Middle-East Journal of Scientific Research 17 (12): 1752-1755, 2013
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2013.17.12.12365

Criminal Law Problems of IT-Crimes in Kazakhstan and Turkey

[1]Alya Shukan and [2]Yavuz Erdogan

[1]Kazakh Humanities and Law University, Astana, Republic of Kazakhstan
[2]Military Prosecutor of the Supreme Military Court, Ankara, Turkey

Abstract: In this study, the situation in Kazakhstan and the Turkish Penallaws on the basis of "Cyber Crimes Report" which was prepared by the United Nations on 11 June 1999 and thereafter have been subject to many legal regulation and scientific work was evaluated. While the content of the provisions of the Council of Europe Convention on Cybercrime is reviewed, what the countries need to do is also addressed. As a result of this study, it is concluded that the current legal regulations in the both countries are not sufficient.

Key words: United Nations % Convention on Cybercrime % ¤nformatics % Computer Crime (Cybercrime) % Computer % Criminal Code

INTRODUCTION

Revolutionary development of information technologies became a part of our life and simplified it so much that we already cannot do without mobile phones, computers, the Internet etc. At the same time, one should remember that the novelty creates a new field for criminal offences.

Crimes committed with the help of information technologies have larger dimensions and complicate investigation in comparison with classical criminal methods [1].

The above mentioned facts oblige to create new criminal law rules. Every country must work out legal norms to prevent such crimes and to ensure the punishment of guilty persons [2]. If a country does not control IT-crimes, these technologies can cause criminal danger in future. This can lead to worsening of country's status on the international stage. Besides, it can endanger homeland security and cause material damage [3].

The first step towards protection of electronic information was made on April 4, 1973 in Sweden when the "Data protection law" was adopted. This law introduced a new concept of "computer abuse" [4]. In such a context, we can see that legislation of this kind was absent in Turkey and Kazakhstan as recently as 20-25 years ago. They made IT-abuse a criminal offence in 1991 in Turkey and in 1997 in Kazakhstan.

The notion of information should not be defined in connection with fast development of computer networks and the Internet. It is true that the number of questions contained in the definition is insufficient under conditions of technological development. As a result, criminal actions go unpunished. That is why, it is necessary to identify elements instead of defining information. In our view, elements of information technologies include:

- Data storage;
- Opportunity to control saved data;
- Sending and receiving data (data transmission) [5].

Definition of "electronic information" appeared as a natural result. It caused the necessity to set limits for the term "cybercrime". For example, Toleubekova defines cybercrime as "all kinds of actions performed against law and morality or unauthorized actions in the system of automatic data processing or actions promoting data transmission". Gavrilin, instead of giving a direct definition, agrees that cybercrimes include computer crimes, malware distributed via Internet, hacking passwords, theft of credit-card numbers or other bank details, illicit transmission of data (slander, obscene materials, incitement of ethnic or religious hatred etc.) [6]. In our view, it is wrong to connect cybercrimes first of all with the Internet. The fact is cybercrimes can be performed without using the global network.

Corresponding Author: Shukan, Kazakh Humanities and Law University, Korgakzhynski prospect, 8, Astana, Republic of Kazakhstan, Military Prosecutor of the Supreme Military Court, Ankara, Turkey.

In IT-sphere, there are other networks besides the Internet (for instance, Intranet)[1]. Moreover, new technologies will possibly appear in time and substitute the Internet. In our opinion, it is also wrong to define cybercrimes by enumerating actions according to one factor. If it is necessary to define then cybercrimes can be defined as follows: "Cybercrimes are crimes committed using IT-tools". Nevertheless, it is notable that one should take into account the principle of legality in fast development of information technologies and crimes instead of defining cybercrimes. It would be more reasonable to categorize them while studying.

It is possible to distinguish six basic motives for cybercrimes [7]:

- To show one's technical knowledge and skills;
- To demonstrate the weakness of computer security system;
- To punish and to take revenge;
- To take part in information radiography;
- To protect the idea of free access to computer systems;
- Sabotage.

In our research, we will appraise the situation of cybercrimes in two different countries. That is why we think that it will be more appropriate to use foreign texts sources. We took as a basis the articles from the report about cybercrimes prepared by the United Nations Organization and the European Community in 1999. Then we conducted a research of these contents.

Here are the main crimes studied in this article:

- Computer sabotage;
- Computer fraud.

We'd like to perform a comparative analysis of the criminal legislation of Turley and Kazakhstan in the same context.

Computer Sabotage: First of all, though the notion "computer sabotage" is used in the article, we think that this notion should be considered as "IT-tools sabotage" because these crimes can be committed not only with the help of computers but also using all IT-tools.

Unauthorized data editing and hiding or deleting some information or function aimed at blocking normal operation of a system are criminal actions named generally as computer sabotage [8].

As of today, informational systems and technologies became essential tools in many vital basic spheres such as economics, health care, education, scientific research, administration, defence and others. That's why great losses may be caused by damaging these systems or temporarily malfunctions due to hacker attacks or assaults. Malware such as virus, worm, "Trojan Horse" spreading across the network can do even a greater damage than criminals planned. Computer sabotage is governed by article 227 of the Criminal Code of the Republic of Kazakhstan, in articles 243/3 and 244/1, 2 of the Criminal Code of Turkey.

Computer sabotage is subject to the article 4 of the Convention of Cybercrime of the European Council (AKSSS). In accordance with this article, participating states made the following actions criminal offences: data damaging, spoiling, deletion, changing, access limitation and data destruction.

Computer sabotage has two main directions:

- deletion, destruction, change of data in a system by remote access with the help of information technologies;
- deletion, destruction, change of data in a system with physical damage or direct using.

It does not matter if a computer is damaged physically or as an article of trade. But it is important that data are damaged in the system or the system is damaged partially or completely. In the context of committing this kind of crime, it does not matter whether a criminal has or does not have access rights. The purpose of computer sabotage, i. e. the reason that makes a person commit an offence is not as important for the Criminal Code of Kazakhstan as it is for the Criminal Code of Turkey. Crime is a crime committed intentionally. So, a crime is committed for a joke or in order to wreck the work is not matter from the point of view of corpus delicti. But it is important if a crime was committed consciously and intentionally. Computer sabotage can be used as a tool for selling stolen data or software, obtaining an economic advantage over a partner, achieving ideological goals or terrorism etc.

[1] **Intranet** is an internal private network of an organization, in spite of the Internet www.ru.wikipedia.org/wiki/ 15.09.13.

For instance, there are hacker grpoups that mostly act in Russia, Eastern Europe and Far East within the framework of a certain organizational hierarhy and operational system. They commit such crimes as theft and spoiling digital data (E-mafia) [9].

From the point of view of computer sabotage, creation of codes (programs) that cause data damage and prevent from using data in computer system are not prosecuted by Turkish law but are considered by article 222/3 of the Criminal Code of Kazakhstan.

In our opinion, creation of a program is only a preparatory process. Preparatory process is not punishable in criminal law. That's why we think that writing harmful codes is not a crime, but usage and distribution of them, even for free, should be prosecuted at criminal law.

Computer Fraud (With the Help of IT-Tools): A crime committed by fraud can be defined as "gaining for oneself or another person by means of cheating a third party using fraud behaviour to his detriment".

Computer fraud is defined by European Council as "any interference in the form of loading, changing, deleting or receiving data and software that can lead to economic loss or loss of somebody's property, for unlawful advantage sui juris or alia juris**+** [10]. There is one more definition of computer fraud: "an unauthorized impairment of somebody's property with malice and for profit by means of change, deletion or external interference, or any kind of interference into the functions of computer system**+** [11].

In most cases, computer fraud deals with credit cards, programmed iput and output operations or unauthorized and illegal use of communications.

One of the oldest methods of IT-fraud is fishing. Here is the shortest definition of fishing: fishing is a password hunt method. Fishing attacks carried out in the USA, China and Korea resulted in huge financial losses of users living in these countries [12].

Along with electronic commercial quickly created web-sites that disappear after getting money from clients, there are similar web-sites with external view identical to widely known and reliable trade web-site [13].

In article 157 of the Criminal Code of Turkey, fraud is considered as "a person who obtains benefit by cheating another person and using tricks to his/her detriment or the detriment of someone else gets prison punishment for the period form one to five years or amersiament". A fraud committed with the help of information technologies is described in article 158 ((1) f) as a qualified form of crime. In our view, it is a right measure because frauds with the help of informational systems became easier and new crime forms appear due to the fast development of information technologies. [14].

They say in "Commentaries on the Criminal Code of Turkey": "Using such reliable unions as IT-systems, banks or credit companies as tools ensures ease of fraudulent actions".

Article 177 of the Criminal Code of Kazakhstan contains the following: "a fraud, a theft or a misappropriation of somebody's property by cheating is punished by penalty at the rate of 200-700 of minimum calculation index or salary of 2-6 months, or imprisonment for a period up to 6 months, or imprisonment for a period of up to 3 years with suspended execution [15].

If studying the Criminal Code of Kazakhstan, we can see that there are no special regulations for IT-frauds. That is why, it is important to work out appropriate legislative acts taking into account fast technological progress. For example, we consider necessary to add paragraph f to article 177 (as in the Criminal Code of Turkey) containing the following: "Crimes committed with the help of informational systems of banks and credit companies as tools are punished by imprisonment for a period of 1-5 years or by penalty of 500-1000 minimum calculation index".

If studying the Criminal Code of Germany, that was a source for the Criminal Code of Turkey, one can see that this action is singled out for separate procedure as "Computer fraud".

In the context of regulation mentioned in the Criminal Code of Turkey, it is up for discussion whether there is or there is no possibiliry for the fraud described in article 158 ((1) f) or in article 244 (4)of the Criminal Code of Turkey.

Article 158 ((1) f) of the Criminal Code of Turkey makes provisions for a fraud or profit with the help of informational systems. Article 244 (4) of the Criminal Code of Turkey regulates profiting with committing crimes from the first two paragraphs, or in other words profiting by informational systems and data.

In this case, it is of great importance what article will be useful in each particular case, because it is noted in article 244 (4) of the Criminal Code of Turkey that if there are no other actions this article will be applied.

It should be noted that, according to the definition of fraud, the action should be performed towards one person. In this case, informational systems are used only as a tool for a crime as described in articles 157 and 158 ((1) f) of the Criminal Code of Turkey, while the action should again be performed towards one person. If considering this decision together with article 244 (4) of the Criminal Code of Turkey, one can notice a

discrepancy between articles ((1) f) and 244 (4) of the Criminal Code of Turkey. However, this discrepancy does not contradict the main doctrine. In our view, the question is whether a profit is ensured for the other person by the actions of a criminal.

In other words, if it is proved that a profit was got by means of interference into an informational system by a criminal, article 244 (4) of the Criminal Code of Turkey should be applied.

CONCLUSION

After the analysis of domestic and foreign legislations on informatization we came to a conclusion that it is necessary to study bodies of IT offences in details for their right classification and the improvement of penal struggle against them. Besides, we think that it is important to unify criminal legislation of different countries including the Republic of Kazakhstan in the sphere of IT crimes.

Moreover, it is necessary to add a section named “Informatization Crimes” to the Criminal Code of Kazakhstan, as many countries did.

Besides, in the Criminal Code of Turkey, there are articles about theft and fraud with the help of information technologies (article 142, paragraph d; article 157, paragraph e: *****Use of informational systems”; article 142, paragraph d; article 157, paragraph å: *****Use of informational systems as a tool for robbery of banks and credit companies”).

In terms of the above, we think that it would be right to add these articles to the Criminal Code of Kazakhstan.

The research conducted shows that many questions on IT crimes are not systematized and work inefficiently. Consequently, definitions differ in some questions concerning particularly computer, computer system, computer crimes and unauthorized access. Thereby, a new law on criminal liability in IT sphere should be thoroughly analyzed and worked through. We think that, in the framework of Internet-conferences and Internet-forums, it is necessary to put a number of detailed questions in order to discuss this problem.

Prosecutors and courts do not have enough knowledge on legal and technical issues concerning IT crimes. They do not act in accordance with similar cases. This can lead to wrong classification and groundless sentences. In spite of the fact that criminal departments for IT crimes were created in regional administrations of the Internal Affairs Directorate, the personnel of these departments are unqualified in technical questions or in IT law. If legislation does not keep up with technological progress, there will be gaps in laws against this kind of actions and there will be impossible to take criminal proceedings against people who caused a great damage by these crimes. In this case, authorities, jurists and police officers should constantly follow innovations and improve legislation. This will make it possible to ensure a top-level reliability of communication service conducted via the Internet.

REFERENCES

1. Russel, D. and R. Con, 2012. IT-Crimes. Moscow, pp: 48.
2. Kozlov, V., 2012. Theory and Practice of Fight against Computer Crimes. Moscow, pp: 62.
3. Idyn, E., 1992. Introduction in Informational Crimes and Jurisprudence. Ankara: Doruk, pp: 13.
4. Baranov, A.A., 2000. Human Rights and Personal Data Protection. Kiev: State Committee of Communications and Informatization of Ukraine, pp: 280.
5. Dylyan, G.D., E.S. Ratobylskaya and M.S. Tsvetkova, XXXX. Control Models for Complex Informatization in General Secondary Education. Moscow: Knowledge Laboratory, pp: 199.
6. Gavrilin, Y.V., 2001. Investigation of Unauthorized Access to Computer Information. Moscow, pp: 120.
7. Rizgar, M.K., 2010. The Scope and the Nature of Computer Crimes Statutes A Critical Comparative Study. German Law Journal, 6: 617.
8. Akcham, B., 1999. For Those Who Fight with Internet Crimes. Ankara: Design Ltd. of SFN Television, pp: 54.
9. Tashdemir, K. and R. Yazidgioglu, 2002. Computer Network Crimes According to the Criminal Code of Turkey. International Web-Symposium. Izmir: Dokuz Eylul University, pp: 461.
10. Flanagan, A., 2005. The Law and Computer Crime: Reading the Script of Reform. ¤nternational Journal of Law and Information Technology, 13(1): 114.
11. Guneid, E.R., 2004. Cybercrimes. Istanbul: Bilgy University, pp: 25.
12. Kurt, L., 2005. Case Law of All Aspects of Cybercrimes. Ankara: Sechkin Publishing House, pp: 171.
13. The Criminal Code of the Republic of Kazakhstan., 2012. Almaty, pp: 84.
14. Tanrikulu, C., 2009. Decisions of the Supreme Court of German Republic on Cybercrimes. Ankara, pp: 246.
15. Yazidgioglu, R., 2005. General Assessment of New Criminal Code of Turkey on Cybercrimes. Yeditepe University Journal, (2): 399.