html/bt/AYK.CBT6.htm Retrieved from the Internet on Sept 2, 2008. (In Turkish)

[3] Gürol, M.A. (2007). *Possible Role of Information Technology in the Future of Turkish Economy and Industry.* Visiting Speaker, International Conference on the Industrialization of Ubiquitous Technology and Balanced Development of the Nation. Hanyang University. Seoul, Korea. Oct 2, 2007.

[4] Interpol (2008). *Information Technology Crime.* http://www.interpol.int/public/TechnologyCrime/Default.asp Retrieved from the Internet on Sept 11, 2008.

[5] Nebil, F.S. (2008). *TİD; 5651 ile İlk Defa Anayasal Bir Özgürlük olan 'Haberleşme Özgürlüğü' Bir İdari Birimin Kararına Bırakılıyor-2. (TID; For the First Time a Constitutional Freedom such as the 'Communication Freedom' is Left to the Decision of an Administrative Unit With 5651-2).* turk.internet.com.(29.08.2008). http://turk.internet.com/haber/yazigoster.php3?yaziid=21811 Retrieved from the Internet on Sept 11, 2008. (In Turkish)

[6] Özdilek, A. (2008). *Türkiye ve Bilişim Suçları (Turkey and IT Crimes).* PC World Ocak 2008. http://www.pcworld.com.tr/turkiye-ve-bilisim-suclari-makale_1845.html Retrieved from the Internet on Sept 9, 2008. (In Turkish)

[7] Project Lexelerator (2008). *Turkey Passes New Internet Crimes Law.* http://www.lexelerator.si/?paged=3 Retrieved from the Internet on Sept 10, 2008.

[8] Sansüre Sansür. org (2007). *5651, Yasalaşan Yeni İnternet Kanunu ve Zihnimdeki Soru İşaretleri. (Passing New Internet Law and Question Marks in My Mind).* http://flynxs.blogspot.com/2007/05/5651-yasalaan-yeni-internet-kanunu-ve.html Retrieved from the Internet on Sept 12, 2008. (In Turkish)

[9] Sevim, Ş. (n.a.). *Stratejik Bakış Açısile Bilişim Teknolojileri. (Information Technologies from a Strategic Perspective).* http://www.muhasebetr.com Retrieved from the Internet on Sept 3, 2008. (In Turkish)

[10] Tedarik.com (2008). *Türkiye'deBilişim* Suçları ve Cezalar. (IT Crimes and Punishments in Turkey)http://www.tedarik.com/makale/26/turkiye-de-bilisim-suclari-ve-cezalar Retrieved from the Internet on Sept 11, 2008. (In Turkish)

[11] TÜSİAD, 2006. *Avrupa Birliği Sürecinde Türkiye'de Bilişimve Telekominikasyon Teknolojileri Sektörü Üzerine Görüşve Öneriler. (View and Comments on Information and Telecommunication Technologies in Turkey within the EU Process).* http://akgul.bilkent.edu.tr/Tusiad/ABbilisim.pdf

Retrieved from the Internet on Sept 24, 2008. (In Turkish)

[12] World Economic Forum (2008). *The Global Information Technology Report 2007 - 2008.* http://www.weforum.org/en/initiatives/gcp/Global%20Information%20Technology%20Report/index.htm Retrieved from the Internet on Sept 11, 2008.

[13] YASAD (n.a.). *Bilişim Ağı Hizmetlerinin Düzenlemnesi ve Bilişim Suçları Hakkında Kanun Tasarısı (Bill on Arrangement of Information Network Services and IT Crimes).* http://www.yasad.org.tr/?page=browse/index&page_id=337 Retrieved from the Internet on Sept 8, 2008. (In Turkish)

Mehmet Ali Gürol

EDUCATON

1978 (MBA) Institute of Social Sciences, Gazi University, Ankara

1988 (Ph.D.) Institute of Social Sciences, Gazi University, Ankara

1993 (Associate Prof.) Istanbul Economy Faculty, Istanbul

2006 (Professor) Selcuk University, KBF, Karaman

ACADEMIC POSITIONS

2007~08 Vice Rector, Dean to Economic and Administrative Sciences Faculty, Karamanoglu Mehmetbey University, Karaman, Turkey

2007~08 Member of Inter-University Council

2006~Now Professor, Dean, Selcuk University, Karaman Economic and Administrative Sciences Faculty, Karaman

1996 Board of Directors, MEYSU, Kayseri.

1997 Board of Directors, ISIKLAR HOLDNG, Istanbul.

FIELD OF RESEARCH

Female entrepreneurship, Employee ownership (Employee Stock Ownership Plans), Privatization, Small business management.

E-Mail : magurolus@yahoo.com